LA GOVERNANCE DELL'ICT: COME GESTIRE LA SICUREZZA NEL PROCESSO DI PROCUREMENT

Aldo Lupi (esperto di protezione dati personali e di progetti ad alta innovazione tecnologica.)

La situazione emergenziale ha costretto le pubbliche amministrazioni ad un repentino passaggio allo smart working: in pochi giorni, gli enti hanno dovuto allestire sistemi di connessione remota per la maggior parte del proprio personale, andando ben oltre le sporadiche connessioni remote attivate in passato per consentire il lavoro da casa.

Qualcuno è riuscito a reagire meglio di altri, grazie ad una infrastruttura già predisposta per gestire accessi remoti. Nella maggior parte dei casi, però, le soluzioni di fortuna implementate hanno dato la priorità all'operatività del personale, piuttosto che alla sicurezza delle infrastrutture e dei dati.

A qualche mese dal primo impatto, lo *smart working* ha rafforzato la sua diffusione tra gli uffici della pubblica amministrazione, ma spesso non si è alzata l'asticella alla voce "sicurezza". Questa **gracile resilienza** ha evidenziato tre aspetti importanti:

1. **Le soluzioni esistono e potrebbero garantire un efficace funzionamento dei servizi pubblici** anche in situazioni di emergenza: la continuità operativa, concetto nuovo introdotto dall'art. 50-bis del Codice dell'Amministrazione Digitale (ora paradossalmente abrogato) potrebbe essere concretamente applicabile.
2. **La pubblica amministrazione ha ancora una scarsa consapevolezza degli strumenti disponibili**, e soprattutto dei nuovi rischi di sicurezza che occorre fronteggiare per implementare soluzioni efficienti, efficaci e sicure.
3. **L'implementazione della sicurezza oggettivamente è un fattore costoso ed impegnativo**, ed il suo valore è spesso difficilmente quantificabile. Le organizzazioni poco lungimiranti non comprendono l'importanza di investire nella sicurezza, perché le minacce ad essa correlate sono poco conosciute e i costi di un eventuale incidente (sempre più probabile, nei contesti attuali) non sono adeguatamente valorizzati: basti pensare alle conseguenze di un sistema informatico completamente indisponibile a seguito della diffusione di un *cryptovirus*…

Si delinea una situazione piena di punti di domanda, di cui vanno capite le dinamiche per trovare delle risposte efficaci.

Un mondo difficile

Andando oltre la circostanza emergenziale, l'innovazione tecnologica della pubblica amministrazione è un contesto strutturato che presenta molti fattori, anche critici, di cui si deve tenere conto:

- **Tecnologia e normativa seguono percorsi diversi**. La prima è il risultato di una frenetica rincorsa all'innovazione, per garantire profitti e un ritorno degli investimenti fatti. La seconda deve necessariamente tenere conto di elementi estranei alle logiche economiche, come le evoluzioni sociali e i diritti umani. Per questo motivo, le soluzioni tecnologiche disponibili sul mercato vanno spesso ben oltre quanto permesso dalle normative vigenti. Un esempio lampante è dato dalla rilevazione delle impronte digitali: da molti anni sono disponibili sul mercato sistemi di accesso in grado di rilevare questi tracciati biometrici, ma la tutela dei diritti dei lavoratori ne impedisce l'utilizzo

nei normali contesti lavorativi (salvo rare eccezioni dettate dalla necessità di garantire l'accesso a zone "pericolose"). Neanche le iniziative normative volte a combattere il fenomeno dei "furbetti del cartellino" è riuscito ad andare oltre il principio di salvaguardia dei diritti inalienabili dell'uomo. Un altro esempio: diversi "termoscanner" adottati da molte pubbliche amministrazioni per controllare gli accessi agli uffici offrono molte funzionalità avanzate di riconoscimento biometrico, che però sono inutilizzabili poiché confliggono con i limiti dettati dalla protezione dei dati personali.

- **Spesso la tecnologia utilizzata dalla PA nasce per altre finalità**. Le necessità operative spingono talvolta le pubbliche amministrazioni a reperire sul mercato soluzioni e strumenti nati originariamente per altre finalità, che poi si rivelano difficilmente adottabili nei nuovi contesti. Ad esempio, il contrasto al fenomeno dell'abbandono dei rifiuti ha portato molte amministrazioni ad introdurre le "fototrappole", cioè dispositivi installati in zone a rischio per rilevare fotografie o video di potenziali trasgressori. Un aspetto ignorato dai più è che molte delle soluzioni disponibili sul mercato sono nate per l'osservazione faunistica: strumenti opportuni per rilevare la vita animale in zone selvagge, ma inadeguati dal punto di vista della sicurezza. Se si pensa che le immagini acquisite potrebbero costituire prove di reato penale, diventa essenziale garantire l'inaccessibilità delle immagini a soggetti non autorizzati (un aspetto sicuramente non contemplato in ambito naturalistico). Diventa quindi inderogabile conoscere approfonditamente le funzionalità delle soluzioni adottate.
- **L'essenziale è invisibile agli occhi**. Parafrasando "Il Piccolo Principe" di Saint-Exupéry, spesso sfugge la criticità di elementi fondamentali per la propria infrastruttura, la cui compromissione potrebbe portare danni rilevanti non solo per l'organizzazione ma anche per altri soggetti. Basti pensare alla casella di Posta Elettronica Certificata (PEC) istituzionale: quasi tutta la corrispondenza di una organizzazione passa da tale canale, che per la sua natura viene considerato come uno strumento di comunicazione attendibile. Funziona come una normalissima casella di posta - e come tale soggetta ad attacchi informatici - ma spesso non se ne cambia la password per non inficiare l'interoperabilità con il software di protocollo informatico. La sua violazione è pertanto un evento probabile, che potrebbe portare effetti nefasti: ad esempio, tempo fa alcuni criminali hanno veicolato attraverso PEC violate di enti pubblici messaggi contenenti false sanzioni per violazione al Codice della Strada, sfruttando l'attendibilità del mittente per inviare *malware* o altre minacce informatiche, colpendo molti malcapitati destinatari che hanno considerato credibili i messaggi ricevuti. Per non parlare del rischio sulla riservatezza delle comunicazioni che deriverebbe da un accesso non autorizzato.
- **Il** cloud **è una zona di frontiera, spesso inesplorata.** La razionalizzazione del patrimonio ICT, il consolidamento dei data center e l'adozione progressiva del paradigma del "cloud *computing*" rappresentano specifiche azioni trasversali della Strategia per la Crescita digitale del Paese. Questo terreno di confronto è nuovo per tutti, pubbliche amministrazioni e fornitori, che stanno prendendo gradualmente confidenza con questi nuovi strumenti di erogazione dei servizi. Si tratta però di contesti ancora poco conosciuti, che devono indurre a riconcepire ruoli, ambienti tecnologici e rapporti contrattuali. E se gli enti pubblici faticano a definire i perimetri di questo nuovo paradigma, i loro fornitori non sono da meno: la qualificazione AgID necessaria per erogare i servizi della PA è solo il primo passo nel lungo percorso che porta alla definizione di servizi cloud. Non è infrequente che i contratti "*on demand*" che regolano l'erogazione di servizi in cloud contengano ancora elementi tipici dei vecchi servizi "*on premise*", che si basano sulla logica delle licenze d'uso del canone di assistenza e manutenzione. Si tratta di impianti documentali inadeguati a rispondere alle necessità emergenti dal nuovo paradigma, che le PA devono comprendere e imparare a governare, per non essere sopraffatte dalle carenze contrattuali.

- **Il crimine organizzato ha un vantaggio competitivo.** C'è una spaventosa asimmetria informativa fra la conoscenza del web da parte degli attori istituzionali e di mercato rispetto a quella dei criminali, chiaramente a vantaggio di questi ultimi. Mentre quasi tutte le PA si stanno affacciando per la prima volta ai servizi on line in maniera strutturata, la rete è un terreno di caccia consolidato per quei soggetti che la sfruttano in maniera fraudolenta: si tratta spesso di organizzazioni che hanno costruito negli anni un *know-how* importante in tema di vulnerabilità dei sistemi informatici, con un livello di motivazione molto elevato. Il contrasto ai crimini sulla rete è una continua rincorsa contro soggetti che hanno più esperienza, risorse economiche e motivazioni: una lotta impari.
- **L'usabilità e la sicurezza sono concetti molto diversi.** Le APP e gli strumenti di conference e collaborazione costituiranno sempre di più lo spazio di confronto fra le pubbliche amministrazioni e i loro utenti: oltre alla APP IO, che sarà il punto di raccolta di informazioni e documenti per cittadini ed imprese, gli enti locali si doteranno di strumenti di interazione - sincroni e asincroni – per dialogare con la collettività. Come visto ai punti precedenti, queste nuove tecnologie hanno un grande potenziale ma riservano molteplici aspetti da regolamentare.

LE MISURE MINIME DI SICUREZZA ICT PER LE PA

In questo scenario poco rassicurante, l'Agenzia per l'Italia Digitale (di seguito AgID) sta operando ormai da diversi anni per fornire alle Pubbliche Amministrazioni degli strumenti finalizzati a diffondere la consapevolezza dei rischi che si corrono e ad implementare sistemi di sicurezza idonei a contrastare le minacce. Uno degli apporti più rilevanti in questo tema risale al 2017, anno in cui sono state emanate le **Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni**, una checklist di controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica. A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo **tre livelli di attuazione**.

a) **Minimo**: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.

b) **Standard**: è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.

c) **Avanzato**: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Le misure minime consentono alle amministrazioni di qualsiasi dimensione e complessità di verificare autonomamente la propria situazione e avviare un percorso di monitoraggio e miglioramento. Il più grande merito che si può riconoscere alle Misure Minime è quello di avere creato un linguaggio comune di confronto in tema di sicurezza, attraverso la definizione di un set di controlli presenti in tutti i principali framework di sicurezza cibernetica, dai *Critical Security Controls for Effective Cyber Defense* elaborati dal CSC (Center for Internet Security) al *Framework Nazionale per la Sicurezza Cibernetica* elaborato dall'Università La Sapienza.

Purtroppo, questo strumento ad oggi non sta avendo il successo che meriterebbe, non tanto per colpa di AgID quanto per la scarsa consapevolezza delle PA sul tema. Dalla loro emanazione sono passati oltre 3 anni, eppure le PA ancora faticano a misurare la propria infrastruttura tecnologica attraverso un set di regole concrete ed inequivocabili.

Il tema del "*cloud first*" e ciò che comporta

Nel frattempo, l'evoluzione del ICT e l'affermazione del paradigma del "*cloud first*" ha spostato il terreno di confronto fuori dall'ambiente autarchico del CED dei singoli enti, rendendo ancora più astratto il concetto di sicurezza. La "nuvola" ha portato i dati in una dimensione immateriale, localizzato in ambienti virtuali gestiti da soggetti terzi che di fatto sono destinati a diventare i depositari del patrimonio informativo della PA italiana.

AgID ha costruito un percorso di qualificazione per i soggetti pubblici e privati che intendono fornire infrastrutture e servizi Cloud alle Pubbliche Amministrazioni, definendo le caratteristiche organizzative, di sicurezza, di performance e scalabilità, interoperabilità, portabilità e conformità legislativa a cui dovranno uniformarsi.

Sia che si tratti di Infrastrutture (IaaS – *Infrastructure as a Service*), Piattaforme (PaaS – *Platform as a Service*) o di Software (SaaS – *Software as a Service*), gli attori che intendano erogare tali servizi alle PA devono conseguire un'apposita qualificazione rilasciata da AgID, che dovrebbe – il condizionale è d'obbligo – garantire il rispetto di determinati standard da parte dei fornitori.

LE LINEE GUIDA IN MATERIA DI SICUREZZA INFORMATICA NEL PROCUREMENT PUBBLICO

Pur ammettendo l'efficacia dell'intero percorso di qualificazione, mancherebbe ancora *l'ultimo miglio*, cioè la formalizzazione del rapporto contrattuale fra i fornitori e le Pubbliche Amministrazioni che fruiranno di questi servizi, le quali saranno tenute a utilizzarli monitorandone e amministrandone l'erogazione.

E questo è **il nuovo, cruciale, terreno di sfida**: le PA, infatti, dovranno passare da un contesto in cui la governance dell'ICT era tecnica ad una nuova fase, in cui **la governance diventa contrattuale**. Le professionalità che operano nell'ICT della PA devono cambiare pelle: se prima le competenze richieste erano di natura prevalentemente tecnica, adesso gli *skill* si devono posizionare sul controllo ponderato degli elementi contrattuali, che devono essere compresi in profondità.

Facciamo un banale esempio numerico: se la continuità di un servizio cloud su cui verranno localizzati elementi informativi critici viene contrattualmente garantita al 98% su base trimestrale, significa che sarà considerata ammissibile un'indisponibilità del servizio – anche continuativa - di oltre 40 ore a trimestre. Se portiamo tale soglia su scala annuale, il tempo di indisponibilità contrattualmente ammissibile sarà di oltre una settimana…

I soggetti deputati alla gestione dell'ICT dovranno prendere dimestichezza con questa nuova dimensione, in cui molti aspetti verranno interamente delegati al fornitore (ad esempio la gestione degli amministratori di sistema e al loro monitoraggio come previsto dal provvedimento del Garante Privacy del 2008) e l'unica forma di controllo sul buon funzionamento del sistema sarà la misura di livelli di servizio predefiniti (i famosi *Service Level Agreements* – SLA).

Ancora una volta AgID ha messo a disposizione uno strumento di supporto alle decisioni, adottando le **linee guida in materia di sicurezza informatica nel *procurement* pubblico finalizzato all'acquisto di beni e servizi informatici**. Le linee guida illustrano la tematica della sicurezza nel procurement ICT, formalizzando definizioni e concetti legati alla sicurezza ed instanziandoli al contesto della pubblica amministrazione, con l'obiettivo di costruire un processo di acquisizione coerente e finalizzato al governo della fornitura – dalle fasi preliminari di definizione delle necessità alle fasi successive all'acquisizione, attraverso il monitoraggio dei livelli di servizio e il controllo del rispetto delle condizioni contrattuali.

Il documento ha un taglio oggettivamente alto (basti pensare che al tavolo di lavoro per la sua redazione erano seduti AgID, CONSIP, 6 Ministeri e 2 Dipartimenti nazionali) e difficilmente applicabile nel contesto di una piccola/media amministrazione locale, però offre degli **spunti molto interessanti che possono essere adottati per implementare un efficace governo contrattuale delle forniture ICT**.

Le tipologie di contratti ICT vengono classificati, al paragrafo 1.1 nelle seguenti tipologie:

a) contratti di sviluppo, realizzazione e manutenzione evolutiva di applicazioni informatiche;

b) contratti di **acquisizione di prodotti** (hardware o software);

c) contratti per attività di *operation* e **conduzione** dei sistemi;

d) contratti per servizi diversi da a) e c) (es. **supporto, consulenza, formazione, help desk**, …);

e) contratti per forniture miste, combinazioni delle precedenti tipologie.

A seconda della tipologia di fornitura, il documento definirà dei parametri utili al governo del contratto che verrà stipulato con i fornitori.

Ma prima di analizzare questo aspetto, vale la pena di approfondire alcuni step organizzativi ed operativi utili illustrati nel documento.

La ricognizione delle risorse interne ICT

Il primo spunto dovrebbe essere già un *mantra* per gli ICT manager: **conosci te stesso**. Tra gli interventi da svolgere prima dell'acquisizione, l'azione AG4 prescrive di "*Effettuare una **ricognizione dei beni informatici e dei servizi***". Questa azione va ad affinare le prime due classi di controlli delle Misure Minime di Sicurezza ICT per le PA, cioè la tenuta dell'inventario dei dispositivi e dei software autorizzati e non autorizzati. Oltre alle risorse tecnologiche, la ricognizione si focalizza anche sui servizi erogati a cittadini ed imprese, in modo da evitare sovrapposizioni e gestire in maniera efficace eventuali esternalizzazioni presso infrastrutture tecnologiche di soggetti terzi. Non solo: per ogni risorsa inventaria andrebbe definito un "*owner*", cioè un soggetto a cui fa capo la responsabilità di garantire la sicurezza della risorsa.

Il tema dell'inventario delle risorse diventerà sempre più caldo, in virtù dell'immaterialità delle infrastrutture e delle risorse dati. Diventerà sempre più imprescindibile disporre di **un inventario strutturato dei dati trattati e delle architetture utilizzate per gestirli**. A queste risorse ne va aggiunta un'altra, che già ora corre un grosso rischio di frammentazione: **la documentazione portata in conservazione dagli enti**, destinata sempre più a disperdersi in perimetri esterni al dominio del protocollo informatico dell'ente. Senza un approccio organizzato il rischio di disperdere il proprio patrimonio informativo è destinato a crescere con la proliferazione delle soluzioni impiegate.

Le linee guida, inoltre, all'azione AG5 spingono per classificare beni e servizi sotto il profilo della sicurezza, valutandoli in termini di criticità, rischi, minacce, vulnerabilità. Nelle piccole amministrazioni tale valutazione potrà essere solamente di tipo qualitativo, mentre negli enti più strutturati il **tool di Gestione del Rischio implementato da AgID** potrebbe costituire un valido supporto: lo strumento si sta sempre più affinando, grazie al contributo delle PA che lo stanno utilizzando e che inseriscono contenuti "riutilizzabili" dagli altri enti per la definizione delle risorse e dei servizi da gestire. Il **meccanismo "partecipativo"** che permette di richiamare ed adottare i contenuti di altri consentirà di introdurre una **metrica comune** sugli elementi da valutare e semplificherà la prima (impegnativa) fase di caricamento. Il risultato, una volta a regime, andrà ben oltre gli obiettivi di definizione e valutazione delle risorse e dei rischi correlati, poiché consentirà di fissare

degli step di monitoraggio del rischio nel tempo e fornirà uno strumento di supporto alle decisioni per veicolare gli investimenti in sicurezza, massimizzando l'efficacia dell'azione di mitigazione dei rischi.

L'importanza delle competenze

Nelle linee guida si affronta in più punti il tema della competenza in tema di sicurezza, sia nella fase preliminare di definizione dei ruoli che fase di gestione del procedimento di scelta, evidenziando la necessità di avere nella commissione giudicatrice un **esperto di sicurezza**. A questo naturalmente si deve aggiungere un contributo nella fase di definizione dei requisiti che devono soddisfare la soluzione e il fornitore.

È inevitabile che nella fase ricognitiva ci si interfacci con i consulenti commerciali che lavorano per i *vendor* delle soluzioni presenti sul mercato, ma anche volendo riconoscere la massima onestà intellettuale di questi professionisti è sicuramente insufficiente basarsi solo sulle informazioni veicolate da loro.

Il tema è rilevante e va contestualizzato tenendo conto della complessità della soluzione che si deve reperire sul mercato.

Nei **casi più semplici** può essere sufficiente un **approfondimento esplorativo** sulle caratteristiche del servizio da acquisire.

Nelle **situazioni un po' più complesse** può essere molto utile confrontarsi con gli altri addetti del settore, che hanno già affrontato il tema e possono fornire importanti indicazioni di carattere tecnico e organizzativo. Importanti opportunità di confronto sono offerti dalle **comunità digitali tematiche** come ad esempio:

- Comuni Digitali - la community promossa da ANCI Lombardia in collaborazione con Regione Lombardia),
- OpenSIPA - la Comunità e l'Associazione dei Sistemisti Informatici della Pubblica Amministrazione),
- InnovatoriPA - la rete per l'innovazione nella Pubblica Amministrazione Italiana,

Oppure ci sono iniziative come i tavoli AgID dedicati al Responsabile per la Transizione al Digitale (RTD) o ancora come i Cantieri PA, laboratori permanenti di ForumPA dedicati ai temi dell'innovazione tecnologica e organizzativa della PA.

Quando invece la soluzione adottata possa presentare delle **criticità rilevanti in tema di sicurezza** o la **componente contrattuale** si riveli particolarmente **complessa**, conviene **ricorrere a professionisti esperti del settore** che possano accompagnare l'amministrazione nell'intero percorso di approvvigionamento, onde evitare l'acquisizione di prodotti inadeguati o l'impostazione di condizioni contrattuali inefficaci.

Audit e monitoraggio della fornitura

Le linee guida introducono, nell'azione AG6, il concetto di valutazione del fornitore in materia di sicurezza, attraverso la **definizione di audit** che dovranno essere svolti durante la durata del progetto e quindi preliminarmente definiti nei capitolati di gara.

Questo elemento è francamente complesso da sviluppare per una piccola/media amministrazione: è fondamentale monitorare l'efficacia delle azioni di sicurezza che il fornitore dovrebbe svolgere per proteggere le risorse gestite, ma nel concreto è difficile definire dei parametri da verificare periodicamente, perché la conoscenza dell'infrastruttura fornita è limitata e perché molte delle misure rilevabili sono messe a disposizione dal fornitore stesso. E' come chiedere all'oste se il vino è buono…

Un approccio percorribile è richiedere al fornitore l'**esistenza e la persistenza durante la durata del contratto dell'adozione di strumenti di mitigazione del rischio,** ricorrendo a delle metriche comuni che verranno analizzate nei paragrafi seguenti.

Anche il **Regolamento UE 2016/679** introduce all'**art. 28** la possibilità di effettuare ispezioni che consentano di verificare il rispetto delle misure di sicurezza da parte del fornitore. In alcuni servizi tale attività è più concreta, in altri più difficilmente realizzabile. A seconda della tipologia di servizio reso, si potranno definire dei parametri e dei vincoli documentali da verificare durante lo svolgimento della fornitura.

Azioni da implementare

Il cap. 2 delle linee guida approfondisce il percorso da svolgere per definire l'oggetto della fornitura e le leve su cui si potrà agire per governare contrattualmente gli elementi di sicurezza. Il paragrafo 2.3 nello specifico fornisce una *checklist* di azioni da implementare, in particolare:

- **Account management**, cioè la fornitura di utenze di accesso ai sistemi specificamente nominativi per i dipendenti del fornitore;
- Utilizzo di **dispositivi di proprietà del fornitore** per accedere a dati e reti dell'amministrazione;
- **Profilazione degli accessi** alla rete dell'amministrazione da parte del fornitore, con limitazione di accesso solamente alle risorse necessarie;
- Autorizzazione dell'**accesso esclusivamente ai server/database di competenza** per la fornitura del servizio previsto;
- Redazione di accordi di autorizzazione, riservatezza, confidenzialità;
- Verifica delle **misure di sicurezza** previste per forniture di sviluppo applicativo e/o manutenzione evolutiva;
- **Monitoraggio** delle **utenze** e degli **accessi** dei fornitori;
- **Verifica della documentazione** di progetto nella fase conclusiva di rilascio delle risorse.

Questa *checklist* è molto utile per la determinazione di una procedura, anche semplice, per impostare correttamente il rapporto con il fornitore e monitorarlo nel tempo.

Requisiti di sicurezza

L'**appendice A** delle linee guida fornisce la risorsa più utile di tutto il documento. In relazione alle tipologie di contratto definite al paragrafo 1 del documento (sviluppo applicativo, acquisizione di prodotti, conduzione di servizi/attività, servizi supplementari), le tabelle 8-11 definiscono dei requisiti di tipo tecnico-operativo che possono essere richiesti al fornitore per garantire un adeguato livello di sicurezza per il servizio reso.

La tabella 8 definisce dei requisiti generali indipendenti dalla tipologia di fornitura che possono essere istanziati e sviluppati a seconda del livello del servizio svolto: si entra nel dettaglio relativamente alle certificazioni richiedibili in tema di sicurezza dei dati, così come la presenza nell'organizzazione del fornitore di una struttura per la gestione degli incidenti informatici, o l'adozione di sistemi di sicurezza per l'adozione del rischio di attacchi informatici.

I requisiti indicati nelle tabelle successive (9-11) sono applicabili su specifiche tipologie di servizio e forniscono elementi su cui ragionare nel concreto, come le caratteristiche degli accessi sicuri nel caso di forniture di oggetti connessi in rete o la cifratura delle connessioni per i servizi di gestione remota.

Si tratta di elementi basilari, che comunque è utile trovarli raccolti a fatto comune.

La cassetta degli attrezzi

Per venire nel concreto, la governance di un contratto non può prescindere da alcuni elementi che dovrebbero essere garantiti nelle forniture. Fra questi:

- **Le Misure Minime di Sicurezza ICT per le PA**. Se le pubbliche amministrazioni sono tenute a rispettare i requisiti richiesti dalla circolare 2/2017 di AgID, in caso di esternalizzazione di questi servizi è del tutto plausibile trasferire questo obbligo verso i fornitori. E' corretto non solo richiedere in fase di fornitura una attestazione del loro livello di attuazione nel contesto di fornitura, ma anche richiedere una revisione annuale del documento previa liquidazione delle fatture.
- ***Vulnerability assessment e penetration test***. Nel caso di servizi erogati in rete (tutti i servizi in cloud, ad esempio), è necessario che tali servizi siano stati testati da soggetti esterni per valutare i rispettivi livelli di sicurezza. È corretto richiedere la prova documentale dell'effettuazione di *vulnerability assessment* e *penetration test* non precedenti agli ultimi 12 mesi.
- **Gestione degli incidenti**. Deve essere espressamente richiesta la comunicazione degli incidenti occorsi in un tempo ragionevole dal momento della scoperta, ad esempio 24 ore. Se possono sembrare poche, è doveroso ricordare che il titolare del trattamento ha l'obbligo di notificare al Garante della Privacy eventuali violazioni di dati entro 72 ore dalla scoperta. Imponendo l'obbligo di una prima segnalazione entro 24 ore, l'amministrazione si riserva 48 ore di tempo per valutare l'incidente e l'eventuale necessità della notifica. Un altro elemento importante è la valutazione della gravità dell'incidente, che non può essere lasciata in capo al fornitore. Il fornitore è tenuto a segnalare quanto è accaduto, la sua valutazione spetta inevitabilmente all'amministrazione, titolare del trattamento dati. Infine, la prima segnalazione spesso non è sufficiente: nei periodi successivi il dialogo tra committente e fornitore dovrà essere serrato ed esaustivo, al fine di implementare misure di sicurezza atte a prevenire incidenti futuri (o mitigarne il rischio di accadimento).
- **Monitoraggio del servizio reso.** E' importante definire dei parametri facilmente osservabili e classificabili per misurare l'adeguatezza del servizio fornito, che dipendono inevitabilmente dalla sua tipologia. Si possono misurare i tempi di risposta alle richieste, oppure gli interventi effettuati o altro. I sistemi di ticketing, in questi casi possono essere un ottimo supporto per misurare l'andamento del servizio.
- **Controllo degli amministratori di sistema** – sebbene sia un tema incluso nelle Misure Minime di Sicurezza ICT, il tema degli amministratori di sistema va trattato in maniera approfondita, specie per servizi erogati on line. E' buona norma richiedere l'elencazione periodica (anche con cadenza annuale) dei soggetti che agiscono come amministratori di sistema e un estratto dei log di accesso (anche per un ristretto periodo di tempo). Si tratta di dati la cui veridicità è difficilmente verificabile dal cliente, ma già il fatto di disporre di tali informazioni è sintomo dell'esistenza di una procedura concreta adottata dal fornitore.
- **Cifratura dei dati critici** – nel caso di servizi applicativi, è importante che il fornitore attesti la presenza di tecniche di cifratura dei dati ritenuti critici nelle proprie banche dati. Ad esempio, la password degli utenti non devono essere disponibili in chiaro sui sistemi, poiché la violazione di tali informazioni con conseguente perdita di riservatezza potrebbe costituire un gravissimo danno per gli utenti stessi. Anche in questo caso dovrebbe essere un requisito già presente nelle misure minime, ma è importante svolgere una specifica verifica documentale di tale aspetto.

LA NECESSITÀ DI FARE SISTEMA

Molti dei requisiti richiesti – nel contesto dei servizi cloud – rientrano nei requisiti che i fornitori che intendono fornire infrastrutture e servizi Cloud alle Pubbliche Amministrazioni devono garantire ad AgID nelle fasi di qualificazione.

In questo momento si tratta di semplici attestazioni di tipo documentale, la cui verifica è lasciata in capo alle amministrazioni che fruiranno dei servizi qualificati. È auspicabile che in futuro **le attestazioni siano soggette ad un monitoraggio concreto e periodico svolto direttamente dall'Agenzia**, in modo che i fruitori finali possano limitarsi a richiedere le attestazioni di qualificazione per disporre già di idonea documentazione comprovante l'esistenza di adeguate misure di sicurezza.

Ma in questa fase le incognite sono ancora molte, le amministrazioni devono quindi organizzarsi per spostare la governance dell'ICT dal perimetro tecnico a quello contrattuale, costruendo un corretto rapporto con coloro che tratteranno i loro dati.

Articolo pubblicato sul sito comunidigitali.it