Linee Guida Protezione Informazioni nei Servizi (SaaS, PaaS, Iaas) in Cloud

A CHI E' RIVOLTO IL SERVIZIO

Le Linee Guida sono rivolte a:

- aziende che offrono servizi software specialistici per la Pubblica Amministrazione, così come indicato da AgID, ma anche le altre aziende che intendano fornire ai propri clienti garanzie aggiuntive che i servizi informatici in Cloud offerti abbiano il corretto livello di sicurezza e protezione delle informazioni dei clienti.

La certificazione ISO 27001, integrata con le linee guida ISO 27017 e ISO 27018, permette alle aziende che erogano servizi in SaaS, IaaS e PaaS o sono Cloud Service Provider di garantire ai propri clienti una maggiore protezione dei dati trattati.

Le linee guida si basano e rinforzano gli standard ISO/IEC 27001 e ISO/IEC 27002 in materia di Gestione della Sicurezza delle Informazioni, e stabiliscono obiettivi di controllo, regole e procedure per implementare adeguate misure di protezione per i fornitori di Servizi in Cloud

Le linee guida per la protezione delle informazioni ISO/IEC 27018:2014 – "Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors" e ISO/IEC 27017:2015 "Information Technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services" si basano sui requisiti della ISO/IEC 27002 e della ISO/IEC 29100, e li estendono con controlli specifici relativi alla protezione delle informazioni in ambito cloud.

Le linee guida non sono certificabili da sole, ma per poter essere considerate valide devono essere integrate all'interno di un certificato ISO 27001 che copra il campo di applicazione relativo ai servizi Cloud.

La verifica del rispetto di tali linee guida deve essere effettuata da un ente terzo accreditato.

ITER DI CERTIFICAZIONE

L'iter di certificazione, prevede:

- ✓ la richiesta di offerta;
- ✓ l'accettazione dell'offerta;
- ✓ lo svolgimento di un audit di Certificazione (suddiviso in due stage);
- ✓ la gestione di eventuali carenze rilasciate;
- ✓ la delibera di certificazione da parte della Commissione Tecnica di QMS Italia.

Il certificato rilasciato all'Organizzazione ha validità triennale. A seguito della certificazione, sono effettuate con frequenza annuale le verifiche di mantenimento. Alla scadenza dei tre anni, si svolgerà poi la verifica di rinnovo del certificato.