Strategia Cloud Italia e principio Cloud First

Questo approccio dà priorità alle soluzioni cloud rispetto alle infrastrutture on-premise per scalabilità, sicurezza e interoperabilità, elementi chiave per una PA efficiente e resiliente.

Cosa è un cloud

Il cloud computing è un modello di erogazione di risorse IT che consente l'accesso a **server, storage, database, reti e software** tramite internet, senza la necessità di gestire infrastrutture fisiche.

Caratteristiche principali del cloud computing:

✅ **Elasticità e Scalabilità:** Il sistema può adattarsi automaticamente ai picchi di domanda.

✅ **On-Demand Self-Service:** Le risorse possono essere attivate e gestite autonomamente, senza necessità di intervento manuale.

✅ **Accesso Remoto:** Le risorse cloud sono accessibili via Internet da qualsiasi dispositivo.

✅ **Misurazione dei Servizi:** Il consumo di risorse è tracciato e si paga in base all'utilizzo.

✅ **Multitenancy:** Più utenti possono condividere la stessa infrastruttura con ambienti isolati.

Maggiori cloud provider

=65% del mercato detenuto da Google Cloud, AWS e Azure

Quadro Normativo e Strategico

La strategia **Cloud First** è disciplinata da normative e piani strategici come il Codice dell'Amministrazione Digitale (CAD), la Strategia Nazionale per il Cloud della PA (2021), il Piano Triennale per l'Informatica nella PA e il Regolamento Europeo sul Cloud.

Il documento "PNRR e trasformazione digitale" evidenzia l'importanza del Cloud First per modernizzare la PA e garantire servizi efficienti ai cittadini.

1. **CAD**

   Quadro normativo per la trasformazione digitale.

2. **Strategia Nazionale**

   Linee guida per la migrazione al cloud.

3. **Piano Triennale**

   Obbligo di soluzioni cloud qualificate da ACN.

Strategia Cloud Italia

La **Strategia Cloud Italia**, pubblicata nel settembre 2021 dal Dipartimento per la Trasformazione Digitale (DTD) e dall'Agenzia per la Cybersicurezza Nazionale (ACN), rappresenta un pilastro fondamentale per la riorganizzazione strutturale e gestionale della Pubblica Amministrazione (PA)

È parte integrante del percorso attuativo definito dall'articolo 33-septies del decreto legge 179/2012 e dagli investimenti del PNR

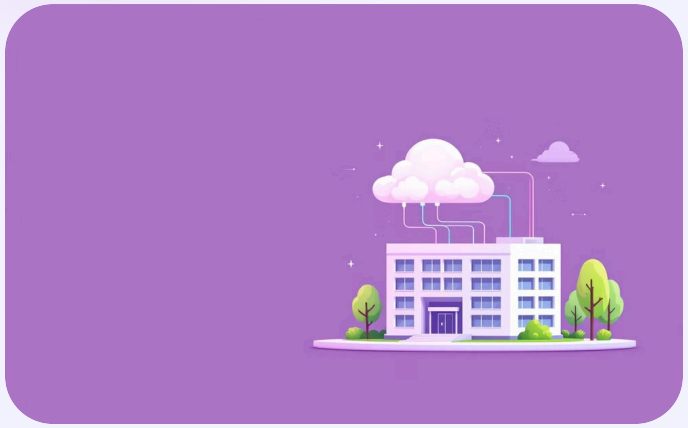
Obiettivi Strategici del Cloud nella PA

Autonomia Tecnologica del Paese

Ridurre la dipendenza da fornitori esteri, garantendo che la PA abbia il controllo delle proprie infrastrutture e dei propri dati. Questo implica lo sviluppo di competenze interne e la promozione di soluzioni tecnologiche nazionali.

Controllo sui Dati

La sovranità sui dati è un aspetto cruciale. La strategia mira a garantire che i dati della PA siano gestiti in modo sicuro e trasparente, nel rispetto delle normative europee e nazionali sulla privacy.



Resilienza dei Servizi Digitali

Rendere i servizi digitali della PA più affidabili e resistenti a interruzioni o attacchi informatici. Questo si traduce in una maggiore continuità operativa e in una migliore esperienza per i cittadini e le imprese.

Cos’è il Cloud First?

Un principio che dice che prima di intraprendere qualsiasi nuovo progetto IT o sviluppo di servizi, la PA deve valutare prioritariamente **l'adozione di soluzioni cloud**

Il principio del **Cloud First** impone alle amministrazioni pubbliche di valutare prioritariamente soluzioni basate su cloud per sviluppare o aggiornare servizi digitali, salvo esigenze specifiche. I vantaggi includono scalabilità, resilienza, sicurezza, efficienza economica e interoperabilità.

- **Scalabilità**: risorse IT adattabili in tempo reale.
- **Resilienza**: maggiore disponibilità e ridondanza.
- **Sicurezza**: standard avanzati di protezione dati.

Scalabilità

Adattamento delle risorse IT in tempo reale.

Resilienza

Maggiore disponibilità e ridondanza dei sistemi.

Sicurezza

Standard avanzati di protezione dei dati.

Principi Fondamentali della Strategia Cloud Italia

L'approccio **Cloud First** è *strategico per la modernizzazione della PA*, ma richiede pianificazione accurata per garantire sicurezza, interoperabilità e sostenibilità economica. L'adozione di modelli cloud deve essere accompagnata da investimenti in infrastrutture e competenze tecniche.

1 Competenze Specialistiche

È fondamentale che ogni ente della PA sviluppi competenze specialistiche interne, in particolare all'interno dell'ufficio del Responsabile per la Transizione Digitale (RTD). Questo implica la formazione del personale e l'acquisizione di nuove figure professionali.

2 Evoluzione oltre il "Lift and Shift"

La strategia richiede un approccio evoluto che preveda la riprogettazione **(re-architecting),** il riadattamento **(re-platforming)** o la sostituzione **(repurchase)** delle applicazioni per sfruttare appieno i vantaggi del cloud.

3 Prevenzione del Lock-in

È necessario evitare situazioni di "lock-in" con i fornitori di servizi cloud attraverso soluzioni interoperabili e basate su standard aperti, garantendo la portabilità dei dati e delle applicazioni.

4 Cloud Federato

Il modello prevede un ambiente in cui i servizi cloud sono forniti da due o più fornitori, uniti da procedure e regole comuni per aumentare resilienza e flessibilità.

5 Selezione dei Fornitori

Per i piccoli enti, è essenziale verificare che il fornitore conosca gli obiettivi della Strategia Cloud Italia e offra soluzioni conformi ai principi di sicurezza, interoperabilità e portabilità.

6 Integrazione con Piani Strategici

È fondamentale integrare gli obiettivi del **Piano Triennale ICT** con il **Piano Integrato di Attività e Organizzazione (PIAO)** di ogni ente, definendo obiettivi specifici per la migrazione al cloud.

7 Supporto e Risorse

Il sito cloud.italia.it fornisce strumenti, suggerimenti e modelli organizzativi per gestire il processo di migrazione, incluse raccomandazioni su backup e disaster recovery.

Modelli di Cloud nella PA

Le amministrazioni possono scegliere tra cloud pubblico (AWS, Azure, Google Cloud), cloud privato (infrastruttura dedicata), cloud ibrido (combinazione di pubblico e privato) e multi-cloud (più provider per diversificare le soluzioni).

Cloud Pubblico

L'infrastruttura è gestita da un provider esterno e condivisa tra più clienti (multitenancy).

Cloud Privato

L'infrastruttura è dedicata esclusivamente a un cliente e può essere gestita internamente o da un provider terzo.

Cloud Ibrido

Un mix di cloud pubblico e privato che consente di combinare i vantaggi di entrambi.

Multi-Cloud

Utilizzo di più provider cloud per diversificare le soluzioni e ottimizzare le prestazioni.

Cloud Pubblico

L'infrastruttura è gestita da un provider esterno e condivisa tra più clienti (multitenancy).

Caratteristiche Tecniche

- Architettura scalabile e distribuita
- Accesso tramite API e console web
- Modelli pay-as-you-go
- Alta disponibilità (HA) e disaster recovery facili da implementare

Esempi

- Amazon EC2, Google Compute Engine
- AWS Lambda, Google App Engine
- Google Workspace, Microsoft 365

Considerazioni Tecniche

- Vendor Lock-in tra provider diversi
- Dipendenza dalla connessione Internet
- Gestione compliance e sicurezza dati

Cloud Privato

L’infrastruttura è dedicata esclusivamente alla PA e può essere gestita internamente o da un provider terzo.

Caratteristiche Tecniche

- Risorse isolate (single tenancy).
- Maggiore controllo su configurazione, sicurezza e rete.
- Architettura personalizzata in base alle esigenze dell’ente.

Alcune tecnologie

- **Virtualizzazione:** VMware, Hyper-V, KVM.
- **Containerizzazione:** Kubernetes, Docker.
- **Storage distribuito:** Ceph, GlusterFS.

Considerazioni Tecniche

- Maggiore controllo su **SLA (Service Level Agreement)** e sicurezza.
- Possibilità di **certificazioni di sicurezza personalizzate**.
- **Ottimizzazione delle risorse** per esigenze specifiche della PA

Svantaggi Tecnici

• Costi di gestione elevati.

• Minor scalabilità rispetto al cloud pubblico.

• Necessità di un team IT qualificato per la manutenzione.

Cloud Ibrido

Un ambiente cloud che combina **cloud privato e cloud pubblico**, permettendo lo spostamento dinamico di dati e applicazioni tra i due.

Caratteristiche Tecniche

- **Connettività tra ambienti:** Tramite VPN, SD-WAN, o Direct Connect.
- **Integrazione tra pubblico e privato:** Le due infrastrutture devono comunicare tra loro.
- **Dati e applicazioni possono spostarsi tra i due ambienti in base alle necessità.**

Vantaggi tecnici

- **Flessibilità:** Possibilità di spostare i workload in base a carichi di lavoro e sicurezza.
- **Bilanciamento tra prestazioni e costi.**
- **Backup e disaster recovery** con ridondanza tra diversi ambienti.

Svantaggi tecnici

• **Gestione complessa:** Richiede strumenti avanzati per l'integrazione.

• **Rischi di latenza e compatibilità tra cloud diversi.**

Esempio: Un ente sanitario conserva i dati sensibili dei pazienti su un **cloud privato**, ma usa un **cloud pubblico** per le prenotazioni online, per ridurre i costi e garantire scalabilità.

Multi-Cloud

Si utilizzano **più cloud pubblici di provider diversi** (AWS, Azure, Google Cloud), senza necessariamente avere un'integrazione tra loro.

Caratteristiche Tecniche

- **Interoperabilità tra cloud provider** con API standardizzate.
- **Nessun cloud privato coinvolto**, solo più cloud pubblici.
- **Diversi fornitori cloud per diversi servizi** (es. database su AWS, analisi dati su Google Cloud).
- **Possibilità di distribuire carico lavoro tra più provider per maggiore resilienza.**

Vantaggi tecnici

- **Alta affidabilità (HA) e disaster recovery.**
- **Indipendenza dal singolo provider (no vendor lock-in).**
- **Possibilità di ottimizzare i costi tra provider diversi.**

Svantaggi tecnici

- **Maggiore complessità di gestione e monitoraggio.**
- **Necessità di skill avanzate per orchestrare le risorse tra provider diversi.**

Esempio: Un Ministero usa **AWS per il sito web**, **Azure per i database** e **Google Cloud per l'analisi dati**. I tre cloud non sono direttamente connessi tra loro, ma servono esigenze diverse.

Passi pratici da seguire:

1

Valutazione Preliminare

Analisi delle esigenze specifiche del progetto e verifica della disponibilità di soluzioni cloud adatte.

2

Scelta della Soluzione Cloud

Selezione della soluzione cloud più appropriata, tenendo conto di fattori come sicurezza, costi, scalabilità e conformità normativa.

3

Migrazione al Cloud

Trasferimento dei dati e delle applicazioni verso l'ambiente cloud scelto.

Privacy by Design

Progettazione Iniziale

La privacy deve essere integrata fin dalla fase di progettazione di qualsiasi servizio o applicazione

Protezione dei Dati

È necessario garantire la protezione dei dati personali degli utenti in ogni fase

Conformità GDPR

Adozione di misure tecniche e organizzative adeguate in conformità con il Regolamento Generale sulla Protezione dei Dati

Criticità dell'Adozione del Cloud

La transizione al cloud presenta diverse sfide interconnesse che devono essere affrontate in modo sistematico. Una gestione efficace di queste criticità è fondamentale per il successo della strategia Cloud First.

1 Sicurezza e Sovranità

La protezione dei dati sensibili e la conformità normativa rappresentano una sfida primaria nell'adozione del cloud. Le amministrazioni devono garantire elevati standard di sicurezza mantenendo il controllo sui dati critici.

2 Vendor Lock-in

Il rischio di dipendenza da un singolo provider cloud può limitare la flessibilità operativa e aumentare i costi nel lungo termine. È necessario sviluppare strategie per mantenere la portabilità dei dati e delle applicazioni.

3 Costi e Competenze

La migrazione al cloud richiede significativi investimenti iniziali, sia per l'infrastruttura che per la formazione del personale. È fondamentale pianificare accuratamente le risorse necessarie.

Queste sfide richiedono un approccio strutturato e una pianificazione accurata per garantire una transizione efficace al cloud.

Esempi di Implementazione del Cloud nella PA

Diverse amministrazioni hanno adottato il Cloud First con successo: l'Agenzia delle Entrate ha migrato al cloud per migliorare l'accessibilità e la sicurezza dei servizi fiscali online, l'INPS utilizza soluzioni cloud per la gestione delle domande di prestazioni sociali e la Sanità Digitale impiega il cloud per la condivisione sicura dei dati sanitari.

1 **Agenzia delle Entrate**

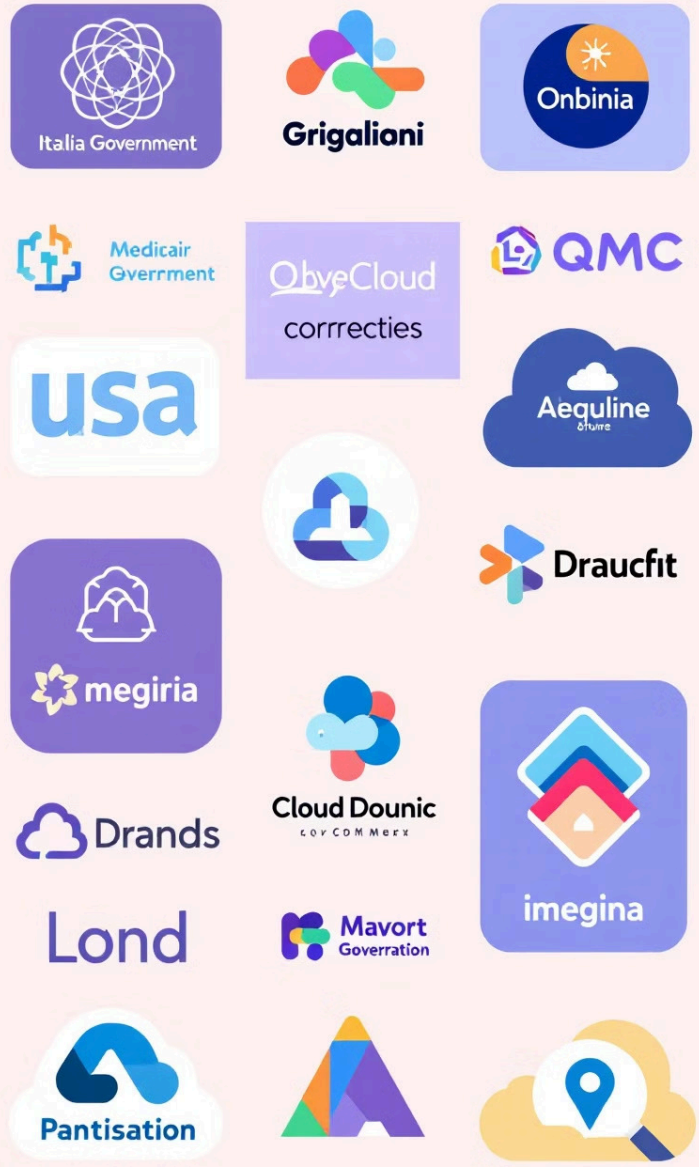
Miglioramento accessibilità e sicurezza servizi fiscali.

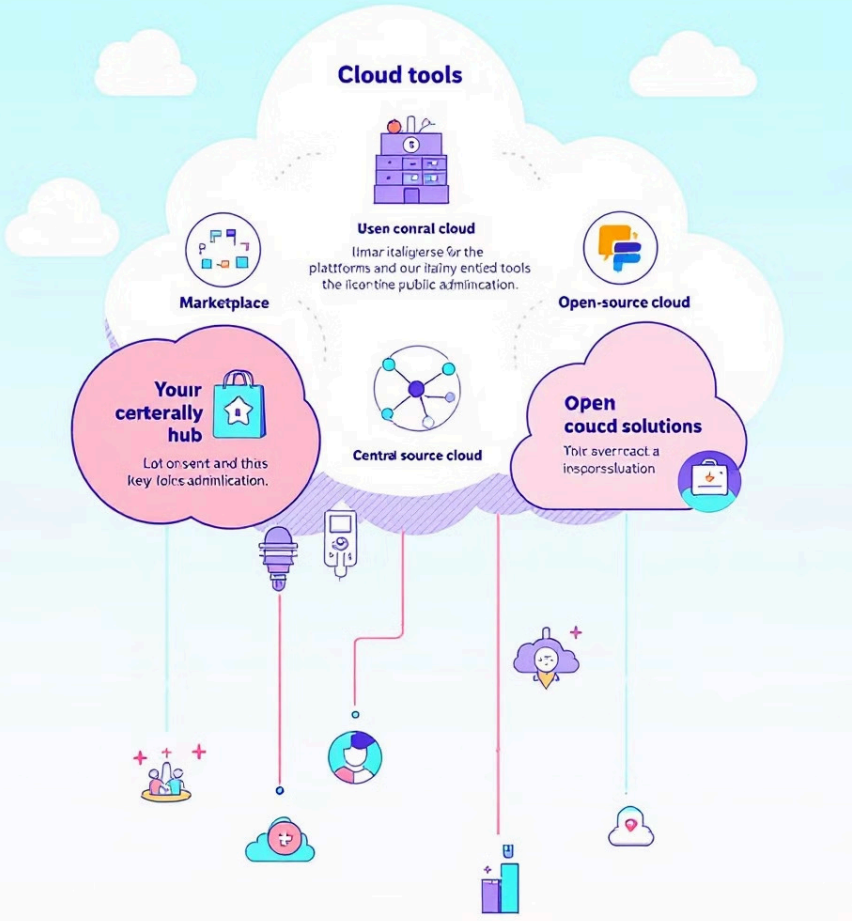
2 **INPS**

Gestione delle domande di prestazioni sociali.

3 **Sanità Digitale**

Condivisione sicura dei dati sanitari.





Strumenti e Piattaforme Cloud per la PA

Per facilitare l'adozione del cloud, le PA possono utilizzare piattaforme e strumenti qualificati come il Marketplace Cloud di AgID, il Polo Strategico Nazionale (PSN), soluzioni Open Source e il Framework di Sicurezza Cloud di ACN.

Marketplace AgID

Elenco di fornitori certificati per servizi cloud.

Polo Strategico Nazionale

Infrastruttura cloud dedicata alla PA italiana.

Soluzioni Open Source

Software cloud-based per evitare il lock-in.

Governance del Cloud

Le amministrazioni devono adottare un modello di governance del cloud efficace, assicurandosi di rispettare le normative e di scegliere soluzioni che garantiscano flessibilità e indipendenza tecnologica. Questo include la definizione di politiche chiare, la gestione dei rischi e la formazione del personale.