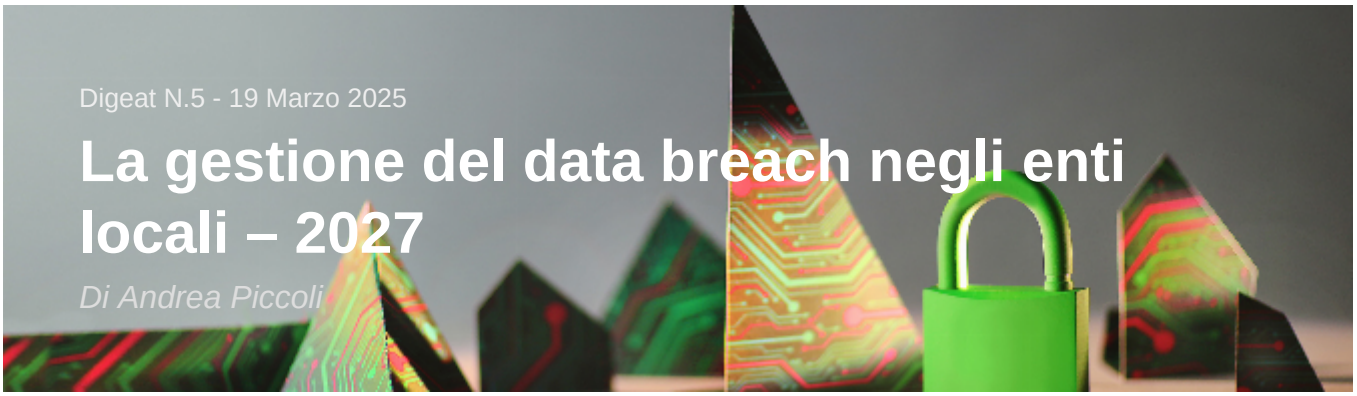

Digeat N.5 - 19 Marzo 2025

La gestione del data breach negli enti locali – 2027

Di Andrea Piccoli

Rubrica: Gestione documentale 2027

Abstract

Il quinto articolo di questa rubrica accoglie alcune riflessioni sulla gestione della sicurezza e della protezione dei dati negli enti locali a valle delle migrazioni cloud dei progetti MC1.1 misura 1.2. Si tratta di un tema centrale per la convergenza di alcune tra le principali strategie nazionali contenute rispettivamente nel Piano Triennale della Pubblica Amministrazione, nella Strategia Cloud Italia, nelle azioni dell'Agenzia Nazionale per la Cibersicurezza e relativo CSIRT nazionale. Tuttavia, ad oggi sono poche le amministrazioni che hanno approfittato dell'occasione per mettere mano alla trasformazione dei propri processi in chiave digitale, affrontando anche le necessarie modifiche organizzative e operative.

Indice

Le migrazioni al cloud

Il tema della migrazione dei servizi delle pubbliche amministrazioni al cloud è stato al centro della convergenza tra il **Piano Triennale della Pubblica Amministrazione**, la **Strategia Cloud Italia**, le **azioni dell'Agenzia Nazionale per la Cibersicurezza** e relativo **CSIRT nazionale**.

Attraverso la spinta economica e la visione strategica realizzativa dei finanziamenti della misura MC1.1 del PNRR, in particolare degli avvisi 1.2 cloud, accompagnata dalla capillare presenza sul territorio del **Trasformation Office del Dipartimento della Trasformazione Digitale**, le amministrazioni locali sono state stimolate ed accompagnate nella migrazione al cloud dei propri servizi.

La classificazione dei servizi con dati ordinari, critici e strategici, operata secondo i **cataloghi dei servizi** delle diverse tipologie di pubbliche amministrazioni, ha semplificato la gestione della corrispondenza tra i rischi per i diritti degli interessati e i requisiti minimi di sicurezza per la qualificazione dei servizi.

Tuttavia, **i data breach continuano ad essere frequenti** e con impatti significativi per i diritti degli interessati: c'è da chiedersi se, compiute le migrazioni al cloud finanziate, **un ente locale possa sentirsi al sicuro** da eventi di questo tipo e quale sia il **grado di consapevolezza** sulle attività di

gestione delle criticità a fronte di un data breach.

Adeguatezza e qualificazione: tutto sicuro e protetto?

Nella larga maggioranza dei casi, le pubbliche amministrazioni locali hanno effettuato le migrazioni al cloud con gli stessi fornitori dei diversi applicativi che usavano localmente o in cloud non qualificati. Da un lato, poche sono le amministrazioni che hanno approfittato dell'occasione per **mettere mano alla trasformazione dei propri processi in chiave digitale**, affrontando anche le necessarie modifiche organizzative e operative; dall'altro, i fornitori delle soluzioni e servizi cloud hanno offerto una evoluzione tecnologica architetturale, ma pochi interventi in ambito di trasformazione in digitale dei procedimenti e delle attività amministrative.

> Ad evidenza di questo, basti ricordare che la gestione documentale, intesa come gestione dell'archivio digitale dell'ente, non è nemmeno presente come servizio classificato nel catalogo, che si limita ad un timido Protocollo e ad una Produttività Individuale e Conservazione.

Inoltre, come conseguenza dei meccanismi di classificazione dei servizi nei piani di migrazione e per la struttura conseguente degli avvisi 1.2 cloud, le migrazioni su soluzioni qualificate e infrastrutture adeguate sono nella maggioranza dei casi parziali, vale a dire che **non hanno migrato tutte le applicazioni e infrastrutture su cui l'ente locale tratta i dati**. La limitata interoperabilità tra le soluzioni, la mancata trasformazione in digitale dell'organizzazione e della operatività ha comportato spesso la scelta di migrare al cloud le medesime soluzioni che erano già in uso, limitando la scelta a soluzioni e servizi che non presentassero problemi rispetto all'ammissibilità della migrazione finanziata.

> La percezione diffusa, negli RTD e referenti IT delle singole amministrazioni locali, è che quanto migrato al cloud sia sicuro e garantisca la protezione dei dati personali trattati: una sorta di "scudo contro qualunque evento". Una equazione, una convinzione pericolosa che "adeguato e qualificato" sia uguale a "sicuro e protetto".

Chi si occupa di sicurezza e di protezione dei dati personali, chi segue i modelli di gestione per la sicurezza e protezione delle informazioni, sa che **tale uguaglianza è in realtà asintotica**, ossia guidata dalla valutazione dei rischi, ove il rischio nullo non esiste.

Manca spesso, da parte dei referenti degli enti locali, la consapevolezza dei livelli di servizio, delle misure di sicurezza contrattualizzati con i fornitori, il livello di supporto e risorse messe a disposizione da parte del fornitore in caso di incidenti di sicurezza e di data breach. Inoltre, essendo lo **scenario infrastrutturale ibrido**, tra una parte di risorse locali e una parte di risorse cloud, l'esposizione verso la sicurezza e protezione dei canali di comunicazione è alta se non mitigata con adeguate misure e attività di monitoraggio continue.

La gestione della sicurezza e protezione dei dati nell'ente locale

Da sempre abbiamo condiviso che la gestione della sicurezza e della protezione delle informazioni richiede un **approccio multidisciplinare** all'interno dell'ente e che, essendo un argomento complesso, non può essere delegato o assegnato all'esterno.

> L'RTD dell'ente è chiamato ad un ruolo manageriale di coordinamento tra le figure che più hanno impatto sugli aspetti funzionali e organizzativi e quelle tecniche coinvolte nella evoluzione e conduzione delle soluzioni applicative e dell'infrastruttura informatica.

Il punto di riferimento, l'apporto di vigilanza e accompagnamento, deve essere svolto dal DPO che deve, con **un approccio consulenziale e di controllo,** aiutare a tracciare e attuare il percorso di miglioramento continuo nella **mitigazione dei rischi** nei trattamenti dei dati. Scegliere il DPO deve essere un elemento di **visione strategica** e non legato ad un semplice assolvimento di un obbligo basando la scelta alla miglior offerta o cercando, peggio, di assegnare al DPO ruoli e responsabilità non pertinenti, cercando di risolvere il problema della sicurezza e protezione dei dati da assegnare ad una "divinità factotum" esterna.

Il **registro dei trattamenti**, uno dei pochi obblighi del GDPR, non deve essere vissuto come un mero adempimento, ma come prima evidenza del censimento dei processi e procedimenti in cui l'ente tratta i dati personali, individuando per ciascuno di essi quali asset dell'infrastruttura tecnica e applicativa dell'ente vi sono coinvolti. Nel caso di servizi cloud esterni, andando oltre ai temi di nomine previste dal GDPR ci si deve assicurare, anche contrattualmente, la disponibilità di risorse e informazioni tempestive per la gestione degli incidenti.

Le **norme NIS 2[1]** e le valutazioni conseguenti di ACN, che si applicano solo a determinate categorie di enti che offrono servizi essenziali o di dimensioni rilevanti[2], offrono una linea guida che pone al centro **la gestione del rischio per la sicurezza delle informazioni** e le conseguenti misure di sicurezza adeguate e un modello organizzativo idoneo alla gestione e notifica degli incidenti in modo reattivo.

La valutazione dei rischi per la sicurezza e protezione delle informazioni può essere condotta a partire dal censimento delle basi dati più critiche per la rilevanza delle informazioni trattate ed individuando le possibili minacce, ovvero possibili cause di eventi avversi, che possono portare ad incidenti, valutandone la probabilità e l'impatto. Gli strumenti di ENISA, ed in particolare anche le regole per il miglioramento della cybersicurezza, sono un valido punto di riferimento[3].

Il tema delle misure di sicurezza diviene, quindi, un punto di attenzione conseguente alle valutazioni di rischio per la sicurezza delle informazioni.

Il primo punto di attenzione deve essere posto alle tematiche di **connettività e di sicurezza** delle comunicazioni e alla adeguatezza del parco applicativo, controllando, rispetto ai bollettini del CSIRT nazionale,[4] eventuali aggiornamenti da effettuare.

> Le attività costanti di monitoraggio della infrastruttura ibrida, comprensiva della connettività, e delle soluzioni sono fra le misure di mitigazione degli impatti di possibili incidenti per la sicurezza e protezione dei dati personali. La prima cosa da fare rispetto ad un *data breach* è accorgersi che è avvenuto o che è in corso!

La **formazione del personale** è sicuramente uno degli aspetti più importanti per la conduzione delle misure di sicurezza, sia per indirizzare una corretta gestione dell'utilizzo degli strumenti informatici sia per prevenire la diffusione di attacchi provenienti da posta elettronica o altre comunicazioni malevoli.

Conclusioni

I punti fondamentali da ricordare sono:

- Cloud qualificato non vuol dire assolutamente sicuro
- La prima misura di sicurezza è la consapevolezza che si matura a partire dall'analisi dei rischi.
- La sicurezza non è un problema tecnico, serve un approccio multidisciplinare
- La sicurezza e protezione delle informazioni hanno molto in comune

---

NOTE

[1] NIS – Network Information Security – ACN

[2] Ambito – ACN

[3] New rules to boost cybersecurity of EU’s critical entities and networks | Shaping Europe’s digital future

[4] Alert e Bollettini – ACN