PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3777 di martedì 10 maggio 2016

Gli obiettivi della norma ISO/IEC 27018

La norma internazionale ISO/IEC 27018 Tecnologia dell'informazione - Tecniche di sicurezza - Codice in materia di protezione dei dati personali (PII) in cloud pubblici in qualità di processori PII. Di Adalberto Biasiotti.

La commissione responsabile per lo sviluppo di questo documento è la ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

È facile individuare la ragione per cui questa norma sta assumendo una grande importanza, soprattutto con l'aumento delle informazioni, in particolare dati personali, che vengono immessi nel cloud.

I gestori di servizi di cloud trattano delle informazioni personali identificabili, in altre parole dati personali, nell'ambito di un contratto con i propri clienti. Questo contratto prevede che entrambe le parti operino in maniera da rispettare i requisiti di tutte le disposizioni legislativi e regolamenti applicabili, che proteggono i dati personali. I requisiti e le modalità tra cui può essere suddivisa la responsabilità del trattamento fra il gestore del servizio cloud e i suoi clienti, titolari del trattamento, possono variare in funzione della legislazione in vigore in ogni singolo paese, e anche in funzione dei termini contrattuali concordati. La differenza di disposizioni legislative in vigore in vari paesi può rendere oltremodo complessa la gestione di questi dati personali.

Secondo le correnti definizioni, un gestore di servizi del cloud è un responsabile del trattamento, quando tratta dati personali in conformità alle istruzioni che sono state date da un suo cliente. Il cliente, che ha una relazione contrattuale con il gestore del cloud, può essere una persona fisica o giuridica, che opera come titolare del trattamento.

È facoltà del titolare del trattamento designare anche più di un gestore del cloud come responsabile del trattamento, per inserire un elevato livello di flessibilità nei servizi offerti.
A questo proposito, si deve rilevare che il titolare del trattamento ha piena autorità e responsabilità sulle modalità di trattamento dei dati nell'ambito del cloud. Ciò significa che egli ha responsabilità maggiori rispetto al gestore del cloud. Una netta distinzione fra le responsabilità del titolare e quelle del responsabile del trattamento rappresenta un aspetto fondamentale della impostazione formalizzazione del rapporto contrattuale.
Si noti comunque che anche il gestore del cloud potrebbe assumere il ruolo di titolare del trattamento, ad esempio quando egli gestisce dati di fatturazione di traffico relativi all'attività svolta dal suo cliente.

L'obiettivo di questa norma internazionale, che deve essere letta in abbinamento con gli obiettivi di sicurezza dell'informazione e dei controlli elencati nella ISO/IEC 27002, è quello di creare un gruppo omogeneo di categorie di sicurezza e di controlli, che possono essere attuati dal gestore del cloud, operante come responsabile del trattamento.

Questa norma ha i seguenti obiettivi:

- assistere il gestore del cloud nel rispetto di tutti gli obblighi che gli competono, trattando dati personali in qualità di responsabile del trattamento,
- consentire al responsabile del trattamento di operare in modo trasparente, in modo che il titolare del trattamento possano scegliere un fornitore che dia adeguate garanzie,

- assistere nella elaborazione di un accordo contrattuale tra il titolare ed il responsabile del trattamento,
- offrire ai titolari del trattamento un meccanismo che permetta di esercitare il diritto di audit e di verifica di conformità, con attribuzioni di responsabilità laddove può essere difficile sviluppare degli audit approfonditi, in quanto i dati trasmessi dal titolare al responsabile possono essere distribuiti in un ambiente difficilmente controllabile che può accrescere i rischi legati alla inadeguatezza dei controlli di sicurezza fisici e logici di rete.

È evidente che questa norma internazionale non può sostituire la legislazione ed i regolamenti in vigore, ma può offrire assistenza nell'individuare un quadro di riferimento di congruità per i gestori di servizi di cloud, che operano in un mercato multinazionale.

Un'altra funzione importante di questa norma è quella di aiutare i titolari del trattamento a scegliere quali siano i controlli di sicurezza applicabili al trattamento dei dati personali, in un contesto di sicurezza dell'informazioni gestite nel cloud. A questo ambiente si applica la norma ISO/IEC 27001; questo documento può anche essere una utile linea guida per attuare i principi più largamente riconosciuti in tema di protezione dei dati personali.

Ecco perché una analisi di rischio, elaborata secondo ISO/IEC 27002, rappresenta un aspetto essenziale della impostazione del rapporto contrattuale delle misure di sicurezza.
Una differenza fondamentale sta però nel fatto che un ente che attua le linee guida ISO/IEC 27001 sta proteggendo le proprie informazioni. In questo specifico contesto, un fornitore servizi di cloud protegge invece i dati personali che gli vengono forniti da un titolare esterno, che a sua volta ha ricevuto questi dati dagli interessati, che in lui hanno riposto fiducia.
Ecco il motivo per cui l'attuazione dei controlli di cui alla norma ISO/IEC 27002, da parte del responsabile del trattamento, risulta opportune addirittura necessaria.
Questa norma accresce i controlli già elencati nella norma ISO/IEC 27002, per tenere conto della natura distribuita del rischio e dell'esistenza del rapporto contrattuale specifico.
L'annesso A offre tutta una serie di controlli e linee guida specificamente riferiti alla gestione di dati personali nel cloud e che non sono presenti nella normativa ISO/IEC 27002.

Le tre aree principali da prendere in considerazione sono le seguenti:

- avere a disposizione un panorama legislativo e regolamentare completo e vigente nel paese in cui si trova il titolare, che alla fin fine è il responsabile finale nei confronti dell'interessato e dell'autorità Garante nazionale,
- condurre una attenta analisi di rischio, che prenda in considerazione le minacce e le vulnerabilità e le probabilità, con le conseguenze possibili. A questo proposito viene utile la norma ISO/IEC 29134, che può essere utile per sviluppare una valutazione di impatto sulla protezione dei dati, come richiesto specificamente dal regolamento generale europeo;
- infine, occorre tenere conto delle politiche aziendali in vigore, che possono anche andare oltre il rispetto dei requisiti regolamentari minimi.

La selezione dei controlli dipende da decisioni organizzative, che fanno riferimento ai criteri adottati per la valutazione di rischio, le opzioni di trattamento del rischio e all'approccio generale alla gestione del rischio, che viene scelto dall'organizzazione e, attraverso accordi contrattuali, dei suoi clienti e fornitori; questa selezione è anche soggetta a prescrizioni legislative e regolamentari nazionali ed internazionali.

Quando i controlli che sono previsti da questa norma internazionale non vengono adottati, la scelta deve essere documentata con adeguata giustificazione per il mancato rispetto.
Non bisogna infine dimenticare che la selezione e l'attuazione dei controlli dipende dall'effettivo ruolo svolto dal fornitore del servizio di cloud, nel contesto dell'intera infrastruttura, che si appoggia al cloud (vedi ISO/IEC 17789).

Al proposito, occorre sottolineare che molte e diverse organizzazioni possono essere coinvolte nel fornire l'infrastruttura dei servizi di elaborazione in un cloud. In alcune circostanze, i controlli adottati possono essere specifici per una particolare categoria di servizi. Gli accordi contrattuali devono chiaramente indicare le responsabilità nella protezione dei dati personali per tutte le organizzazioni coinvolte nel fornire ed utilizzare i servizi del cloud, incluso il responsabile del trattamento di dati personali in un cloud pubblico, i suoi subfornitori e i suoi clienti.

L'attuazione delle prescrizioni di questa norma diventa molto più semplice, se nel progetto del sistema informativo del

responsabile del trattamento nel cloud sono stati presi in considerazione elementi specifici, come ad esempio sviluppando un progetto di protezione dei dati personali fin dalla progettazione.

La bibliografia della norma illustra questi documenti, tre quali si cita ISO/IEC 29101.
Nulla impedisce che vengano sviluppate delle linee guida aggiuntive, utilizzando questa norma come punto di partenza, nel contesto della protezione dei dati personali. Si precisa anche che è possibile che non tutti i controlli e le linee guida di questa norma possano essere applicati integralmente. Laddove si decida di utilizzare dei controlli aggiuntivi, non inclusi in questa norma, può essere utile introdurre dei riferimenti alle clausole di questa norma, al fine di facilitare le verifiche di conformità da parte degli auditors ed altri soggetti coinvolti.
Infine, è bene sottolineare che i dati personali hanno un ciclo di vita naturale, dal momento della creazione, che passa attraverso la archiviazione, il trattamento, l'uso e la trasmissione, fino a giungere alla fase di cancellazione o di distruzione. I rischi legati ai dati personali possono variare durante il ciclo di vita, ma in ogni fase occorre rispettare i requisiti importanti di protezione.

Per questa ragione è importante che i requisiti di protezione dati personali vengano presi considerazione mano a mano che nuovi sistemi informativi vengono attivati e gestiti, attraverso l'intero ciclo di vita.

Adalberto Biasiotti
