La sicurezza dei dati sul Cloud Seeweb

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

seeweb
THINK CLOUD

01. 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.

02. 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.

03. 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.

Misure di sicurezza interne al data center

Cosa succede nel caso in cui un cliente cancelli un dato su un server Seeweb?

La conservazione e la tutela dei propri dati conservati nel Cloud è strettamente legata alla scelta di una soluzione di **backup**. In particolare, sulle piattaforme Cloud, Seeweb fornisce un backup di tipo IBM Spectrum Protect.

IBM Spectrum Protect effettua un primo processo di archiviazione su server esterno di tutti i dati fisici (file e cartelle) presenti sulla propria istanza Cloud e, in seguito alla prima esecuzione del backup, effettua periodicamente la **copia incrementale** dei dati, a seconda del piano scelto (settimanale o giornaliero). Fin quando non verrà eliminato dal proprio disco il file/directory, tale copia rimarrà per sempre registrata sul sistema di backup. Il dato viene infatti

definitivamente cancellato *solo dopo 60 giorni dalla sua eliminazione dal server*.

Se invece verrà effettuata una modifica al file, alla successiva esecuzione del backup l' IBM Spectrum Protect archivierà la versione più' vecchia del file come "copia inattiva" e la versione attuale come "copia attiva". In caso di necessità, tramite IBM Spectrum Protect è possibile effettuare restore dei dati in autonomia oppure richiederli a mezzo ticket di assistenza.

Cosa succede ai dati quando il cliente revoca un servizio Seeweb?

Quando un cliente revoca un servizio dall'apposito portale, il servizio stesso viene messo in disdetta (la comunicazione di disdetta va fatta con un preavviso di 15 giorni rispetto alla data di rinnovo).

Rispetto alla data di scadenza, il server rimarrà attivo e quindi accessibile per almeno 15 giorni. A fine mese, il server verrà cancellato insieme a tutti i suoi contenuti. La policy indicata vale per alcune classi di servizio, come per esempio il Cloud Server, per altri come l'easy Cloud Server la cancellazione di server e dati correlati è immediata a seguito della richiesta del cliente.

04. 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?

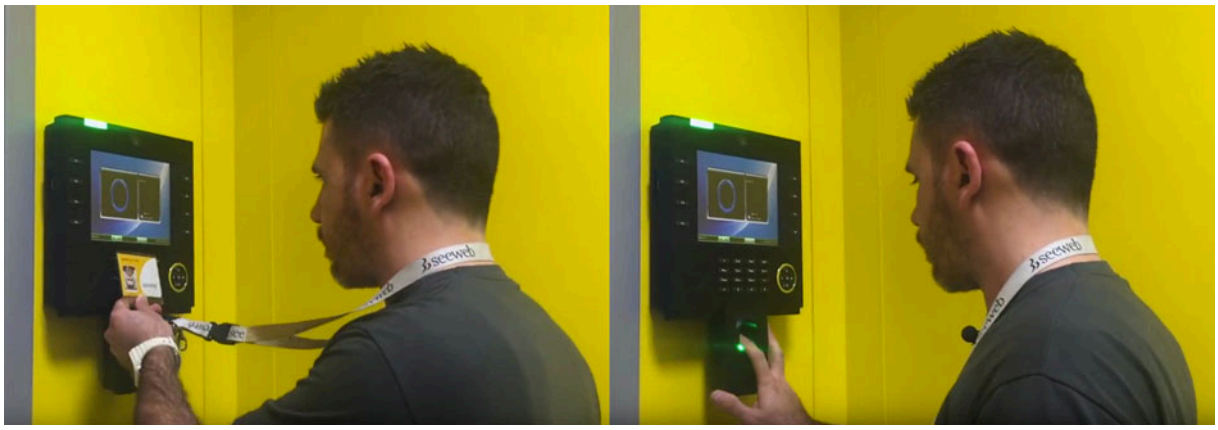
I datacenter Seeweb si trovano a Frosinone, Milano, Sesto San Giovanni, Lugano e Zurigo. Il cliente, se vuole, può scegliere in quale sede debba essere installato il suo server, semplicemente indicando, al momento dell'ordine (o dell'attivazione per i servizi volatili come *easy Cloud Server*), su quale 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?

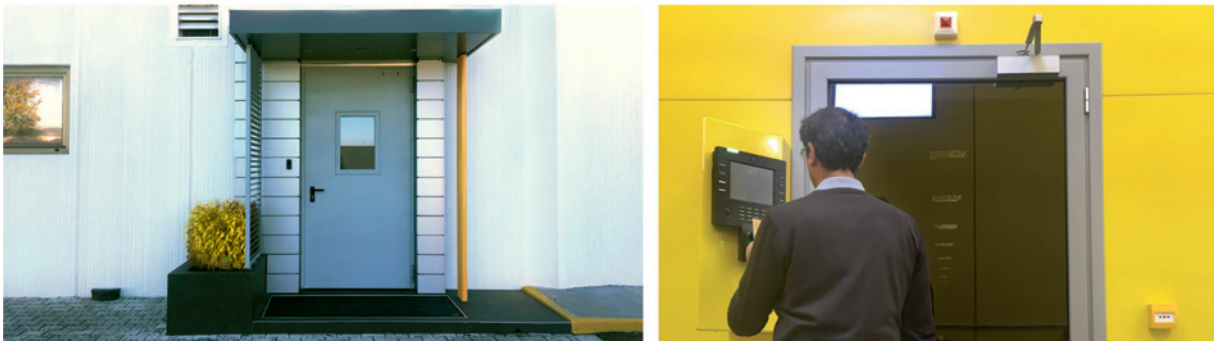
I dati dei clienti che utilizzano i nostri servizi vengono protetti, oltre che da misure logiche, da misure fisiche e legate alle infrastrutture di data center.In particolare, l'accesso ai data center Seeweb, riservato esclusivamente ai dipendenti Seeweb e a personale terzo opportunamente

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

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.



Accesso data center riservato ai Clienti

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.

Video sui sistemi di sicurezza
per l'accesso al data center
https://www.youtube.com/watch?v=Dn1T_18nYf0

La **sicurezza infrastrutturale** 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 menzione meritano i **sistemi di alimentazione** Seeweb, completamente ridondati, nonché i sistemi antincendio, di rilevazione fumi e del fuoco e di condizionamento.

Attraverso quali certificazioni Seeweb dimostra di avere implementato al massimo la sicurezza dei dati?

Le certificazioni attraverso le quali Seeweb dimostra di tutelare la riservatezza, l'integrità e la disponibilità dei dati sono:

- **ISO 27001**, ossia 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
- **ISO 27017**, "Sicurezza e Privacy nel Cloud": fornisce indicazioni e raccomandazioni sugli aspetti di sicurezza informatica specifici per il cloud computing
- **ISO 27018**, "Protezione dei Dati Personali nel Cloud": definisce i requisiti per garantire la tutela dei dati personali da parte dei fornitori di servizi di public cloud e rappresenta una risposta concreta alle principali questioni di natura legale e contrattuale, legate alla gestione dei dati personali in infrastrutture informatiche distribuite seguendo il modello del cloud pubblico.
- **ISO 22301**: Certifica la progettazione e la fornitura dei servizi di Cloud Computing e Cloud Storage.

Seeweb è inoltre certificata **CISPE**, e presente sul suo registro pubblico come fornitore di servizi cloud compliant alle best practice dettate dal GDPR.

05. 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.

Seeweb srl
Via Armando Vona 66
03100, Frosinone

Via Caldera, 21 - edificio B
20153 Milano

https://www.seeweb.it
info@seeweb.it
https://www.facebook.com/seeweb.it
https://twitter.com/seeweblive

Contatti:
Chiara Grande
chiara.g@seeweb.it

14dicembre2023

seeweb
THINK CLOUD