White Paper

La responsabilità condivisa

Scappare tra le nuvole non ti libera dalle tue responsabilità

Se in questi ultimi anni hai prestato anche solo un minimo di attenzione a quanto avviene nel settore informatico, di certo non ti sei perso la crescente diffusione del termine "**cloud**" negli ambiti più disparati. In effetti si tratta di una tecnologia che ha ridefinito in poco tempo l'intero panorama IT diffondendosi con soluzioni variegate per ogni genere di esigenza e tipologia di cliente.

Sinteticamente, si può dire che il cloud sia nato come **alternativa virtuale all'utilizzo dei tradizionali server fisici**. L'idea è concettualmente semplice: ogni volta che ti occorre una qualche risorsa informatica – la capacità di calcolo di un computer piuttosto che spazio di archiviazione storage – la puoi recuperare in modo dematerializzato all'interno di un ambiente condiviso chiamato cloud anziché doverti procurare e configurare hardware apposta come server o hard disk.

Ovviamente non si tratta di magia poiché il cloud si compone a sua volta di server e hard disk, e non potrebbe essere altrimenti; ma il bello di questa tecnologia è che li rende di fatto invisibili agli utilizzatori, che ne vedono solamente la capacità complessiva messa a disposizione senza dover badare ai dettagli dell'implementazione.

Quindi puoi guardare al cloud come a un enorme data center immateriale che ti mette a **disposizione quel di cui hai esattamente bisogno nel momento in cui ti occorre** senza dover installare o configurare alcunché. Nel momento in cui decidi di trasferirti presso un cloud più performante o più economico, è sufficiente spostare i flussi di dati attraverso una connessione di rete anziché traslocare l'intero parco hardware.

C'è poi un altro risvolto della tecnologia cloud che ha avuto e continua ad avere un forte impatto sul modo di lavorare di tutti noi. Il cloud è diventata infatti la piattaforma attraverso la quale è possibile ricevere sotto forma di servizio anche **intere applicazioni**. In questo modo il software che usi per il tuo lavoro non risiede più sui tuoi server o PC, il che ti evita di doverti occupare di installarlo, configurarlo e aggiornarlo. Sarà infatti il fornitore del servizio applicativo che penserà a tutto quanto.

Le potenzialità del cloud sono notevoli: restando in Italia, si tratta infatti di un mercato che nel 2021 ha totalizzato un valore di 3,84 miliardi di euro con una crescita del 16% rispetto all'anno precedente[1]. Tra le PMI, il 70% si avvale del cloud in un modo o nell'altro[2] anche grazie all'accelerazione impressa dalla pandemia e dal contestuale ricorso allo smart working. Lavoro delocalizzato, risorse IT delocalizzate: è semplice.

Ma allora il cloud è la soluzione tanto attesa a tutte le problematiche legate all'informatica? Come sempre la risposta è: dipende dai casi, non è un rimedio universale e comunque introduce a sua volta una serie di punti delicati di cui è bene tenere conto.

Il cielo informatico è pieno di nuvole differenti

All'interno del cloud è oggi possibile trovare di tutto, da intere infrastrutture IT fino a soluzioni specifiche per l'archiviazione e lo storage, applicazioni verticali e così via. Lo stesso cloud si è diversificato nel corso degli anni, tanto che oggi si parla di **cloud pubblico, cloud privato, cloud ibrido e multicloud**. Tu stesso probabilmente usi già un mix di soluzioni cloud senza esserne consapevole: ad esempio se condividi o sincronizzi file e documenti tramite Google Drive o Dropbox e se per le applicazioni office ti avvali di un abbonamento a Microsoft 365. Magari in azienda il tuo consulente IT ha configurato uno spazio di backup su Amazon Web Services (AWS)? Si tratta di cloud. Molto probabilmente anche il tuo sito web si trova nel cloud di un hosting provider. Se hai un reparto che si occupa di marketing e comunicazione, è facile che grafici e creativi abbiano un abbonamento alle app di Adobe Creative Cloud. Nell'area commerciale le applicazioni CRM (Customer Relationship Management) più diffuse come Salesforce vengono da tempo proposte in cloud.

Insomma, per quanto tradizionale possa essere il tuo ambiente IT, come vedi il cloud è ormai dappertutto. La comodità che offre è effettivamente innegabile. Senza il cloud, infatti, tutto ricade **sotto la tua responsabilità**:

1 www.osservatori.net/it/ricerche/comunicati-stampa/cloud-italia-mercato

2 www.ictbusiness.it/cont/news/la-diffusione-del-cloud-in-italia-e-il-suo-impatto-economico/44647/1.html

devi quindi procurarti l'hardware necessario, stendere l'infrastruttura di rete adatta, installare un sistema operativo e le applicazioni necessarie occupandoti anche di configurazioni e aggiornamenti, creare gli account per i tuoi utenti, gestire i dispositivi necessari per l'accesso e infine badare alla protezione, alla sicurezza e al backup di file e informazioni. Il che significa immobilizzare risorse economiche in conto capitale e doversi dotare di figure IT interne o consulenti esterni che seguano costantemente tutto l'ambiente tecnico e le richieste degli utenti.

La differenza con il cloud non potrebbe essere più netta: molto spesso per attivare un servizio o una risorsa cloud è sufficiente creare delle credenziali utente, fornire il numero di una carta di credito e attendere qualche minuto, magari direttamente dallo smartphone lungo il tragitto casa-ufficio. C'è anche un ulteriore vantaggio in **termini economici**, dal momento che molte proposte cloud vengono addebitate a consumo o con abbonamenti mensili o annuali, finendo quindi nel calderone delle spese correnti senza incidere su conti patrimoniali e ammortamenti.

Da ricordare anche come il modello pay-per-use o pay-as-you-go prevalente in ambito cloud permetta di risolvere l'annosa questione del dimensionamento delle risorse IT delle aziende, storicamente costrette a un costoso sovradimensionamento dell'ambiente informatico per non incorrere nel rischio di rallentare o fermarsi per mancanza di capacità sufficiente – un problema particolarmente sentito in caso di stagionalità o andamento ciclico dell'attività di business.

Ricapitolando, i vantaggi del cloud si possono ricondurre a un alleggerimento degli oneri a carico delle aziende in termini di investimento iniziale e gestione, oltre a un miglior allineamento tra risorse consumate ed esigenze effettive.

In questo senso il cloud risolve davvero una serie di esigenze e spalanca le porte a nuove possibilità operative, come peraltro si è visto molto bene nel periodo della pandemia.

Ma attenzione: ciò non significa che il cloud ti tolga di dosso ogni e qualsiasi responsabilità! È vero, il provider pensa a molte cose, ma ci sono elementi che rimangono di pertinenza dell'utilizzatore. Quali elementi, dipende dal tipo di soluzione cloud adottata:

- nel caso più semplice, quello del software applicativo erogato sotto forma di servizio (quel che viene denominato **SaaS**, Software-as-a-Service), la responsabilità del fornitore si ferma davanti ai dati, di cui si deve occupare il cliente;

- quando invece opti per una soluzione Platform-as-a-Service o **PaaS**, come un servizio di web hosting, devi occuparti non solo dei dati ma anche dell'applicazione (nel nostro esempio potrebbero essere Wordpress o Joomla);

- facendo un passo oltre, potresti aver bisogno di un server virtuale, magari a scopo di sviluppo e test: entriamo allora in una sfera che viene denominata **IaaS**, o Infrastructure-as-a-Service, dove sotto il tuo controllo ricade anche il sistema operativo della macchina con relative licenze, configurazioni e attività di aggiornamento.

Come vedi da tutte queste sigle e casistiche di utilizzo, il cloud è davvero una tecnologia flessibile che si adatta ad approntare soluzioni di ogni genere: un ventaglio completo e in costante ampliamento nel quale puoi trovare senz'altro le proposte che cerchi. Ma a questa varietà di risposte alle possibili esigenze si accompagna una pari varietà nella suddivisione di responsabilità e competenze tra provider e cliente. Essere consapevoli di questo fattore è essenziale per non incorrere in brutte sorprese.

Benvenuto nel mondo della responsabilità condivisa

A seconda del tipo di soluzione cloud, dunque, cambia il mix di obblighi che ciascuna parte (cliente e provider) si assume. L'errore più grande che potresti commettere è quello di credere che, affidando una parte del tuo ambiente informatico al cloud di un fornitore esterno, quest'ultimo si faccia carico automaticamente dell'intero spettro delle possibili responsabilità. Per dirla con una battuta, stai lavorando con un provider, non con una compagnia assicurativa!

Indipendentemente da ogni altra considerazione, devi ricordarti che ci sono alcuni elementi che saranno sempre di tua esclusiva pertinenza:

- **sicurezza delle credenziali utente**. Nemmeno il cloud provider più attento potrà proteggerti se assegni credenziali a chiunque senza alcun controllo o se riutilizzi le stesse password più volte. Puoi dotarti della cassaforte più sicura del mondo, ma non ti servirà a nulla se ci appiccichi sopra un post-it con scritta la combinazione;
- **sicurezza dei dispositivi usati per l'accesso**. Anche le credenziali più solide non ti possono aiutare se accedi al cloud con un PC non aggiornato e infestato dai virus o uno smartphone contenente spyware. La protezione dei dispositivi client è dunque un prerequisito che devi soddisfare prima ancora di avvicinarti a un potenziale fornitore di servizi cloud;
- **sicurezza dei dati**. Sei tu che decidi con chi condividere i dati residenti nella tua soluzione cloud, ed è compito tuo verificare che tali dati non vengano consultati o utilizzati da chi non è autorizzato a farlo o per scopi diversi da quelli lecitamente previsti.

A una serie di altre cose, invece, ci deve pensare indiscutibilmente il tuo provider:

- **disponibilità del sistema**. In un'epoca in cui le aziende lavorano in tempo reale affidandosi completamente all'informatica, un cloud che va a singhiozzo è un cloud fondamentalmente inutile. I provider quantificano il loro impegno al costante funzionamento dei loro apparati attraverso i cosiddetti parametri SLA (Service Level Agreement), in genere corrispondenti alla percentuale del tempo di operatività garantita: uno SLA del 99,9% annuale equivale a poco meno di 9 ore di *possibili* interruzioni ogni dodici mesi, mentre uno SLA del 99,99% abbatte questa eventualità a soli 52 minuti all'anno e così via;
- **continuità operativa**. Termine che spesso viene confuso con il precedente, ma che in realtà si riferisce alla capacità del provider di spostare trasparentemente le attività – attraverso un apposito piano di ridondanza – verso un secondo ambiente o data center in caso di problemi con quello principale;
- **sicurezza dell'infrastruttura**. È compito del provider garantire la massima protezione possibile dei propri sistemi dagli accessi non autorizzati di tipo sia fisico che virtuale. Questo significa limitare e controllare l'ingresso agli edifici e alle sale del data center, disporre di capacità di analisi e verifica del traffico di rete, e mantenere tutti i sistemi regolarmente aggiornati in modo da neutralizzarne le vulnerabilità note. Un'infrastruttura sicura prevede anche contromisure contro eventi calamitosi come interruzioni dell'alimentazione o incendi;
- **integrità dei dati**. Il provider ti deve assicurare che i tuoi dati siano sempre tracciati, integri e separati da quelli degli altri clienti che condividono i medesimi sistemi fisici e logici che compongono il cloud nel quale lavori. Puoi pensare al tuo provider come a un hotel: l'ultima cosa che vorresti è che gli altri ospiti possano usare la loro chiave per entrare anche nella tua camera!

Quello a cui devi fare attenzione è però quell'area grigia che si basa su una collaborazione efficace tra cliente e provider. È la cosiddetta ***responsabilità condivisa***, che va opportunamente verificata di volta in volta dal momento che ha caratteristiche differenti a seconda del provider o del tipo di servizio cloud scelto. In genere riguarda i seguenti elementi:

- **identità e accessi**. Il provider implementa le funzionalità tecniche necessarie a creare, gestire e verificare gli utenti e le relative credenziali. Il tuo compito è quello di fare in modo che il sistema non venga abusato o finisca fuori controllo: per esempio dovresti regolarmente controllare:
    - che ciascun utente disponga di privilegi coerenti con il proprio ruolo lavorativo,

- che non rimangano attive credenziali di utenti non più esistenti,
- che non vi siano accessi da dispositivi non autorizzati,
- che tutti rispettino le buone pratiche correnti per la gestione degli account (ad esempio attivando l'autenticazione a due fattori, dove disponibile, e cambiando periodicamente le password);

- **gestione dei dati**. Anche qui, in genere il cloud provider ha il compito di mettere in atto tutte le soluzioni tecniche che occorrono per la consultazione, la conservazione, la movimentazione e lo smaltimento dei dati. Ovviamente resta una tua precisa competenza quella di accertarti che i dati raccolti siano conformi alle normative applicabili (dal GDPR, che riguarda tutti, ai regolamenti più specifici che toccano determinati settori come quello dei servizi finanziari o della sanità) e agire di conseguenza, ad esempio:
  - selezionando un data center territorialmente adatto,
  - procurandoti il consenso al trattamento di eventuali dati personali,
  - evitando di acquisire dati non strettamente necessari alla tua attività,
  - rispettando le richieste di aggiornamento o cancellazione provenienti da terzi e così via;
- **backup**. Non esiste provider che non preveda una qualche forma di backup nella propria offerta di servizi in cloud. Eppure si tratta di un'area talmente diversificata che ti consigliamo vivamente di verificare molto bene che cosa intenda il tuo provider con questo termine:
  - cosa sia effettivamente coperto,
  - con quale frequenza,
  - con quale modalità,
  - con quale rispondenza alle tue necessità operative.

  Un esempio banale è quello di un provider che effettua il regolare backup dei propri database server per poterli ripristinare complessivamente in caso di guasti o attacchi informatici; si tratta però di un backup generale di sistema dal quale non è possibile estrarre lo specifico database di un singolo cliente. Anche la periodicità dei backup effettuati dal provider potrebbe essere diversa da quella che occorre alle tue applicazioni. Il suggerimento è quello di effettuare sempre i propri backup da sé indipendentemente da quelli del provider; alla peggio, avrai una maggior ridondanza che non guasta mai;
- **crittografia**. Ecco un tema che negli anni è cresciuto costantemente di importanza, tanto che oggi è difficile trovare un provider che non implementi tecnologie crittografiche in un punto o nell'altro della propria infrastruttura. L'efficacia di questa tecnica di difesa dei dati – in transito per la rete o a riposo sullo storage del cloud – dipende però da una sua corretta applicazione in ogni anello della catena che unisce il provider ai suoi clienti. Questo significa evitare che i tuoi dati possano circolare in chiaro, magari quando li importi sul cloud per poterci lavorare o li scarichi per un backup. Le capacità di cifratura offerte dai provider da sole non bastano: devi considerarle come un componente di un approccio complessivo alla protezione crittografica dei tuoi dati.

Come vedi, il mondo del cloud non ha poi cambiato così tanto alcune abitudini nel rapporto cliente/fornitore IT. Se presti attenzione, anche in un ambiente tradizionale on-premise ci sono alcune responsabilità di cui si fa carico il tuo consulente IT, altre che sono di tua pertinenza e altre ancora che vengono condivise tra le parti. Quindi, se sei già adeguatamente organizzato per gestire una condivisione delle responsabilità, il passaggio al cloud non dovrebbe crearti particolari difficoltà anche se ovviamente dovrai verificare con cura tutti i singoli punti che compongono il rapporto col provider che hai scelto. Viceversa, l'adozione di una soluzione cloud potrebbe essere la buona occasione per iniziare a disciplinare in modo adeguato la suddivisione dei vari obblighi. Di certo, come già accennato, il cloud non può essere considerato come la soluzione per un totale scaricabarile sulle spalle del provider!

Anche saper scegliere è una competenza preziosa

Se vuoi che la tua soluzione cloud apporti un efficace contributo al buon funzionamento della tua attività minimizzando l'impegno da parte tua e soprattutto le sorprese impreviste, il primo passo deve essere quello di selezionare la **combinazione servizio/provider** più adatta. Il ventaglio dell'offerta è quanto mai ampio, infatti, ed esiste il rischio di essere sviati da richiami commerciali che distraggono da questioni basilari ben più importanti.

Puoi avviare una prima scrematura interessandoti agli aspetti del servizio più facilmente quantificabili dal punto di vista numerico o qualitativo: gamma di opzioni esistenti, parametri SLA, livelli di disponibilità del servizio, penali riconosciute in caso di disservizio, capacità di personalizzazione, struttura contrattuale e rapporto qualità/prezzo.

Questo significa che il servizio più adatto non è necessariamente quello che appare più economico – un errore che purtroppo si tende a compiere di fronte alle priorità di budget. Un fornitore può infatti ingolosirti con cifre di partenza molto contenute, salvo nella pratica rendere non calcolabile un preventivo a causa della quantità, complessità, aleatorietà e imprevedibilità dei parametri sui quali viene costruita la tariffa finale.

Altre proposte possono essere invece perfette per le tue necessità del momento ma non prevedere spazi di crescita o evoluzione successiva. Occhio poi al cosiddetto ***vendor lock-in***, o vincolo sul fornitore, un vecchio trucco in auge in molti comparti del settore informatico e che all'interno del cloud ha trovato una nuova ragion d'essere: sotto questa etichetta ricadono tutte le tattiche commerciali, limitazioni tecniche e clausole contrattuali finalizzate a rendere oltremodo difficoltosa se non addirittura impossibile la successiva migrazione di dati e configurazioni verso un provider differente.

Tutto questo presupponendo naturalmente che tu ti sia assicurato in primo luogo di delineare correttamente le caratteristiche del servizio da acquistare. Sembra una cosa scontata, ma può accadere di concentrarsi talmente tanto sulle funzionalità fondamentali di una soluzione da dimenticare quelle complementari e tuttavia importanti.

Considera a titolo di esempio quanto accaduto ai clienti del provider francese Ovh, il cui data center di Strasburgo è andato a fuoco nel marzo 2021: in questa occasione chi aveva sottoscritto opzioni accessorie di data recovery con replica off-site dei dati ha potuto recuperare tutto il proprio patrimonio informativo, contrariamente a chi non aveva considerato questo aspetto accontentandosi magari di un semplice backup base su sistemi fisicamente adiacenti a quelli di produzione. A distanza di un anno la questione è oggetto di una disputa in tribunale[3] sulle clausole contrattuali, ma qualunque eventuale risarcimento non restituirà certo i dati andati irrimediabilmente distrutti.

Una volta che avrai definito l'elenco ristretto dei servizi più convincenti, potrai passare a valutare i relativi cloud provider sulla base di altre caratteristiche di più ampio respiro:

- **standardizzazione**. Un buon provider agisce sulla base di procedure standard che regolano tanto la propria attività interna (gestione, aggiornamenti, controlli) quanto il rapporto con il cliente (SLA, interventi, interfacce, test, gestione ticket ecc.). Procedure formalizzate sono indice di un provider ben organizzato e offrono buone garanzie per evitare dimenticanze, confusioni di ruoli ed errori vari;

- **completezza dell'offerta**. Anche se hai definito con grande precisione le tue esigenze attuali, non escludere che queste possano cambiare nel tempo. Un cloud provider dotato di un ventaglio di proposte più ampio di quello che ti occorre oggi può facilitare la tua evoluzione futura: sia che si tratti di infrastrutture (magari un cloud ibrido) che di applicazioni (piani di abbonamento scalabili per volumi e funzionalità);

3 www.repubblica.it/economia/2022/03/15/news/contro_un_disastro_cloud_la_prima_class_action_in_italia_3milioni_di_euro_di_risarcimento_chiesti_a_ovh-340669161

- **capacità di supporto**. Quando sei alle prese con un problema, non vuoi semplicemente aprire un ticket e sperare che qualcuno ti risponda. Un provider che si impegni nei confronti di un tempo massimo di intervento o che ti metta a disposizione un contatto diretto per ogni tua esigenza di assistenza tecnica e amministrativa è indubbiamente preferibile rispetto a un fornitore che non ti offre alcun mezzo di comunicazione diverso da un modulo sul suo sito web o un numero di call center estero;

- **misurazione del rapporto**. Non basta definire i parametri SLA o l'impegno a rispettare determinate caratteristiche del servizio; un buon provider non manca di misurare la propria attività rispetto a quanto promesso comunicando regolarmente con i suoi clienti attraverso appositi report. Documenti del genere sono indispensabili anche per capire se il piano o la soluzione che stai usando in quel momento continuino a essere adeguati alle tue necessità o se non sia piuttosto opportuno passare a un'offerta diversa, meno costosa o maggiormente performante a seconda dei casi;

- **affidabilità societaria**. Quanto più la tua attività dipende dall'IT, tanto più è essenziale che il tuo cloud provider sia solido sotto tutti i punti di vista. Vale cioè quella che dovrebbe essere la regola vigente per qualunque fornitore strategico: si tratta di una società in salute e di ottima reputazione? Opera in sintonia con i tuoi principi operativi ed etici? Qual è la storia alle sue spalle? È una società indipendente o appartiene a qualche gruppo particolare? È solita lavorare con clienti simili a te per settore o dimensioni? Possiede certificazioni specifiche e si sottopone regolarmente ad audit esterni?

Come vedi, il cloud è certamente una tecnologia che può aiutarti sotto tanti punti di vista alleviando una serie di impegni operativi e finanziari con cui hai dovuto finora fare i conti in prima persona. Di più: dedicando un po' di tempo all'approfondimento delle numerose proposte esistenti sul mercato puoi avere la possibilità non solo di risolvere le tue esigenze del momento, ma di delineare anche una strada di crescita ed evoluzione sfruttando capacità che magari non immaginavi neppure fossero disponibili o praticabili.

In qualsiasi caso non devi mai perdere di vista il fatto che nessun cloud e nessun provider **potranno mai sostituirti al 100%** nella gestione delle responsabilità, le quali saranno sempre condivise con ripartizioni differenti a seconda delle situazioni. Avere una chiara visione degli obblighi e delle aspettative di ciascuna parte rappresenta il primo passo di un percorso di successo nella nuova era dell'informatica tra le nuvole.

Glossario

Cloud – Un modello di erogazione di servizi informatici attraverso un'architettura distribuita. Le risorse che costituiscono un ambiente cloud vengono condivise tra i diversi utilizzatori e possono essere scalate in modo elastico senza provocare interruzioni operative. Vi sono differenti tipologie di cloud: pubblico, la cui infrastruttura non appartiene all'utente finale a differenza del cloud privato; ibrido, formato da un mix di ambienti cloud e tradizionali; e multicloud, composto da più servizi cloud di tipologie e fornitori differenti.

GDPR - Il Regolamento Generale sulla Protezione dei Dati è il riferimento normativo europeo delle leggi che dal 2018 definiscono la possibilità di raccogliere, conservare e utilizzare dati sensibili e personali appartenenti a cittadini e residenti della Comunità Europea. L'entrata in vigore del GDPR ha costretto le aziende a implementare meccanismi di controllo e governance delle informazioni che devono essere regolarmente verificati per garantire il corretto rispetto della norma evitando violazioni che comportano sanzioni rilevanti.

IaaS – Acronimo di Infrastructure-as-a-Service, ovvero un tipo di soluzione cloud che mette a disposizione risorse di calcolo, connettività di rete e capacità storage sotto forma di servizio, generalmente addebitato a consumo (pay-as-you-go).

On-premise – Anche on-premises, in informatica è un termine che indica qualcosa che viene installato, gestito e utilizzato all'interno di un'azienda anziché presso un provider esterno, nel qual caso viene identificato dal termine off-site. Può essere un sistema, un'applicazione, un backup, un intero data center o persino un cloud privato.

PaaS – Acronimo di Platform-as-a-Service, ovvero un tipo di soluzione cloud che mette a disposizione un ambiente adatto allo sviluppo e alla distribuzione di applicazioni software.

SaaS – Acronimo di Software-as-a-Service, ovvero un tipo di soluzione cloud che mette a disposizione un'applicazione software sotto forma di servizio utilizzabile su abbonamento accedendovi tramite interfaccia web o apposite API.

Spyware – Una particolare tipologia di malware che ha lo scopo di raccogliere quante più informazioni possibili sull'utilizzatore del computer o del dispositivo sul quale risiede. A differenza del ransomware e di altri malware, lo spyware è scritto per restare ben nascosto più a lungo possibile raccogliendo dati sensibili che possono essere rilevati tramite sia la lettura dei file presenti sul sistema, sia il monitoraggio dei tasti premuti alla tastiera. Gli esemplari di spyware più sofisticati possono estendere il loro raggio d'azione anche alla rete alla quale è collegato il dispositivo infetto.