



Cloud Transformation

La sfida verso i servizi "managed" per il settore FSI

Michele Dotti

Managed Service Provider Strategia

Modello MSP

I Managed Service Provider agiscono come «one-stop shop» per i servizi Cloud, intermediando principalmente i servizi IaaS e PaaS ed offrendoli in logica gestita



Componenti di Servizio

IaaS

- Elementi infrastrutturali per utilizzare e gestire le piattaforme/ app (Es. Ambienti Dev/Prod, server farm clienti, ...)

PaaS

- Ambienti di sviluppo per implementare e distribuire applicazioni (Es. sviluppi MSA cloud native, Platform personalizzate, ...)

SaaS

- Software ready to use personalizzati per rispondere a specifici ambiti applicativi (Es. Corporate Banking, DDS, TRA, open banking, ...)

VAS

- Servizi professionali per la gestione E2E e l'ottimizzazione dei servizi Cloud offerti

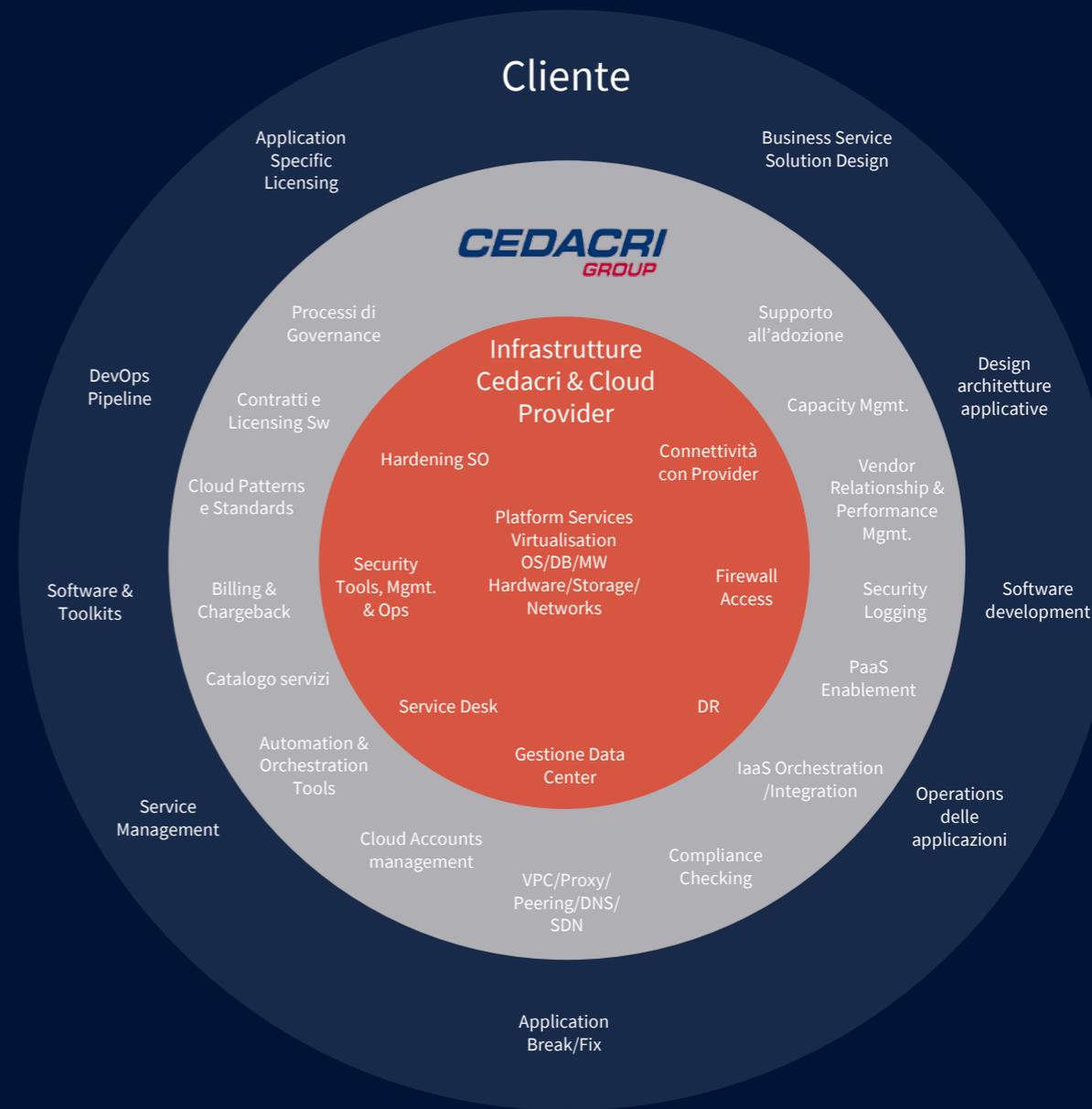
Obiettivi

- Evolvere verso modelli cloud per i clienti Cedacri e per il mercato FSI
- Sfruttare le potenzialità dei modelli di Hybrid e Public cloud per l'evoluzione del core banking system

Il catalogo servizi cloud si appoggia ad un modello di responsabilità definito

Cedacri gestisce il cloud per consentire al cliente di utilizzare i servizi adatti allo scopo. I servizi condivisi infrastrutturali sono gestiti dal team dell'infrastruttura Cedacri e/o dai cloud provider [a seconda del modello di delivery target \(on-prem vs public vs hybrid\)](#), in particolare:

- Il **provider cloud** esterno fornisce il proprio stack tecnologico fino a IaaS, PaaS e managed services inclusi.
- Il **team dedicato alla gestione dell'infrastruttura Cedacri** fornisce le immagini del sistema operativo di base securizzate per tutti i servizi IaaS. Fornisce inoltre la gestione dei firewall, tool di sicurezza, security operations, e gestisce centralmente gli incident ed il relativo coordinamento delle risposte.
- **Cedacri** adatta le immagini dei sistemi operativi securizzati per l'utilizzo specifico del cliente, assicura che il cliente sia ben informato sugli scenari d'uso ottimali, gestisce gli account cloud e imposta standard e pattern cloud, assicura che siano in atto gli opportuni processi di governance, crea, abilita e manutene i servizi IaaS e PaaS a valore aggiunto.
- **Le linee di sviluppo del cliente** mantengono la responsabilità e titolarità dei servizi di business, la loro progettazione, disponibilità e responsabilità complessiva a livello applicativo.



Riduzione della complessità operativa

- Dal punto di vista del cliente l'utilizzo di uno stack di servizi completamente gestiti riduce drasticamente la complessità operativa soprattutto per topologie e architetture complesse.

Infrastructure as Code (software defined)

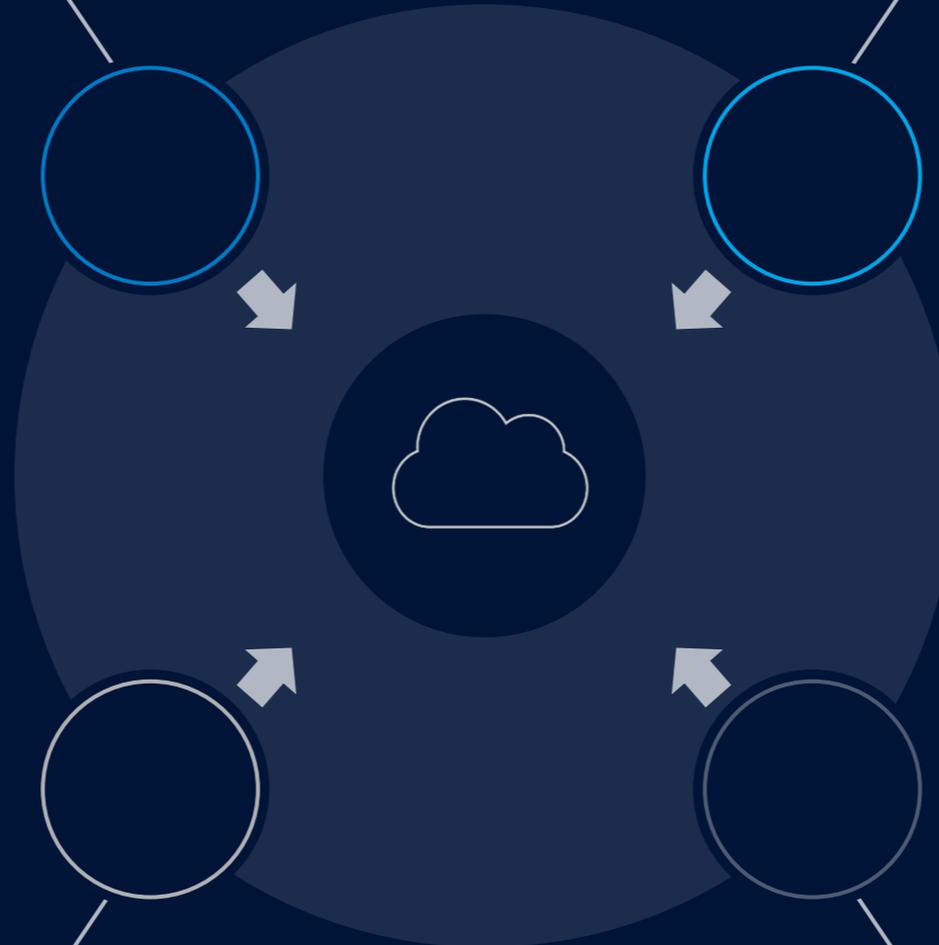
- L'intera topologia viene gestita utilizzando "infrastructure as code", questo approccio codificato via software ci garantisce controllo completo e riproducibilità, anche su regioni diverse.

Integrazione

- L'implementazione dei servizi all'interno delle nostre "landing zone" ci garantisce la possibilità di integrare facilmente l'intero catalogo dei servizi dei CSP.

Scalabilità

- L'utilizzo di servizi scalabili on-demand con opzioni specifiche (Es. Spot Instances) ci garantisce una granularità estrema sia dal punto di vista computazione che di ottimizzazione delle risorse.





Managed service provider

Fattori chiave di successo



Privacy, dati e crittografia

La protezione dei dati personali è fondamentale e va affrontata sotto diversi punti di vista: valutazione dell'adeguatezza dei Data Processing Agreement in quanto i CSP sono sub-responsabili del trattamento, territorialità del dato in area EU, crittografia "on-transit" e "at rest" ...



Valutazione dei Rischi

Un'attenta analisi dei rischi è indispensabile, occorre avere un perimetro delineato (connettività, governance, sicurezza, monitoraggio, HA/DR, ...) e dei processi di aggiornamento periodico, non dimenticando che il cloud impone anche una valutazione sul servizio/prodotto applicativo rispetto alle proprie peculiarità architetturali. Infine non dimentichiamo la "due diligence" dei CSP.



Audit

Fondamentale definire da subito e contrattualizzare gli aspetti collegati alle tematiche e ai relative processi di audit anche sui datacenter fisici!



Alta Affidabilità e Disaster Recovery

Il cloud ci dà la possibilità di valutare più opzioni: Tier0 – configurazione single AZ, Tier1 multi AZ, Tier2 multi AZ con backup dati su altra region, ... La granularità di analisi passa dal "datacenter" all'applicazione!



Exit strategy

La strategia di "uscita" è spesso sottovalutata ma è un preciso requisito normativo. Serve un approccio rigoroso che passa dal definire architetture il più possibili indipendenti da soluzioni proprietarie dei CSP (No-lock-in).

CEDACRI
GROUP