# Microsoft Azure

di Carlo Mauceli

## Sicurezza e privacy integrate nello sviluppo di Azure

Per rendersi conto dei vantaggi offerti dal cloud, i clienti aziendali devono essere pronti ad affidare al provider di servizi cloud una delle loro risorse più preziose: i dati. Chi investe in un servizio cloud deve poter fare affidamento sul fatto che i dati dei clienti siano al sicuro, che la privacy dei dati sia protetta e di poter mantenere la proprietà dei dati e il controllo su di essi, sapendo che verranno usati solo in modo coerente alle aspettative.
Microsoft fa tutto il possibile per guadagnare la fiducia dei clienti in Microsoft Azure. La lunga esperienza nella fornitura di servizi online ha comportato ingenti investimenti in una tecnologia di base per l'integrazione di sicurezza e privacy nel processo di sviluppo. Col tempo, Microsoft ha sviluppato informative sulla privacy e misure di sicurezza leader del settore e ha partecipato a programmi internazionali per la conformità con verifiche indipendenti dei risultati raggiunti.

Per Microsoft la sicurezza e la privacy sono aspetti prioritari in ogni fase, dallo sviluppo del codice alla risposta agli eventi imprevisti. Microsoft progetta i prodotti software tenendo presente la sicurezza fin dall'inizio. La sicurezza viene integrata nel codice del software seguendo un approccio noto come Security Development Lifecycle (SDL). Questo processo di sviluppo obbligatorio, applicato a livello aziendale, integra i requisiti di sicurezza nell'intero ciclo di vita del software, dalla pianificazione alla distribuzione. Per garantire che le attività operative seguano le stesse priorità di sicurezza, Microsoft ha sviluppato rigorose linee guida per la sicurezza, esposte nel processo Operational Security Assurance (OSA). Quando si verificano problemi, un ciclo di feedback aiuta a garantire che le revisioni future del processo OSA prendano in considerazione tali problemi (https://www.microsoft.com/en-us/sdl/default.aspx).

La protezione della privacy è integrata in Azure grazie al programma Privacy by Design, che definisce le modalità di creazione e gestione di prodotti e servizi al fine di proteggere la privacy. Gli standard e i processi sono definiti in Microsoft Privacy Standard, uno standard che specifica in modo dettagliato i requisiti e le procedure principali di Microsoft per la privacy (http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/privacy_by_design.pdf).

### Sicurezza: Microsoft protegge i dati dei Clienti

Microsoft ha sfruttato la sua esperienza di decenni nella creazione di software aziendale e nella fornitura di alcuni tra i più estesi servizi online al mondo per creare un solido set di tecnologie e procedure per la sicurezza. Lo scopo è quello di garantire che l'infrastruttura di Azure sia resiliente agli attacchi, salvaguardi l'accesso degli utenti all'ambiente Azure e protegga i dati dei clienti tramite comunicazioni crittografate e procedure di prevenzione e gestione delle minacce, inclusi regolari test di penetrazione.

- **Gestione e controllo delle identità e dell'accesso degli utenti** agli ambienti, ai dati e alle applicazioni, tramite federazione delle identità utente in Azure Active Directory e abilitazione di Multi-Factor Authentication per un accesso più sicuro.
- **Crittografia delle comunicazioni e dei processi operativi**. Per i dati in transito, Azure usa protocolli di trasporto standard del settore tra dispositivi utente e data center Microsoft e all'interno dei data center. Per i dati inattivi, Azure offre un'ampia gamma di funzionalità di crittografia fino a AES-256, garantendo flessibilità di scelta della soluzione più adatta alle esigenze specifiche.
- **Protezione delle reti**. Azure fornisce l'infrastruttura necessaria per connettere in modo sicuro le macchine virtuali tra loro e per connettere i data center locali a VM di Azure. Azure blocca il traffico non autorizzato verso i data center Microsoft e al loro interno, usando un'ampia gamma di tecnologie. Rete virtuale di Azure estende la rete locale nel cloud tramite VPN da sito a sito.
- **Gestione delle minacce**. Per garantire la protezione contro le minacce online, Azure offre Microsoft Antimalware per i servizi cloud e le macchine virtuali. Microsoft adotta anche soluzioni di identificazione di intrusione, prevenzione degli attacchi Denial of Service (DDoS), test di penetrazione regolari e strumenti di analisi dei dati e Machine Learning per prevenire le minacce alla piattaforma Azure (https://www.microsoft.com/en-us/TrustCenter/Security/default.aspx).

### Privacy: il Cliente ha la proprietà e il controllo dei dati

Per più di 20 anni, Microsoft è stata leader nella creazione di affidabili soluzioni online progettate per proteggere la privacy dei clienti. L'approccio alla privacy e alla protezione dei dati, collaudato negli anni, è basato sull'impegno di Microsoft a garantire alle organizzazioni la proprietà e il controllo su raccolta, uso e distribuzione delle loro informazioni.
Microsoft si impegna a definire procedure trasparenti per la privacy, offrire ai clienti opzioni significative e gestire responsabilmente i dati archiviati ed elaborati. L'entità dell'impegno verso la privacy dei dati dei clienti è testimoniata dall'adozione del primo codice delle procedure per la privacy nel cloud a livello mondiale, ISO/IEC 27018.



**Il cliente è proprietario dei suoi dati**. Con Azure, il cliente è proprietario dei suoi dati, ovvero tutti i dati, inclusi software e file di testo, audio, video o immagine, forniti a Microsoft dal cliente o per suo conto, tramite l'uso di Azure. Il cliente può accedere ai suoi dati in qualsiasi momento e per qualunque motivo, senza assistenza da parte di Microsoft. Microsoft non userà i dati dei clienti per ricavare informazioni a scopo pubblicitario o di data mining.

**Il cliente ha il controllo sui suoi dati**. Poiché i dati del cliente ospitati in Azure appartengono al cliente stesso, questo ha il controllo sulla posizione di archiviazione e sulle modalità di accesso sicuro ed eliminazione.

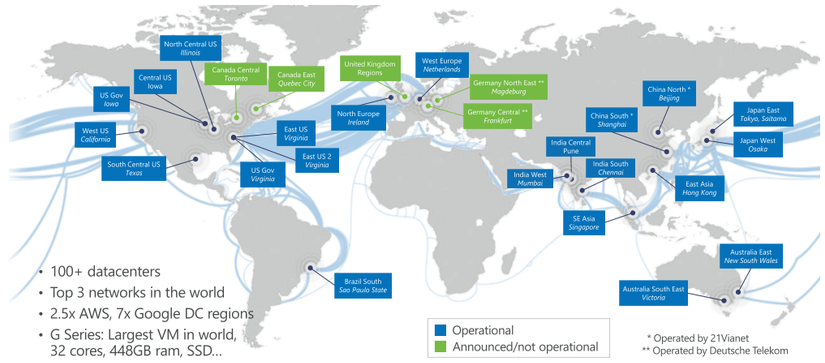
**Risposta di Microsoft alle richieste di accesso ai dati da parte di autorità governative e giudiziarie**. Quando un'autorità governativa desidera i dati dei clienti, anche per motivi di sicurezza nazionale, deve seguire il procedimento legale applicabile, presentando un'istanza del tribunale per la richiesta dei contenuti o una citazione in giudizio per le informazioni sull'account. Qualora obbligata a divulgare i dati del cliente, Microsoft avviserà tempestivamente il cliente e fornirà una copia della richiesta, a meno che ciò non sia vietato dalla legge. Microsoft non fornisce ad alcuna autorità governativa accesso diretto o senza limitazioni ai dati dei clienti, fatto salvo quando richiesto dal cliente stesso o ai sensi della legge (https://www.microsoft.com/en-us/TrustCenter/Privacy/default.aspx).

### Trasparenza: il cliente conosce le modalità di archiviazione e accesso ai dati e le misure adottate per garantire la sicurezza

Microsoft Azure si basa sulla premessa che, per consentire al cliente di controllare i suoi dati nel cloud, è necessario offrirgli visibilità sui dati. Il cliente deve sapere dove sono archiviati i dati. Deve inoltre sapere, tramite prassi e procedure esposte in modo chiaro e subito disponibili, come viene garantita la sicurezza dei dati dei clienti, chi è autorizzato ad accedere ai dati e in quali casi è consentito l'accesso. E non è necessario fidarsi esclusivamente di quello che afferma Microsoft: è possibile esaminare i controlli e le certificazioni di terzi per assicurarsi che gli standard vengano rispettati (https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx).

### Conformità: Microsoft rispetta gli standard globali

Azure soddisfa un'ampia gamma di standard di conformità internazionali e specifici del settore, come ISO 27001, HIPAA, FedRAMP, SOC 1 e SOC 2, nonché standard specifici di singoli paesi come IRAP in Australia, G-Cloud nel Regno Unito e MTCS a Singapore.




Controlli rigorosi di terzi, come il British Standards Institute, verificano la conformità di Azure alle rigide normative di sicurezza definite da questi standard. Come parte dell'impegno di Microsoft in materia di trasparenza, è possibile verificare l'implementazione di numerosi controlli di sicurezza richiedendo i risultati dei controlli svolti da terzi per il rilascio delle certificazioni.

Quando Microsoft verifica che i suoi servizi soddisfano gli standard di conformità e dimostra come viene raggiunta la conformità, per i clienti diventa più facile garantire la conformità per l'infrastruttura e le applicazioni eseguite in Azure (https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx). ©