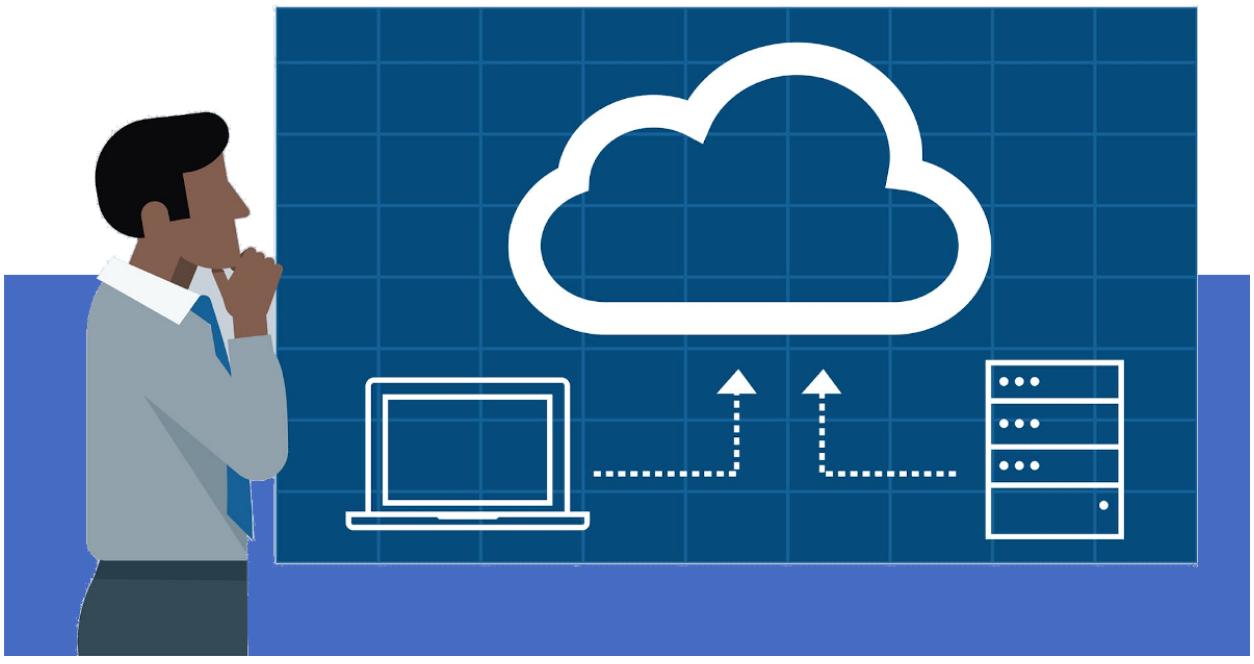
UNIVERSITÀ
DI SIENA
1240

UniSIcuri in Rete - Nel cloud

Marzo 2021



Cos’è il cloud?

“Il Cloud non esiste, è solo il computer di qualcun altro” .

Il “cloud” (nuvola) è un termine usato per descrivere una Rete di server che appaiono, dal punto di vista dell’utente/cliente, come una unica entità. Il cloud non è un'entità fisica a sé stante, ma è una Rete più o meno vasta di server remoti ubicati in tutto il mondo, collegati tra loro e che operano come un unico ecosistema. **Il cloud può essere progettato per archiviare e gestire dati, eseguire applicazioni, distribuire contenuti o servizi (es. video o audio in streaming), posta elettronica, piattaforme Web...**

Dal punto di vista utente, invece di accedere ai files e ai dati sul proprio PC, vi si accede attraverso la Rete o Internet, così che il materiale sia sempre disponibile ovunque vi si trovi.

I vantaggi di questa tecnologia sono innegabili, ma questa comodità e delocalizzazione dei dati (e relativi oneri di gestione) portano con sé anche nuovi rischi e problematiche che andremo ad affrontare in questo articolo.

Essenzialmente esistono 3 tipologie diverse di infrastrutture “cloud”:

- **cloud pubblico**, che condivide le risorse e offre servizi pubblicamente via Internet;
- **cloud privato**, generalmente ospitato all’interno della Rete istituzionale locale e non condiviso pubblicamente;
- **cloud ibrido**, che offre sia servizi pubblici che privati, una via di mezzo delle precedenti categorie;

👉 Entro il 2025 ci saranno sul cloud 100 zettabytes di dati, circa metà della capacità di archiviazione mondiale.

Un esempio di **cloud pubblico può essere Dropbox, MEGA, One Drive o il Drive di Google**[1]: si tratta di soluzioni dove si può accedere via Internet ovunque vi sia una connessione, previa autenticazione sul portale del servizio.

Un **cloud privato può essere un NAS installato nel proprio ufficio**, ad uso e consumo del personale dell'ufficio stesso.

Il **cloud ibrido è un servizio che permette di integrare spazio in cloud privato con spazio in cloud pubblico**, in modo che le due realtà interagiscano in ogni momento. La soluzione è particolarmente utile per quei contesti che necessitano di operare con regolarità, anche quando non è disponibile la connessione alla Rete. Un esempio è la soluzione *Azure Stack*[2] offerta da Microsoft. Al momento, tuttavia, questa particolare tipologia di cloud non verrà affrontata.

Cloud pubblici

Spesso troviamo i loro client già pre-installati nei nostri dispositivi, magari con qualche offerta speciale di spazio disponibile aggiuntivo. Il funzionamento è generalmente molto semplice: mi registro al portale, ottengo il mio spazio gratuito sul loro cloud, configuro il client sul mio dispositivo e automaticamente tutto quello che salvo nella cartella scelta per la sincronizzazione viene, appunto, salvato anche sul cloud remoto. Con la tranquillità di poter accedere a quei file anche da altri dispositivi, semplicemente autenticandomi sul portale del cloud anche via web.

I nostri dati, quindi, non saranno solamente sui nostri dispositivi ma anche sul cloud del provider, che *a seconda della privacy policy adottata* può avere dei diritti su quei dati di cui non sempre siamo consapevoli.

Ad esempio, **il Regolamento generale sulla protezione dei dati ("GDPR") definisce regole precise per il trasferimento dei dati personali fuori dall'Unione europea** e vieta, in linea di principio, il trasferimento "anche temporaneo" di dati personali verso uno Stato extraeuropeo, qualora l'ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela: *la soluzione cloud scelta, quindi,*

[1] dropbox.com, mega.co.nz, onedrive.live.com, drive.google.com
[2] azure.microsoft.com/it-it/overview/azure-stack/

dove ha i data center che conservano i dati dei cittadini europei? La tipologia di account utilizzata rispetta la normativa GDPR?

Dobbiamo anche assicurarci che **il fornitore del servizio adotti tecnologie di sicurezza e tutela dei dati adeguate**, poiché sono avvenuti nel passato pesanti *data breach* (ad esempio, nel 2016 Dropbox ha subìto un data breach da 68 milioni di account utente) che hanno minato il falso mito del "cloud sicuro" (non è più "sicuro" di qualsiasi altro servizio in Rete).

👉 Attenzione alla normativa quando si trattano dati istituzionali su una soluzione cloud pubblica

---

In ambito istituzionale e aziendale, oltre a doversi assicurare che il fornitore del servizio cloud garantisca il rispetto dei requisiti normativi (incluso il GDPR), è bene sincerarsi che la *policy* ne consenta l'utilizzo anche per i dati di lavoro: **i rischi derivanti dall'utilizzo di soluzioni cloud "personali" anche per la conservazione dei dati aziendali o istituzionali sono alti**, dai data breach alla divulgazione di dati personali, che possono esporre il dipendente a conseguenze anche penali.

Consigliamo pertanto di mantenere separati eventuali soluzioni cloud “personali” da quelle professionali, evitando di utilizzarle per memorizzare materiale o documenti di lavoro.

Come ulteriore suggerimento, **consigliamo di utilizzare soluzioni cloud pubbliche solo per dati non riservati**. Nel caso vi sia l’esigenza di utilizzarlo anche per salvare materiale riservato, suggeriamo di adottare soluzioni crittografiche sicure[3] come ulteriore protezione dei dati.

Attenzione ai Termini di servizio per eventuali account gratuiti che, rispetto alle soluzioni a pagamento (abbonamento annuale o una tantum), generalmente **offrono meno garanzie rispetto alla possibilità di veder disattivato improvvisamente il proprio account** (con conseguente perdita di tutti i dati memorizzati) per generici “utilizzi indebiti”.

Concludendo, se **l’uso di un cloud privato ci solleva dagli oneri di gestione e manutenzione dei servers** e dispositivi deputati alla conservazione dei dati e del servizio stesso, ci impone comunque maggiore attenzione sul fronte normativo in merito alla salvaguardia dei nostri dati e della nostra privacy.

Cloud privati

I NAS o file servers casalinghi e istituzionali, più o meno grandi, includono già la possibilità di essere utilizzati come soluzioni cloud private: accessibili solo dalla Rete casalinga o istituzionale, anche se viene offerta la possibilità di accedervi anche dall’esterno (caratteristica di cui parleremo dopo), offrono una **comoda e ragionevolmente sicura soluzione** per la conservazione dei dati personali e aziendali.

Chiaramente soluzioni di questo tipo, seppur **garantendo maggiore privacy dei dati, includono maggiori oneri per la gestione e conservazione dei dati stessi**: non solo dobbiamo farci carico della corretta configurazione del servizio di cloud (elemento non trascurabile, visto che una errata configurazione può mettere a rischio la riservatezza

[3] VeraCrypt (www.veracrypt.fr/en/Home.html) o 7zip (7-zip.org)

dei dati) ma anche della manutenzione ordinaria e straordinaria dei dispositivi stessi, oltre ovviamente a tutti gli incidenti di sicurezza che potrebbero accadervi.

La semplicità di uso e la relativa economicità ha di fatto favorito il proliferare di queste soluzioni, sia in ambito *SOHO* (*Small Office, Home Office*) che istituzionale, con conseguenze non sempre piacevoli: spesso **una falsa percezione di maggiore sicurezza ha causato disastrose perdite di dati** a causa di attacchi da *ransomware* (ne abbiamo parlato nella precedente newsletter) o furti degli stessi per errata configurazione delle protezioni di accesso e autenticazione.

È opportuno che, soprattutto in ambito istituzionale, **l'installazione e l'uso di questi dispositivi sia regolata da apposite policy e verificata da personale specializzato**, in grado di adottare i necessari protocolli di autenticazione e protezione dei dati, così come le opportune ACL per l'accesso ai dati stessi: capita, purtroppo, di **individuare sulla Rete NAS e file servers senza alcuna protezione**, o con protezioni deboli, esponendo i dati lì conservati a furto, danneggiamento o utilizzo indebito dello spazio disco.

In merito alla **possibilità offerta da alcune di queste soluzioni di essere accessibili anche dall'esterno**, è sempre bene considerare i rischi derivanti dal mantenere una "finestra aperta" su Internet attraverso la quale malintenzionati possono accedere ai nostri dati. Seppur adottando password sicure e implementando periodici aggiornamenti, *eventuali vulnerabilità 0-day potrebbero essere abilmente sfruttate per rubare o danneggiare i dati*, soprattutto in contesti istituzionali o aziendali dove i

dati hanno un valore economico importante e gli attori malevoli sono fortemente motivati.

👉 Le soluzioni di cloud privato richiedono competenze tecniche di cui non si può fare a meno, soprattutto in ambito aziendale

---

Per finire, sebbene il cloud privato possa rappresentare un'ottima soluzione per la conservazione dei dati riservati in ambito casalingo o istituzionale, è sempre bene:

- **effettuare regolarmente tutti gli aggiornamenti di sistema e del software**;
- **utilizzare sempre account personali con password sicure**: evitare account generici e password deboli, che potrebbero essere facilmente indovinabili;
- **disattivare eventuali servizi non necessari**, ad esempio se utilizziamo solo il trasferimento files via SMB, disattivare FTP;
- **adottare soluzioni di logging e monitoraggio**, soprattutto in ambito istituzionale, che possano allertare in merito a tentativi di accesso non autorizzati o trasferimenti di dati sospetti;
- affidarsi sempre, per la configurazione iniziale, a personale adeguatamente formato ed esperto;

Ricordiamo che, in ambito istituzionale, **l'eventuale sottrazione di dati da una soluzione cloud privata comporta le procedure di data breach indicate dalla normativa**[4], rendendo il responsabile del dispositivo passibile di sanzioni nel caso non siano state adottate adeguate misure di sicurezza e protezione.

[4] Violazioni di dati personali (Data Breach), www.garanteprivacy.it/regolamentoue/databreach

Riferimenti normativi

La normativa europea sulla protezione dei dati personali ("GDPR") impone **la definizione di contromisure atte a minimizzare la possibilità del furto di dati** ("*data breach*") e le eventuali conseguenze.

La Rete Internet è diventata strumento indispensabile per l'espletamento di gran parte delle attività lavorative dell'Ateneo. Attraverso la Rete, l'Ateneo permette agli studenti, ai docenti, ai ricercatori, ai tecnici, agli amministrativi, ai collaboratori e a tutto il restante personale, l'accesso ai dati e ai servizi necessari allo svolgimento delle attività didattiche e amministrative. **La sicurezza dei dati e delle infrastrutture assume, pertanto, un ruolo essenziale per le libertà e i diritti degli interessati e per il mantenimento della *business continuity*.**

Qualsiasi dispositivo connesso in Rete diventa attore del processo di business e deve rispettare alcuni requisiti minimi per la salvaguardia dell'infrastruttura ICT e dei suoi servizi.

- ➔ **Parere 05/2012 sul cloud computing adottato il 1° luglio 2012 - www.garanteprivacy.it/documents/10160/2045741/WP+196+-+Parere+052012+sul++cloud+computing.pdf**
- ➔ **Garante per la protezione dei dati personali** - Regolamento europeo in materia di protezione dei dati personali - www.garanteprivacy.it/regolamentoue
- ➔ **Agenzia per l'Italia digitale** - Misure minime di sicurezza ICT per le PA - www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Contatti e siti web utili

- ➔ Gestione delle **credenziali unisiPass** e **aggiornamento password**: my.unisi.it
- ➔ **Avvisi di sicurezza** dell'Università di Siena: www.uet.unisi.it/category/sicurezza/
- ➔ Servizio di **assistenza tecnico-informatica** dell'Università degli Studi di Siena: helpdesk@unisi.it
- ➔ Segnalazione **violazioni al trattamento dei dati personali**: abuse@unisi.it