Risposte di AWS alle principali domande sulla conformità

Gennaio 2017

Note

Il presente documento è fornito a solo scopo informativo. In esso sono illustrate le attuali offerte di prodotti e le prassi di AWS alla data di pubblicazione del documento, offerte che sono soggette a modifica senza preavviso. È responsabilità dei clienti effettuare una propria valutazione indipendente delle informazioni contenute nel presente documento e dell'uso dei prodotti o dei servizi di AWS, ciascuno dei quali viene fornito "così com'è", senza garanzie di alcun tipo, né esplicite né implicite. Il presente documento non dà origine a garanzie, rappresentazioni, impegni contrattuali, condizioni o assicurazioni da parte di AWS, delle sue società affiliate, dei suoi fornitori o dei licenzianti. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica qualsivoglia contratto tra AWS e i suoi clienti.

Indice

Sintesi

In questo documento vengono esaminate le domande comuni sulla conformità del cloud computing in relazione ad AWS. Le risposte a queste domande possono risultare interessanti quando si valuta e si sceglie un ambiente di cloud computing e possono aiutare i clienti AWS nell'attività di gestione dei controlli.

Principali domande sulla conformità e relative risposte

Categoria	Domanda sul cloud computing	Informazioni AWS
Titolarità del controllo	Chi controlla l'infrastruttura distribuita nel cloud?	Per la parte distribuita in AWS, è AWS a controllare i componenti fisici di tale tecnologia. Il cliente è titolare di e controlla tutti gli altri aspetti, compreso il controllo sui punti di connessione e le trasmissioni. Per aiutare i clienti a comprendere meglio quali sono i controlli esistenti e qual è il loro grado di efficienza operativa, viene pubblicato un rapporto SOC 1 di tipo II che riguarda i controlli definiti sulla base di EC2, S3 e VPC, oltre a controlli dettagliati sulla sicurezza fisica e ambientale. Tali controlli sono definiti ad un alto livello di specificità, che dovrebbe riuscire a soddisfare la maggior parte delle esigenze dei clienti. I clienti AWS che hanno sottoscritto un accordo di non divulgazione con AWS possono richiedere una copia del report SOC 1 Type II.
Audit informatico	Come si può effettuare il controllo del fornitore di servizi cloud?	L'audit della maggior parte dei layer e dei controlli al di sopra dei controlli fisici resta una responsabilità del cliente. La definizione dei controlli logici e fisici di AWS è documentata nel rapporto SOC 1 di tipo II, consultabile da parte dei team di controllo e conformità. AWS ISO 27001 e le altre certificazioni sono anch'esse a disposizione dei revisori per l'eventuale consultazione.
Conformità alla legge Sarbanes-Oxley	Come si ottiene la conformità SOX se i sistemi compresi nell'ambito di applicazione sono distribuiti nell'ambiente del fornitore di servizi cloud?	Se un cliente elabora informazioni finanziarie nel cloud AWS, i revisori del cliente possono stabilire che alcuni dei sistemi AWS rientrano nell'ambito di applicazione dei requisiti Sarbanes-Oxley (SOX). I revisori del cliente devono effettuare una propria valutazione circa l'applicabilità SOX. Dato che la maggior parte dei controlli di accesso logico è gestita dal cliente, è quest'ultimo a trovarsi nella posizione migliore per stabilire se le sue attività di controllo soddisfano gli standard pertinenti. Se i revisori SOX richiedono le specifiche relative ai controlli fisici di AWS, possono fare riferimento al rapporto AWS SOC 1 di tipo II che riporta nel dettaglio i controlli previsti da AWS.

Categoria	Domanda sul cloud computing	Informazioni AWS
Conformità ai requisiti HIPAA	È possibile soddisfare i requisiti di conformità HIPAA se la distribuzione è stata effettuata nell'ambiente del fornitore di servizi cloud?	I requisiti HIPAA si applicano al cliente AWS e sono controllati da quest'ultimo. La piattaforma AWS consente di distribuire soluzioni capaci di soddisfare requisiti specifici di certificazione del settore, come HIPAA. I clienti possono utilizzare i servizi AWS per mantenere un livello di sicurezza equivalente o superiore a quello richiesto per proteggere le cartelle cliniche elettroniche. I clienti hanno sviluppato in AWS applicazioni per il settore sanitario conformi alle norme in materia di sicurezza e privacy HIPAA. AWS fornisce ulteriori informazioni sulla conformità ai requisiti HIPAA nel proprio sito Web, dove è disponibile anche un whitepaper sull'argomento.
Conformità alla certificazione GLBA	È possibile soddisfare i requisiti di certificazione GLBA se la distribuzione è stata effettuata nell'ambiente del fornitore di servizi cloud?	La maggior parte dei requisiti GLBA è controllata dal cliente AWS. AWS offre ai clienti i mezzi per proteggere i dati, gestire i permessi e sviluppare applicazioni conformi ai requisiti GLBA nell'infrastruttura AWS. Se al cliente occorre una garanzia specifica del fatto che i controlli di sicurezza fisica stiano funzionando in modo efficace, può fare riferimento al rapporto AWS SOC 1 di tipo II, ove pertinente.
Conformità alle normative federali	È possibile per un'agenzia governativa degli Stati Uniti essere conforme alla regolamentazione in materia di sicurezza e privacy se ha effettuato la distribuzione nell'ambiente del fornitore di servizi cloud?	La conformità delle agenzie federali degli Stati Uniti è stabilita in base a una serie di standard, compresi il Federal Information Security Management Act (FISMA) del 2002, il Federal Risk and Authorization Management Program (FedRAMP), il Federal Information Processing Standard (FIPS) Publication 140-2 e l'International Traffic in Arms Regulations (ITAR). È inoltre possibile ottenere la conformità ad altre leggi e regolamenti, in base ai requisiti definiti dalla legislazione applicabile.
Ubicazione dei dati	Dove si trovano i dati dei clienti?	I clienti AWS indicano in quale regione fisica saranno ubicati i propri dati e server. La replica dei dati per gli oggetti dati S3 viene effettuata all'interno del cluster regionale in cui sono archiviati i dati e non viene ripetuta in altri cluster di data center di altre regioni. I clienti AWS indicano in quale regione fisica saranno ubicati i propri dati e server. AWS non sposterà i contenuti dei clienti dalle regioni selezionate senza avvisare il cliente, a meno che ciò non sia necessario in osservanza della legge o di richieste da parte di enti governativi. Per un elenco completo delle regioni, vedere aws.amazon.com/about-aws/global-infrastructure.

Categoria	Domanda sul cloud computing	Informazioni AWS
E-Discovery	Il fornitore di servizi cloud soddisfa le esigenze del cliente di rispettare procedure e requisiti di individuazione elettronica (e-discovery)?	AWS fornisce l'infrastruttura e il cliente gestisce tutto il resto, compreso il sistema operativo, la configurazione di rete e le applicazioni installate. I clienti sono responsabili del rispetto delle procedure legali che prevedono l'identificazione, la raccolta, l'elaborazione, l'analisi e la produzione dei documenti elettronici che i clienti archiviano o elaborano con l'ausilio di AWS. Su richiesta, AWS può collaborare con i clienti che necessitano dell'assistenza di AWS nelle procedure legali.
Tour dei data center	Il fornitore di servizi cloud consente ai clienti di effettuare tour dei data center?	No. I data center ospitano più clienti, pertanto AWS non consente tour dei data center, in quanto ciò esporrebbe una vasta gamma di clienti all'accesso fisico da parte di terzi. Per soddisfare le esigenze di questo cliente, un revisore indipendente e competente convalida la presenza e il funzionamento di controlli nel quadro del rapporto SOC 1 di tipo II. Questa convalida da parte di terzi diffusamente accettata offre ai clienti un punto di vista indipendente sull'efficacia dei controlli esistenti. I clienti AWS che hanno sottoscritto un accordo di non divulgazione con AWS possono richiedere una copia del rapporto SOC 1 di tipo II. Verifiche indipendenti della sicurezza fisica dei data center sono anche previste dagli audit di conformità agli standard ISO 27001, PCI, ITAR e dai programmi di test FedRAMP[sm].
Accesso di terze parti	L'accesso ai data center del fornitore di servizi cloud è consentito a terze parti?	AWS controlla rigorosamente l'accesso ai data center, anche nel caso dei dipendenti interni. Le terze parti hanno accesso ai data center AWS solo se espressamente autorizzate dal responsabile del data center AWS secondo la policy di accesso AWS. Per i controlli specifici relativi all'accesso fisico, alle autorizzazioni di accesso ai data center e ad altri controlli correlati, consultare il report SOC 1 Type II.
Azioni con privilegi	Le azioni con privilegi sono monitorate e controllate?	I controlli esistenti limitano l'accesso ai sistemi e ai dati e fanno sì che l'accesso venga monitorato e sottoposto a restrizioni. I dati dei clienti e le istanze server, inoltre, sono isolati a livello logico da quelli di altri clienti per impostazione predefinita. Il controllo degli accessi da parte di utenti con privilegi viene verificato da un revisore indipendente durante gli audit AWS SOC 1, ISO 27001, PCI, ITAR e FedRAMP[sm].

Categoria	Domanda sul cloud computing	Informazioni AWS
Accesso a informazioni privilegiate	Il fornitore di servizi cloud prende misure contro la minaccia di un accesso non autorizzato a informazioni privilegiate relative ai dati e alle applicazioni dei clienti	AWS prevede controlli SOC 1 specifici per gestire la minaccia di accessi non autorizzati a informazioni privilegiate e la certificazione pubblica e le iniziative di conformità illustrate nel presente documento affrontano la questione di tali accessi. Tutte le certificazioni e le attestazioni di terze parti effettuano una valutazione dei controlli di prevenzione e rilevazione degli accessi logici. Valutazioni periodiche del rischio, inoltre, sono incentrate sulle modalità di controllo e monitoraggio dell'accesso a informazioni privilegiate.
Multi-tenancy	La separazione tra i clienti viene implementata in modo sicuro?	L'ambiente di AWS è virtualizzato e multi-tenant. AWS ha implementato processi di gestione della sicurezza, controlli PCI e altri controlli di sicurezza pensati per isolare ciascun cliente dagli altri clienti. I sistemi AWS sono progettati per impedire ai clienti di accedere a host fisici o istanze non assegnate loro mediante l'applicazione di filtri attraverso il software di virtualizzazione. Tale architettura è stata convalidata da un revisore indipendente PCI Qualified Security Assessor (QSA) ed è stata giudicata conforme a tutti i requisiti PCI DSS versione 3.1 pubblicata ad aprile 2015. **Nota**: AWS offre anche opzioni single-tenancy. Le istanze dedicate sono istanze di Amazon EC2 avviate in Amazon Virtual Private Cloud (Amazon VPC) che eseguono hardware dedicato a un unico cliente. Le istanze dedicate consentono di sfruttare pienamente i vantaggi di Amazon VPC e del cloud AWS, isolando allo stesso tempo le istanze di calcolo di Amazon EC2 a livello hardware.
Vulnerabilità dell'hypervisor	Il fornitore di servizi cloud ha affrontato le vulnerabilità note dell'hypervisor?	Attualmente, Amazon EC2 utilizza una versione dell'hypervisor Xen con elevata personalizzazione. L'hypervisor viene sottoposto a valutazioni regolari sulle vulnerabilità nuove ed esistenti e sui vettori di attacco da parte di team di intrusione interni ed esterni ed è idoneo a mantenere un forte isolamento tra macchine virtuali ospiti. La sicurezza dell'hypervisor AWS Xen viene verificata regolarmente da revisori indipendenti durante valutazioni e controlli. Si veda il whitepaper sulla sicurezza AWS per avere ulteriori informazioni sull'hypervisor Xen e l'isolamento delle istanze.

Categoria	Domanda sul cloud computing	Informazioni AWS
Gestione delle vulnerabilità	L'applicazione di patch ai sistemi viene effettuata idoneamente?	AWS è responsabile dell'applicazione delle patch ai sistemi che supportano la fornitura di servizi ai clienti, come l'hypervisor e i servizi di rete. Tale operazione viene eseguita come prescritto dalla policy AWS e ai sensi dei requisiti di ISO 27001, NIST e PCI. I clienti controllano i propri sistemi operativi, software e applicazioni guest e sono quindi responsabili dell'applicazione delle patch ai propri sistemi.
Crittografia	I servizi forniti supportano la crittografia?	Sì. AWS consente ai clienti di utilizzare i propri meccanismi di crittografia per quasi tutti i servizi, inclusi S3, EBS, SimpleDB ed EC2. I tunnel da IPSec a VPC sono anch'essi crittografati. Amazon S3 offre inoltre, come opzione per i clienti, la crittografia lato server. I clienti possono utilizzare anche tecnologie di crittografia di terze parti. Per ulteriori informazioni, consultare il whitepaper sulla sicurezza di AWS.
Proprietà dei dati	Quali sono i diritti che il fornitore di servizi cloud può vantare sui dati dei clienti?	I clienti AWS detengono il controllo e la proprietà dei propri dati. AWS si impegna a proteggere la privacy dei clienti ed è vigile nel determinare quali richieste imposte dalle forze dell'ordine devono essere rispettate. AWS non esita a contestare i provvedimenti delle forze dell'ordine qualora ritenga che tali misure siano prive di un solido fondamento.
Isolamento dei dati	Il fornitore di servizi cloud isola adeguatamente i dati dei clienti?	Tutti i dati archiviati da AWS per conto dei clienti dispongono di solide funzionalità di sicurezza e controllo dell'isolamento dei tenant. Amazon S3 fornisce controlli avanzati sull'accesso ai dati. Per ulteriori informazioni sulla sicurezza di specifici servizi dati consultare il whitepaper sulla sicurezza AWS.
Servizi compositi	Il fornitore di servizi cloud integra il proprio servizio con i servizi di altri fornitori cloud?	AWS non ricorre a fornitori terzi di servizi cloud per erogare i servizi AWS ai clienti.
Controlli fisici e ambientali	Questi controlli sono gestiti dal fornitore di servizi cloud specificato?	Sì. Sono descritti specificamente nel rapporto SOC 1 di tipo II. Altre certificazioni supportate da AWS, come ad esempio ISO 27001 e FedRAMP[sm], richiedono l'implementazione di controlli fisici e ambientali conformi alle best practice.
Protezione dal lato client	Il fornitore di servizi cloud consente ai clienti di proteggere e gestire l'accesso dai client, come PC e dispositivi mobili?	Sì. In AWS, i clienti possono gestire le applicazioni client e per dispositivi mobili in base alle loro esigenze.

Categoria	Domanda sul cloud computing	Informazioni AWS
Sicurezza dei server	Il fornitore di servizi cloud consente ai clienti di proteggere i propri server virtuali?	Sì. AWS consente ai clienti di implementare l'architettura di sicurezza desiderata. Per maggiori dettagli sulla sicurezza dei server e della rete consultare il whitepaper sulla sicurezza AWS.
Identity and Access Management	Il servizio prevede funzionalità IAM?	AWS prevede una serie di offerte relative a Identity and Access Management che consentono ai clienti di gestire le identità degli utenti, assegnare le credenziali di sicurezza, organizzare gli utenti in gruppi e gestire le autorizzazioni degli utenti in maniera centralizzata. Per maggiori informazioni consultare il sito Web di AWS.
Interruzioni per manutenzione programmata	Il fornitore specifica quando i sistemi subiranno interruzioni per la manutenzione?	Non occorre che i sistemi AWS siano offline per gli interventi di manutenzione ordinaria e l'applicazione di patch ai sistemi. La manutenzione e l'applicazione di patch ai sistemi AWS non ha, in genere, alcun impatto sui clienti. La manutenzione delle istanze è controllata dal cliente.
Scalabilità	Il fornitore consente ai clienti di ampliare le risorse oltre quanto previsto originariamente dal contratto?	Il cloud AWS è distribuito, estremamente sicuro e resiliente, così da offrire ai clienti una scalabilità elevata. I clienti possono aumentare o diminuire le risorse, pagando solo per ciò che utilizzano.
Disponibilità del servizio	Il fornitore si impegna a offrire un alto livello di disponibilità?	Nei contratti sul livello di servizio AWS si impegna a offrire alti livelli di disponibilità. Amazon EC2, ad esempio, si impegna a offrire una percentuale di tempo di operatività annuale di almeno il 99,95% durante l'anno di servizio. Amazon S3 si impegna a fornire una percentuale di tempo di operatività mensile di almeno il 99,9%. In caso di mancato rispetto di tali parametri di disponibilità, vengono forniti crediti di servizio.
Attacchi Distributed Denial Of Service (DDoS)	In che modo il fornitore protegge il proprio servizio da attacchi DDoS?	La rete AWS offre una protezione elevata contro i tradizionali problemi di sicurezza della rete e il cliente può implementare un'ulteriore protezione. Per maggiori informazioni sull'argomento, compresa la trattazione degli attacchi DDoS, consultare il whitepaper sulla sicurezza AWS.
Portabilità dei dati	I dati archiviati presso un fornitore di servizi possono essere esportati su richiesta del cliente?	AWS permette ai clienti di spostare i dati all'interno e fuori dallo storage AWS in base alle necessità. Il servizio AWS Import/Export per S3 accelera lo spostamento di grandi quantità di dati all'interno e all'esterno di AWS utilizzando dispositivi di storage portatili per il trasporto.

Categoria	Domanda sul cloud computing	Informazioni AWS
Continuità operativa del fornitore di servizi	Il fornitore di servizi gestisce un programma di continuità operativa?	AWS gestisce un programma di continuità operativa. Nel whitepaper sulla sicurezza AWS sono disponibili informazioni dettagliate in merito.
Continuità operativa del cliente	Il fornitore di servizi consente ai clienti di implementare un piano di continuità operativa?	AWS offre ai clienti la possibilità di implementare un solido piano di continuità, che comprende l'utilizzo di backup frequenti delle istanze del server, repliche per la ridondanza dei dati e architetture di distribuzione su più regioni o zone di disponibilità.
Durabilità dei dati	Il servizio specifica la durabilità dei dati?	Amazon S3 fornisce un'infrastruttura di storage estremamente durevole. Gli oggetti sono archiviati in modo ridondante su più dispositivi, in più strutture di una regione Amazon S3. Una volta effettuato lo storage, Amazon S3 preserva la durabilità degli oggetti individuando e riparando l'eventuale ridondanza andata perduta. Amazon S3, inoltre, verifica periodicamente l'integrità dei dati archiviati con l'ausilio di checksum. Gli eventuali elementi danneggiati individuati vengono riparati con i dati ridondanti. S3 è progettato per assicurare ai dati archiviati una durabilità del 99,999999999% e una disponibilità degli oggetti del 99,99% su base annua.
Backup	Il servizio consente di effettuare backup su nastro?	AWS consente ai clienti di eseguire backup su nastro utilizzando il fornitore di servizi da loro scelto. Tuttavia, AWS non fornisce il servizio di backup su nastro. Il servizio Amazon S3 è stato progettato per ridurre pressoché a zero il rischio di perdita di dati e la durabilità equivalente a copie multisito degli oggetti dati è ottenuta tramite la ridondanza dello storage dei dati. Per informazioni sulla durabilità dei dati e la ridondanza consultare il sito Web AWS.
Aumenti di prezzo	Il fornitore dei servizi aumenterà i prezzi senza preavviso?	Le diminuzioni dei prezzi sono una costante nel caso di AWS, dato che il costo legato alla fornitura di questi servizi si riduce nel tempo. Negli ultimi anni, infatti, AWS ha ridotto costantemente i prezzi.
Sostenibilità	L'azienda che fornisce i servizi dispone dei presupposti per una sostenibilità a lungo termine?	AWS è leader nella fornitura di servizi cloud e costituisce un tassello importante della strategia aziendale a lungo termine di Amazon.com. AWS ha tutti i presupposti per una sostenibilità a lungo termine.

Approfondimenti

Per ulteriori informazioni, consultare le seguenti fonti:

- Panoramica su gestione dei rischi e conformità in AWS
- Certificazioni AWS, programmi, rapporti e attestazioni di terze parti
- CAIQ (Consensus Assessments Initiative Questionnaire) della CSA

Revisioni del documento

Data	Descrizione
Gennaio 2017	Migrazione a un nuovo modello
Gennaio 2016	Prima pubblicazione