8 Sicurezza

La sicurezza 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.

A tal fine sarà potenziato il ruolo di CERT-PA in modo da strutturare i piani di sicurezza delle Pubbliche amministrazioni, vigilare con azioni di monitoraggio e verifiche periodiche sull'attuazione dei piani. Questa è un'area tecnologica in continua evoluzione, quasi giornaliera, nella quale gli investimenti devono essere rafforzati in continuazione.

Il Piano, tenendo conto del Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico[72] *(QNS)*, pone l'accento sulla razionalizzazione delle risorse ICT descritta nel capitolo 3 "Infrastrutture fisiche" come metodo prioritario per aumentare il livello di sicurezza attraverso la riduzione della "superficie" esposta agli attacchi informatici. Questo è, infatti, l'aspetto più critico tra quelli individuati nel Rapporto "*Italian Cyber Security Report 2014*".

Le attività gestite da AgID sono raggruppate nelle seguenti aree:

- *CERT-PA*, in cui ricadono le attività svolte dal CERT-PA (*Computer Emergency Readiness/Response Team*, ovvero "squadra per la risposta ad emergenze informatiche" a supporto dei sistemi informatici della Pubblica amministrazione) che opera all'interno dell'AgID e che supporta le Pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica del dominio costituito dalle Pubbliche amministrazioni;
- regolazione e regolamentazione, in cui ricadono le attività di emanazione di normative, regole tecniche, linee guida e documenti di riferimento sugli aspetti di sicurezza (ad es. le Misure minime di sicurezza ICT per le Pubbliche amministrazioni[73]), anche sulla base della contestualizzazione del *Framework Nazionale per la Cyber Security (FNCS)* [74];
- accreditamento e vigilanza, ai sensi del CAD, dei soggetti che erogano servizi fiduciari qualificati o svolgono altre attività normate, quali la conservazione dei documenti informatici, per le quali sono rilevanti gli aspetti di sicurezza;
- *assessment* e test, in cui ricadono le attività di verifica della corretta implementazione e della conformità agli standard delle funzionalità di sicurezza delle componenti di sistema o di servizio delle Pubbliche amministrazioni. Questa attività è attualmente in via di ridefinizione e rafforzamento.

8.1 Scenario attuale

Presso AgID è già operativo il CERT-PA, che offre alle Pubbliche amministrazioni:

- servizi di analisi e di indirizzo, finalizzati a supportare la definizione dei processi di gestione della sicurezza, lo sviluppo di metodologie, il disegno di processi e di metriche valutative per il governo della sicurezza cibernetica;

---

72 https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

73 http://www.agid.gov.it/sites/default/files/documentazione/misure_minime_di_sicurezza_v.1.0.pdf

74 "Framework Nazionale per la Cyber Security" è il contenuto dell'"Italian Cyber Security Report 2015" del CIS Sapienza, pubblicato a febbraio 2016 e realizzato con il contributo di AgID.

- servizi proattivi, aventi come scopo la raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emissione di bollettini e segnalazioni di sicurezza, l'implementazione e la gestione di basi dati informative;
- servizi reattivi, aventi come scopo la gestione degli allarmi di sicurezza, il supporto ai processi di gestione e la risoluzione degli incidenti di sicurezza all'interno del dominio delle PA;
- servizi di formazione e comunicazione, per promuovere la cultura della sicurezza cibernetica, favorendo il grado di consapevolezza e competenza all'interno delle Pubbliche amministrazioni, attraverso la condivisione di informazioni relative a specifici eventi in corso, nuovi scenari di rischio o specifiche tematiche di sicurezza delle informazioni.

AgID definisce i profili di sicurezza per gli elementi costituenti la Mappa del Modello strategico, con riferimento al Framework Nazionale per la Cyber Security e agli standard internazionali come ISO/IEC 27000 e COBIT e si assume che tutte le amministrazioni seguano gli standard medesimi.

In attesa dell'emanazione da parte del Dipartimento della Funzione Pubblica delle Regole Tecniche per la sicurezza ICT delle Pubbliche amministrazioni proposte da AgID, tenuto conto dell'urgenza conseguente all'evoluzione delle minacce cibernetiche sul panorama internazionale, ed in particolare nei riguardi della Pubblica amministrazione, nel settembre 2016 AgID ha pubblicato il documento delle *Misure minime per la sicurezza ICT delle Pubbliche amministrazioni* che fornisce indicazioni puntuali su come raggiungere livelli di sicurezza prefissati a partire da quello minimo, obbligatorio per tutti.

Per quanto riguarda le attività relative ad Accreditamento e vigilanza, AgID è responsabile della qualificazione dei soggetti che intendono avviare la prestazione di servizi fiduciari qualificati[75] e dell'accreditamento dei gestori di posta elettronica certificata[76], dei conservatori di documenti informatici[77], dei Certificatori di firma digitale accreditati[78] e degli Identity Provider di SPID[79], per i quali cura la pubblicazione degli elenchi di fiducia. AgID, inoltre, svolge funzioni di vigilanza su tali soggetti e, per i servizi fiduciari, è l'organismo designato in Italia ai sensi del Regolamento UE n° 910/2014 (Regolamento eIDAS[80]). Sono a tal fine in corso le azioni per l'adeguamento dei processi di qualificazione, accreditamento e vigilanza alle nuove disposizioni.

8.2 Obiettivi strategici

➢ Definire i profili di sicurezza delle componenti ICT della Pubblica amministrazione, anche istanziando il *Framework Nazionale per la Cyber Security (FNCS)* in tutte le componenti del Modello strategico e, a valle di una specifica analisi del rischio, fornire i riferimenti tecnici e normativi che le Pubbliche amministrazioni dovranno adottare. La mancata attuazione dei profili di sicurezza potrebbe comportare, proporzionalmente al tipo di inadempimento, anche la necessità di interrompere l'erogazione dei servizi connessi.

---

75 http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/il-regolamento-ue-ndeg-9102014-eidas/servizi-fiduciari

76 http://www.agid.gov.it/infrastrutture-sicurezza/pec-elenco-gestori

77 http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-attivi

78 http://www.agid.gov.it/certificatori-firma-digitale-accreditati-italia

79 http://www.agid.gov.it/infrastrutture-architetture/spid/identity-provider-accreditati

80 Il Regolamento eIDAS (electronic IDentification Authentication and Signature) ha l'obiettivo di fornire una base normativa, a livello comunitario, per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.

- Offrire alle Pubbliche amministrazioni supporto alla prevenzione e al trattamento degli incidenti di sicurezza informatica.
- Provvedere a effettuare *assessment* e verifiche di sicurezza onde accertare l'applicazione delle regole di sicurezza individuate da parte delle Pubbliche amministrazioni.
- Dare seguito alle attività in essere in materia di accreditamento e verifica provvedendo, in primis, alla piena attuazione del Regolamento eIDAS.

8.3 Linee di azione

Al fine di raggiungere gli obiettivi del Piano, il CERT-PA provvederà entro la fine del 2017 a:

- realizzare la *Cyber Security Knowledge Base* nella quale sono raccolte le informazioni sulle infrastrutture realizzate nel dominio della Pubblica amministrazione e sugli eventi di sicurezza occorsi nel tempo al loro interno;
- realizzare e gestire il *National Vulnerability Database* (NVD), catalogo delle vulnerabilità informatiche che integra i cataloghi disponibili a livello internazionale (ad es. MITRE) con le vulnerabilità riscontrate sui sistemi sviluppati in ambito nazionale;
- rendere prontamente disponibili strumenti e informazioni utili per prevenire e rispondere ad eventuali attacchi informatici;
- fornire supporto alle amministrazioni nella predisposizione di risposte agli incidenti;
- fornire supporto alle amministrazioni e approfondire la funzione di monitoraggio dello spazio cibernetico delle Pubbliche amministrazioni, anche attivando specifiche collaborazioni con le comunità di riferimento nazionali ed internazionali;
- fornire supporto alle amministrazioni nella gestione degli incidenti e nel successivo ripristino.

A tal fine è in corso un progressivo incremento della capacità operativa del CERT-PA, completando l'infrastruttura ICT di erogazione dei servizi di base e realizzando il primo embrione di sistema informativo sulle minacce cibernetiche, sul modello di quello del MITRE[81] statunitense.

Un altro passaggio importante sarà l'emanazione delle Regole tecniche per la sicurezza ICT delle Pubbliche amministrazioni che forniranno a indicazioni sulle misure da adottare in ciascuna componente della Mappa del Modello strategico.

Tra queste si anticipano alcune indicazioni relative alle Infrastrutture fisiche:

- ciascuna Pubblica amministrazione dovrà dotarsi di un Sistema di gestione della sicurezza delle informazioni (SGSI) e della relativa struttura organizzativa;
- ciascuna Pubblica amministrazione dovrà, sulla base di una specifica analisi del rischio, individuare il profilo di sicurezza adeguato per la propria infrastruttura e, tenendo anche conto degli aggiornamenti sulle minacce provenienti dal CERT-PA, adottare le misure opportune.

Per dare seguito alle attività dell'area *Assessment e test,* si individuano le azioni di seguito descritte, la cui realizzazione risulta di pertinenza delle singole amministrazioni.

Sotto le ipotesi indicate, *l'assessment* e l'esecuzione delle verifiche è da intendersi come:

- esecuzione periodica di verifiche della configurazione operativa e della presenza di vulnerabilità nei prodotti e sistemi ICT e nelle procedure ad essi correlate: dovranno essere previste attività

[81] https://www.mitre.org/

periodiche di verifica dell'integrità dei software impiegati nelle amministrazioni almeno due volte l'anno, scansioni dello stato di aggiornamento di tali software e dell'esistenza di vulnerabilità sfruttabili. Tale verifica include, oltre alla verifica dell'integrità del codice sorgente in esecuzione, la configurazione del software in esame;

- valutazione della corretta implementazione e relativa configurazione delle funzionalità di sicurezza adottate nei sistemi e prodotti ICT impiegati da ogni amministrazione: dovrà essere prevista l'esecuzione di specifici test di sicurezza per autorizzare l'impiego di prodotti (e dei relativi sistemi che integrano tali prodotti) che realizzano funzionalità di sicurezza critiche per l'operatività della Pubblica amministrazione in esame. In tal senso può risultare utile adottare l'approccio già descritto in standard o metodologie per lo sviluppo e la valutazione e certificazione della sicurezza ICT quali ad esempio la famiglia di standard ISO/IEC 15408. L'adozione di prodotti certificati ISO/IEC 15408 fornisce garanzie di sicurezza sia perché coinvolge personale con competenza comprovata (i valutatori dei laboratori di sicurezza) sia perché prevede un'analisi di sicurezza approfondita (tramite l'analisi della documentazione di riferimento e la realizzazione di prove di intrusione documentate e ripetibili) sia perché assegna alle comunità tecniche europee ed internazionali il compito di monitorare eventuali vulnerabilità dei prodotti certificati. Ai sensi dell'art. 68 del CAD, l'adozione di software e applicativi *open source* è da intendersi come prioritaria, nell'ambito di una valutazione complessiva di rischio, di *total cost of ownership* e di capacità di utilizzo.

Oggetto	CERT-PA
Tempi	In corso
Attori	AgID
Descrizione	CERT-PA, già operante dal 2013, aumenterà progressivamente la sua capacità operativa, completando l'infrastruttura ICT di erogazione dei servizi di base e realizzando il primo embrione di sistema informativo sulle minacce cibernetiche, anche attraverso l'implementazione delle soluzioni: *Infosharing* CERT PA[82] e *National Vulnerability* Database.
Risultato	---

Oggetto	Pubblicazione e adeguamento alle Regole tecniche per la sicurezza ICT delle Pubbliche amministrazioni
Tempi	Entro settembre 2017
Attori	AgID, Dipartimento della Funzione Pubblica, PA
Descrizione	AgID redige le Regole tecniche per la sicurezza ICT delle Pubbliche amministrazioni che forniranno alle PA le indicazioni sulle misure da adottare.

[82] https://portal.cert-pa.it/web/guest/login

	Il Dipartimento della Funzione Pubblica emana le Regole tecniche predisposte da AgID. Le Pubbliche amministrazioni si adeguano alle Regole tecniche per la sicurezza ICT delle Pubbliche amministrazioni, attraverso la predisposizione e l'esecuzione di Piani di adeguamento alle regole tecniche emanate da AgID. In attesa dell'emanazione delle suddette Regole tecniche, tutte le Pubbliche amministrazioni sono in grado di adeguarsi alle "Misure Minime Di Sicurezza ICT per le Pubbliche amministrazioni" già pubblicate da AgID[83].
Risultato	Regole tecniche per la sicurezza ICT delle Pubbliche amministrazioni *(data di rilascio: giugno 2017)* Piani di adeguamento delle PA (data di rilascio: nel rispetto dei vincoli di norma determinati dall'emanazione delle Regole tecniche)

Oggetto	Architettura della sicurezza per servizi critici
Tempi	Entro settembre 2017
Attori	AgID , PA
Descrizione	Definizione dei principi e delle linee guida del modello architetturale di gestione dei servizi critici e contestualizzazione rispetto al cluster dei dati gestiti. Le PA *owner* di servizi critici predispongono un Piano di adeguamento e adeguano o realizzano i servizi critici nel rispetto delle linee guida.
Risultato	Linee guida del modello architetturale di gestione dei servizi critici *(data di rilascio: giugno 2017)* Piano di adeguamento delle amministrazioni *owner* di servizi critici *(da avviare entro settembre 2017)*

Oggetto	Continuous monitoring
Tempi	In corso
Attori	PA
Descrizione	Per assicurare il *continuous monitoring,* raccomandato dalle best practices di sicurezza (es. ISO 27001, documentazione NIST), le Pubbliche amministrazioni provvederanno alla verifica dello stato di aggiornamento dei software impiegati in ogni singola amministrazione rispetto a vulnerabilità note pubblicate da uno o più soggetti di riferimento (ad es.

[83] http://www.agid.gov.it/notizie/2017/04/07/pubblicate-gazzetta-ufficiale-misure-minime-sicurezza-informatica-pa

	CERT nazionali o basi di dati di vulnerabilità). Per dare seguito alla presente azione si provvederà alla scansione dei software mediante strumenti automatici e alla successiva analisi dei risultati (e del possibile impatto di una vulnerabilità nota eventualmente non corretta) demandata ad un soggetto competente. AgID si riserva la possibilità di eseguire *penetration test* a campione.
Risultato	Pubblicazione periodica dei risultati.

Oggetto	Segnalazioni incidenti Informatici al CERT-PA
Tempi	In corso
Attori	PA
Descrizione	Tutte le Pubbliche amministrazioni sono tenute a monitorare e segnalare prontamente al CERT-PA gli incidenti informatici e ogni situazione di potenziale rischio, utilizzando i canali di comunicazione riportati nella sezione dedicata del sito AgID[84]. Per tutti i soggetti accreditati su *Infosharing* CERT PA è disponibile un'apposita funzionalità di segnalazione.
Risultato	---

Oggetto	Riorganizzazione del dominio "gov.it"
Tempi	Entro giugno 2018
Attori	AgID, PA
Descrizione	AgID emana le disposizioni per il riordino del dominio "gov.it", al fine di riorganizzarlo con una segmentazione che risponda a criteri internazionali e consenta di raggruppare i siti delle amministrazioni centrali. Simmetricamente entro 12 mesi le PA completano le attività.
Risultato	Disposizioni per il riordino del dominio "gov.it" *(data di rilascio: giugno 2017)*. Adeguamento da parte delle PA alle suddette disposizioni *(entro giugno 2018)*.

[84] http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa