Prot. DC2019SSV044 Milano, 31-01-2019

Agli Organismi di Certificazione accreditati ISO/IEC 17021

Alle Associazioni degli organismi di valutazione della conformità
Loro Sedi

Oggetto: **Dipartimento DC - Circolare Informativa N° 01/2019**
Accreditamento schema di certificazione ISO/IEC 27001:2013 con integrazione delle linee guida ISO/IEC 27017:2015 e 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

Questa Informativa annulla e sostituisce la precedente Circolare DC N° 13/2017 rif. DC2017SSV206 del 21-07-2017

Introduzione

Con la diffusione del cloud computing crescono le preoccupazioni dei clienti per la trasparenza, la riservatezza e il controllo sul servizio erogato: i clienti spesso non sono a conoscenza di come sono protette le informazioni archiviate nel cloud, dove sono localizzate e cosa succede nel caso in cui si volesse passare a un altro fornitore o il fornitore cessasse la propria attività.

Inoltre, in base alle norme vigenti, la responsabilità per la violazione delle norme sulla protezione dei dati personali spetta al titolare del trattamento: pertanto, si rende necessario uno standard verificabile per i fornitori di servizi cloud per dimostrare la loro capacità di ripresa e 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 i nuovi standard ISO/IEC 27017:2015 (Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services) e ISO / IEC 27018 (Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).

Contesto Normativo

ISO/IEC 27017 e 27018 sono i primi standard a livello internazionale per contribuire a garantire il rispetto dei principi e delle norme privacy, da parte dei providers di public cloud che se ne dotano: le norme, infatti, sono 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.
Definiscono delle linee guida basate su ISO / IEC 27002, 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, le norme ISO 27017 e 27018 non sono quindi norme certificabili: ciò nonostante, è possibile ottenere una integrazione di un certificato ISO/IEC 27001 esistente e rilasciato da un Ente Certificatore riconosciuto, a dimostrazione della capacità del Provider di assicurare la protezione dei dati personali, basato sulla integrazione delle Norme citate con la Norma ISO/IEC 27001.

Sede operativa e amministrativa: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Sede legale: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | Partita IVA - Codice Fiscale 10566361001

Le norme si basano e rinforzano i precedenti standard ISO/IEC 27001 e ISO/IEC 27002 (essendo il secondo la linea guida per l'applicazione dei controlli operativi riportati in Allegato A del primo) in materia di Gestione della Sicurezza delle Informazioni, e stabiliscono 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, per i fornitori di servizi cloud.

1) Norma e regole di Certificazione

Norma di Accreditamento	ISO/IEC 17021-1:2015, ISO/IEC 27006:2015
Norma di Certificazione	ISO/IEC 27017:2015 e ISO/IEC 27018:2014, come addendum alla Norma ISO/IEC 27001:2013 La Norma 27017:2015 può essere oggetto di estensione della certificazione anche da sola. Ove si intenda considerare tale estensione anche in ottica di Protezione Dati Personali, l'estensione alla Norma ISO/IEC 27017:2015 dovrà essere integrata con la Norma ISO/IEC 27018:2014. Dalla data di entrata in vigore della presente circolare, non è ammessa l'estensione alla sola Norma ISO/IEC 27018:2014. Le certificazioni a fronte della ISO/IEC 27001:2013 integrate con la Norma ISO/IEC 27018:2014 dovranno essere integrate anche con la Norma ISO/IEC 27017:2015 entro il successivo rinnovo della certificazione ISO/IEC 27001:2013 in vigore.
Criteri da adottare per la Certificazione	Ai fini della integrazione di un certificato ISO/IEC 27001 esistente, a fronte delle Linee Guida ISO/IEC 27017 e ISO/IEC 27018, valgono i seguenti criteri: a. L'estensione può essere garantita solo dopo una verifica che dovrà essere eseguita presso il sito/i siti interessati dell'organizzazione. b. Se l'organizzazione è già in possesso di una certificazione ISO/IEC 27001, emessa dallo stesso CAB e con uno scopo di certificazione compatibile con i processi coperti dalle Norme ISO/IEC 27017 e 27018, l'audit di estensione sarà condotto in un'unica fase, integralmente svolta presso la sede dell'organizzazione. La durata dell'audit di estensione dovrà essere di almeno il 30% del tempo di audit di un rinnovo di certificazione ISO/IEC 27001 (tempo necessario all'audit di ogni linea guida), con una durata minima di una giornata per il sito principale e mezza giornata per ogni sito interessato dall'estensione. c. Se l'organizzazione è in possesso di altra certificazione ISO/IEC 27001 sotto MLA, dovrà richiedere il tasferimento della stessa al CAB accreditato ACCREDIA, per consentire l'emissione del certificato integrato. d. Se l'organizzazione non è già in possesso di una certificazione valida e riconosciuta sotto accreditamento per la Norma ISO/IEC 27001, l'audit sarà svolto secondo i criteri di una nuova certificazione a fronte delle Norme ISO/IEC 27001, con l'aggiunta per la 27017 e 27018 di un incremento minimo del tempo di audit non inferiore al 30% del tempo per una prima certificazione ISO/IEC 27001 (tempo necessario per ogni linea guida; quindi per

	due linee guida il tempo sarà il doppio) e, comunque, non inferiore a un giorno per il sito principale e mezza giornata per ogni sito aggiuntivo campionato. e. Per le sorveglianze, si applica sempre l'aumento di almeno mezza giornata per il sito principale e mezza giornata per ogni sito campionato, per linea guida. f. Le modalità di auditing dovranno sempre prevedere la registrazione delle evidenze necessarie a garantire la completa ed esaustiva applicazione sia dei requisiti della Norma ISO/IEC 27001, sia dei requisiti aggiuntivi pertinenti alle Norme ISO/IEC 27017 e 27018. Prima del rilascio della certificazione devono essere verificati tutti i data center presso cui sono dislocati i server che gestiscono il cloud. Estensioni incrementali: Ove l'organizzazione richieda l'estensione della certificazione alle due Norme ISO/IEC 27017:2015 e ISO/IEC 27018:2014 separatamente, l'iter deve prevedere che la prima estensione sia alla Norma (linea guida) ISO/IEC 27017. Non è ammessa l'estensione alla Norma (linea guida) ISO/IEC 27018:2014 senza il supporto della ISO/IEC 27017:2015. Audit di sorveglianza e rinnovo: Tali audit saranno condotti sempre su tutte le Norme (linee guida) applicabili di estensione alla ISO/IEC 27001:2013 assieme, prevedendo: Sorveglianza: un incremento minimo del tempo di audit non inferiore al 30% del tempo di una sorveglianza (tempo necessario all'audit di ogni linea guida, pertanto per due linee guida il tempo aggiuntivo sarà almeno due volte il 30%) e non inferiore a mezza giornata per ogni sito aggiuntivo campionato. Rinnovo: dovrà prevedere un incremento minimo del tempo di audit non inferiore al 30% del tempo di una ricertificativa (tempo necessario all'audit di ogni linea guida, pertanto per due linee guida il tempo aggiuntivo sarà almeno due volte il 30%) e una mezza giornata per ogni sito aggiuntivo campionato.
Data Cernter in Outsourcing	Se i Data Center utilizzati per le attività "cloud" sono in outsourcing presso fornitori in possesso di certificazioni ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 accreditate e riconosciute a livello MLA si potrà evitare di aggiungere tempo di audit presso tali siti. In tutti gli altri casi, dovranno essere aggiunte tante mezze giornate quanti sono i siti in outsourcing da verificare "de visu". Nel caso di siti ove non fosse possibile svolgere un audit diretto (es. fornitori come AWS, AZURE), dovrà essere utilizzata presso il sito centrale mezza giornata aggiuntiva, per la valutazione degli aspetti contrattuali e di controllo operativo con tali fornitori. Questo ultimo requisito è applicabile solamente nel caso di Data Center in possesso di certificazioni TIER III o TIER IV.

Criteri di competenza del Gruppo di Verifica dell'OdC	All'interno del gruppo di verifica devono essere disponibili queste competenze, facenti capo ad una persona singola, o al Team nel suo complesso: • auditor ISO/IEC 27001:2013, con esperienza specifica di audit nella ISO/IEC 27001 di almeno 5 anni, preferibilmente in possesso di certificazione professionale. • ovvero auditor ISO 20000-1:2012, con esperienza specifica di audit nella ISO/IEC 20000 di almeno 5 anni, preferibilmente in possesso di certificazione professionale. Deve inoltre essere data dimostrazione della conoscenza delle norme ISO/IEC 27017 o ISO/IEC 27018.
Criteri di competenza del Decision maker	Per almeno un membro dell'Organo di Delibera è richiesta agli Odc la dimostrazione della: • Qualifica come ispettore ISO/IEC 27001, rilasciata in conformità alla ISO/IEC 27006 • Conoscenza delle norme ISO/IEC 27017 o ISO/IEC 27018
Certificato	Deve fare sempre riferimento alla Norma ISO/IEC 27001 citando l'utilizzo della linea guida ISO/IEC 27017 o ISO/IEC 27018 nella sua applicazione. Devono essere indicati i prodotti / servizi / applicazioni / processi coperti dalla certificazione.
Documenti IAF e EA	Si applicano tutti i documenti IAF ed EA in vigore per lo schema ISO/IEC 27001.

2) Processo di Accreditamento ACCREDIA

Si potranno presentare diverse casistiche, in base agli accreditamenti ACCREDIA già posseduti dall'Organismo di Certificazione che presenta la domanda di accreditamento o estensione.

Rimangono invariati i prerequisiti previsti dal RG-01 ed RG-01-01 per la concessione dell'accreditamento ed estensione.
Per organismi già accreditati ISO/IEC 27001 con ACCREDIA, non occorre che questi abbiano già rilasciato dei certificati in questo schema per fare domanda di estensione dell'accreditamento.

Il certificato di accreditamento non riporta settori di accreditamento.

Nel caso in cui l'OdC possegga già accreditamenti rilasciati da altri enti di accreditamento, dovrà essere fatta una valutazione caso per caso, in base agli accordi EA / IAF MLA applicabili.

A	OdC già accreditato per lo schema ISO/IEC 27001	Esame documentale di 1 giornata. 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni scelte per l'accompagnamento ai fini del processo di accreditamento e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
B	OdC non accreditato ISO/IEC 27001	Occorre accreditarsi ISO/IEC 27001

Documentazione da presentare ad ACCREDIA per l'esame documentale

- Lista di riscontro o linea guida o istruzioni predisposte dall'OdC per il GVI;
- Curricula degli ispettori e dei Decision Maker
- Modulo del Rapporto di Audit;
- Attestato/Certificato rilasciato dall'OdC;
- Lista dei certificati già emessi, e delle prossime attività di verifica (nel caso sia necessario condurre una verifica in accompagnamento)
- Procedure / regolamenti contrattuali applicabili al processo di valutazione, nonché le procedure interne per la gestione della pratica di certificazione;
- Per gli OdC NON accreditati ISO/IEC 17021, oltre ai documenti sopra riportati, occorre inviare la documentazione richiesta nella domanda di accreditamento.

3) Mantenimento dell'Accreditamento

Per il mantenimento dell'accreditamento, durante l'intero ciclo di accreditamento, salvo situazioni particolari (Es: gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo…), verranno condotte le seguenti verifiche:

- Verifica in sede:
  - 1 giornata ogni anno per organismi accreditati ISO/IEC 27001 con ACCREDIA

- Verifica in accompagnamento da svolgersi nel ciclo di accreditamento:
  - se l'OdC ha emesso meno di 50 certificati nello schema di certificazione, deve essere effettuata una verifica in accompagnamento ogni 4 anni
  - se l'OdC ha emesso tra 51 e 200 certificati nello schema di certificazione, devono essere effettuate 2 verifiche in accompagnamento
  - se l'OdC ha emesso più di 201 certificati nello schema, devono essere effettuate 3 verifiche in accompagnamento

Rimaniamo a disposizione per chiarimenti e con l'occasione porgiamo i nostri migliori saluti.

Dott. Emanuele Riva
Direttore Dipartimento
Certificazione e Ispezione