Sicurezza informatica e Pubblica Amministrazione: quale direzione e quali strumenti?

Date : 18 dicembre 2017

Contesto nazionale di riferimento

L'Agenzia per l'Italia Digitale (AgID) ha pubblicato nel corso dell'anno il Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione (PA).

Si tratta del documento di indirizzo **strategico** ed **economico** che accompagna la trasformazione digitale del Paese e definisce:

- linee operative di sviluppo dell'informatica pubblica;
- modello strategico di evoluzione del sistema informativo della PA;
- investimenti ICT del settore pubblico secondo le linee guida europee e del Governo.

Il Piano triennale fornisce la cornice di riferimento per indirizzare la trasformazione dell'ICT pubblico razionalizzandone la spesa e promuovendo, contestualmente, le dinamiche di innovazione tecnologica.

Il Piano recepisce inoltre il contesto normativo, gli indirizzi AgID e i fabbisogni espressi dalla PA, indica strategie e priorità pianificando, al contempo, gli strumenti di realizzazione (Gare e finanziamenti):

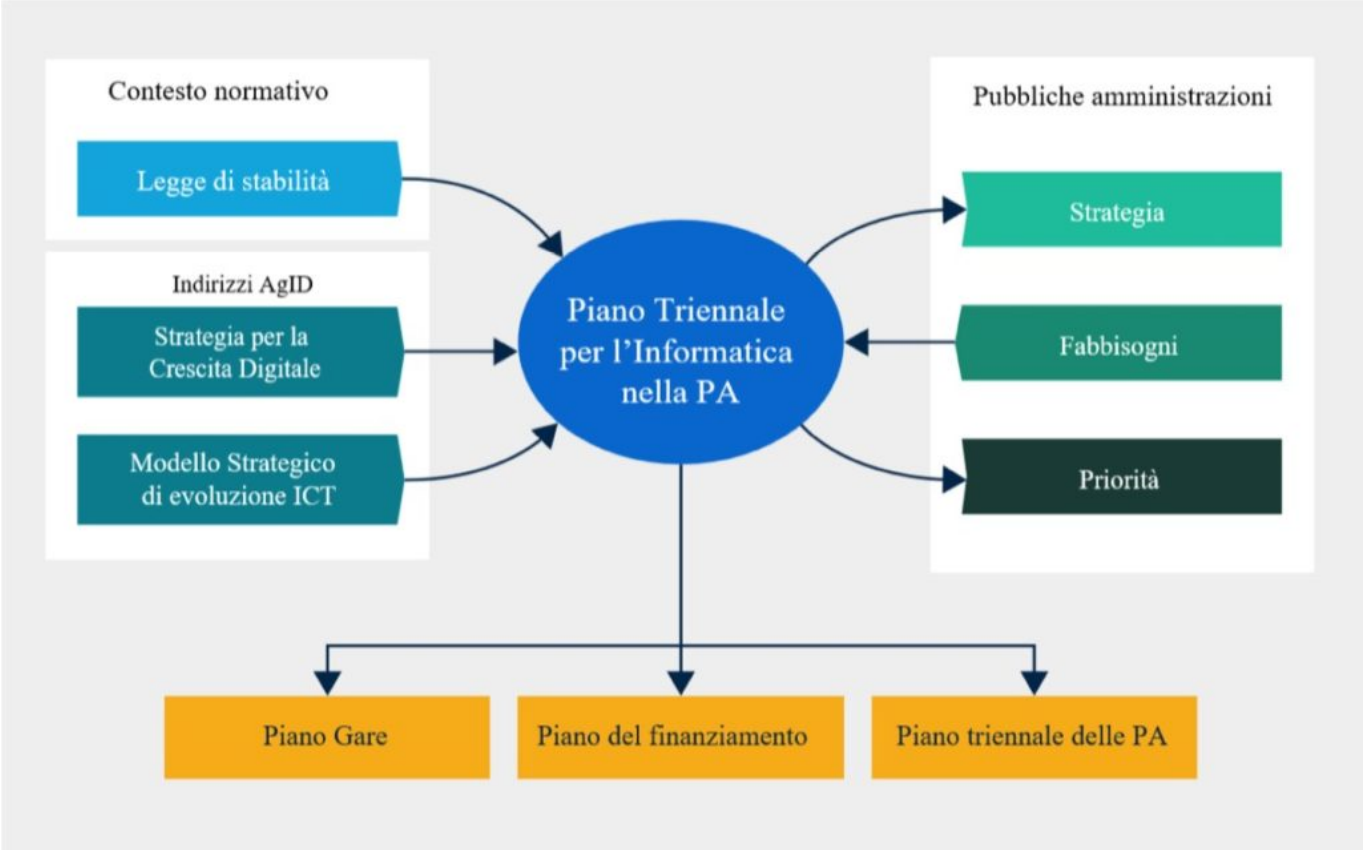

Figura 1 - Piano triennale AgID

Tra le indicazioni fondamentali per le PA emerge l'eliminazione delle *legacy* tecnologiche, con superamento delle relative logiche di *lock-in*, unitamente alla promozione del paradigma di consolidamento e virtualizzazione delle applicazioni e dei Data Center.

La **sicurezza informatica**, secondo il Piano, "ha **un'importanza fondamentale** in quanto è necessaria per garantire la **disponibilità, l'integrità** e **la riservatezza delle informazioni** proprie del Sistema informativo della Pubblica amministrazione. Essa è inoltre direttamente collegata ai principi di privacy previsti dall'ordinamento giuridico[1]". Il Piano esprime chiaramente l'esigenza, per ciascuna PA, di dotarsi di un **Sistema di gestione della sicurezza delle informazioni (SGSI)** e di individuare il profilo di sicurezza adeguato alla propria infrastruttura, definito attraverso una specifica **analisi del rischio**.

Sicurezza e Privacy nella Pubblica Amministrazione

AgID mette a disposizione delle Amministrazioni strumenti di diversa natura per **innalzare il livello globale di sicurezza cibernetica** e per **diminuire la superficie complessiva di attacco** (ad esempio, il CERT-PA[2]). Tra le iniziative più importanti è necessario annoverare il documento delle **Misure minime per la sicurezza ICT delle Pubbliche amministrazioni**[3], reso disponibile nel 2016 in attuazione della direttiva del Presidente del Consiglio dei Ministri del

2015[4] e pubblicato in Gazzetta Ufficiale ad Aprile 2017[5], in cui sono fornite indicazioni puntuali su come raggiungere livelli di sicurezza prefissati a partire da quello minimo, obbligatorio per tutti.

Il documento indica "**misure di natura tecnologica, organizzativa e procedurale** e **prevede tre livelli di attuazione**: **il livello minimo è quello al quale ogni PA, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme**. 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".

L'adeguamento delle PA alle Misure Minime dovrà avvenire entro il **31 Dicembre 2017**.

È importante sottolineare che le misure previste all'interno del documento sono basate su 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. In particolare, AgID si è ispirata all'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security nella versione 6.0 CCSC "CIS Critical Security Controls for Effective Cyber Defense"[6]. L'elenco dei 20 controlli in cui si articola, normalmente conosciuti come Critical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi. I primi 5 controlli sono considerati indispensabili per il livello minimo di protezione e da questi AgID è partita per stabilire le misure minime di sicurezza per la PA italiana, definendo i cosiddetti **AgID Basic Security Control (ABSC)**.

AgID ha stabilito relazioni di corrispondenza fra i propri controlli e gli identificatori del Framework Nazionale per la Cyber Security, proposto nel "2015 Italian Cyber Security Report" del CIS La Sapienza[7].

Figura 2 - Misure Minime di Sicurezza ICT per le PA

In aggiunta al quadro di riferimento finora rappresentato, afferente al dominio della **Sicurezza**, le PA devono anche fronteggiare requisiti di **Privacy**, determinati dal Regolamento U.E. n.679/2016 meglio noto sotto il nome di "**GDPR**". La combinazione dei due driver genera una lista di misure tecniche e organizzative a tutela e protezione dei dati, spesso preziosi, gestiti dalle PA.

Ma quali sono gli strumenti a disposizione della PA per adeguarsi alle Misure Minime, dotarsi di Sistemi di Gestione della Sicurezza delle Informazioni, adottare un approccio *risk-based* e abbracciare concetti quali *security* o *privacy by design* ?

Strumenti a disposizione della Pubblica Amministrazione

Consip ha bandito e aggiudicato un pacchetto di "gare SPC"[8] per l'affidamento dei servizi di Cloud Computing, di **sicurezza**, di realizzazione di portali e servizi online e di cooperazione applicativa per la PA. Il progetto, del valore complessivo di quasi 2 miliardi di euro, è stato suddiviso in 4 lotti, uno dei quali (**Lotto 2**) dedicato esclusivamente a soluzioni e servizi di sicurezza. Lo strumento a disposizione delle PA è il cosiddetto **Contratto Quadro SPC Cloud Lotto 2**[9], aggiudicato al raggruppamento temporaneo di imprese costituito da Leonardo

S.p.A, IBM Italia S.p.A. , Fastweb S.p.A. e Sistemi Informativi S.r.l.. Il Contratto è attivo da Luglio 2016 e ha durata 5 anni, orizzonte temporale abbastanza esteso e compatibile con la definizione di un programma di *security improvement*. I servizi previsti dal Contratto Quadro sono articolati all'interno di un catalogo suscettibile di essere ampliato e migliorato nel tempo: la natura estremamente dinamica del panorama delle minacce cibernetiche (*threat landscape*) determina infatti scenari continui di innovazione tecnologica, sia dal punto di vista dell'attaccante, sia dal punto di vista di chi è chiamato a proteggere le informazioni.

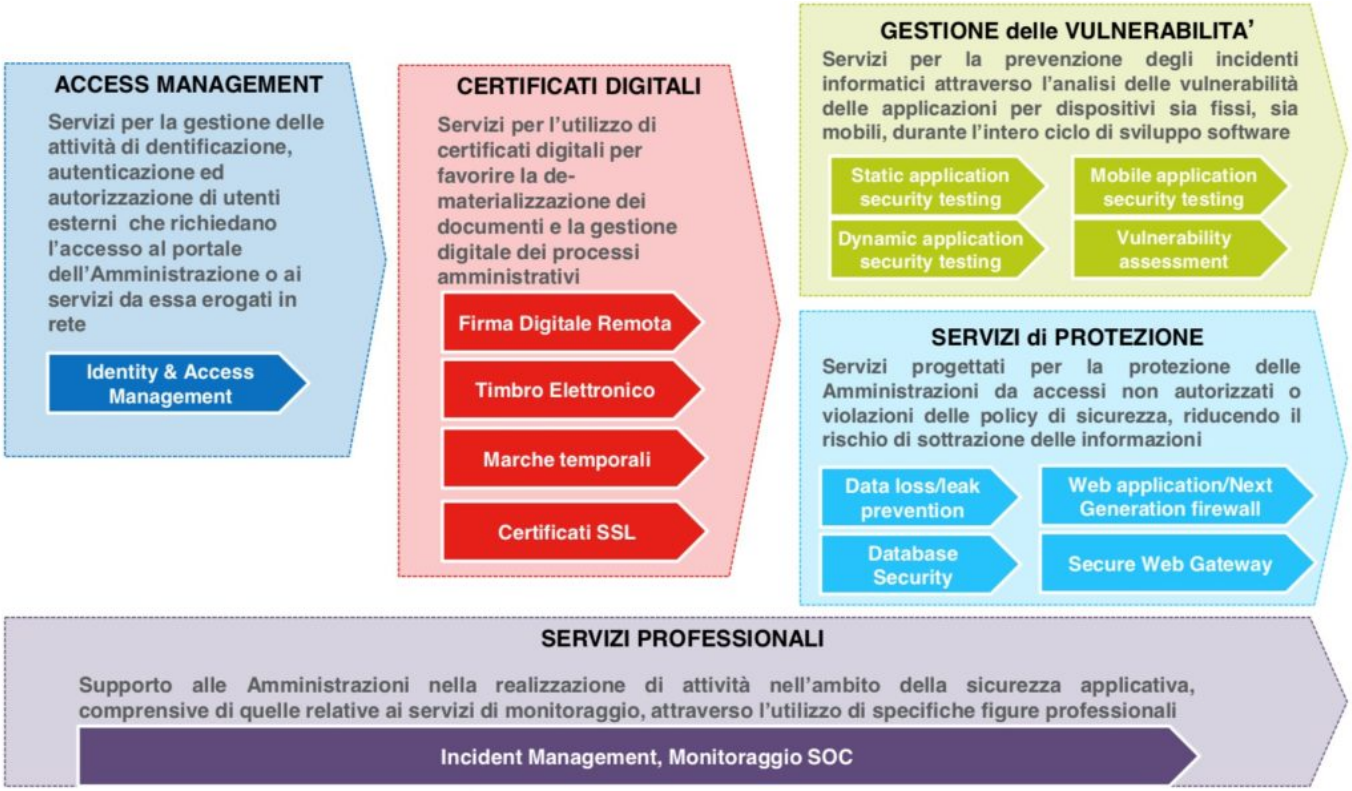

Figura 3 - Catalogo servizi SPC Cloud Lotto 2

Le soluzioni sono erogate tramite "Centri Servizi" del Fornitore, dislocati su sedi ubicate sul territorio nazionale, certificati ISO 27001 e strutturati in centri di competenza ed eccellenza: tale approccio, tipico dei *managed security service provider*, consente alle Amministrazioni di fare *offloading* di competenze verso un Fornitore esperto di materia e organizzato per effettuare monitoraggio di sicurezza H24 tramite apposite strutture organizzative quali i **Security Operations Center (SOC)**. I *Service Level Agreement*, i *report* e gli indicatori di *performance* del Contratto (ad esempio, i tempi di gestione degli incidenti di sicurezza) ne garantiscono l'efficacia in termini di qualità di erogazione del servizio.

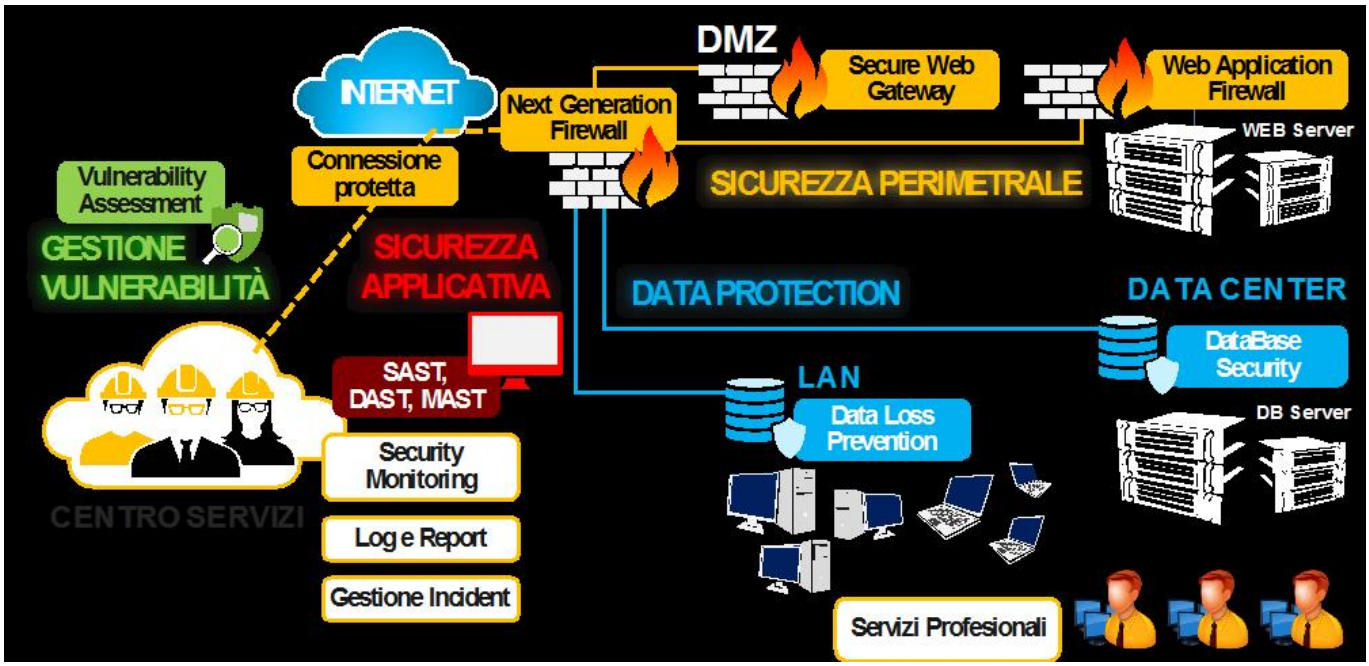

Figura 4 - Modello di erogazione dei Servizi SPC Cloud Lotto 2

Le PA possono quindi soddisfare il proprio fabbisogno di sicurezza informatica all'interno del catalogo servizi SPC Cloud Lotto 2.

Ad esempio, l'esecuzione periodica di verifiche relative alla presenza di vulnerabilità informatiche su prodotti e sistemi ICT dell'Amministrazione è garantita dal servizio di **Vulnerability Assessment**, così come l'esecuzione periodica dell'integrità dei software utilizzati è garantita dai servizi di **Static** e **Dynamic Application Testing**. La protezione da codice malevolo e la protezione dei dati sono garantite da diversi servizi quali **Data Loss/Leak Prevention**, **Web Application/Next Generation Firewall**, **Database Security** e **Secure Web Gateway**. Tutte le attività di *assessment* e di supporto finalizzate a rilevare eventuali esposizioni con relative azioni di contrasto (*remediation*) sono realizzabili tramite i **Servizi Professionali**, concepiti per affiancare e aiutare le Amministrazioni nelle attività specialistiche di sicurezza. Tutte le Misure Minime previste da AgID relative all'inventario di dispositivi e software autorizzati, alla protezione delle configurazioni, alla valutazione e correzione continua delle vulnerabilità, alle difese da codice malevolo e alla protezione dei dati sono attuabili tramite i servizi previsti a catalogo. Analogamente, le fasi di analisi, progettazione ed esecuzione riconducibili ai requisiti definiti dal GDPR sono attuabili tramite i Servizi Professionali disponibili.

Conclusioni

Nonostante le oggettive difficoltà rappresentate dall'aumento degli attacchi informatici, dai vincoli di spesa, dalla crescente complessità della materia e dal conseguente *skill shortage*, attualmente i livelli di attenzione istituzionale al tema della sicurezza informatica sono elevati ed esistono per le PA adeguati strumenti di acquisizione delle necessarie *capability* di

cyber-security. Tra gli strumenti disponibili, il Contratto Quadro SPC Cloud Lotto 2 è quello principale e può consentire la riduzione della superficie di attacco complessiva e la protezione dei dati pubblici e dei privati cittadini, abilitando un efficace partenariato pubblico-privato (PPP) tra PA e aziende specializzate.

[1] https://pianotriennale-ict.readthedocs.io/it/latest/doc/08_sicurezza.html

[2] https://www.cert-pa.it

[3] http://www.agid.gov.it/sites/default/files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf

[4] https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html

[5] https://www.cert-pa.it/documents/10184/27607/CircolareAgID_170418_n_2_2017_Mis_minime_sicurezza_ICT_PA-GU-103-050517.pdf/7ca821ea-f8cc-4310-9fad-3c6ec1ca7f85

[6] https://www.cisecurity.org

[7] http://www.cybersecurityframework.it

[8] http://www.consip.it/media/approfondimenti/gare-spc-consip-e-agenda-digitale-italiana-contributi-servizi-contenuti-e-date

[9] https://www.spc-lotto2-sicurezza.it/

A cura di: **Andrea Boggio**