



LA SICUREZZA DEI DATI SUL CLOUD SEEWEB

**I dati sul Cloud:
come sono gestiti e preservati,
a chi sono accessibili**



Indice

1. Premessa
2. Sicurezza dei dati: non facciamo confusione
3. Sicurezza logica e indicazioni pratiche
4. Sicurezza fisica e misure Seeweb
5. Conclusioni
6. Informazioni di contatto



1. Premessa

La sicurezza dei propri dati è un argomento di grande dibattito da sempre, in particolare da quando il Cloud Computing ha iniziato a diffondersi come tecnologia all'interno delle aziende. Infatti, quando si parla di tecnologia cloud, "sia *private* che *public*, nell'immaginario collettivo subentra il concetto di *perdita di controllo* sul dato.

Ciò è vero principalmente dal punto di vista *percettivo* in quanto il dato è nel cloud e non nel dispositivo fisico e visibile. In realtà, la maggiore attenzione al tema in ambito cloud finisce per gestire meglio di quanto si faccia tipicamente nell'approccio *on premise* le problematiche di sicurezza" (cit. Antonio Baldassarra, CEO Seeweb in un intervento sul tema).

Al fine di fare chiarezza su come i dati nel Cloud vengano gestiti e protetti, in questo white paper abbiamo voluto fare un elenco delle domande più frequenti che i clienti ci pongono sul tema.

2. Sicurezza dei dati: non facciamo confusione

Quello della sicurezza è un ambito molto delicato e che non attiene a un unico soggetto. Nell'ambito di un contratto cloud, infatti, sono due le parti che si occupano, insieme, di contribuire a tutelare i dati: il fornitore e il cliente.

La sicurezza dei dati viene quindi garantita su più livelli, in particolare:

lato provider	con misure e strategie di sicurezza messe in atto con i servizi cloud offerti, le infrastrutture tecnologiche (data center), i programmi di monitoraggio e sorveglianza, i sistemi di backup proposti etc.
lato cliente	con misure e strategie di sicurezza adottate dal cliente nelle procedure quotidiane di gestione e diffusione dati all'interno della sua azienda e dal punto di vista applicativo.

Questa distinzione è molto importante perché stabilisce un confine tra quanto di pertinenza dell'operatore di servizi Cloud e quanto invece dell'utilizzatore dei servizi stessi.



3. Sicurezza logica e indicazioni pratiche

Come si pone Seeweb rispetto ai contenuti che il cliente pubblica e mantiene sul Cloud?

Seeweb come fornitore non ha contezza del tipo di dati che il cliente ospita sulle sue infrastrutture: il cliente è di fatto l'unico responsabile dei dati inseriti nel Cloud e ne determina la diffusione.

Seeweb non interviene quindi in nessun modo sui contenuti del cliente e non conosce quali dati il cliente immetta all'interno della sua rete.

Come si pone Seeweb rispetto all'accesso ai servizi che fornisce al cliente?

È sempre il cliente la persona deputata a controllare chi sia autorizzato ad accedere al suo account e a monitorare l'uso e la distribuzione dei dati di accesso alle sue piattaforme Cloud. Seeweb suggerisce di prestare particolare attenzione alla scelta del contatto tecnico da inserire nel contratto al momento della registrazione del proprio account cliente perché è il responsabile tecnico che, dopo l'ordine di un servizio Seeweb, riceverà la mail di attivazione contenente i dati di accesso.

Allo stesso modo, in caso di variazione del referente tecnico della propria azienda, sarà necessario aggiornare immediatamente il contatto tecnico all'interno dell'area clienti modificando contestualmente le password di accesso al server Seeweb.

C'è la possibilità che Seeweb autorizzi terzi ad accedere ai dati del cliente?

L'unico caso in cui Seeweb possa mettere un terzo in condizione di accedere al server che ospita i dati del cliente, è quello in cui ci sia espressa e formale richiesta da parte di organi quali per esempio la Polizia Giudiziaria a scopo di indagine informatica e accertamenti. Si badi che, per l'ordinamento Italiano, occorre un decreto firmato da un giudice per poter accedere ai dati conservati nel cloud; per fornitori soggetti ad altri regimi giuridici, per esempio per quelli statunitensi, le regole per accedere ai dati da parte del governo o delle agenzie di sicurezza sono molto più facili e non necessitano di un avallo da parte di un giudice.



4. Sicurezza fisica e misure seeweb

I dati nel Cloud sono meno tutelati rispetto alle soluzioni dedicate fisiche?

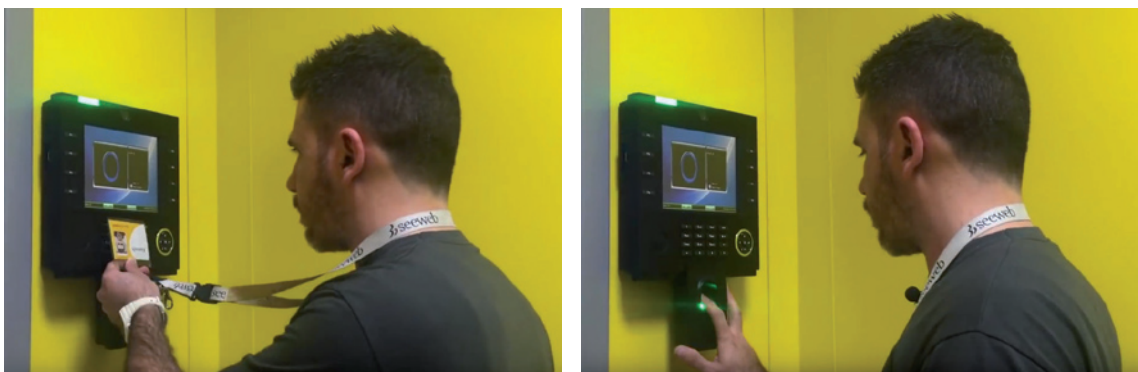
Nonostante i dubbi diffusi sulla sicurezza della nuvola e la “sensazione” che con il Cloud si perda il controllo dei dati, un Cloud provider che si doti di infrastrutture mirate a garantire la massima sicurezza fisica e i migliori programmi di sorveglianza e monitoraggio potrà garantire al cliente una tranquillità ancora maggiore che in scenari *on premise*.

Dove sono fisicamente i dati se si sceglie un servizio Seeweb?

I data center Seeweb si trovano in Italia, nelle sedi di Milano e Frosinone. Il cliente, se vuole, può scegliere in quale sede debba essere installato il suo server, semplicemente indicando, al momento dell’ordine (o dell’attivazione per i servizi volatili come *easy Cloud Server*), su quale dei data center disponibili attivare il servizio. In caso di scelta dell’opzione di backup, ad ogni modo, se il server verrà installato a Milano, per esempio, il backup dei dati, per garantire la massima sicurezza, verrà eseguito a Frosinone (*backup remoto*).

Come viene garantita la sicurezza fisica delle infrastrutture?

I dati dei clienti che utilizzano i nostri servizi vengono protetti, oltre che da misure logiche, da misure fisiche e legate alle infrastrutture di data center. In particolare, l’accesso ai data center Seeweb, riservato esclusivamente ai dipendenti Seeweb e a personale terzo opportunamente autorizzato, avviene unicamente a mezzo protetto da un sistema di riconoscimento a doppio fattore (Badge e impronta digitale).



Modalità di riconoscimento per l’accesso al data center



Accesso data center riservato ai Clienti

L'accesso all'area di data center è ulteriormente subordinato ad autorizzazione a mezzo SmartCard e Impronta Digitale in possesso del solo personale autorizzato alle attività di data center. Tutti gli accessi sono sottoposti a logging su sistema informatico, eventuali terzi che accedono unicamente accompagnati da personale interno vengono registrati previo accertamento dell'identità e verifica della motivazione/autorizzazione all'accesso.



Video sui sistemi di sicurezza per l'accesso al data center

https://www.youtube.com/watch?v=Dn1T_18nYf0

I locali vengono sorvegliati 365/7/24 con personale Seeweb o esterno autorizzato e con sistemi di monitoraggio remotizzato. Un sofisticato sistema di videosorveglianza perimetrale esterna e interna a mezzo telecamere con registrazione e ritenzione a norma di legge permette la rilevazione dei movimenti in aree critiche e la conseguente attivazione di circuito di allarme.

Nelle ore di minore frequentazione la sicurezza dei locali è garantita dalla presenza di una sorveglianza armata.

E' presente un sistema di rilevazione delle intrusioni per tutti i locali Seeweb con segnalazione di tipo ottico/acustico locale e remota a mezzo radio allarme verso istituto di vigilanza.



Anche il ruolo della sicurezza elettronica in Seeweb riveste particolare attenzione, a partire dalla scelta della sede del data center: al di sopra del piano campagna, con un tipo di percolazione in grado di proteggere da eventuali perdite di acqua degli impianti di refrigerazione. Particolare attenzione meritano anche i sistemi di alimentazione Seeweb, completamente ridondati, nonché i sistemi antincendio, di rilevazione fumi e del fuoco e di condizionamento.

Attraverso quale specifica certificazione Seeweb dimostra di avere implementato al massimo la sicurezza dei dati?

La certificazione attraverso la quale si verificano il ciclo di vita delle informazioni e le best practices atte a tutelare la riservatezza, l'integrità e la disponibilità dei dati è la ISO/IEC 27001, norma alla quale Seeweb è conforme.

La norma ISO 27001 ha l'obiettivo di proteggere le risorse informative da eventuali minacce e assicurare una corretta gestione dei dati sensibili dell'azienda. E', specificamente, la "Certificazione del sistema di gestione della sicurezza delle informazioni".

Essa si basa sull'analisi dei rischi e sul loro trattamento, verifica l'utilizzo di procedure e di strumenti ed eventuali non conformità, individua possibili azioni correttive e di prevenzione.

5. Conclusioni

In questo whitepaper abbiamo brevemente indicato quali sono le misure per una corretta e sicura gestione dei dati sul Cloud. Le indicazioni fornite permettono di concludere che scegliere soluzioni in Cloud anche *public* (con infrastrutture e piattaforme gestite dal provider e di proprietà del provider) non significa rinunciare a proteggere i propri dati; al contrario, gestire i dati su piattaforme proprietarie (server dedicati magari installati nel CED del cliente) può rappresentare un rischio serio senza un'opportuna ridondanza e senza i corretti criteri di utilizzo.

Il Cloud Computing ha offerto l'enorme vantaggio di rendere i dati accessibili e disponibili sempre e con estreme flessibilità e prestazioni per cui, se abbinato a policy di sicurezza adeguate e se affidato al giusto fornitore, è quanto di meglio si possa avere per essere sul web oggi.



6. Informazioni di contatto

Seeweb srl

Via Armando Vona 66

03100, Frosinone

Via Caldera, 21 - edificio B

20153 Milano

<https://www.seeweb.com>

info@seeweb.com

<https://www.facebook.com/seeweb.it>

<https://twitter.com/seeweblive>

Autrice White Paper:

Chiara Grande

chiara.g@seeweb.it



seeweb