ARTICOLO

Conservatori elettronici, terremoto in vista: ma accreditarli è stato utile, ecco perchè

Riccardo Bianconi – Ispettore ACCREDIA

Il Codice dell'Amministrazione Digitale apre la strada a una rivoluzione del processo di accreditamento dei conservatori elettronici e crea uno scenario al momento incerto.

La scelta del Legislatore di introdurre la figura del conservatore accreditato di documenti informatici si è rivelata utile.

È ormai passato circa un anno dalla pubblicazione dello schema di accreditamento degli Organismi di certificazione destinati a certificare i cosiddetti conservatori di documenti informatici, ai sensi dell'art. 29, comma 1, del Decreto Legislativo n. 82 del 7 marzo 2005.

Tale attività fu richiesta pressantemente da AgID ad Accredia in risposta alla richiesta tassativa presente nel Decreto Legislativo n. 179/2016, che ne prevedeva esplicitamente l'attuazione, garantendo anche la conformità all'art. 24 del Regolamento UE n. 910/2014 "eIDAS".

Lo schema è stato pensato fin da subito come strumento per offrire fiducia sia a fronte del rispetto dei livelli di servizio dei conservatori, sia, in modo ancor più significativo, per fornire fiducia alla Pubblica Amministrazione e ai cittadini tutti sulla robustezza delle infrastrutture ICT deputate allo svolgimento di tale processo.

Non si può ignorare, infatti, che già oggi e sempre più nel futuro i conservatori di documenti informatici avranno la responsabilità di garantire una vera e propria "resilienza" nei confronti di tutte le minacce che insistono sulla propria infrastruttura e, di riflesso, sui servizi offerti.

Ciò significa che un conservatore deve avere una particolare attenzione alla capacità della propria infrastruttura e della organizzazione che la governa, di rispondere agli effetti delle minacce che insistono su tale "macchina operativa" in modo adeguato e coerente con i Service Level Agreement (SLA), ovvero gli accordi sul livello del servizio, definiti sia contrattualmente, sia per legge.

Quindi, dovranno essere garantite la disponibilità, l'integrità e l'accessibilità dei dati e delle informazioni che questi materializzano.

Parlare di "resilienza" è sia tecnicamente corretto, sia un riferimento giuridico applicabile. Infatti, la conservazione dei documenti informatici sarà rivolta anche alle informazioni di privati cittadini, talora dati sensibili, che in quanto "persone interessate" si attenderanno legittimamente l'applicazione del Regolamento UE n. 679/2016 in merito alla Protezione dei Dati Personali (GDPR).

Lo stesso Regolamento, all'art. 32 cita proprio la caratteristica della "resilienza" quale fattore di qualificazione dei trattamenti dei dati e quale responsabilità afferente all'ambito della cosiddetta *accountability* di coloro che, in quanto conservatori, dovranno sentirsi e ritenersi coinvolti a pieno titolo nel processo di trattamento di tali dati e conseguenti informazioni.

Anche la Direttiva NIS riporta il concetto di resilienza, che ormai appare destinato a contenere e sostanziare quello di sicurezza delle informazioni e di capacità di garantire la sopravvivenza di un'attività istituzionale o d'affari, conglobando a pieno diritto i principi di continuità operativa e capacità di ripristino dei dati e relative informazioni.

In questo periodo è in corso l'ennesima revisione del Codice dell'Amministrazione Digitale, che fa tabula rasa del processo di accreditamento così come lo conosciamo, e rinvia a linee guida future per definire come sarà il nuovo processo.

Ecco perché vale la pena di trarre le somme di un anno di attività, nata in sordina e piano piano cresciuta, sulla base delle indicazioni cogenti del processo di certificazione, indicate dalla stessa AgID al mercato dei conservatori.

Oggi, il drappello di conservatori a norma già in possesso di una certificazione di conformità ai requisiti definiti da AgID e riportati nello schema di accreditamento può essere considerato un campione significativo di tutti i conservatori esistenti e i dati e le analisi condotte su tale processo hanno un significato che va oltre il mero parere personale di chi scrive.

Qualcuno, sulla scorta di dicerie o di pregiudizi culturali, magari alimentati da altre esperienze di certificazione, che nulla hanno a che vedere con l'argomento qui trattato, potrebbe essere portato a pensare che questo processo (accreditamento e certificazione) sia stato solo un orpello burocratico.

Oggi possiamo dimostrare l'utilità e il grande valore che garantisce la certificazione accreditata da Accredia del processo di conservazione di documenti informatici a norma di legge.

Per esercizio e per opportuna rendicontazione abbiamo fatto una sintesi delle molteplici anomalie riscontrate nei processi di certificazione condotti dagli Organismi di certificazione accreditati sui processi gestiti dai conservatori a norma.

Di seguito una sintesi – davvero ridotta all'essenziale, senza riferimenti e con il testo dei rilievi estremamente sintetizzato – di tali aree di debolezza, talora anche significativamente ripetitivi.

Tipo di Risultanza di Audit	**Area della Risultanza di Audit**
Non Conformità maggiori	Valutazione dei rischi non attendibile
	Mancata configurazione "firewall" protezione rete conservazione
	Assenza di procedure di test dei Controlli Operativi
	Debole gestione accessi e/o Password
	Mancata definizione dei piani di cessazione del servizio
Non Conformità minori	Gestione Log di sistema
	Gestione incidenti informatici e gestione "problem"
	Debole processo di Audit Interno. Talora per debolezza metodologica, frequenza a fronte del tipo di rischio gestito dal Controllo Operativo. Talora per inconsistenza degli stessi Audit (check list crocettate…)
	Lacune nelle Politiche, in primo piano quella sulla terminazione del servizio
	Lacune sulla definizione di ruoli e responsabilità per i diversi processi e attività, anche con rispetto ai vincoli di AgID
	Gestione molto carente dei fornitori: • Scarsa o assente definizione SLA • Mancata definizione requisiti di BC e DR, tra cui mancata definizione RTO e RPO • Mancata richiesta tassativa di piani di BC e DR • Mancata (in toto) definizione o specificazione requisiti sicurezza IT • Mancata disponibilità di VA e PT per Outsourcee • Mancata indicazione contrattuale del diritto di Audit
Raccomandazioni	Carenze minori nella valutazione dei rischi (metodo, metriche, azioni conseguenti alla definizione dei criteri di mitigazione, mancata approvazione dal Borad del Rischio Residuo, mancata documentazione di fasi della valutazione…)
	Debole pianificazione dei test sui piani di BC e DR, in particolare debolezza nelle procedure di test sul "restoring" dei dati, pur previsto dai piani di DR.
	Audit Interni sia internamente, sia verso fornitori anche critici
	Definizione processo gestione dei dati personali, anche sensibili…, mancata pianificazione azioni per allineamento GDPR
	Debole qualifica e monitoraggio fornitori (vedi sopra, con minore intensità)
	Mancato aggiornamento Piani di Sicurezza, nonostante modifiche intercorse dalla loro consegna ad AgID
	Carenza (estenuante) nella descrizione progettuale del sistema di gestione interno (aspetti documentali sulla progettazione del sistema di gestione interno)
	Allocazione privilegi di accesso alla infrastruttura fisica e logica
	Mancata segmentazione della rete di conservazione
	Gestione Log, compresi i Log dei backup

Le informazioni riportate nella tabella non devono far pensare ad un sistema che non funziona, sarebbe una valutazione non giusta e neanche veritiera.

Ci sono conservatori che hanno dimostrato infatti una professionalità e un'attenzione sin da subito eccellenti, tanto da non ricevere alcun rilievo, se non delle raccomandazioni e forse neanche quelle. Ce ne sono altri, per la verità, che grazie all'operato degli Organismi di certificazione hanno avuto la possibilità di riscontrare oggettivamente l'esistenza di Non Conformità, anche maggiori (bloccanti il processo di certificazione, sino alla loro risoluzione).

Proprio grazie a queste risultanze, tali conservatori hanno potuto fare delle riflessioni e irrobustire sia la propria infrastruttura, sia la propria organizzazione, sia il proprio processo decisionale. Un risultato di altissimo valore, se si pensa che, essendo già entità accreditate e operative, avevano delle carenze tali da mettere a repentaglio la sicurezza del processo di conservazione.

Considerando che il processo di conservazione di documenti informatici a norma è un processo governato prima ancora che dalle norme tecniche dalle leggi cogenti, il verificarsi di perdite di dati o di crepe sulla riservatezza o sull'integrità di tali dati/informazioni, magari sensibili per il cittadino, rappresenta, prima ancora che un problema tecnico, economico o gestionale un rischio elevatissimo soprattutto in area "Compliance", quindi in primo luogo "reputazionale". In questa chiave vanno letti i provvedimenti di legge, a partire dalla Legge n. 547 del 1993, fino alle più recenti modifiche apportate al Codice Penale dalla Legge n. 48 del 2008, con le correlazioni previste al Decreto Legislativo n. 231/01.

Alla luce di quanto esposto, si ritiene di poter tracciare un bilancio positivo di questo processo di valutazione e certificazione, svolto dagli Organismi di certificazione che operano con l'accreditamento di Accredia.

Si ritiene che la scelta operata dal Legislatore nel 2016 si sia dimostrata lungimirante e appropriata, ma soprattutto "economicamente utile" e non una sovrastruttura burocratica da dover abbandonare sulla base del recente, ma importante mantra della "semplificazione". Infatti, "semplificare" significa elidere a buon diritto, ciò che è ridondanza burocratica e che genera spese e non costi tipici di un investimento.

Elidere spese superflue è un dovere di chi governa. Anche indirizzare dei costi utili a rendere robusta, resiliente ed efficace una infrastruttura critica nazionale, come può essere considerata quella della conservazione è un atto altrettanto doveroso. Non ultimo, alla luce delle evidenze che queste pagine si sforzano di documentare.

***Accredia** è l'Ente unico nazionale di accreditamento designato dal Governo italiano. Il suo compito è attestare la competenza, l'imparzialità e l'indipendenza di Laboratori e Organismi che verificano la conformità di prodotti, servizi e professionisti agli standard di riferimento, facilitandone la circolazione internazionale e garantendo la protezione di interessi pubblici come salute, sicurezza e ambiente.*

Accredia è un'associazione privata senza scopo di lucro che opera sotto la vigilanza del Ministero dello Sviluppo Economico e svolge un'attività di interesse pubblico, a garanzia delle istituzioni, delle imprese e dei consumatori.

Accredia ha 67 soci che rappresentano tutte le parti interessate alle attività di accreditamento e certificazione, tra cui 9 Ministeri (Sviluppo Economico, Ambiente, Difesa, Infrastrutture e Trasporti, Interno, Istruzione, Lavoro, Politiche Agricole, Salute), 7 Enti pubblici di rilievo nazionale, i 2 Enti di normazione nazionali, UNI e CEI, 13 organizzazioni imprenditoriali e del lavoro, le associazioni degli organismi di certificazione e ispezione e dei laboratori di prova e taratura accreditati, le associazioni dei consulenti e dei consumatori e le imprese fornitrici di servizi di pubblica utilità come Ferrovie dello Stato ed Enel.

L'Ente è membro dei network comunitari e internazionali di accreditamento ed è firmatario dei relativi Accordi di mutuo riconoscimento, in virtù dei quali le prove di laboratorio e le certificazioni degli organismi accreditati da Accredia sono riconosciute e accettate in Europa e nel mondo.

Articolo pubblicato su www.agendadigitale.eu del 14 novembre 2017