# Sicurezza

Coerentemente con il ruolo strategico che negli ultimi anni la Sicurezza ICT riveste nell’ambito dei processi di informatizzazione della PA, e come è ormai consolidata pratica di DigitPA, è stata inserita nella relazione sullo stato di informatizzazione della PA redatta annualmente dagli esperti di DigitPA una sezione interamente dedicata ad una sintesi dei dati raccolti per fotografare lo stato dell’arte per quanto riguarda la sicurezza ICT tra le varie Amministrazioni appartenenti alla Pubblica Amministrazione Centrale.

Per l’anno 2010, come per le ultime 4 edizioni, è stato adottato lo stesso modello di sicurezza e la relativa metodologia di raccolta e di analisi dei dati al fine di ottenere dati confrontabili anno per anno e poterne valutare i trend all’interno del campione. Infatti nel corso del tempo molte amministrazioni sono state soggette a dinamiche esterne di accorpamento e crescita intersecate dai normali processi di evoluzione dei sistemi informativi interni.

Nei primi mesi del 2011, come è ormai consuetudine, è stato somministrato un questionario on-line ai responsabili dei CED delle Amministrazioni afferenti alla PAC per valutare come all’interno del campione le varie amministrazioni si sono evolute rispetto ad un modello di sicurezza individuato già nel 2005. E’ utile precisare che gli obiettivi del questionario sono duplici: da un lato è da ritenersi strumento principale per l’individuazione di particolari criticità sulle quali intervenire con urgenza proponendo i correttivi più appropriati; dall’altro DigitPA punta attraverso questo strumento a misurare la sensibilità degli utenti sul tema sicurezza ICT e a sviluppare con tutti i responsabili un comune modello verso il quale tendere con azioni mirate.

Accanto alla necessaria crescita del livello di informatizzazione della PA ed alle ricadute attese in termini di efficienza e qualità dei servizi offerti, DigitPA ha infatti da tempo dedicato uno sforzo considerevole per garantire una costante opera di sensibilizzazione e informazione sul sema Sicurezza ICT mantenendo sempre alti i livelli di specializzazione e gli standard qualitativi. Tutto ciò avviene ormai da anni e tali attività sono fondate sulla adozione e consolidamento di comuni obiettivi, tecnologie e buone pratiche che di fatto definiscono un modello di sicurezza.

Lo stesso modello può essere espresso da una serie di indicatori oggettivamente rilevabili. Attraverso il questionario e le iniziative di formazione su temi specifici si intende pertanto misurare l’effettiva aderenza delle strutture informatiche della PAC a tale modello monitorando i processi di informatizzazione delle amministrazioni coinvolte. Solo in questo modo è possibile garantire all’intera PA l’attuazione di strategie comuni, preventivamente testate e messe a punto, anticipando ogni criticità prima ancora che diventi una minaccia per l’intera comunità.

Questo approccio consente quindi alle amministrazioni di affrontare il tema innovazione tecnologica dei processi interni alla PA in maniera serena senza introdurre ansie o rischi non calcolati. E’ facile intuire, infatti, che più si evolvono i sistemi informativi in uso, più si accentuano le dipendenze e le criticità. Ovviamente, all’aumento di questa dipendenza corrisponde sempre una crescita esponenziale della rilevanza del ruolo rivestito dai sistemi informativi nel contesto PA.

Va infine chiarito che l’adozione e lo sviluppo costante di un modello per la sicurezza può avvenire solamente attraverso un organismo centrale, riconosciuto non solo per qualità tecnica ma anche come autorità sul piano formale. Oltre all’aspetto divulgazione e condivisione dei risultati va valutata anche la possibilità di cogliere l’opportunità di raggruppare le esigenze tra tutti i componenti del campione ottenendo così delle importanti economie di scala a tutto vantaggio della qualità delle soluzioni e dei risparmi in termini di risorse economiche, come ampiamente testimoniato dal progetto SPC.

## La metodologia di analisi

Prima di esporre i risultati è necessario condividere gli aspetti principali della metodologia di analisi che DigitPA ha sviluppato e consolidato nel tempo. Attraverso un processo top-down tale metodologia ha permesso di ottenere un’istantanea dello stato attuale delle amministrazioni appartenenti alla PAC in termini di sicurezza. Contemporaneamente, il modello, la cui consistenza è stata verificata anno per anno rimanendo sostanzialmente inalterato, ha fornito alle Amministrazioni una serie di obiettivi a cui tendere per migliorare il proprio risultato nell’anno successivo. Nel formulare questa metodologia si è deciso si utilizzare esclusivamente dati numerici, rilevabili oggettivamente ed in maniera non ambigua dagli stessi responsabili di ogni singola amministrazione.

Come per le precedenti edizioni il processo si avvia dopo che i responsabili di ogni struttura informatica della Pubblica Amministrazione Centrale, opportunamente sollecitati e guidati laddove richiesto, hanno compilato il questionario on-line. Questo è organizzato in 4 sezioni ed ognuna rappresenta una specifica dimensione da analizzare riguardo al tema Sicurezza ICT. Il risultato di ogni sezione viene espresso sinteticamente da un valore numerico compreso tra 0 e 10 detto *Key Performance Indicator* (KPI). Per ogni amministrazione i 4 KPI vengono calcolati attraverso l’attribuzione di punteggi numerici ad ognuno delle risposte formulate ai quesiti che lo caratterizzano. La media dei risultati relativi ai quesiti della specifica sezione rappresenta il valore del KPI attribuito all’amministrazione in esame.

Inoltre ogni amministrazione è stata classificata in funzione delle dimensioni (numero di dipendenti) in una delle tre categorie: *piccole*, fino a 1.000 dipendenti, *medie* tra 1000 e 10.000 dipendenti, *grandi* oltre i 10.000. In questo modo per ogni categoria sono stati calcolati i valori medi dei 4 KPI.

In questo modo l’analisi effettuata è in grado di fornire indicazioni molto più precise e puntuali esprimendo attraverso i valori medi della categoria indicazioni puntuali rispetto a problematiche molto più omogenee tra amministrazioni della stessa classe. Anche le eventuali azioni correttive hanno una maggiore significatività se analizzate nella prospettiva di un insieme di amministrazioni con dimensioni confrontabili.

Per l’analisi dei dati è stata adottata una metodologia multilivello a raffinamenti successivi che procede in maniera top-down attraverso 4 gradi di approssimazione (livelli):

1. Dapprima vengono analizzati i dati grezzi rappresentati dai valori dei 4 KPI ottenuti come valore medio tra tutte le Amministrazioni che hanno partecipato alla rilevazione (livello 1).
2. Successivamente vengono analizzati i valori medi dei KPI relativi alle 3 categorie omogene dopo aver classificato ogni amministrazione in funzione delle dimensioni e dopo aver depurato il campione da eventuali dati incompleti[[1]](#footnote-1) (livello 2).
3. Scendendo ad un maggiore livello di dettaglio è possibile valutare il risultato di ogni singola Amministrazione espresso dai 4 KPI (livello 3).
4. L’ultimo passo, necessario soprattutto in presenza di particolari criticità, consiste nell’analisi delle risposte ai singoli quesiti del questionario per ciascuna amministrazione, producendo delle schede personalizzate (livello 4) che consentono di individuare per ogni singola amministrazione gli ambiti su cui investigare per un eventuale miglioramento.

Per semplificare l’analisi numerica, ogni valore dei 4 KPI è stato confrontato rispetto a 3 soglie che delimitano i criteri di ottimalità, accettabilità, criticità lieve ed elevata. Valori prossimi o inferiori alla soglia di criticità elevata richiedono evidentemente interventi urgenti.

Nella rilevazione 2010, decisamente segnata dai tagli ai bilanci delle amministrazioni intervistate in funzione della crisi economica, le amministrazioni hanno reagito in maniera differenziata in funzione delle dimensioni. Infatti, paradossalmente, come verrà mostrato nei prossimi paragrafi, le grandi amministrazioni hanno subito effetti recessivi, più ancora delle piccole e medie, che comunque sono riuscite a completare i progetti già avviati negli anni precedenti, prescindendo dalle riduzioni di budget.

Purtroppo va ancora una volta sottolineato che la sicurezza viene ancora percepita come un costo aggiuntivo e non come un reale valore, per cui, in molti casi, si tende a risparmiare risorse accettando pericolosi compromessi in termini di livelli di sicurezza attesi per gli impianti realizzati o per le procedure installate. Nello stesso tempo nel corso degli ultimi 3 anni i risultati del questionario, seppur non prevedendo alcun quesito esplicitamente dedicato alla connettività, hanno potuto misurare i vantaggi e le ricadute prodotte dal progetto Sistema Pubblico di Connettività (SPC). Evidentemente il progetto originale tra i vari lotti ha incluso soluzioni esplicitamente connesse alla implementazione del “*modello comune per la sicurezza*” messo a punto dall’esperienza di DigitPA. Gli effetti del progetto si sono diffusi estendendo le ricadute anche e soprattutto alle Amministrazioni di medie e piccole dimensioni, mentre inizialmente le soluzioni tecnologicamente all’avanguardia erano presenti solo tra le Amministrazioni di grandi dimensioni con maggiori disponibilità di risorse.

Va rilevato che i listini di SPC offrono anche servizi professionali per la Sicurezza, dispositivi ed apparati per la sicurezza oltre che specifici servizi di monitoraggio della rete ed assistenza da parte dei fornitori di connettività.

Il questionario è stato formulato individuando l’insieme degli elementi ritenuti essenziali in termini di sicurezza per la PA che costituiscono l’insieme degli oggetti di controllo (obiettivi) sui quali raccogliere i dati statistici. Alla base della definizione del modello adottato sono state poste le principali norme internazionali come la ISO 27001 declinando opportunamente il risultato sulle specifiche realtà della Pubblica Amministrazione italiana ben note a DigitPA.

La lista degli oggetti di controllo è stata poi stata raggruppata secondo le aree di pertinenza individuate dai 4 KPI di seguito descritti:

* **KPI1 sicurezza logica**; valuta la sensibilità dell’Amministrazione rispetto alle scelte adottate in termini di organizzazione interna, prodotti software e soluzioni per la sicurezza logica del CED. I principali temi trattati sono: Autenticazione e controllo accessi, Certificazioni di prodotti e servizi, gestione degli aggiornamenti, sicurezza dei dati sui dispositivi mobili, backup.
* **KPI2 sicurezza dell’infrastruttura**; valuta gli aspetti fisici della sicurezza dell’impianto ed in particolare quelli legati alla infrastruttura di rete, raccogliendo informazioni rispetto a temi quali: sicurezza perimetrale, controllo accessi ai locali tecnici, apparati attivi per la sicurezza degli accessi da remoto, sistemi per la rilevazione delle intrusioni, protezione delle reti wireless, modalità di accesso da remoto e VPN.
* **KPI3 sicurezza dei servizi**; misura gli sforzi spesi dalle amministrazioni per incrementare l’affidabilità e la robustezza dei propri servizi ICT. In particolare centrali per questo KPI sono i temi della continuità operativa e del disaster recovery. In questa stessa sezione, sempre per garantire la robustezza dei servizi offerti, vengono misurati anche temi più consolidati quali antivirus o antispam per la posta elettronica considerati strumenti preventivi per ridurre i rischi di malfunzionamenti dei sistemi informativi.
* **KPI4 sicurezza dell’organizzazione**; rileva lo sforzo espresso dalle Amministrazioni in termini organizzativi, allocando risorse umane per la corretta gestione della sicurezza, ricoprendo ad esempio i ruoli previsti dal codice per l’amministrazione digitale, o gestendo adeguatamente gli eventuali attacchi, gestire adeguatamente le eventuali risorse esterne gestione dedicate alla sicurezza ed avviare iniziative per garantire ulteriori sviluppi su questi temi.

Successivamente ogni oggetto di controllo è stato tradotto in uno o più quesiti a risposte chiuse attraverso i quali sono state raccolte le indicazioni sullo stato dell’arte di ogni singola amministrazione. La risposta corrispondente al valore atteso dal modello adottato è stata sempre valutata con il punteggio massimo di 10, mentre le altre ottengono un punteggio decrescente fino a 0 che corrisponde anche al punteggio assegnato alla risposta non fornita (non sono stati previsti punteggi negativi per differenziare risposte errate da risposte non date). In questo modo ogni indicatore raccoglie un insieme di elementi di valutazione stabilendo così una metrica sufficientemente oggettiva per misurare il livello di attenzione di ciascuna Amministrazione intervistata sul tema Sicurezza ICT. I 4 KPI ricoprono il tema Sicurezza ICT in maniera ampia analizzandolo sotto 4 prospettive diverse e forniscono così indicazioni precise sulle eventuali contromisure da intraprendere in caso di risultati negativi.

I valori dei KPI rilevati rappresentano così diverse viste sul modello per la sicurezza su descritto che DigitPA ha affinato e condiviso attraverso gli anni. Tale modello si è arricchito ed irrobustito nel corso degli anni risultando sempre più aderente ad una realtà complessa ed eterogenea come la PAC italiana. Sfruttando le serie storiche degli anni precedenti, ogni regressione è facilmente rilevabile. In passato, si è potuto verificare su casi reali che a fronte di un punteggio decrescente nel tempo, singole amministrazioni effettivamente riflettono cattive impostazioni o errori altrimenti difficilmente percepibili.

Ovviamente, l’evoluzione delle tecnologie, come pure la spinta indotta a livello del governo centrale attraverso norme o incentivi rivolti alla PA hanno fatto si che rapidamente alcuni obiettivi siano diventati obsoleti o incompleti per cui, come di seguito verrà motivato, si ritiene che il modello adottato abbia raggiunto la sua piena maturità. Molti obiettivi che agli inizi apparivano irraggiungibili oggi rappresentano correttamente le pratiche quotidiane senza da parte dell’intero campione. Pertanto, il buon risultato complessivo raggiunto con la rilevazione 2010 spinge a fare una riflessione sul modello adattato ormai da oltre 5 anni che potrebbe cominciare ad mostrare i primi sintomi di invecchiamentoà. Al contrario, il modello potrebbe essere arricchito (svecchiato/aggiornato) con tematiche più ampie come ad esempio il tema della Business Continuity ed all’outsourcing della sicurezza che attualmente sono affrontati solo superficialmente. Si ritiene pertanto necessario uno sforzo collettivo per aggiornare il modello per la sicurezza ICT, pianificando gli obiettivi attesi per i prossimi 5 anni e lanciando quindi una nuova e concreta sfida al rinnovamento delle amministrazioni. La strategia rimarrebbe invariata, proseguendo il lavoro intrapreso nel 2005, prima con attività di condivisione, diffusione e successivamente con un monitoraggio costante per misurare i progressi ottenuti o individuare i correttivi eventualmente necessari.

## Risultati e linee di tendenza

In questo paragrafo si presentano i risultati di primo e secondo livello (fino ai valori medi per le 3 categorie che suddividono il campione) ottenuti dall’analisi dei dati raccolti. Si rimanda il lettore interessato ai risultati degli ulteriori livelli di analisi alla relazione annuale sullo stato della sicurezza ICT nelle pubbliche amministrazioni per l’anno 2010, ancora in fase di elaborazione. In questo documento saranno riportati i dati di dettaglio con le risposte ai singoli quesiti e le conclusioni elaborate per fornire una chiave interpretativa ai fenomeni osservati e le naturali proposte migliorative.

Figura : Distribuzione delle amministrazioni all’interno del campione in funzioni delle dimensioni (numero di dipendenti)

Inoltre, sfruttando la serie storica raccolta negli anni, in questo paragrafo saranno presentate le linee di tendenza ottenute raccogliendo e confrontando i risultati delle ultime 4 rilevazioni che meglio di ogni altro strumento sintetizzano i risultati conseguiti dall’intero campione in materia di sicurezza ICT grazie agli sforzi profusi dalle Amministrazioni intervistate ed all’impegno di DigitPA.

Nei primi mesi del 2011 il questionario nel suo consueto formato è stato proposto alle Amministrazioni. Al termine della raccolta dati 46 amministrazioni hanno completato l’inserimento dei dati. Solo una amministrazione non ha inserito dati sufficienti per essere inclusa nei risultati complessivi. Le rimanenti sono state raccolte nelle 3 categorie citate in funzione delle dimensioni valutate in base al numero di dipendenti informatizzati secondo i dati pubblicati dal rapporto annuale sulla PAC del 2009. Il risultato è riportato nel diagramma nella Figura 1. 6 “*Grandi*” con più di 10.000 dipendenti, 22 “*Medie*” tra 1.000 e 10.000 dipendenti e 11 “*Piccole*” con meno di 1.000 dipendenti.

Figura : Andamento dei 4 KPI negli ultimi 4 anni per le 3 classi di amministrazioni

Sono stati così disegnati i 3 grafici seguenti che riportano l’andamento dei valori medi dei 4 KPI negli ultimi 4 anni per ciascuna classe di Amministrazioni, evidenziando miglioramenti e arretramenti conseguiti nel settore sicurezza oltre che i valori assoluti ormai sufficientemente alti.

Il primo dato da notare è un complessivo andamento positivo per le Grandi Amministrazioni, che in valore assoluto mostrano valori molto alti (vicini all’ottimo) per tutti i KPI e sufficientemente stabili per l’intero periodo di osservazione.

Nel contempo sempre per le grandi amministrazioni ha prodotto lievi flessioni per KPI2 (-2,4%) e KPI3 (-4,3%) che comunque restano stabilmente vicini all’ottimo. Considerando che KPI2 è riguarda in larga misura attrezzature per la sicurezza e KPI3 la sicurezza dei servizi, il fenomeno potrebbe essere spiegato in virtù della riduzione di fondi dedicati alla sicurezza.

D’altra parte KPI4 storicamente l’indicatore che ha espresso maggiori criticità migliora ulteriormente raggiungendo anch’esso un valore ottimale ed allineandosi con gli altri indicatori.

Per quanto riguarda la classe delle medie amministrazioni, che rappresentano oltre la metà del campione (30/46), migliorano su tutti gli indicatori ma KPI4, che nell’anno precedente aveva subito un consistente arretramento, nonostante una consistente crescita (+15%) raggiunge appena la sufficienza. In termini di linee di tendenza c’è sicuramente da prendere atto che ormai l’intero campione ha adottato un modello di sicurezza ICT molto vicino a quello auspicato ed è solo questione di tempo la il raggiungimento della piena copertura dell’intero campione.

Questa riflessione è confermata con maggiore evidenza dal dato rilevato per le piccole amministrazioni (9/46), hanno esibito risultati in netto miglioramento (anche in controtendenza rispetto ai risultati negativi degli anni precedenti), per gli indicatori KPI3 (+32%) e KPI4 (+28,9%) che storicamente rappresentavano le maggiori criticità dell’intero campione. D’altro canto sempre le piccole amministrazioni, in maniera contradditoria hanno anche esibito consistenti quanto inspiegabili arretramenti per gli indicatori KPI1 (-5,8%) e KPI2 (-12,7%). Anche in questo caso, soprattutto per le piccole amministrazioni c’è da considerare l’aspetto risorse economiche che quindi ha condizionato le scelte costringendo le amministrazioni, concentrate sui progetti per rafforzare la sicurezza dei servizi e dell’organizzazione, a tralasciare gli altri aspetti.

Nei prossimi paragrafi saranno analizzati i singoli KPI commentando i quesiti che hanno fornito le indicazioni ritenute più interessanti.

### Sicurezza logica

Come si evince dai grafici discussi nel paragrafo precedente, l’indicatore KPI1 (Sicurezza Logica) ha conseguito miglioramenti costanti nel tempo precedenti indipendentemente dalla dimensione delle Amministrazioni. Partendo da posizioni distanti (evidentemente le piccole amministrazioni avevano un gap da colmare) oggi è possibile affermare che tutte le amministrazioni del campione mostrano una buona competenza/sensibilità in termini di sicurezza logica prestando attenzione al tema sicurezza soprattutto in fase di adozione di nuove procedure / soluzioni capaci di garantire i necessari livelli di affidabilità. La tabella finale riporta un dato significativo e cioè che per KPI1 medio sull’intero campione il valore dell’anno precedente (2009) è stato confermato nel 2010 fino alla seconda cifra decimale.

Esaminando più nel dettaglio i risultati per ogni singolo quesito del KPI1 la principale criticità è rappresentata da KPI1.7 che denuncia una scarsa attenzione verso la sicurezza (protezione) dei dati presenti su postazioni e dispositivi mobili che viaggiano all’esterno dell’organizzazione. Rispetto a questo dato, da sempre sotto la media dell’indicatore e sotto la sufficienza (4,94 nel 2010 rispetto al valore complessivo di 7,43 per KPI1) sarebbe importante avviare una campagna di sensibilizzazione per promuovere l’uso delle migliori pratiche per la sicurezza dei dati su dispositivi mobili. D’altro canto seppur lievemente il dato è in miglioramento (4,52 nel 2009, 4,18 nel 2008, 4,56 nel 2007).

Il dato più interessante tra i quesiti di KPI1 riguarda KPI1.3 e cioè la corretta attenzione da parte delle Amministrazioni verso le certificazioni per la sicurezza in fase di acquisizione di prodotti o servizi. Dalle risposte fornite al quesito KPI1.3 si rileva che quasi il 72% del campione richiede esplicitamente ai fornitori le certificazioni ufficialmente riconosciute e rilasciate. Questo dato è molto incoraggiante e testimonia un crescente interesse verso un tema che purtroppo ancora non è adeguatamente supportato da un impianto legislativo che imponga un processo di certificazione a chiunque intenda fornire prodotti o servizi alla Pubblica Amministrazione.

Seppur applicando tutti gli accorgimenti per rendere il sistema maggiormente affidabile, per la quasi totalità del campione (96%) il meccanismo di autenticazione per l’accesso alle postazioni di lavoro è sempre quello bassato su username e password (con scadenza automatica e controllo proattivo della robustezza). E’ già stata avviata una discussione interna per decidere se e quanto penalizzare questo meccanismo ormai datato e debole, puntando maggiormente sull’utilizzo di token o Smart card possibilmente utilizzando certificati già rilasciati da altri Enti come ad esempio la Carta Regionale dei Servizi ormai largamente diffusa e standardizzata.

Sempre positivi ed in costante miglioramento anche KPI1.8 (90%) e KPI1.9 (85%) relativi alla disponibilità di sistemi di backup e sistemi di controllo accessi. Il dato conferma che ormai tutte le amministrazioni hanno affrontato e risolto il problema del Backup/Restore dei dati gestendo correttamente il processo di salvataggio ed archiviazione dei dati in un locale separato ed ignifugo.

### Sicurezza dell’infrastruttura

Riguardo al tema della sicurezza fisica delle infrastrutture, KPI2 complessivamente ha registrato un anomalo -4,4% attestandosi ad un valore complessivo di 7,85. Su questo risultato pesa significativamente il regresso delle piccole Amministrazioni (-12,7%) che però nel 2009 avevano avuto una brusca impennata. In valore assoluto il dato rimane positivo con un valore complessivo pari a 7,85 molto vicino alla soglia dell’ottimo. Su questo dato sicuramente incide ancora molto la disponibilità nel listino di SPC di prodotti per la sicurezza (molto spesso inclusi in bundle con le forniture standard di accesso alla rete) e la naturale propensione delle amministrazioni ad investire in termini di dispositivi hardware per la protezione delle proprie dotazioni informatiche piuttosto che in formazione e risorse umane.

Unica nota dolente è rappresentata dai quesiti KPI2.5 e KPI2.5a. In sintesi 26 amministrazioni fanno uso di reti Wireless (Wi-Fi) ma solo 12 utilizzano il protocollo WPA per garantire la sicurezza del canale radio. 4 Utilizzano il protocollo WEP con note debolezze e tutte le altre non adottano particolari accorgimenti. Il valore complessivo dei 2 indici di 5,57 non traduce correttamente la gravità del dato. Anche in questo caso sarebbe utile aggiornare il modello. Ormai innegabile la praticità e l’utilità delle reti wireless purché queste siano adeguatamente protette. D’altra parte il modello attuale tende ad assegnare la sufficienza (6 punti) a chi dichiara di non utilizzare reti Wi-Fi. Ancora una volta è particolarmente significativo il ruolo che DigitPA potrebbe assumere rispetto a queste problematiche: da un lato occorre formazione specifica, dall’altro un meccanismo più rigido di certificazione degli impianti della PA per essere certi che rispettino almeno i requisiti minimi di sicurezza.

I primi due quesiti confermano che circa il 90% del campione dispone di barriere fisiche per limitare e perimetrare l'accesso alle risorse di calcolo (91,3%), e di un sistema di controllo degli accessi fisici ai locali dove si trovano le risorse di calcolo (89,1%). Molto più ridotto invece il numero delle amministrazioni che si sono dotate di un sistema di videosorveglianza H24 che passa dal 56,5% al 69,6%. Anche questi 3 quesiti rappresentano temi davvero consolidati e potrebbero far parte dei quesiti da svecchiare in un modello più ambizioso e robusto.

Analoghe considerazioni, sia per la rigida applicazione del listino SPC sia perché ormai rappresentano pratiche consolidate, vanno fatte per il tema firewall, sistemi di rilevazione e prevenzione delle intrusioni. Anche in questo caso i quesiti andrebbero riformulati per meglio cogliere le motivazioni che spingono una amministrazione a gestire in-house una DMZ anziché ricorrere a servizi centralizzati in outsourcing delegando al fornitore il problema della robustezza dei servizi fruibili via rete pubblica.

### Sicurezza dei servizi

KPI3, l’indicatore che misura la robustezza dei servizi, nel corso dell’anno 2010 ha avuto un duplice comportamento indicando un lieve arretramento per quanto riguarda la grandi Amministrazioni ed un netto miglioramento per le medie e piccole amministrazioni. Infatti il valore medio è passato da 6,61 a 7,13 mentre le piccole amministrazioni sono cresciute del 32% passando dal valore di 4,78 nel 2009 a 6,31 nel 2010. Andando oltre i valori numerici c’è da rilevare per questo indicatore in particolare la presenza di temi ormai decisamente consolidati e poco indicativi, come la presenza di antivirus ad esempio, insieme a temi decisamente importanti e nuovi come quello della Continuità Operativa.

In altre parole questo indicatore è quello che più di ogni altro risente del tempo trascorso dalla prima formulazione dei quesiti e deve essere sicuramente aggiornato nelle prossime edizioni. Il risultato mediamente positivo non deve invece nascondere clamorose defiance come la scarsa attenzione rivolta dalle amministrazioni al tema “Disaster Recovery” nonostante esplicitamente contemplato dal nuovo Codice dell’Amministrazione Digitale (CAD2). Nonostante il netto miglioramento, i punteggi relativi ai quesiti KPI3.1, KPI3.2 e KPI3.3, rispettivamente 4,3, 5,3 e 4,0, i valori sono restati sotto la soglia critica. Volendo analizzare i risultati conseguiti nella serie storica, è evidente che dopo 5 anni ancora rimane molto da fare rispetto a questi temi e sicuramente dovranno essere intraprese strategie diverse. Ad esempio per rendere più accessibile le buone pratiche anche alle piccole amministrazioni, risparminado risorse e riducendo i rischi di insuccesso, si potrebbero pensare alla realizzazione di centri operativi in grado di erogare in maniera centralizzata servizi di disaster recovery. Un’azione ancora più radicale potrebbe prevedere l’attivazione di sistemi informativi basati su architetture di cloud computing, inerentemente più robuste e indipendenti dal luogo fisico di installazione del centro. Tutte queste scelte attengono alla definizione di un modello unico frutto di un gruppo di lavoro che dopo aver fissato gli obiettivi primari a cui tendere, intende offrire alle amministrazioni anche soluzioni e strumenti per garantire il raggiungimento dei livelli di qualità attesi.

In sintesi sul tema sicurezza dei servizi, oltre ai servizi di base quali la posta elettronica e i siti web, le tumultuose novità tecnologiche in termini di architetture e modalità di erogazione dei servizi hanno spinto ad un completo riformulazione degli impianti sia in termini architetturali che in termini di attori preposti alla realizzazione e mantenimento degli impianti, spingendo sempre più a considerare l’outsourcing e l’hosting come soluzioni privilegiate almeno per le piccole e medie realtà.

E’ sempre più naturale investire in questa direzione anche perché è evidente che crescendo il livello di informatizzazione della PA aumentano anche l’importanza del ruolo rivestito dai servizi erogati on-line e contemporaneamente ed il rischio di subire danni derivanti dalla indisponibilità, seppur temporanea, dei servizi offerti.

Ultimo discorso riguarda il quesito KPI3.9 e cioè la rilevazione delle intrusioni e la capacità di reagire o semplicemente tenere traccia di quanto avvenuto. Anche grazie al supporto multilevello di SPC ormai il numero di intrusioni (non di tentativi) è in netto calo ed ogni amministrazione che accede alla rete pubblica attraverso SPC può fruire di un servizio di monitoraggio analogo a quello erogato dai CERT. Anche questi quesiti andrebbero riformulati in modo da riflettere il senso ampio del concetto di intrusione che può avvenire anche attraverso canali diversi dalla rete e soprattutto avvalendosi di tecniche di attacco più sofisticate e difficili da rilevare. Il dato positivo è che, nonostante il minor numero di intrusioni rilevate, è cresciuta comunque la sensibilità degli utenti e la capacità tecnica di rilevare tentativi di intrusioni che molto verosimilmente in passato passavano inosservati.

### Sicurezza dell’organizzazione

KPI4 da sempre è l’indicatore che ha espresso le maggiori debolezze fornendo anche indicazioni rilevanti sui principali correttivi da mettere in atto per migliorare lo stato complessivo della PAC, avvicinando le Amministrazioni al modello atteso. Il valore medio di 6,86 ha finalmente superato la soglia della sufficienza riflettendo un miglioramento diffuso per tutte le tipologie di amministrazione. Ovviamente le grandi (valore 8,23) si comportano decisamente meglio. Unico caso in tutto il questionario, per KPI4 le amministrazioni di medie dimensioni esibiscono comportamenti peggiori rispetto alle piccole (5,78 per le medie vs. 6,58 per le piccole).

Entrando nel merito dei singoli quesiti, rispetto alla sicurezza delle proprie organizzazione, le Amministrazioni intervistate hanno stranamente mostrato le maggiori debolezze proprio nell’attuazione delle norme ormai consolidate come ad esempio le prescrizioni del primo Codice dell’Amministrazione Digitale o il DM del 16/2/2002. KPI4.1 infatti con un valore medio di 5,43 denuncia che sono ancora molte le Amministrazioni che non hanno definito ed approvato un piano per la sicurezza ICT. In maniera ancora più netta, KPI4.3 con un valore di 4,35 testimonia che in molti casi all’interno del campione intervistato non sono stati attribuito i ruoli e le responsabilità previste dal Decreto Ministeriale. Tutti gli altri quesiti tranne KPI4.10 e KPI4.13 sono ormai stabilmente sopra la soglia della sufficienza, indicando buoni risultati diffusi su tutto il campione per quanto riguarda le altre pratiche come la corretta tenuta dei dati personali, la corretta gestione del ricorso all’outsourcing, le responsabilità della gestione dei log, dei backup, ed in generale nella gestione degli incidenti informatici.

Criticità ancora maggiori sono emerse nella gestione dei budget per la sicurezza KPI4.10 e nella pianificazione di attività specifiche di formazione sul tema sicurezza ICT per il personale interno KPI4.13. Con un valore di 2,78, KPI4.10, anche in funzione dei noti tagli ai budget delle Pubbliche Amministrazioni, riflette il fatto che solo un’Amministrazione su 46 ha definito un budget per la sicurezza maggiore del 10% del totale e solo 8 con un budget per la sicurezza compreso tra il 5% ed il 10% del totale.

Analogamente KPI4.13 con un valore medio di 3,91 denuncia che pochissime energie vengono spese per la formazione del personale interno, suggerendo in maniera evidente che iniziative per la definizione di programmi di formazione erogati anche in modalità FAD potrebbero avere un grande successo migliorando il risultato complessivo. Infatti, utenti non adeguatamente formati alla cultura della sicurezza, rischiano di vanificare tutti gli sforzi spesi per rafforzare le misure di sicurezza.

## Considerazioni finali

In quest’ultimo paragrafo, saranno fornite alcune considerazioni che, frutto dell’analisi dei dati raccolti, possono motivare i fenomeni descritti nei precedenti paragrafi. In particolare, si tenderà ad illustrare i macrofenomeni osservati attraverso rappresentazioni grafiche di estrema sintesi e tavole sinottiche per riportare le serie storiche e quindi le linee di tendenza relative alle rilevazioni effettuate negli ultimi 4 anni.

Inoltre aver ripartito il campione in 3 classi omogenee ha consentito di differenziare sia le interpretazione delle problematiche e le possibile cause, sia le contromisure da attuare.

Il grafico riportato nella Figura 3 rappresenta il massimo livello di sintesi raggiungibile. Per interpretare il grafico correttamente occorre considerare i colori e le dimensione delle sfere rappresentate. Infatti nell’area verde sono stati collocate le Amministrazioni che hanno raggiunto un livello ottimale di sicurezza (il valore del KPI è maggiore di 7). Nell’area gialla sono state collocate le amministrazioni che hanno raggiunto un valore dei KPI prossimo alla sufficienza (compreso tra 5 e 7), e nell’area rossa tutte le amministrazioni che si sono collocate al di sotto della soglia di criticità, per le quali quindi è assolutamente necessario intraprendere una serie di interventi mirati ad aumentare la sensibilità nei confronti del tema Sicurezza ICT. La dimensione delle sfere è proporzionale al numero di Amministrazioni che ricadono nel range prestabilito. Come si vede la grande maggioranza delle amministrazioni si colloca ormai nella parte alta del grafico in particolare per KPI1 (44/46) e KPI2 (41/46). Per KPI3 e KPI4 invece molte di queste passano nella zona critica (7 per KPI3 e 12 per KPI4).

Figura : Classificazione delle amministrazioni in funzione del punteggio conseguito per ciascun KPI

L’altro fenomeno da investigare ulteriormente è la presenza di ben 5 amministrazioni nell’area di forte criticità per l’indicatore KPI2. In realtà la cosa risulta particolarmente sorprendente se si considera che KPI2 ha il maggiore numero di amministrazioni classificate nella fascia ottimale. Per tutte le Amministrazioni classificate nell’area di forte criticità (ben 7 per KPI4) sarà necessaria una indagine di secondo livello per trovare le motivazioni ed individuare degli accorgimenti per migliorare la situazione.

Infine la tabella seguente riporta in maniera numerica per maggiore dettaglio l’andamento dei 4 KPI calcolati per le tre classi omogenee e come media per l’intero campione anno per anno a partire dalla rilevazione del 2007, indicando anche le variazioni in percentuale ottenute confrontando il dato con quello dell’anno precedente.

A meno di alcuni netti regressi, in generale collocati nei periodi di maggiore mancanza di risorse economiche destinate alla sicurezza, è possibile affermare che le specifiche esperienze, note come best practice per la sicurezza ICT, si vanno via via affermando e diffondendo all’interno del campione.

Gran parte dei miglioramenti ottenuti sono anche da imputare alle iniziative che DigitPA ha intrapreso per sostenere la diffusione del modello adottato riducendo drasticamente il numero delle amministrazioni che si collocano sotto la soglia di criticità.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 2007 | 2008 | 2009 | 2010 | Δ% 2008 | Δ% 2009 | Δ% 2010 |
| Grandi | KPI 1 | 8,42 | 7,33 | 8,40 | 8,50 | -13,0% | 14,6% | 1,2% |
| KPI 2 | 8,53 | 8,29 | 8,77 | 8,56 | -2,9% | 5,8% | -2,4% |
| KPI 3 | 7,89 | 7,48 | 8,40 | 8,04 | -5,2% | 12,3% | -4,3% |
| KPI 4 | 7,62 | 7,76 | 8,05 | 8,23 | 1,8% | 3,8% | 2,2% |
| Medie | KPI 1 | 6,97 | 7,29 | 7,22 | 7,57 | 4,6% | -0,9% | 4,8% |
| KPI 2 | 8,01 | 8,21 | 8,44 | 8,51 | 2,4% | 2,9% | 0,8% |
| KPI 3 | 7,00 | 7,05 | 6,65 | 7,03 | 0,7% | -5,7% | 5,7% |
| KPI 4 | 6,12 | 6,21 | 5,00 | 5,78 | 1,5% | -19,4% | 15,6% |
| Piccole | KPI 1 | 6,58 | 7,32 | 7,53 | 7,09 | 11,4% | 2,8% | -5,8% |
| KPI 2 | 5,95 | 6,62 | 7,42 | 6,48 | 11,2% | 12,1% | -12,7% |
| KPI 3 | 5,66 | 6,05 | 4,78 | 6,31 | 6,9% | -21,0% | 32,0% |
| KPI 4 | 4,46 | 5,17 | 5,10 | 6,58 | 15,9% | -1,3% | 28,9% |
| Tutte | KPI1 | 7,32 | 7,31 | 7,72 | 7,72 | -0,1% | 5,5% | 0,0% |
| KPI2 | 7,50 | 7,70 | 8,21 | 7,85 | 2,7% | 6,6% | -4,4% |
| KPI3 | 6,85 | 6,86 | 6,61 | 7,13 | 0,1% | -3,7% | 7,8% |
| KPI4 | 6,07 | 6,38 | 6,05 | 6,86 | 5,1% | -5,1% | 13,4% |

Tabella 1: Andamento dei 4 indicatori negli ultimi 4 anni

L’altra considerazione che scaturisce dalla lettura dei dati in tabella è la conferma che il modello per la sicurezza ICT si è consolidato ed ormai richiede un accurato lavoro per essere tenuto aggiornato e per programmare l’indirizzo da dare alle amministrazioni per i prossimi 5 anni. Ad esempio per le grandi amministrazioni ormai i 4 indicatori sono stabilmente oltre il valore 8 che significa che nessuna amministrazione si discosta (in media) dal modello atteso per più di 2 quesiti (100 punti su 12 quesiti).

E’ altresì chiaro che l’anello debole della catena è quello che rischia di pregiudicare gli sforzi di tutti. Va segnalato che vi sono ancora amministrazioni nel campione che hanno disatteso più del 50% dei quesiti. In particolare occorre concentrare tutti gli sforzi verso queste amministrazioni, ed in particolare verso le amministrazioni più piccole che in virtù di una cronica mancanza di risorse da sempre hanno mostrato minore sensibilità nei confronti della sicurezza ICT, percependo le norme relative alla sicurezza ICT come una imposizione che produce solo maggiori costi, anziché come una opportunità verso la quale tendere per migliorare i propri servizi e quelli offerti al pubblico.

Anche quest’anno saranno prodotte schede singole a disposizione delle Amministrazioni che ne faranno richiesta per avere un approfondimento sulle proprie performance in termini di sicurezza rispetto all’intero campione e le medie per ciascuna categoria. Per quelle Amministrazioni che hanno esibito risultati particolarmente critici, attraverso indagini di secondo livello sarà possibile verificare il dato rilevato e nel caso questo venga confermato, saranno definite le attività necessarie per produrre una netta inversione di tendenza per gli anni a venire.

Sempre pensando alle piccole e medie amministrazioni, sfruttando la possibilità offerte dalle nuove tecnologie del cloud computing è finalmente possibile realizzare centri servizi che in maniera centralizzata potranno rispondere, su temi specifici quali il disaster recovery, alle esigenze di più amministrazioni. In questo modo oltre a raggiungere una massa critica che consente alti livelli qualitativi, sarà possibile realizzare concreti risparmi, condividendo le infrastrutture ed evitando duplicazioni. E’ utile sottolineare che soprattutto nel contesto del cloud computing, l’aspetto sicurezza ICT assume un ruolo ancora più determinante, dovendo necessariamente portare i dati fuori dal perimetro fisico della amministrazione che intende aderire all’iniziativa. Solo attraverso un uso sistematico e consapevole delle moderne tecniche crittografiche sarà possibile effettivamente digitalizzare il proprio patrimonio informativo e garantire al tempo stesso l’integrità e la confidenzialità delle informazioni trattate.

Si ribadisce infine che la metodologia sottesa dal questionario somministrato per la raccolta dei dati puntuali intende misurare l’attenzione dei responsabili rispetto al tema sicurezza ICT ma così come concepita non può essere impiegata per rilevare l’esposizione al rischio di ciascuna amministrazione. Le uniche informazioni specifiche alla singola Amministrazione potranno essere ottenute solo attraverso indagini di secondo livello incrociando i dati rilevati sul campo (rete SPC) o ricostruendo i dati provenienti dall’osservatorio sugli incidenti di sicurezza del Sistema Pubblico di Connettività, gli unici in grado di confermare la reale esattezza dei risultati valutati attraverso il questionario.

In conclusione, nella rilevazione 2010 è emerso un quadro certamente rassicurante per la stragrande maggioranza delle Amministrazioni appartenenti al campione, in netto miglioramento rispetto ai valori raccolti nelle prime edizioni. Per ogni ulteriore approfondimento si rimanda alla relazione estesa sull o stato della sicurezza della PAC.

1. Tutte le amministrazioni che non hanno risposto almeno a 4 quesiti per ciascuna sezione vengono automaticamente escluse dal calcolo del valore medio [↑](#footnote-ref-1)