LA PROTEZIONE DEI DATI PERSONALI NEI SERVIZI DI CLOUD COMPUTING E LA NORMA ISO/IEC 27018

Mariangela Fagnani

INTRODUZIONE

Con la diffusione del cloud computing crescono le preoccupazioni dei clienti per la trasparenza, la riservatezza e il controllo sul servizio erogato. Il cloud infatti sta rapidamente trasformando le aziende, espande gli accessi, cambia le responsabilità, i controlli e la velocità di accesso a risorse e applicazioni, con impatti su tutti gli aspetti di IT Security e Privacy Compliance, che richiedono un approccio diverso rispetto agli ambienti IT tradizionali.

I clienti spesso non sono a conoscenza di come sono protette le informazioni spostate nel cloud, dove sono localizzate, chi accede alle informazioni e cosa succede nel caso in cui si volesse passare a un altro fornitore o il fornitore cessasse la propria attività.

I servizi Cloud XaaS hanno differenti requisiti di sicurezza e privacy, in funzione delle loro caratteristiche, ma anche una diversa distribuzione delle responsabilità di sicurezza fra il fornitore e il cliente. Nell'ambito di modelli SaaS la responsabilità di buona parte degli aspetti di sicurezza è demandata al fornitore, in quanto è lui che si occupa direttamente della messa in opera e della gestione degli aspetti infrastrutturali, di middleware ed applicativi. Ma spetta indubbiamente al cliente occuparsi della sicurezza dei processi operativi ed anche di tutti quegli aspetti di sicurezza che consentono ai propri utenti di utilizzare gli ambienti applicativi messi a disposizione dal fornitore, quali ad esempio Politiche e Procedure per l'utilizzo corretto delle risorse informative, la gestione del ciclo di vita delle utenze, dei relativi profili di abilitazione e delle credenziali di identificazione ed autenticazione, il controllo sull'operato degli utenti, etc.

Passando verso modelli di Cloud di tipo PaaS e di tipo IaaS la componente di responsabilità del fornitore in merito agli aspetti di sicurezza si concentra verso i livelli più bassi dell'infrastruttura, mentre ovviamente si estende in modo complementare la componente di responsabilità del cliente sui livelli più alti.

La criticità per un corretto ed integrato governo delle rispettive competenze è data dalla possibile discontinuità che si localizza nei punti di confine delle responsabilità lato cliente e lato fornitore. Pertanto, è importante che il cliente ed il fornitore affrontino la tematica concordando con la massima trasparenza tutti gli elementi necessari ad indirizzare adeguatamente la Governance della Sicurezza delle Informazioni.

In particolare è importante che siano ben delineati tutti gli aspetti organizzativi e tecnologici che richiedono la stretta interrelazione tra le strutture organizzative preposte alla Sicurezza lato cliente e le corrispondenti lato fornitore.

In base alle norme vigenti in materia di protezione dati personali, la responsabilità per la violazione delle norme sulla protezione dei dati spetta al titolare del trattamento: pertanto, si rende necessario uno standard verificabile per i fornitori di servizi cloud per dimostrare la loro capacità di garantire la sicurezza e la protezione dei dati, inclusi quelli personali soggetti alle normative privacy.

Sulla spinta della Commissione Europea, delle Autorità Nazionali e delle Commissioni per la protezione dei dati, ISO e IEC hanno quindi sviluppato lo standard ISO / IEC 27108[1] (Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors), pubblicato nel 2014.

ISO 27018 è il **primo standard a livello internazionale** per garantire il rispetto dei principi e delle norme privacy, da parte dei fornitori di servizi public cloud che se ne dotano: la norma, infatti, è specificamente indirizzata ai **service providers di public cloud** che elaborano dati personali (PII - Personally Identifiable Information) e che agiscano in qualità di **Data (PII) Processor**.

Lo standard definisce delle **linee guida basate su ISO / IEC 27002[2],** prendendo in considerazione i requisiti normativi per la protezione dei dati personali che possono essere applicabili nel contesto del panorama dei rischi di sicurezza informatica di un fornitore di servizi public cloud.

Trattandosi di Linee guida, la norma ISO 27018 **non è quindi una norma certificabile:** è possibile ottenere un "**Certificato di Conformità**" rilasciato da un Ente Certificatore riconosciuto, a dimostrazione della capacità del Provider di assicurare la protezione dei dati personali.

La norma si basa e rinforza i precedenti standard ISO/IEC 27001 e ISO/IEC 27002 (che sempre più si confermano come gli standard di riferimento in ambito sicurezza delle informazioni) in materia di Gestione della Sicurezza delle Informazioni, e stabilisce obiettivi di controllo, regole e procedure per implementare misure di protezione dei dati personali (PII) in conformità con i principi di privacy di ISO / IEC 29100[3], per i fornitori di servizi cloud.

Ciò allo scopo di accrescere la fiducia verso i fornitori di cloud pubblico, fornendo indicazioni sugli obiettivi da raggiungere in termini di obblighi contrattuali e normativi, consentendo inoltre ai clienti di soddisfare i propri obblighi normativi sulla sicurezza dei dati.

CON LA DIFFUSIONE DEL CLOUD COMPUTING CRESCONO LE PREOCCUPAZIONI DEI CLIENTI PER LA TRASPARENZA, LA RISERVATEZZA E IL CONTROLLO SUL SERVIZIO EROGATO

IN BASE ALLE NORME VIGENTI IN MATERIA DI PROTEZIONE DATI PERSONALI, LA RESPONSABILITÀ PER LA VIOLAZIONE DELLE NORME SULLA PROTEZIONE DEI DATI SPETTA AL TITOLARE DEL TRATTAMENTO: PERTANTO, SI RENDE NECESSARIO UNO STANDARD VERIFICABILE PER I FORNITORI DI SERVIZI CLOUD PER DIMOSTRARE LA LORO CAPACITÀ DI GARANTIRE LA SICUREZZA E LA PROTEZIONE DEI DATI, INCLUSI QUELLI PERSONALI SOGGETTI ALLE NORMATIVE PRIVACY

Mariangela Fagnani, Laureata in Matematica presso l'Universita' degli Studi di Milano, da Ottobre 2014 opera presso Sernet S.p.A. nel ruolo di ICT Security & Governance Senior Advisor dopo aver maturato significative esperienze nell'Information Technology e nella sicurezza Informatica presso IBM. Membro del direttivo di Clusit, CISA e LA 27001, con numerose esperienze di progetti consulenziali e formativi in ambito privacy, sicurezza, certificazione e conformità verso le norme ISO27001 e ISO27018.

CSA Italy è un'associazione no profit italiana nata nel 2011 come capitolo nazionale dell'associazione internazionale CSA (Cloud Security Alliance) a cui aderiscono le maggiori aziende del settore ICT ed Information Security che hanno scelto il Cloud Computing come parte rilevante del loro business. CSA coordina una community di professionisti che contribuiscono attivamente a sviluppare linee guida e buone pratiche per uno sviluppo ed utilizzo in sicurezza del Cloud.

AMBITO E CARATTERISTICHE DELLA NORMA

L'ambito della norma ISO / IEC 27018 (vedi fig. 1) è limitato ai controlli di rilevanza per un fornitore di servizi Public Cloud che tratta dati personali, allo scopo di indirizzare gli specifici rischi di sicurezza informatica e di privacy.
ISO 27018 è applicabile a tutti i tipi e dimensioni di organizzazioni, pubbliche e private, enti governativi e non-profit, che forniscono, nel ruolo di Data Processor, servizi di elaborazione delle informazioni personali via cloud computing nell'ambito di un contratto con altre organizzazioni.
Gli obiettivi che lo standard si pone sono quelli di consentire ai service provider di cloud pubblici di **rispettare gli obblighi** applicabili al contesto, garantire **trasparenza** nelle questioni rilevanti, in modo che i clienti possano scegliere servizi di elaborazione dei dati personali in cloud ben governati, **assistere** tutte le parti coinvolte quando si stabilisce un accordo contrattuale e fornire un meccanismo per **esercitare i diritti di audit e compliance.**
I suddetti obiettivi vengono raggiunti attraverso le linee guida principali:

- **Consenso**: i Cloud Service Provider non devono utilizzare i dati personali per pubblicità e azioni di marketing se non espressamente accettato da parte dell'utente. Inoltre, per l'utente deve essere possibile utilizzare il servizio offerto senza l'obbligo di accettare che i propri dati personali vengano utilizzati per fini pubblicitari e di marketing
- **Controllo**: gli utenti devono avere il controllo esplicito di come vengono utilizzate le loro informazioni
- **Trasparenza**: i Cloud Service Provider devono informare i propri utenti sul luogo in cui i loro dati risiedono e sull'eventuale utilizzo di subfornitori per l'elaborazione e la gestione delle informazioni personali
- **Comunicazione**: i Cloud Service Provider devono disporre di un registro che tenga traccia di eventuali violazioni, e devono informare tempestivamente i clienti dell'accaduto
- **Revisione annuale indipendente**: per rimanere conformi allo standard ISO 27018, il Provider deve essere oggetto di revisione e verifica annuale da parte di società terze.

Inoltre lo standard è da ritenersi utile anche per i PII Controller (ovvero i titolari di dati) che possono utilizzare tale linea guida come "Check List" per selezionare i requisiti importanti per il trattamento di dati personali da richiedere al Cloud Provider.

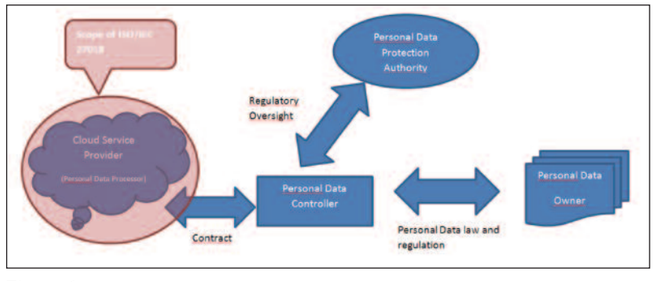
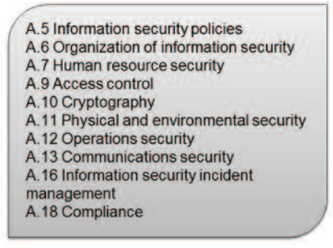


Figura 1

STRUTTURA DELLA NORMA

ISO 27018 richiama, puntualizza le best practices già enucleate dall'ISO 27002, **aggiungendo dei controlli specifici per i servizi cloud** nell'Annex A ISO 27002 (elencate nella figura sotto), in materia di security policy, sicurezza organizzativa, fisica ed ambientale, gestione della continuità operativa, controllo degli accessi e sicurezza del personale, sicurezza delle trasmissioni e della gestione dei devices.



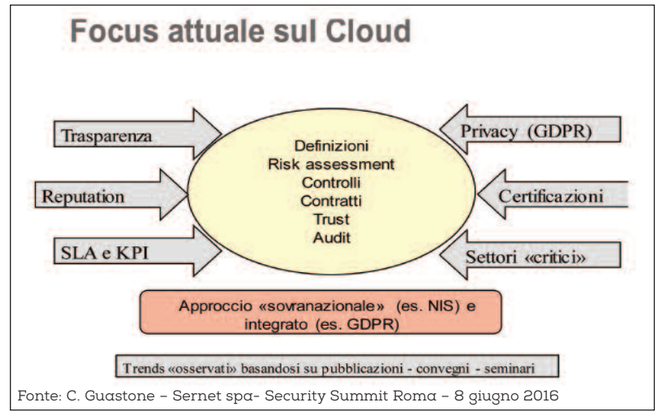
ISO 27002 – controlli aggiuntivi

L'Annex A ISO 27018 include **nuovi controlli e linee guida** per l'implementazione che, in combinazione con i controlli aggiuntivi della ISO 27002, costituiscono un set di regole per rispondere ai requisiti di protezione dei dati personali, che si applicano ai fornitori di servizi public cloud, in qualità di Data Processor.

ISO 27018 Annex A

I nuovi controlli della ISO 27018 sono organizzati secondo lo schema degli **11** "**Principi Privacy**" della norma ISO/IEC 29100 – Privacy Framework e coprono quindi i seguenti aspetti:

- **Scelta e Consenso (A.1)**
- **Legittimità dello scopo (A.2)**
- **Minimizzazione dei Dati (A.4)**
- **Limitazioni sull'utilizzo, conservazione e diffusione (A.5)**
- **Trasparenza e comunicazione (A.7)**
- **Accountability (A.9)**
- **Sicurezza delle Informazioni (A.10)** a cui è dedicato ampio spazio
- **Privacy Compliance (A.11)**



Fonte: C. Guastone – Sernet spa- Security Summit Roma – 8 giugno 2016

CONCLUSIONI

Oggi la ISO 27018 fornisce una guida chiara e trasparente per i Cloud Service Provider per indirizzare la privacy e consentire alle aziende di prendere decisioni informate e consapevoli sui servizi cloud che utilizzano. I Cloud Service Provider che lavorano e si impegnano ad essere conformi alla norma, aiutano ad accrescere la fiducia dei loro clienti e a promuovere l'adozione delle best practices nel loro mercato.
Come primo standard internazionale sulla privacy nel cloud, ISO27018 inizia a porre le basi su come i Cloud Service Provider possono garantire trasparenza sulla privacy e sulla sicurezza, aiutando in tal modo lo sviluppo del business. Ma, oltre a fornire una guida, ISO 27018 è un punto di riferimento che si affianca ad altri standard indirizzati agli ambienti cloud: a tale proposito citiamo lo standard ISO/IEC 27017 (*Information technology – Security techniques – Code of practice for information security controls based on ISO27002 for cloud services)* pubblicato a fine 2015, che fornisce una guida per l'attuazione dei controlli di sicurezza delle informazioni che sono specifici per servizi cloud computing. Tali criteri sono basati, come già per ISO 27018, sullo standard ISO 27002, a cui si aggiungono ulteriori controlli, appositamente progettati per i fornitori di servizi cloud. Il Mercato Cloud si sta sempre più sviluppando, framework e Norme, come CSA STAR[4] e ISO 27017[5], oltre a ISO 27018, sono ormai pubblicate da tempo fornendo concreti riferimenti per servizi Cloud sempre più sicuri.
L'Unione Europea è particolarmente impegnata per aumentare la cooperazione fra gli stati membri per garantire una risposta efficace alle minacce e agli incidenti a carico dei sistemi informativi, per definire **obblighi di sicurezza** per gli operatori del mercato e le amministrazioni pubbliche e per regolamentare il trattamento dei dati personali. Tale impegno si concretizza con il Nuovo Regolamento Europeo per la Data Protection[6] (GDPR) in vigore dal 25 maggio 2016 e la Direttiva NIS[7] (Network and Information Security) del Parlamento Europeo e del Consiglio Europeo in fase di approvazione finale prevista per fine anno. ■

NOTE

1 https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en
2 https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en
3 https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en
4 https://cloudsecurityalliance.org/star/
5 https://www.iso.org/obp/ui/#iso:std:iso-iec:27017:ed-1:v1:en
6 http://ec.europa.eu/justice/data-protection/index_en.htm
7 https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-nis-directive