Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS
Analisi e prevenzione

2 maggio 2025

Valutazione tecnologica: cloud computing e cibersicurezza

1 Introduzione e situazione iniziale

Il «cloud» o«cloud computing» viene spesso descritto come un cambio di paradigma, una novità che segue regole nuove. Di conseguenza, spesso è difficile una discussione sulla cibersicurezza nell'utilizzo di soluzioni cloud. Ciò è evidente in molti progetti, per esempio quando occorre decidere se impiegare servizi cloud oppure quando si deve migliorare la sicurezza di soluzioni cloud già in uso.

Il presente documento intende fornire ai responsabili e decisori informatici di aziende, autorità o istituti di formazione le basi necessarie per migliorare questa situazione. A tal fine, nel primo capitolo la valutazione tecnologica spiega concretamente cosa s'intende con il termine «cloud», illustra le ragioni per cui le varie soluzioni cloud possono essere molto diverse tra loro e descrive le sfide che l'utilizzo di soluzioni cloud comporta dal punto di vista della sicurezza informatica. Il capitolo mostra anche che il cloud computing non è un nuovo paradigma, ma un modo per realizzare un outsourcing informatico.

Il secondo capitolo si riallaccia a questi temi e illustra una procedura concreta con cui i decisori possono valutare e selezionare i fornitori (di servizi cloud).

Il presente documento non ha l'obiettivo di presentare architetture di soluzione concrete per la cibersicurezza basate su servizi cloud. Questa fase avrà luogo nel quadro della pianificazione e dello sviluppo dei sistemi, in un secondo momento rispetto alla decisione di utilizzare un servizio cloud o di acquistare una soluzione cloud.

1.1 Storia

La storia del cloud computing è affascinante e inizia molto prima di quanto si pensi. Già negli anni Cinquanta IBM sviluppò le prime idee per la distribuzione di dati e attività tra diverse unità di calcolo. Negli anni Sessanta John McCarthy, un pioniere dell'informatica, propose che la potenza di calcolo e le applicazioni potessero essere fornite come infrastrutture di servizio pubbliche. Questi primi concetti gettarono le basi per quello che oggi conosciamo come cloud computing.

Negli anni Settanta, Intel immise sul mercato i primi microprocessori, rendendo possibile lo sviluppo dei personal computer. Gli anni Ottanta videro l'introduzione dei personal computer e lo sviluppo del sistema client-server, che permise alle aziende di fornire ai propri utenti prestazioni informatiche tramite reti interne. Con la diffusione di Internet negli anni Novanta, aziende quali Amazon e Google iniziarono a gettare le basi dei moderni servizi cloud. L'espressione «cloud computing» è entrata nell'uso comune negli anni Duemila, quando Amazon Web Services (AWS) nel 2006 iniziò a offrire risorse informatiche scalabili tramite Internet. Negli anni Dieci del nostro secolo, i servizi cloud hanno continuato a evolversi e diversificarsi e sono entrate sul mercato aziende quali Microsoft, Google e IBM.

Con la crescente popolarità del cloud computing sono aumentate anche le riflessioni sulla sicurezza. Non avendo più il pieno controllo dell'infrastruttura, le aziende hanno iniziato a preoccuparsi per la sicurezza dei loro dati archiviati nei servizi cloud. Inoltre si sono intensificate le riflessioni sull'osservanza di requisiti normativi nell'ambito della protezione dei dati.

Negli anni Dieci sono state introdotte sul mercato numerose soluzioni per la sicurezza del cloud, con funzioni quali la crittografia dei dati, il controllo degli accessi e il monitoraggio, volte a rafforzare la fiducia nel cloud computing.

1.2 Cloud computing

Negli ultimi anni il significato di «cloud» o «cloud computing» è diventato sempre più ampio e oggi è piuttosto vago. A questo sviluppo ha contribuito anche l'uso del termine a scopi pubblicitari. Per poter parlare di cibersicurezza nel cloud, occorre innanzitutto definire cosa si intende per «cloud»; solo in seguito sarà possibile condurre una discussione sensata e mirata sulla sua cibersicurezza. Inoltre, la discussione sulla sicurezza dev'essere condotta in funzione dei servizi cloud scelti. A tal fine, le sezioni seguenti descrivono le caratteristiche dei servizi cloud, il tipo di prestazioni offerte e i modelli di servizio e di fornitura. Non si tratta di concetti nuovi o sconosciuti, ma le definizioni note sono in parte imprecise e lasciano troppo spazio all'interpretazione.

Qualsiasi tipo di servizio cloud implica che il cliente ceda almeno in parte il controllo fisico dei propri dati e dei propri servizi a terzi. I fornitori di cloud (o «provider di servizi cloud»), quindi, intrattengono sempre un rapporto di fornitura con i propri clienti.

Per evitare fraintendimenti, nella presente valutazione tecnologica non verranno utilizzate espressioni quali «nel cloud» o «passaggio al cloud». Verranno invece utilizzati i seguenti concetti:

- **fornitore di cloud (o provider di servizi cloud)**: ditta che offre (e gestisce) servizi o offerte cloud;
- **servizi, soluzioni o offerte cloud**: soluzioni che soddisfano le caratteristiche di cloud (cfr. 1.2.1);
- **cloud computing**: termine generico che indica tutti i servizi e le offerte cloud.

1.2.1 Caratteristiche fondamentali

Il cloud computing è un modello che consente l'accesso a risorse e servizi informatici attraverso una rete. Invece di acquistare ed effettuare la manutenzione di hardware e software propri, le organizzazioni e i singoli individui possono noleggiare tali risorse da un fornitore di cloud e utilizzarle in base alle proprie esigenze.

Le cinque caratteristiche fondamentali di seguito riportate sono tratte dalla «Definition of Cloud Computing» [1] del National Institute of Standards and Technology (NIST) e sono generalmente riconosciute e accettate.

- **Accesso su richiesta (on demand)**: gli utenti possono accedere ai servizi cloud necessari in qualsiasi momento (preferibilmente tramite un portale self-service o un'interfaccia di programmazione) senza la necessità di un intervento manuale da parte del fornitore di cloud[1].
- **Pooling di risorse**: le risorse del fornitore in termini di rete, archiviazione o processore vengono raggruppate e assegnate a più utenti, consentendo un utilizzo efficiente di tali risorse.

[1] In aziende di grandi dimensioni e nell'Amministrazione federale, la caratteristica «accesso on demand» non è sempre utilizzabile se si tratta di primi acquisti. Nonostante il fornitore di cloud disponga di un portale self-service per l'acquisto dei servizi cloud, i processi di acquisto non sempre ne consentono l'utilizzo.

- **Rapida scalabilità**: le risorse sono scalabili in modo rapido, automatizzato e secondo le necessità per rispondere alle mutate esigenze.
- **Misurabilità**: l'utilizzo delle risorse viene costantemente monitorato e misurato, consentendo un conteggio e un'ottimizzazione trasparenti.
- **Accesso tramite Internet**: l'accesso di gestione all'account cloud è effettuabile tramite Internet[2] .In questo contesto si distingue tra ambiente di gestione (la rete attraverso la quale vengono gestiti e amministrati i servizi) e ambiente di sistema (l'ambiente in cui funzionano i sistemi (server) e vengono memorizzati i dati). L'ambiente di sistema non deve essere necessariamente accessibile tramite Internet.

Figura1: Diagramma del caso d'uso: ambiente di gestione e di sistema nei servizi cloud

Una prestazione cloud pubblica è considerata tale solo se il fornitore soddisfa (almeno) queste cinque caratteristiche[3].

1.2.2 Servizi

I servizi cloud si differenziano in base alle prestazioni offerte, che naturalmente possono anche essere combinate tra loro:

1. archiviazione dati: la prestazione consiste principalmente nella conservazione di dati;
2. potenza di calcolo: viene fornita principalmente capacità di calcolo;
3. rete: si tratta principalmente di mettere a disposizione i dati su Internet in modo efficiente (accesso rapido ai dati indipendentemente dalla località geografica).

1.2.3 Modelli di servizio

Nel cloud computing esistono diversi modelli di servizio che offrono al cliente un margine di manovra più o meno ampio nell'utilizzo delle prestazioni e che comportano anche aspettative diverse per quanto riguarda la responsabilità del fornitore di cloud e del cliente. I tre principali modelli di servizio sono:

- **infrastruttura distribuita come servizio (infrastructure as a service, IaaS)**: il fornitore di cloud offre risorse informatiche di base quali potenza di calcolo, memoria e reti. I clienti possono configurare personalmente reti, server e risorse di archiviazione virtualizzati. Nel caso dell'IaaS, le infrastrutture vengono gestite da terzi su base contrattuale, mentre i clienti sono competenti per la gestione dei server, delle banche dati, delle applicazioni e di altri servizi;

[2] La definizione data dal NIST fa solo riferimento al «broad network access» e non menziona l'accesso di gestione. Nei servizi cloud tuttavia è proprio l'accesso di gestione a essere effettuabile tramite Internet. È il/la cliente a decidere se le risorse virtuali messe a disposizione dal fornitore di cloud sono disponibili o meno anche tramite Internet. Per maggiori informazioni cfr. il capitolo 1.2.4.

[3] Un'altra caratteristica spesso associata ai servizi cloud è l'utilizzo di metodi moderni nello sviluppo e nella gestione nonché l'automazione delle fasi di lavoro. Questa caratteristica tuttavia non è rilevante solo nei servizi cloud, ma contraddistingue un modo di lavorare moderno rispetto a uno classico.

- **piattaforma distribuita come servizio (platform as a service, PaaS)**: il fornitore di cloud mette a disposizione una piattaforma su cui possono essere sviluppate, distribuite e gestite applicazioni. Nel caso del PaaS, le piattaforme vengono gestite da terzi su base contrattuale, mentre i clienti sono competenti per l'esercizio delle applicazioni;
- **software distribuito come servizio (software as a service, SaaS)**: il fornitore di cloud offre l'accesso ad applicazioni software tramite Internet, senza che queste debbano essere installate localmente. Nel caso del SaaS, quindi, soluzioni software vengono gestite da terzi su base contrattuale.

Esistono anche combinazioni dei diversi modelli: M365, per esempio, da un lato mette a disposizione le note applicazioni Office (come soluzione SaaS), dall'altro offre anche la piattaforma per l'amministrazione, l'autenticazione o la fornitura e lo sviluppo di applicazioni proprie (PowerTools).

Sebbene il SaaS venga considerato nel contesto del cloud computing, per l'organizzazione che acquista una soluzione SaaS questo aspetto è meno rilevante nelle riflessioni sulla cibersicurezza e sulla resilienza. I clienti non devono occuparsi delle tecnologie (cloud) in sé, ma solo di questioni relative alla gestione dei fornitori informatici e all'outsourcing informatico[4].

1.2.4 Modelli di distribuzione

I servizi cloud sono inoltre suddivisi nei tre modelli di distribuzione seguenti.

- **Cloud pubblico (public cloud)**: l'accesso all'ambiente di gestione per l'amministrazione dei servizi cloud è distribuito tramite la rete Internet pubblica. L'infrastruttura viene condivisa da più clienti (tenant); ogni cliente può utilizzare ed elaborare i propri dati nonché decidere a chi renderli accessibili. L'ambiente di sistema è accessibile al pubblico solo se il cliente lo prevede.
- **Cloud privato (private cloud)**: i servizi cloud sono forniti a un gruppo chiuso di organizzazioni e offrono un maggiore controllo, solitamente garantito dal fatto che i servizi per l'organizzazione vengono eseguiti su un hardware dedicato. Quest'ultimo può essere situato nei propri locali («on premises» / «on prem») oppure presso il fornitore di servizi cloud. In linea di principio l'ambiente di gestione non è accessibile tramite Internet[5]. Se l'hardware si trova presso il fornitore di cloud, l'accesso all'ambiente di gestione è garantito tramite un canale[6] sicuro.
- **Cloud ibrido (hybrid cloud)**: un cloud ibrido è una combinazione di cloud pubblico e cloud privato, per sfruttare i vantaggi di entrambi i modelli. Tale combinazione si riferisce all'intera struttura di un'organizzazione, quindi un determinato server può funzionare in un ambiente privato e un altro in un ambiente pubblico.

[4] Naturalmente ciò include anche le questioni riguardanti come mettere in sicurezza i dati e come continuare a svolgere i processi in caso di interruzione della fornitura da parte del fornitore.

[5] Mentre l'espressione «cloud pubblico» è definita in modo relativamente chiaro e viene generalmente compresa correttamente, lo stesso non si può dire per «cloud privato». Con questa espressione molti fornitori intendono semplicemente un ambiente che viene gestito sui loro server anziché ricorrere ai servizi di un grande fornitore quale Amazon, Google o Microsoft. Questo modo di intendere il cloud privato non è utile. Secondo l'Ufficio federale della cibersicurezza (UFCS), si può parlare di cloud privato solo se l'accesso di gestione è limitato.

[6] Si può pensare a CDN, peering diretto, SD-WAN, VPN, nonché restrizioni di accesso esplicitamente forzate (spesso denominate accesso condizionale) e altre tecnologie simili.

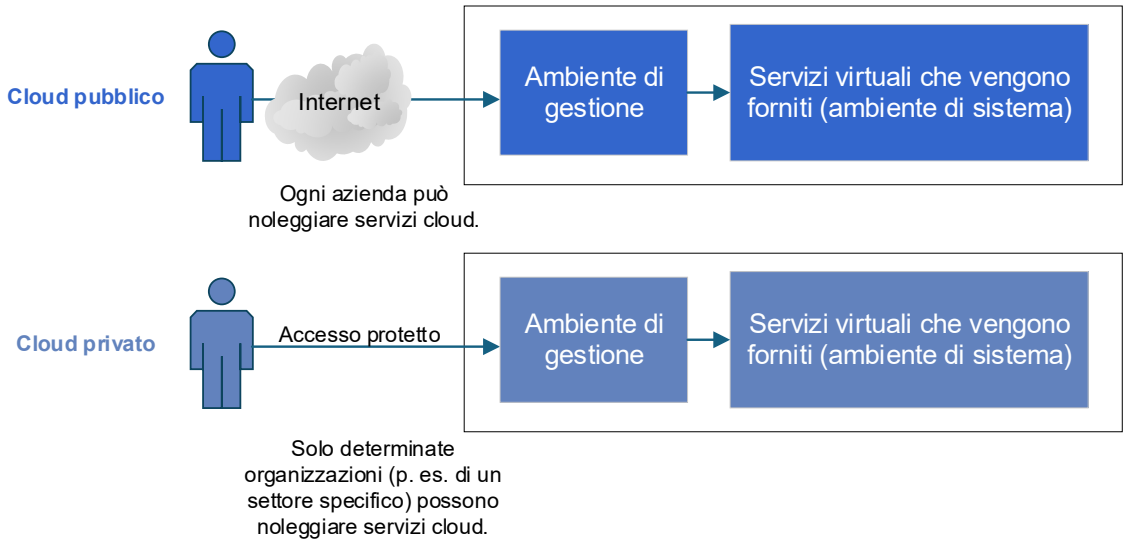

Figura2: Differenza tra cloud pubblico e privato dal punto di vista tecnico secondo l'Ufficio federale della cibersicurezza.

Non è sempre possibile giudicare con chiarezza se l'ambiente utilizzato sia pubblico o privato, poiché sono possibili anche forme miste. Per questo i modelli di distribuzione hanno solo un ruolo secondario nel valutare se una soluzione cloud è quella giusta. Ai fini della cibersicurezza è importante ridurre la superficie d'attacco, che in un ambiente privato è già notevolmente ridotta.

1.2.5 I cloud non sono tutti uguali

Da quanto descritto negli ultimi paragrafi risulta evidente che i cloud non sono tutti uguali. La tabella seguente lo dimostra con esempi concreti. La decisione di acquistare tali prestazioni da un fornitore di cloud dev'essere presa nel contesto delle applicazioni previste. Non si tratta quindi di prendere una decisione binaria a favore o contro un servizio cloud, ma piuttosto di valutare se, nell'architettura finale, quello specifico servizio cloud sia la scelta giusta per il progetto o l'organizzazione[7].

Modelli di servizio	**Prestazioni**	**Modello di distribuzione**	**Esempio**
Infrastructure as a service (IaaS)	Archiviazione dati	Cloud pubblico	Soluzioni di archiviazione online configurabili quali Amazon S3, Google Bucket o Azure Blob
	Archiviazione dati	Cloud privato	Soluzioni di archiviazione on prem configurabili e scalabili quali NetAPP SAN
	Potenza di calcolo	Cloud pubblico	Server virtuali quali Amazon EC2, Azure VM o Google Compute Engine
	Rete	Cloud pubblico	Soluzioni di rete quali AWS NAT Gateway, Azure WAF, Google Cloud Firewall
Platform as a service (PaaS)	Potenza di calcolo	Cloud pubblico	Servizi Kubernetes quali Amazon EKS, Azure AKS, Google GKS o anche servizi serverless quali AWS Lambda o Azure Functions
	Rete	Cloud pubblico	Servizi di rete minimamente configurabili come Google Cloud Armor quale

[7] Questa prospettiva permette di chiarire il concetto di cloud come cambio di paradigma per i servizi informatici.

			protezione DDoS.
	Tutte	Cloud pubblico	Piattaforme per lo sviluppo di applicazioni e piattaforme operative quali Microsoft PowerTools o Google AppSheet.
Software as a service (SaaS)	Potenza di calcolo	Cloud pubblico	Grid computing, o anche il servizio di calcolo quantistico AWS.
	Archiviazione dati	Cloud pubblico	Spazio di archiviazione online come Dropbox, Google Drive o Microsoft OneDrive
	Tutte	Cloud pubblico	Applicazioni quali Microsoft M365, SAP S/4HANA, ChatGPT, Deepl o Miro.

Tabella 1: Esempi di vari servizi cloud.

1.3 Cibersicurezza nell'utilizzo di servizi cloud

Oltre al fatto che ogni utilizzo di servizi cloud è una questione di gestione dei fornitori, altre sfide fondamentali derivano dalle caratteristiche e dai modelli di servizio e distribuzione:

- nel caso dei servizi cloud, i dati non sono sotto il controllo esclusivo dell'organizzazione. In caso di problemi con la connessione di rete o con il fornitore di servizi, può verificarsi una perdita temporanea o, nel peggiore dei casi, definitiva dell'accesso alle informazioni e ai servizi.
- Per la protezione crittografica dei dati archiviati e trasmessi tra i clienti e il fornitore di cloud oggi esistono soluzioni. La grande sfida tuttavia è rappresentata dalla protezione crittografica dei dati in elaborazione (cioè che si trovano nel processore). Questo è un tema di ricerca attivo (p. es. «crittografia completamente omomorfica», per cui si cercano soluzioni che consentano di elaborare dati crittografati senza prima decrittografarli). Dal momento che non è ancora disponibile una soluzione adeguata, si sta cercando di ottenere qualcosa di simile con un apposito hardware (confidential computing).
- Un altro tema importante è la gestione delle chiavi (o «key management»), dal momento che il servizio cloud esegue la decrittografia e quindi gestisce anche le chiavi stesse. Le soluzioni in cui la crittografia e la decrittografia avvengono sul client[8] sono rare. Questo fatto, unito al pooling delle risorse, implica che un aggressore che ottiene l'accesso all'infrastruttura crittografica[9] può accedere ai dati di molti clienti.
- Nelle architetture di rete tradizionali, l'area di gestione viene isolata in modo che l'accesso sia possibile solo attraverso accessi, reti o terminali protetti. Se si utilizzano servizi di cloud pubblico, in caso di perdita dei dati di accesso (p. es. una chiave API), di configurazione errata degli accessi o di vulnerabilità nei servizi cloud normalmente l'accesso diventa possibile a tutti. In tal caso l'intera infrastruttura si trova immediatamente in pericolo e un'ulteriore sfida è data dal fatto che se utenti non autorizzati si trovassero nello stesso account cloud potrebbero anche cancellare o modificare la registrazione (logging) e il backup.
- Configurazioni errate possono causare, per esempio, la pubblicazione involontaria di un archivio cloud. Esse richiedono un monitoraggio e una reattività che sono meno essenziali in altre soluzioni non esposte a Internet. In linea di massima, nel caso dei

[8] Tali soluzioni vengono anche denominate «hold your own key» o HYOK.

[9] A titolo di esempio, l'attacco di Storm0588 all'ambiente Microsoft: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

servizi cloud, questo monitoraggio (spesso denominato anche «osservabilità») è più complesso e impegnativo.

- I costi, anche se non sono direttamente rilevanti per la sicurezza, sono comunque importanti. Le soluzioni di sicurezza nel cloud comportano costi aggiuntivi che spesso crescono linearmente con il numero di utenti. Nelle organizzazioni di grandi dimensioni, di conseguenza, i servizi cloud possono essere più costosi rispetto alla creazione di un'infrastruttura propria. Un altro aspetto da considerare riguarda soprattutto le piccole imprese: in caso di budget limitato, quando si acquistano servizi cloud, si tende a rinunciare a soluzioni di sicurezza aggiuntive ma necessarie.

2 Considerazioni sulla cibersicurezza nell'utilizzo di servizi cloud

Poiché l'utilizzo del cloud computing generalmente comporta l'outsourcing dei servizi informatici, è necessario valutare e selezionare opportunamente i fornitori. La scelta giusta di fornitori, subfornitori e provider è un presupposto importante per garantire un esercizio sicuro. Questa decisione rappresenta la prima fase dell'attuazione. La seconda fase include la pianificazione del sistema, lo sviluppo e la messa in funzione della soluzione cloud. La terza fase prevede l'inserimento dei servizi cloud nella gestione continua dei fornitori dell'organizzazione[10].

Per il processo decisionale (prima fase) individuiamo tre tappe importanti, che esamineremo più nel dettaglio nei paragrafi seguenti:

1. verificare se i requisiti legali relativi al fornitore di cloud sono soddisfatti (cfr. cap. 2.1);
2. verificare se i requisiti tecnici e organizzativi per un funzionamento sicuro e resiliente possano essere soddisfatti (cfr. cap. 2.2);
3. valutare se l'utilizzo dei servizi cloud è la scelta giusta sulla base della soddisfacibilità di tali requisiti e di criteri importanti quali la disponibilità temporale, le conseguenze in caso di perdita dei dati o le capacità informatiche delle proprie organizzazioni (cfr. domande guida nel cap. 2.3).

2.1 Requisiti legali

I requisiti legali dipendono dalla natura giuridica e dalla sede del fornitore di cloud nonché dal tipo di dati trattati. Occorrerebbe verificare i seguenti requisiti e, a seconda dell'organizzazione, è necessario tenere conto anche di altri requisiti o direttive specifici del settore.

1. Se l'organizzazione trasmette dati a un fornitore di cloud e gli consente di elaborarli e/o archiviarli, è necessario un **contratto** tra le parti che disciplini i diritti e gli obblighi reciproci[11]. L'organizzazione deve verificare se eventuali interessi di mantenimento del segreto legali o contrattuali, quali il segreto professionale o il segreto d'ufficio, si oppongano alla conclusione del contratto. In tal caso occorre garantire che il fornitore di cloud sia in grado di adempiere a tali obblighi (previa «due diligence»). Gli obblighi del fornitore prevedono che l'accesso ai sistemi da parte dei collaboratori sia rigorosamente disciplinato e controllato. Inoltre, in caso di trattamento di dati soggetti al segreto d'ufficio o al segreto professionale, solo ausiliari espressamente autorizzati possono ottenere l'accesso a tali dati[12].
2. Se i dati personali di persone fisiche vengono trasmessi al fornitore di cloud e da quest'ultimo elaborati e/o archiviati, è necessario concludere tra le parti un cosiddetto

[10] Cfr. anche: Cibersicurezza nella catena di fornitura, Ufficio federale della cibersicurezza UFCS (2024) [2].

[11] Cfr. anche: Contratti con fornitori: Best Practice in [2].

[12] Art. 320 e art. 321 del Codice penale svizzero (CP)

contratto di affidamento del trattamento a un responsabile del trattamento (**«data processing agreement»)**. Secondo la legislazione in materia di protezione dei dati, l'organizzazione deve adempiere gli obblighi del titolare del trattamento (il privato o l'organizzazione che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento) e il fornitore di cloud quelli del responsabile del trattamento (il privato o l'organizzazione che tratta dati personali per conto del titolare del trattamento). Il trattamento dei dati da parte del fornitore di cloud, in qualità di responsabile del trattamento, è consentito solo se questo effettua soltanto i trattamenti che il titolare del trattamento avrebbe il diritto di effettuare e se nessun obbligo legale o contrattuale di serbare il segreto lo vieta. Le organizzazioni devono in particolare assicurare che il fornitore di cloud sia in grado di garantire la sicurezza dei dati.

3. Se il trattamento dei dati personali comporta un rischio elevato per la personalità o i diritti fondamentali delle persone fisiche interessate, l'organizzazione deve verificare se occorre previamente effettuare una **valutazione d'impatto sulla protezione dei dati**, secondo i requisiti della legislazione in materia di protezione dei dati applicabile.
4. I dati personali possono essere trasmessi a un fornitore di cloud all'**estero** soltanto se è comprovato che il Paese destinatario[13] garantisce una protezione adeguata dei dati. In caso contrario, la trasmissione può essere effettuata comunque qualora una protezione dei dati appropriata sia garantita da un trattato internazionale, da speciali clausole contrattuali, da garanzie specifiche di un organo federale, da clausole tipo di protezione dei dati previamente approvate dall'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) oppure da norme interne dell'organizzazione vincolanti sulla protezione dei dati.

2.2 Requisiti tecnici e organizzativi

I clienti di servizi cloud devono da un lato prevedere misure da adottare nel caso in cui il servizio cloud non sia più disponibile (punto A) e dall'altro poter contare sul fatto che i fornitori attuino le misure tecniche e organizzative concordate. Per creare la fiducia necessaria, occorre trasparenza da parte dei fornitori (punti da B a E). Tutti i requisiti sono descritti in modo tale che il o la cliente possa verificarli autonomamente, senza doversi affidare ciecamente alle promesse del fornitore di cloud.

A. **Pianificazione di emergenza e backup offline:** nell'ambito della pianificazione delle misure d'emergenza i dati nella soluzione cloud devono poter essere esportati e archiviati. Un backup dell'esportazione dovrebbe essere salvato anche offline (per proteggersi dai ransomware). Inoltre sarebbe opportuno definire una strategia di uscita per garantire che sia possibile cambiare fornitore in qualsiasi momento senza subire alcuna perdita di dati[14].
B. **Trasparenza delle funzioni di sicurezza:** l'adempimento dei requisiti di sicurezza fondamentali per la garanzia della sicurezza dei dati da parte del fornitore deve essere documentato in modo trasparente per l'organizzazione. Tali requisiti fondamentali includono quanto segue:
    1. la trasmissione dei dati tra l'organizzazione e il fornitore di cloud deve avvenire sempre in forma cifrata (mediante protocolli di crittografia aggiornati come l'attuale versione di TLS oppure tramite una VPN o una SD WAN crittografata);
    2. il fornitore di cloud dispone di funzioni per il controllo degli accessi secondo il principio «need-to-know» e ogni richiesta di accesso avviene tramite autenticazione. Di default per l'autenticazione si devono utilizzare più fattori

[13] Cfr. anche l'elenco dei Paesi https://www.fedlex.admin.ch/eli/cc/2022/568/it#annex_1/lvl_u1

[14] Per esempio, si potrebbe già pianificare il passaggio a un altro fornitore in caso di emergenza, ma effettuarlo solo se necessario.

(MFA) e l'assegnazione di accessi a collaboratori, partner, fornitori o clienti dell'organizzazione deve essere semplice e chiara[15].

3. L'accesso di gestione ai servizi cloud e l'accesso alle applicazioni cloud è monitorato e protetto da attacchi *denial of service* (sovraccarico dell'applicazione tramite numerose richieste) o da tentativi di accesso mediante attacco di forza bruta (tentativo di provare molte combinazioni di login in rapida successione).
4. La gestione delle chiavi è documentata e corrisponde ai più moderni standard tecnici.
5. Poiché le configurazioni errate possono facilmente condurre a un'esposizione dei dati su Internet, è necessario disporre di un servizio che le rilevi, generi un allarme e, se possibile, le corregga automaticamente.

C. **Trasparenza degli accessi**: esiste una funzione che consente agli amministratori dell'organizzazione di monitorare e tracciare tutti gli accessi ai dati e le relative modifiche, inclusi gli accessi di fornitori e partner del fornitore di cloud. Gli accessi e le modifiche devono poter essere registrati e dovrebbero anche essere inclusi nei backup offline, in modo tale che una compromissione del fornitore di cloud non pregiudichi la tracciabilità.

D. **Sicurezza dei prodotti**: il fornitore di cloud illustra in modo trasparente i metodi utilizzati per sviluppare in modo sicuro i propri servizi cloud.

E. **Segnalazione di incidenti e vulnerabilità**: il fornitore di cloud dispone di una procedura che garantisce che gli incidenti e le vulnerabilità rilevanti per l'organizzazione vengano segnalati rapidamente all'organizzazione. Pubblica patch e modifiche ai propri servizi e dispone di un centro di segnalazione per incidenti e vulnerabilità rilevanti sotto il profilo della sicurezza[16].

2.3 Domande orientative per la valutazione dell'impiego di servizi cloud

Le risposte alle seguenti domande devono, da un lato, servire da base decisionale per l'utilizzo di servizi cloud e, dall'altro, riportare i possibili rischi che devono essere adeguatamente trattati. Le architetture dettagliate delle soluzioni da attuare a seguito di questa decisione non rientrano nell'ambito della presente valutazione.

Domanda 1 - *Requisiti*: i requisiti legali, organizzativi o tecnici (cap. 2.1 e cap. 2.2) possono essere soddisfatti?

Se i requisiti legali non possono essere soddisfatti, si deve rinunciare all'impiego della soluzione cloud.

Se i requisiti tecnici e organizzativi non possono essere soddisfatti, per esempio perché i dati non sono esportabili (e quindi non è possibile preparare un proprio piano di emergenza), o perché il fornitore di cloud non offre le funzioni di sicurezza minime necessarie oppure non è trasparente nella documentazione della sicurezza, è necessario essere cauti. Occorre valutare accuratamente i rischi connessi. In questo caso mancano i presupposti per riporre fiducia nel fornitore. In particolare per quanto riguarda il trattamento dei dati personali, in un caso simile non possono più essere soddisfatti i requisiti in materia di sicurezza dei dati.

Se nessuna delle soluzioni cloud esaminate soddisfa i requisiti, occorre privilegiare una soluzione gestita autonomamente (on premise o ospitata sotto il proprio controllo).

Domanda 2 - *Disponibilità in termini di tempo*: la soluzione cloud è urgente per il mantenimento dei processi aziendali?

[15] Se la gestione delle autorizzazioni è complicata, è facile commettere errori. È quindi necessario disporre di una soluzione o di un'interfaccia chiara e semplice.

[16] Tale segnalazione può avvenire tramite un file security.txt disponibile in Internet conformemente alla RFC 9116.

Questa domanda è importante, perché una caratteristica fondamentale dei servizi cloud è che l'accesso dipende dalla disponibilità di Internet. Per esempio se si offre un sistema informativo dei pazienti tramite Internet che dovrebbe essere disponibile senza interruzioni, devono essere presenti alternative in caso di guasto dell'infrastruttura cloud. Inoltre è necessario garantire la disponibilità permanente della connessione Internet.

Domanda 3 - *Perdita di dati*: quanto sono gravi le conseguenze di una perdita di dati per le persone interessate?

Se un'eventuale perdita dei dati fosse grave per l'organizzazione stessa o per le persone di cui vengono trattati i dati nel sistema (p. es. nel caso di atti giudiziari), deve essere possibile effettuare un backup offline dei dati all'interno dell'organizzazione stessa.

Se un accesso non autorizzato o la pubblicazione di tali dati (violazione della confidenzialità) comportassero gravi conseguenze, l'impiego di soluzioni cloud non è consigliabile, poiché rimarrebbero incertezze su chi può effettivamente accedere ai dati. Se si prevede comunque l'utilizzo di servizi cloud, i dati dovrebbero essere fortemente protetti mediante crittografia e tale minaccia dovrebbe essere segnalata in fase di progettazione e sviluppo del sistema.

Domanda 4 - *Capacità dell'organizzazione informatica*: la nostra organizzazione è in grado di attuare le necessarie misure di protezione?

Se le capacità dell'organizzazione sono limitate, un outsourcing presso un fornitore di cloud è molto rischioso. L'impiego di soluzioni cloud, in particolare nel caso dei modelli di servizio infrastructure as a service, richiede una maggiore maturità dei propri sistemi informatici, poiché il monitoraggio e l'esercizio di queste soluzioni comportano un'ulteriore complessità rispetto alla gestione autonoma. Nel caso di soluzione SaaS, invece, è fondamentale la capacità di pianificazione delle misure d'emergenza in caso di guasto del fornitore. La pianificazione delle misure d'emergenza potrebbe anche essere affidata a un altro partner di outsourcing informatico. Questa opzione tuttavia comporterebbe un aumento dei costi e dell'onere legato alla gestione dei fornitori, pertanto andrebbe ponderata attentamente tenendo conto dei vantaggi.

3 Fonti bibliografiche

[1] Mell, P.; Grance, T. *The NIST Definition of Cloud Computing - NIST SP 800-145* National Institute of Standards and Technology (2011), visitato il 2 maggio 2025, https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] *Cibersicurezza nella catena di fornitura* Ufficio federale della cibersicurezza UFCS (2024), visitato il 2 maggio 2025, https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html