Governare la complessità digitale con il cloud europeo

Architetture consapevoli per autonomia, interoperabilità e controllo strategico.

aruba.it

Sommario

01 | **Evoluzione dei modelli cloud nel contesto Enterprise europeo** 3

02 | **Interoperabilità e architetture composable** 5

03 | **Europeicità e libertà tecnologica** 7

04 | **Compliance by design e governance** 8

05 | **Costi prevedibili e sostenibilità operativa** 10

06 | **Codesign e fattore umano** 12

07 | **L'approccio e la visione di Aruba** 15

08 | **Conclusione: il cloud come abilitatore di controllo strategico** 18

CAPITOLO 01

Evoluzione dei modelli cloud nel contesto Enterprise europeo

Il cloud computing europeo è entrato in una fase di consolidamento. Dopo una prima stagione dominata dall'urgenza di modernizzare, le organizzazioni si trovano oggi a gestire ambienti distribuiti e complessi, per di più seguendo criteri diversi rispetto a quelli che hanno guidato la prima ondata di adozione.
La differenza, tuttavia, non è tecnologica ma di maturità. Il mercato ha imparato che spostare workload sul cloud non è sufficiente: bisogna capire quali workload, su quale infrastruttura, con quale livello di controllo. La domanda non è più se andare sul cloud, ma come governarlo in modo sostenibile, sicuro e coerente anche con i vincoli normativi del contesto europeo.

Molte organizzazioni stanno anche riducendo la dipendenza da data center on-premise tradizionali perché costosi, difficili da manutenere e aggiornare, richiedendo competenze sempre più rare. Passare a infrastrutture off-premise di nuova generazione non è un salto, ma un percorso che parte dalla colocation, attraversa il lift-and-shift e arriva, per chi possiede le risorse, al refactoring applicativo.

Secondo i dati di Statista, **il mercato europeo del cloud computing supererà i 250 miliardi di euro entro il 2030, con un tasso di crescita annuo superiore al 15%**. A livello globale, oltre il 70% delle organizzazioni adotta già modelli hybrid o multi-cloud, confermando come l'adozione di architetture distribuite sia ormai lo standard di riferimento.
Inoltre la crescente digitalizzazione dei processi core ha imposto un cambio di prospettiva: non più infrastrutture statiche, ma ambienti dinamici in grado di orchestrare workload, dati e servizi distribuiti. In questo scenario, il cloud ibrido e distribuito si afferma come architettura di riferimento per le organizzazioni europee più mature.

Questa evoluzione amplia il tema che va oltre una mera questione infrastrutturale: come si gestisce il rischio? Come si controllano i dati? Come si prendono decisioni architetturali nel tempo?

Le architetture enterprise oggi combinano on-premise per i workload critici, data center esterni per resilienza e cloud pubblici per i servizi applicativi.
La sfida, quindi, non è scegliere tra questi modelli, ma tenerli insieme in modo coerente, senza che la complessità diventi un vincolo. Ed è proprio in questo scenari che i servizi gestiti assumono un ruolo fondamentale: supportano le organizzazioni nel governare infrastrutture sempre più distribuite, garantendo continuità operativa, sicurezza e aggiornamento costante. Attraverso competenze specialistiche e modelli di gestione proattiva, **i managed services permettono di ridurre complessità, ottimizzare i costi e accelerare l'evoluzione architetturale**.

Il cloud non è più una scelta tattica, ma una decisione architetturale che impatta direttamente su governance, resilienza e autonomia tecnologica.

Inoltre per le organizzazioni europee, la gestione del dato e la localizzazione delle infrastrutture diventano elementi centrali per la tutela della competitività e la conformità normativa.

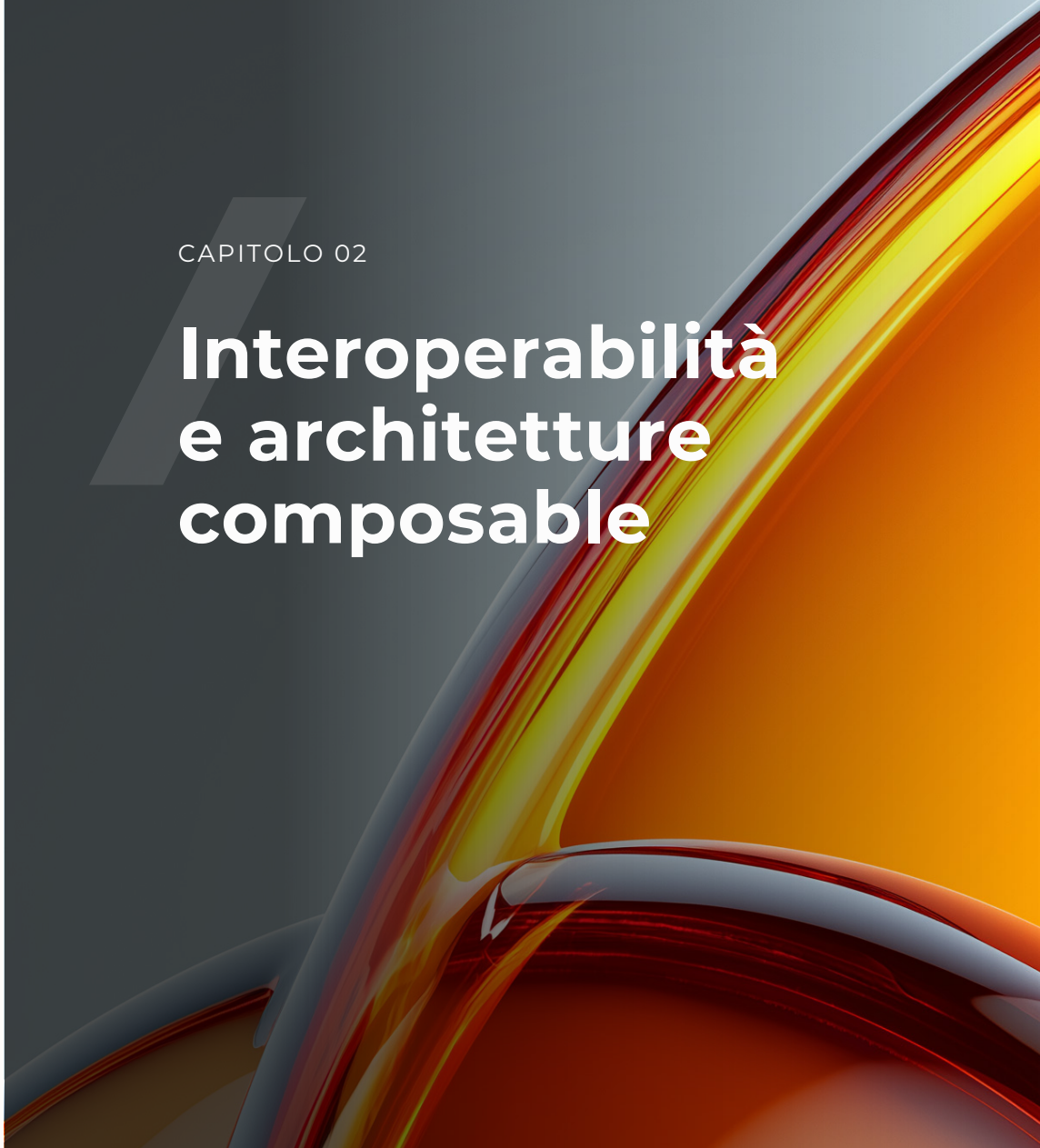
Ad esempio nel settore pubblico, l'evoluzione verso modelli distribuiti consente di mantenere dati sensibili su infrastrutture controllate, integrando al contempo servizi cloud per analytics e interoperabilità. Nel settore enterprise, la possibilità di spostare dinamicamente workload tra ambienti diversi abilita strategie di business più flessibili e riduce la dipendenza da singole piattaforme.

Ne consegue che in un contesto simile, il ruolo del cloud provider cambia radicalmente: non è più un semplice fornitore di risorse infrastrutturali bensì abilitatore di architetture distribuite, capace di garantire **interoperabilità**, **compliance** e **orchestrazione coerente dei servizi**. Questa transizione rappresenta il fondamento su cui costruire modelli digitali resilienti, modulari e pronti all'evoluzione futura.

Il cloud europeo non evolve verso la centralizzazione, ma verso l'orchestrazione intelligente di ambienti distribuiti.

CAPITOLO 02

Interoperabilità e architetture composable



Nel panorama digitale europeo, l'interoperabilità rappresenta una condizione strutturale per garantire continuità operativa e libertà strategica. Le organizzazioni operano su ambienti distribuiti che devono dialogare in modo coerente per evitare quelle frammentazioni che possono compromettere efficienza, sicurezza e capacità evolutiva.

In questo contesto, l'architettura composable emerge come modello di riferimento per costruire ecosistemi modulari e adattabili. Non si tratta di eliminare la complessità ma di governarla, trasformandola in un elemento progettuale: dati, applicazioni e servizi vengono orchestrati lungo un continuum infrastrutturale che integra ambienti diversi in modo coerente.

Infatti la vera sfida per CIO e CTO non è più integrare sistemi isolati, ma progettare ecosistemi tecnologici in grado di evolvere nel tempo. Questo significa adottare modelli che permettano di introdurre nuove tecnologie preservando gli investimenti esistenti e riducendo il debito tecnico.

Le architetture composable, inoltre, introducono un paradigma modulare in cui **risorse e servizi diventano componenti riutilizzabili e orchestrabili dinamicamente**. Un approccio che abilita adattabilità continua a nuovi requisiti di business, alle variazioni della domanda e ai cambiamenti normativi, garantendo al tempo stesso coerenza operativa.

Secondo analisi di mercato basate su dati Statista e altri osservatori, oltre il 60% delle aziende europee considera l'interoperabilità tra piattaforme uno dei principali criteri nella scelta di soluzioni cloud, a conferma della centralità di questo tema nelle strategie IT.
Ne consegue che in un contesto europeo caratterizzato da elevata regolamentazione e pluralità di attori tecnologici, l'interoperabilità si configura quindi come una leva strategica per garantire **resilienza** e **autonomia** nel lungo periodo.

Interoperabilità significa progettare sistemi aperti, capaci di evolvere senza vincoli e di integrare innovazione senza frizioni.

CAPITOLO 03

Europeicità e libertà tecnologica

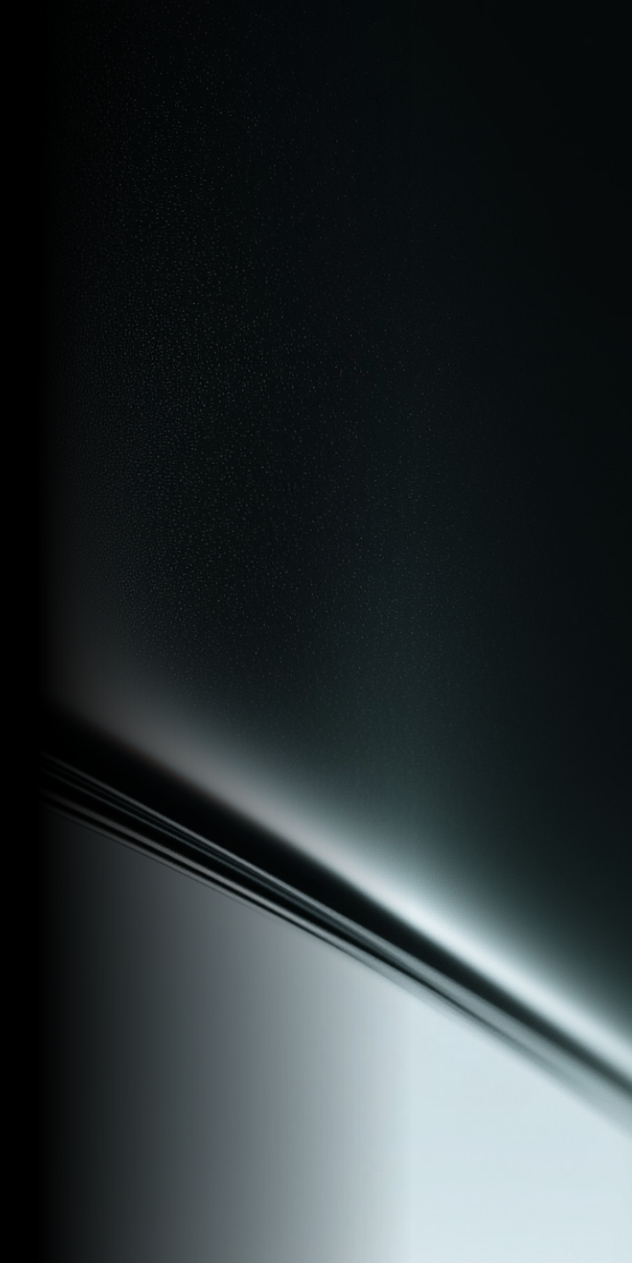
Nel dibattito sul cloud enterprise, anche il tema dell'europeicità assume una centralità crescente come fattore concreto di governance, controllo e autonomia. La giurisdizione dei provider, la localizzazione dei dati e i modelli operativi influenzano direttamente le scelte architetturali delle organizzazioni tanto da diventare leve fondamentali per garantire trasparenza, conformità normativa e libertà tecnologica.

Le principali analisi europee indicano che **oltre il 55% delle aziende considera sovranità del dato e conformità normativa come fattori determinanti nella scelta del cloud provider**.
Questo dato evidenzia come il tema non sia solo regolatorio, ma sempre più strategico. Infatti il rischio di lock-in tecnologico rappresenta una delle principali criticità per le organizzazioni. Dipendenze eccessive da singoli provider possono limitare la capacità di evoluzione e vincolare le scelte future.

Al contrario, modelli basati su standard aperti e portabilità dei workload consentono di mantenere autonomia decisionale e flessibilità strategica.

Un approccio europeo, che privilegia modelli aperti, interoperabili e distribuiti in cui il controllo non è concentrato ma bilanciato tra diversi livelli infrastrutturali, mette le organizzazioni nelle condizioni di scegliere e integrare soluzioni diverse mantenendo il controllo e di restare competitive grazie alla capacità di adattarsi più rapidamente ai cambiamenti di mercato e all'evoluzione tecnologica.

Europeicità significa **autonomia** senza rinunciare all'innovazione.



CAPITOLO 04

Compliance by design e governance

Nel contesto digitale europeo, la compliance non può più essere considerata un'attività a valle dei processi tecnologici. L'evoluzione normativa, dalla protezione dei dati alla cybersecurity, dalla resilienza operativa alla gestione delle infrastrutture critiche, impone alle organizzazioni di integrare i requisiti regolatori direttamente nella progettazione delle architetture cloud.

È questo il principio della **compliance by design**: costruire infrastrutture e modelli operativi che incorporano sicurezza, tracciabilità e controllo sin dall'origine.

Per CIO e CTO, questo approccio rappresenta un cambio di paradigma. La governance del cloud non riguarda soltanto la disponibilità delle risorse o l'efficienza dei workload, ma diventa un elemento strutturale della strategia digitale. Le architetture devono garantire visibilità sui flussi di dati, segregazione delle informazioni sensibili, tracciabilità e verificabilità dei processi e capacità di risposta agli incidenti. In altre parole, **la compliance diventa parte integrante della qualità del sistema**.

Ma se il cloud ibrido e distribuito introduce complessità crescenti (workload che attraversano ambienti diversi, dati che risiedono su più giurisdizioni e integrazioni continue tra piattaforme eterogenee) ne consegue che la governance richiede strumenti e modelli capaci di mantenere coerenza e controllo senza rallentare l'innovazione.

Ed è proprio **la progettazione by design a permettere di bilanciare agilità operativa e rigore normativo, riducendo il rischio di interventi correttivi costosi e invasivi**.
In questo modo le organizzazioni possono affrontare la complessità del modello di responsabilità condivisa, mitigando le difficoltà legate alla gestione multi-cloud e allo skill gap interno, garantendo una governance efficace e sostenibile.

Infatti è proprio il tema dello skill-gap ad essere sotto la lente. Alcune indagini sul mercato europeo rilevano che più del 50% delle organizzazioni in Europa segnala una carenza di competenze cloud avanzate, un fattore che spesso porta a concentrare le risorse sull'operatività tecnica, riducendo l'attenzione sulla governance strategica.

A questo si aggiunge la necessità di rendere la governance misurabile e verificabile nel tempo. Le organizzazioni devono essere in grado non solo di implementare controlli, ma di dimostrarne l'efficacia attraverso audit, reportistica e strumenti di monitoraggio continuo. Questo implica l'adozione di piattaforme che integrano nativamente funzionalità di compliance, riducendo la distanza tra progettazione e operatività e rendendo il controllo parte integrante del ciclo di vita applicativo.

Per alcuni mercati, come la Pubblica Amministrazione, la compliance è anche una questione di responsabilità istituzionale. La gestione di dati critici, ad esempio sanitari, fiscali, giudiziari o infrastrutturali, richiede garanzie elevate di integrità, disponibilità e protezione. Ma anche le imprese private affrontano sfide analoghe, soprattutto in settori regolamentati come finanza, energia o telecomunicazioni. In entrambi i casi, la capacità di dimostrare conformità diventa un fattore di fiducia verso cittadini, clienti e stakeholder.

Un altro elemento chiave della governance moderna è la capacità di automatizzare controlli e policy. Le architetture cloud progettate con logiche di compliance integrata consentono di applicare regole di sicurezza e gestione in modo uniforme, indipendentemente dall'ambiente in cui risiedono i workload. Grazie a questo approccio si riducono errori manuali, si migliora la tracciabilità ed è possibile adattarsi rapidamente alle nuove normative.

Un esempio concreto riguarda le organizzazioni che implementano sistemi di gestione centralizzata delle identità e degli accessi su ambienti multi-cloud. Questo consente di mantenere un controllo coerente su utenti e privilegi, garantendo tracciabilità e verificabilità dei processi e protezione dei dati sensibili. Analogamente, la progettazione di infrastrutture resilienti e ridondate permette di soddisfare requisiti di continuità operativa senza compromettere performance e scalabilità.

Questi scenari evidenziano come la governance integrata nell'architettura non rappresenti un vincolo operativo, ma una scelta progettuale consapevole perché tradurre la compliance in logiche infrastrutturali significa adottare un modello in cui **controllo**, **sicurezza** ed **evoluzione tecnologica** convivono fin dalla fase di design.

La compliance efficace non limita l'innovazione: la rende **sostenibile**.

CAPITOLO 05

Costi prevedibili e sostenibilità operativa

La trasformazione cloud viene spesso raccontata come un percorso orientato alla flessibilità e alla scalabilità.

Tuttavia, per CIO e CTO uno dei temi più critici resta la sostenibilità economica nel medio-lungo periodo. Perché l'adozione del cloud non è solo una scelta tecnologica ma anche una decisione finanziaria e operativa che impatta budgeting, governance e pianificazione strategica. In questo contesto, la prevedibilità dei costi diventa un requisito fondamentale per garantire continuità e controllo.

Secondo diverse indagini condotte sul mercato europeo, **oltre il 45% delle aziende indica la gestione dei costi come una delle principali criticità nell'adozione del cloud**, evidenziando la necessità di modelli più prevedibili e trasparenti.

I modelli di consumo tipici del cloud pubblico hanno introdotto dinamiche di spesa variabili, che se non governate possono generare fenomeni di overspending o difficoltà di pianificazione. Le organizzazioni si trovano spesso a bilanciare esigenze di flessibilità con la necessità di mantenere visibilità e stabilità sui costi. Questo scenario ha spinto molte realtà enterprise e PA verso architetture ibride, dove ambienti dedicati e modelli a capacità garantita convivono con risorse on-demand.

A questo si aggiunge un'altra sfida: la crescente necessità di correlare i costi IT al valore generato per il business. Non è più sufficiente monitorare solo la spesa: è necessario comprendere come le risorse cloud contribuiscono a performance, innovazione e qualità dei servizi. Questo richiede strumenti avanzati di cost management e una maggiore integrazione tra funzioni IT e finance, in una logica sempre più orientata al FinOps.

Inoltre la sostenibilità operativa riguarda anche l'intero ciclo di vita dell'infrastruttura. Migrazione, integrazione, manutenzione e gestione evolutiva rappresentano componenti economiche che devono essere valutate in modo sistemico.

Un'architettura progettata per ridurre la complessità operativa consente di contenere i costi indiretti e di migliorare l'efficienza dei team IT.

Ad esempio per le Pubbliche Amministrazioni la prevedibilità dei costi è strettamente legata a vincoli di bilancio e accountability.
Le decisioni infrastrutturali devono garantire trasparenza e continuità, evitando sorprese finanziarie che possano compromettere la programmazione. Analogamente, le imprese private richiedono modelli economici che permettano di correlare la spesa IT ai risultati di business, favorendo investimenti sostenibili.

La sostenibilità del cloud non si misura solo nel costo unitario, ma nella capacità di pianificare l'evoluzione.

Un ulteriore aspetto riguarda l'ottimizzazione continua delle risorse. Il monitoraggio dinamico dei workload e l'adozione di logiche di right-sizing consentono di adattare l'infrastruttura alle reali esigenze operative, evitando sprechi e migliorando l'efficienza complessiva. Questo approccio trasforma la gestione dei costi in un processo continuo e integrato.

CAPITOLO 06

Codesign e fattore umano

La complessità crescente delle architetture cloud rende sempre meno efficace un approccio standardizzato alla progettazione infrastrutturale.

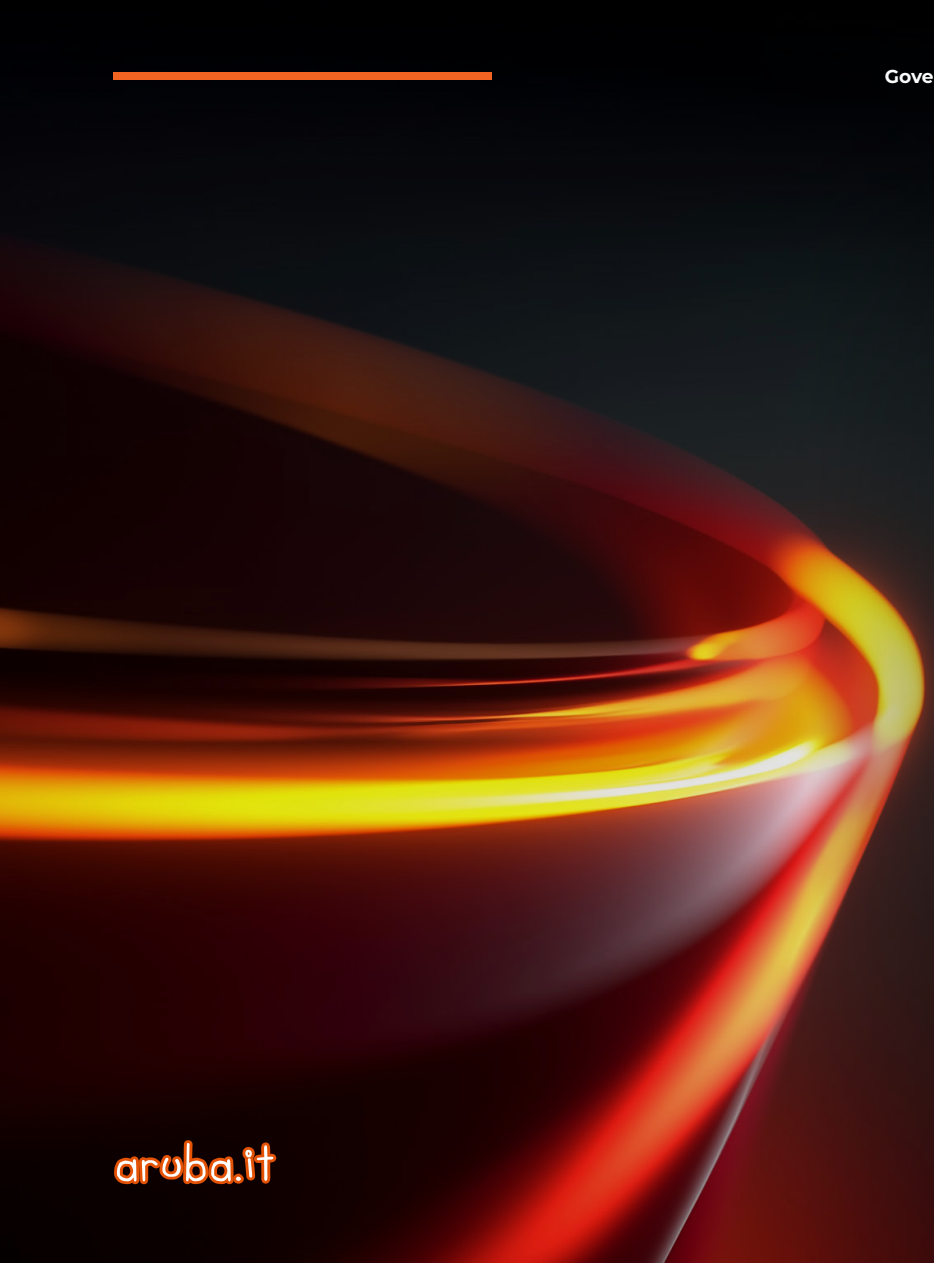
Le organizzazioni operano in contesti caratterizzati da vincoli normativi, legacy tecnologico e obiettivi di business specifici. Date queste premesse, il valore non risiede solo nella tecnologia adottata, ma nella **capacità di progettare soluzioni aderenti alle esigenze reali. È qui che il codesign diventa una leva strategica**.

Il codesign rappresenta un modello di progettazione condivisa in cui cliente, provider e partner collaborano fin dalle fasi iniziali. Non si tratta di personalizzare soluzioni esistenti, ma di costruire ecosistemi coerenti con le priorità strategiche. Questo approccio riduce il rischio di disallineamenti, migliora la qualità delle decisioni e accelera l'adozione.

Un elemento distintivo del codesign è la capacità di **anticipare le criticità**. Il confronto continuo tra le parti consente di identificare vincoli tecnici, normativi e operativi prima che si traducano in problemi, riducendo tempi e costi di implementazione. Questo rende il processo decisionale più solido e consapevole.

Anche il **fattore umano diventa centrale**: competenze, relazione e collaborazione rappresentano elementi chiave per il successo. In un contesto in rapido cambiamento, la capacità di lavorare in modo integrato tra team interni ed esterni diventa un **vantaggio competitivo concreto**. Ne deriva che la progettazione condivisa contribuisce anche a rafforzare la governance. Quando le scelte architetturali sono il risultato di un confronto strutturato, l'organizzazione mantiene maggiore controllo sulle evoluzioni future e riduce la dipendenza da modelli rigidi.

Il cloud efficace non si acquista:
si progetta insieme.



Managed services: dalla complessità operativa alla governance evoluta

Nel percorso di evoluzione verso architetture cloud sempre più distribuite e ibride, la gestione operativa dell'infrastruttura diventa uno dei principali fattori di complessità. In questo contesto, **i managed services rappresentano una leva strategica per trasformare la complessità tecnica in capacità di governo**.

Il modello dei servizi gestiti si basa su un principio chiave: separare l'operatività dalla governance. Le organizzazioni mantengono il controllo strategico su dati, architetture e processi decisionali, mentre demandano a un partner specializzato la gestione quotidiana dell'infrastruttura, della sicurezza e della continuità operativa. Questo approccio consente di riallocare risorse interne verso attività a maggiore valore, riducendo al contempo il rischio operativo.

Secondo MarketsandMarkets, **il mercato globale dei managed services raggiungerà circa 355 miliardi di dollari entro il 2027**, a conferma di una tendenza strutturale: le organizzazioni non cercano più solo tecnologia, ma modelli operativi sostenibili per governarla.

Nel paradigma cloud, il ruolo del Managed Service Provider evolve significativamente. Non si limita all'erogazione di servizi, ma assume una responsabilità **proattiva** nella gestione dell'infrastruttura, contribuendo a prevenire criticità, garantire continuità e supportare l'evoluzione dei sistemi.

Questo è particolarmente rilevante in ambienti multi-cloud, dove la frammentazione tecnologica aumenta la complessità di controllo.

Un elemento distintivo dei managed services è la capacità di operare su scala. Strutture come Network Operation Center (NOC) e Security Operation Center (SOC), attive 24/7, consentono monitoraggio continuo, risposta tempestiva agli incidenti e applicazione coordinata di aggiornamenti e policy di sicurezza. Questo livello di servizio, difficilmente replicabile internamente, permette di migliorare resilienza e compliance mantenendo efficienza economica.

La gestione integrata dell'infrastruttura consente inoltre di affrontare in modo più efficace il modello di responsabilità condivisa tipico del cloud. Attraverso un **approccio collaborativo**, il provider e l'organizzazione definiscono in modo chiaro ruoli e ambiti di intervento, riducendo ambiguità e aumentando il livello di controllo complessivo.

Un ulteriore vantaggio riguarda la **semplificazione della governance**. Affidarsi a un unico interlocutore per la gestione di ambienti complessi permette di superare la frammentazione operativa, migliorare la visibilità sui sistemi e garantire coerenza nell'applicazione delle policy. Questo contribuisce anche a ridurre fenomeni come lo shadow IT, riportando sotto controllo iniziative non governate.

In questa prospettiva, **i managed services non rappresentano una delega, ma un'evoluzione del modello operativo. Consentono alle organizzazioni di affrontare la complessità crescente del digitale mantenendo controllo, sicurezza e capacità decisionale**.

I managed services non riducono il controllo: lo rendono scalabile.

CAPITOLO 07

L'approccio e la visione di Aruba

All’interno di un panorama simile, **il ruolo del provider non può limitarsi alla fornitura di infrastruttura**. Deve diventare un abilitatore strategico, capace di accompagnare le organizzazioni lungo percorsi di trasformazione complessi.

Aruba opera sull'intera catena: dalla progettazione dell'architettura alla gestione operativa, dai data center fisici alla connettività, dalle piattaforme cloud alle logiche di compliance. Non si tratta di un catalogo di servizi ma di un modello in cui le scelte infrastrutturali, di rete e di governance sono progettate in modo coerente invece di essere assemblate a posteriori. Ciò che distingue questo approccio è la continuità: lo stesso interlocutore che aiuta a progettare la migrazione è quello che gestisce l'ambiente in produzione e che rileva per primo quando qualcosa non funziona come previsto. In architetture ibride e distribuite, questa continuità non è solo un vantaggio ma rappresenta anche un elemento di riduzione strutturale del rischio operativo.

Inoltre essere un operatore europeo, con infrastrutture fisiche in Europa e soggetto alla giurisdizione europea, non è solo un dato anagrafico. Significa che quando cambia una normativa (GDPR, NIS2, DORA, AI Act) le implicazioni architetturali vengono gestite dentro il perimetro, non negoziate con un fornitore extra-europeo. E per la PA e per le imprese in settori regolamentati questo riduce in modo concreto il carico di compliance.

Inoltre, **l’approccio Aruba integra logiche di co-design che permettono di ridurre il peso della responsabilità condivisa**, supportando le organizzazioni nella gestione operativa e consentendo ai team IT di concentrarsi sulla governance e sull’innovazione.

ARCHITETTURA COMPOSABLE DI ARUBA

Infrastruttura europea
Aruba serve oltre 200.000 clienti cloud in più di 100 paesi, da 8 cloud region proprietarie distribuite in 6 paesi europei

Piattaforma Cloud con standard aperti, basata su SECA, standard Kubernetes e altri progetti open (Liqo, ArubaKube), garantisce la portabilità dei workload tra ambienti Aruba, hyperscaler e on-premise, senza vincoli proprietari.

Integrazione ibrida e qualificazione per il settore pubblico
Multi-Cloud Link e Hybrid Connect offrono connettività diretta e dedicata verso AWS, Azure, Google Cloud e infrastrutture on-premise, con una struttura di costi trasparente.

Aruba Cloud è qualificata per la Pubblica Amministrazione italiana (ACN QC3, Consip) ed è membro del Board di Gaia-X, operando come nodo attivo del Gaia-X Digital Clearing House.

+200K
CLIENTI CLOUD SERVITI DA ARUBA

8
CLOUD REGION PROPRIETARIE

+16MLN
UTENTI

8
DATA CENTER PROPRIETARI IN EUROPA

evidence box

CAPITOLO 08

Conclusione: il cloud come abilitatore di controllo strategico

L'evoluzione del cloud nel contesto europeo non può essere interpretata solo come una trasformazione tecnologica. È una trasformazione del modo in cui le organizzazioni esercitano la propria capacità decisionale.

Controllo strategico significa poter scegliere: quale workload spostare, quando, su quale ambiente, con quale provider. Non è solo una questione di tecnologia ma anche di architettura progettata per lasciare aperte le opzioni invece di chiuderle. Inoltre interoperabilità, governance e sostenibilità dei costi non sono tre obiettivi separati: sono le tre condizioni che, insieme, rendono la complessità governabile.

L'innovazione non è libertà di fare di più, ma libertà di scegliere meglio.

Un ulteriore elemento chiave riguarda la velocità decisionale. In contesti competitivi e regolati, la capacità di adattarsi rapidamente diventa essenziale. Architetture flessibili e governate consentono di ridurre il time-to-decision e migliorare la reattività organizzativa.

L'AI rende tutto questo più urgente, non di certo più semplice. Modelli che operano su dati sensibili, su infrastrutture distribuite, in contesti normativi stringenti richiedono architetture progettate per il controllo. Il cloud europeo, in questo senso, non è un'alternativa all'innovazione ma la condizione per farla in modo sostenibile.

In questa prospettiva, **il cloud europeo si afferma come infrastruttura strategica capace di restituire controllo, autonomia e capacità evolutiva alle organizzazioni**.

Controllo strategico significa trasformare la complessità in capacità di scelta.

About Aruba

Aruba, fondata nel 1994, è il Cloud Champion italiano e uno dei principali provider europei di infrastrutture e piattaforme digitali basate su asset proprietari. L'azienda progetta e gestisce l'intero stack tecnologico: dalla progettazione e costruzione di data center alle piattaforme cloud, dai servizi di trust e security alla connettività e alle soluzioni software che supportano strategie digitali e applicazioni basate su AI.

Con capitale interamente italiano, Aruba conta 16 milioni di utenti attivi sulle proprie piattaforme provenienti da oltre 100 nazioni e gestisce una infrastruttura distribuita su 8 data center in Europa, che ospita oltre 2,7 milioni di domini, 10 milioni di caselle e-mail, 9 milioni di caselle PEC e migliaia di infrastrutture IT di clienti.

Copyright © Aruba. All rights reserved.
Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it