UNITELMA SAPIENZA

InterLex FORUM20
LA CITTADINANZA DIGITALE

Due “certezze” necessarie nei rapporti con la pubblica amministrazione digitale:

la sicurezza dei documenti e il riconoscimento del cittadino.

UNITELMA SAPIENZA

InterLex FORUM20
LA CITTADINANZA DIGITALE

La sicurezza dei documenti

La sicurezza ICT nella pubblica amministrazione

Il documento informatico

- “caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità”.

- Sicurezza significa anche protezione dei dati personali, gestione dell’identità digitale e integrità e immodificabilità si ottengono all’interno di un sistema gestito in modo sicuro.

- Esistono standard consolidati per la valutazione e certificazione di un sistema di gestione per la sicurezza delle informazioni (ISO/IEC 27001).

- Ma la PA a quale livello può essere collocata in materia di sicurezza ICT e, inoltre, esistono dati “ufficiali” per effettuare una valutazione affidabile ?

La sicurezza ICT nella pubblica amministrazione

Stato dell'arte

- L'ultimo documento "ufficiale" e pubblico sullo stato della sicurezza ICT delle PAC (Pubbliche Amministrazioni Centrali) è del 2007 (pubblicato dal CNIPA nel marzo del 2009).

- Si tratta del "Secondo Rapporto sullo Stato della Sicurezza ICT delle PAC". Un terzo rapporto pur elaborato non è stato diffuso.

- Il lavoro si basava sul "*modello comune per la sicurezza*" elaborato dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) al fine di fornire un modello comune, sul tema, per la PAC.

- I dati forniti dalle PPAA erano in risposta ad un questionario.

La sicurezza ICT nella pubblica amministrazione

Stato dell'arte

- L'elaborazione dei dati riguardava la sicurezza logica, la sicurezza dell'infrastruttura, la sicurezza dei servizi e la sicurezza dell'organizzazione.

- Il questionario, che prevedeva solo risposte "chiuse" era composto di 55 quesiti.

- I risultati ottenuti hanno evidenziato una situazione "media" con adeguata attenzione alle problematiche di base (Es.: Antivirus, firewall, ecc.) e elementi da migliorare per l'organizzazione della sicurezza e la gestione dell'outsourcing della stessa.

- Anche il tema delle specifiche competenze risultava "da migliorare".

La sicurezza ICT nella pubblica amministrazione

Piano triennale 2017-2019

- Il vigente Pianno triennale dedica ampio spazio al tema della sicurezza.

- Viene dato un forte risalto al CERT-PA e alla necessità di potenziamento dello stesso per “strutturare” I piani di sicurezza delle pubbliche amministrazioni ma anche vigilare con azioni di monitoraggio e verifiche periodiche sull’attuazione dei piani.

- Ampio risalto anche al “Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico”.

- Sono attese per settembre 2017 le regole tecniche (Linee Guida ?) per la sicurezza ICT delle pubbliche amministrazioni.

La sicurezza ICT nella pubblica amministrazione

Misure minime sicurezza ICT

- Nel frattempo le PPAA devono adeguarsi entro la fine del 2017 a quanto stabilito nel documento AgID “Misure minime per la sicurezza ICT delle “*Pubbliche amministrazioni*”.

- Il documento fornisce indicazioni puntuali su come raggiungere livelli di sicurezza prefissati a partire da quello minimo, che è obbligatorio per tutti.

- E’ evidente un significativo impegno sulla sicurezza ICT. Ma tale impegno si ripropone, in fasi cicliche, senza che, ad oggi, ci sia una situazione stabile. Forse aiuterà l’applicazione del Regolamento UE sulla protezione dei dati personali (GDPR).

- Nel giro di 12 mesi si potrà valutare se qualcosa si muove nella giusta direzione ma soprattutto se AgID riuscirà a stabilizzare la situazione.

UNITELMA SAPIENZA

InterLex FORUM20
LA CITTADINANZA DIGITALE

Il riconoscimento del cittadino

Il riconoscimento del cittadino

CIE, CNS E SPID

- Il cittadino digitale deve operare in Rete avendo fiducia nel fatto che la sua identità è tutelata..
- L'identità digitale è stata sviluppata prima sulla Carta di Identità Elettronica (CIE). Poi sulla Carta Nazionale dei Servizi (CNS). Infine a partire dal marzo 2016 sul Sistema Pubblico di Identità Digitale (SPID).
- Naturalmente anche i PIN (password) sui servizi previdenziali e fiscali hanno contribuito alla proliferazione di credenziali personali.
- Al momento si "spinge" per lo sviluppo di SPID senza che si chiarisca il ciclo di vita delle altre citate credenziali.

Il riconoscimento del cittadino

CIE, CNS E SPID

- La CIE è nella cosiddetta fase 3.0 e con una certa fatica la sua emissione si sta ampliando all'intero territorio nazionale.

- Continua ad essere emessa la CNS nella sua forma associata alla Tessera Sanitaria (TS-CNS) che è anche Codice Fiscale e Tessera Europea di Assicurazione Malattia (TEAM).

- SPID conta su 7+1 (un soggetto sta completando le attività per l'inizio formale delle attività) gestori dell'identità digitale. E' presumibile che altri soggetti si affianchino ai soggetti già attivi soprattutto se verranno modificate le barriere di ingresso sul capitale sociale.

- Alla data del 30 agosto 2017 (dati AgID) le credenziali rilasciate sono 1.605.309.

Il riconoscimento del cittadino

CIE, CNS E SPID

- E’ evidente che la mancanza di soggetti privati tra I fornitori di servizi (lo schema di convenzione comunque è stato dichiarato da AgID in fase di pubblicazione entro settembre 2017) e la non reale e diffusa utilità e novità dei servizi delle PPAA non ha favorito la richiesta di credenziali.

- Dobbiamo anche aggiungere il fatto che non è ancora ufficialmente stabilito se le credenziali per I cittadini continueranno a essere gratuite nè è evidente il modello economico redditivo per I gestori dell’identità digitale. Questi, come è noto, sono soggetti privati.

- Le linee di azione dovrebbero chiarire quando e se SPID sarà l’unico sistema di identità digitale per I cittadini, le imprese e i professionisti.

Il riconoscimento del cittadino

CIE, CNS E SPID

- Per la CIE 3.0 si punta sulla possibilità di leggere il chip “senza contatti” della carta tramite I cellulari di recente sviluppo che dispongono di hardware adatto (tecnologia NFC).

- E’ attesa la pubblicazione del software di interfaccia per l’utilizzo della CIE 3.0 (annuncio del Team Digitale).

- In base a interventi pubblici del medesimo Team Digitale si può ragionevolmente ipotizzare che con le credenziali SPID si crei una nuova fattispecie di firma elettronica simile alla Firma Elettronica Avanzata (FEA).

- Il decreto correttivo al Codice dell’amministrazione digitale potrebbe contenere queste novità (decreto da pubblicare entro la metà di dicembre 2017).

Sicurezza e identità

Considerazioni finali

- Da quanto esposto si evince che siamo in una fase di apparente modifica della situazione “a regime”.
- In verità siamo di fronte all’ennesimo ciclo “ripetitivo” di cosa già viste ma, purtroppo, mai entrate in uno stato di stabilità permanente.
- Il raggiungimento di una sicurezza ICT “definitiva” è indispensabile.
- SPID affiancato da politiche di supporto chiare e da servizi indispensabili soprattutto dal mercato privato (banche, utilities, e-commerce, ecc.) può diffondersi rapidamente a condizione che le credenziali del cittadino siano permanentemente gratuite.