Contesto di riferimento

Nell'ambito del programma dell'*Agenda Digitale Italiana* – istituita nel 2012 – è prevista una azione infrastrutturale denominata *Digital Security per la PA* per tutelare la *privacy*, l'integrità e la continuità dei servizi della PA. Con Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri è stato affidato ad AgID – *Agenzia per l'Italia Digitale* – il compito di rendere disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte, al fine di agevolare il processo in esito del quale tutte le Amministrazioni rispondano, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici avversi.

In attuazione di tale DPCM, AgID ha provveduto ad emanare l'elenco ufficiale delle *Misure minime per la sicurezza ICT delle pubbliche amministrazioni* che, con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante *Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)*, sono divenute di obbligatoria adozione per tutte le Amministrazioni.

Le Misure, che si articolano sull'attuazione di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di compimento. Il livello minimo è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme entro il 31 dicembre 2017 (con produzione di un documento fornito di data certa). I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.[1]

Le misure sono raggruppate in 8 argomenti, per un totale di 121 item di cui 45 di livello minimo, 44 di livello standard e 32 di livello alto.

Dal **25 maggio 2018** ha inoltre avuto piena attuazione, dopo due anni dall'entrata in vigore, il regolamento generale per la protezione dei dati GDPR (General Data Protection Regulation) n. 679/2016. Il nuovo regolamento presenta un cambiamento sull'approccio della protezione dei dati ponendo l'accento sulla valutazione del rischio e sull'*accountability*, che coinvolge aspetti quali l'affidabilità e la competenza aziendale nella gestione dei dati personali.

In Gazzetta ufficiale n. 205 del 4 settembre 2018, è stato pubblicato il dlgs 10 agosto 2018, n. 101 (ai sensi dell'art. 13 della legge 25 ottobre 2017, n. 163 – legge di delegazione europea) recante disposizioni per adeguare la normativa italiana al GDPR, con riguardo unicamente alle materie in cui lo stesso GDPR prevede la competenza delle normative nazionali. Il decreto rappresenta il raccordo tra la normativa italiana e il GDPR, che disciplina il passaggio dell'ordinamento italiano della privacy (disciplinato sino ad ora dalla Dir 95/46/CEE e dal vecchio Codice della privacy, dlgs 196/2003) al nuovo Regolamento, stabilendo cosa resta in vigore e cosa viene abrogato.

Per quanto attiene alle misure tecniche previste dal GDPR, l'aderenza alle misure minime di sicurezza AgID di cui sopra da parte delle Aziende, deve essere viste come lo strumento necessario per dimostrare il rispetto dello stato dell'arte relativo alle componenti tecnologiche/informatiche.

Va sottolineato che il DPCM 1 agosto 2015 suddetto al capitolo *Misure rivolte alla amministrazione*, comma a. *il potenziamento della capacità di reazione*, recita *"A ciò si deve aggiungere l'impegno, nell'ambito di ciascuna Amministrazione, a provvedere affinché, nel quadro delle pianificazioni organizzative e finanziarie di competenza, siano destinate risorse umane e finanziarie adeguate agli assetti rivolti alla funzione della sicurezza cibernetica ed alla protezione informatica."*

Dall'analisi svolta internamente dalle Aziende del SSR sulla consistenza e sullo stato di funzionamento delle apparecchiature informatiche/telematiche (postazioni di lavoro/periferiche, dispositivi attivi di rete, dispositivi di telecomunicazione) è emersa la necessità di risorse aggiuntive sia in termini di **tecnologiche** (HW, sonde, apparecchiature, software etc.), **sia in termini di servizi e di risorse umane specializzate e qualificate.**

[1] Fonte AgID

Il *Piano Triennale per l'Informatica nella Pubblica amministrazione 2017–2019* realizzato da AgID e dal Team per la Trasformazione Digitale ed approvato dal Presidente del Consiglio dei Ministri in data 31 maggio 2017, identifica tra gli strumenti per l'attuazione del piano le iniziative CONSIP. Mediante l'attivazione di opportune convenzioni, partendo in primis da un ***assessment*, consente la stesura e realizzazione di un piano triennale di miglioramento continuo della sicurezza infomatica tenuto conto delle linee AgID**. Già dai primi report effettuati con gli strumenti di recente acquisizione sono emerse forti vulnerabilità cui *SOC TleC* non potrà dare soluzione in quanto causate da scelte tecniche esterne obsolete (applicativi Insiel o di altre aziende acquisiti perlopiù a seguito di gare di servizi economali o tecnici di contorno a beni vari). Va evidenziato che la norma indica che se le vulnerabilità di un sistema non possono essere sanate e se l'analisi rileva che questo provoca un rischio elevato l'azienda deve tassativamente rifiutarsi di utilizzare il sistema ovvero deve metterlo in disuso.

I riferimenti normativi sopra citati sono alla base di una articolata serie di interventi di rinnovamento ed adeguamento dei Sistemi Informatici/Informativi cui le Aziende del SSR devono necessariamente adempiere per garantire la sicurezza informatica, ovvero per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti (divulgazione, modifica, distruzione). Oltre alle misure preventive, destinate ad impedire attacchi informatici, le Aziende devono attivare, mediante l'attivazione di servizi acquisibili ad esempio su CONSIP, efficaci strumenti di costante analisi e rilevazione delle vulnerabilità del sistema informatico, con la finalità di anticipare l'accadimento di eventi avversi e di abbreviare i tempi che intercorrono dal momento in cui questi avvengono e l'applicazione delle soluzioni di rimedio

IL VICEPRESIDENTE

IL SEGRETARIO GENERALE