**Quarto rapporto sullo stato della sicurezza ICT delle PAC**

|  |  |  |
| --- | --- | --- |
| **Compilato** | **:** |  |
| **Rivisto** | **:** | **G. RELLINI LERZ** |
| **Autorizzato** | **:** |  |
| **Versione** | **:** | **1.** |
| **Distribuito** | **:** | **DIGITPA - PAC** |

# Indice

Indice 2

Indice delle Figure 3

Indice delle Tabelle 3

1 Premesse 4

1.1 Contenuti del documento 4

2 Finalità della rilevazione 5

2.1 Obiettivi 5

2.2 Struttura del questionario 5

2.3 Elementi di novità 6

3 Presentazione della metodologia applicata 7

3.1 Raccolta e Valutazione dei dati 7

3.2 Gli indicatori rilevati 9

3.2.1 KPI1: Sicurezza logica 10

3.2.2 KPI2: Sicurezza dell'infrastruttura 10

3.2.3 KPI3: Sicurezza dei servizi 11

3.2.4 KPI4: Sicurezza dell’organizzazione 11

4 Presentazione dei risultati 12

4.1 Risultati di sintesi e linee di tendenza 12

4.2 KPI1: Sicurezza logica 16

4.3 KPI2: Sicurezza dell'infrastruttura 20

4.4 KPI3: Sicurezza dei servizi 23

4.5 KPI4: Sicurezza dell’organizzazione 27

5 Considerazioni conclusive (TBD) 32

# Indice delle Figure

Figura 1: Distribuzione delle Amministrazioni rispetto al numero di dipendenti 9

Figura 2: Distribuzione dei 4 KPI medi rispetto alle 3 soglie 13

Figura 3: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le grandi amministrazioni 14

Figura 4: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le medie amministrazioni 14

Figura 5: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le piccole amministrazioni 14

Figura 3: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le grandi amministrazioni 14

Figura 4: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le piccole amministrazioni 14

Figura 5: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le medie amministrazioni 14

Figura 10: Distribuzione dei risultati relativi al KPI1 rispetto alle 3 soglie 17

Figura 11: Valori medi delle risposte ai quesiti relativi al KPI1 17

Figura 12: Distribuzione dei risultati relativi al KPI2 rispetto alle 3 soglie 21

Figura 13: Valori medi delle risposte ai quesiti relativi al KPI2 21

Figura 14: Distribuzione dei risultati relativi al KPI3 rispetto alle 3 soglie 25

Figura 15: Valori medi delle risposte ai quesiti relativi al KPI3 25

Figura 16: Distribuzione dei risultati relativi al KPI4 rispetto alle 3 soglie 29

Figura 17: Valori medi delle risposte ai quesiti relativi al KPI4 29

# Indice delle Tabelle

Tabella 1: Soglie numeriche per la interpretazione dei risultati complessivi 12

Tabella 2: Analisi della distribuzione dei 4 KPI nel campione rispetto alle dimensioni delle Amministrazioni 14

Tabella 4: Quesiti e risultati relativi al KPI1 20

Tabella 5: Quesiti e risultati relativi al KPI2 23

Tabella 6: Quesiti e risultati relativi al KPI3 26

Tabella 7: Quesiti e risultati relativi al KPI4 32

# Premesse

## Contenuti del documento

Il documento fa riferimento ai dati raccolti attraverso il questionario per la rilevazione dello stato dell’ICT delle PAC nei primi mesi dell’anno 2011 ed è composto da quattro paragrafi, oltre alla premessa:

* Struttura e obiettivi del questionario;
* Presentazione della metodologia applicata;
* Presentazione dei risultati;
* Valutazioni complessive.

Il paragrafo 2 “Finalità della rilevazione” introduce brevemente gli obiettivi prefissati e la struttura del questionario. Nel paragrafo successivo viene presentata la metodologia utilizzata per analizzare i dati raccolti e tradurli in coefficienti con un significato oggettivo (*Key Performance Indicator*). Il paragrafo 4 Presentazione dei risultati analizza i risultati per ogni singolo quesito mettendo in evidenza eventuali criticità mentre l’ultimo paragrafo raccoglie sotto forma di considerazioni finali le indicazioni scaturite dall’analisi dell’intero campione, proponendo misure correttive ed azioni da intraprendere nel futuro come contromisure.

In estrema sintesi, come risulterà poi dalla presentazione dei dati raccolti, il questionario 2010 ha fornito un quadro dello stato della Sicurezza ICT nella Pubblica Amministrazione Centrale abbastanza confortante e sicuramente sufficientemente maturo per recepire ogni indicazione per migliorare gli standard attuali scaturita da iniziative condivise di DigitPA.

Rispetto alle rilevazioni precedenti il miglioramento è stato netto, anche in virtù di iniziative promosse centralmente come il progetto SPC (Sistema Pubblico di Connettività) che è entrato ormai nella fase piena di esercizio.

Come ulteriore difficoltà nella interpretazione dei dati, occorre dire che il campione analizzato risulta fortemente disomogeneo e caratterizzato da un’estrema diversità di funzioni e di obiettivi. Per meglio affrontare questo problema, quest’anno il campione è stato suddiviso in 3 sottoinsiemi molto più omogenei. Indicazioni più puntuali potranno emergere solo da un’indagine di secondo livello condotta con le singole Amministrazioni.

Altra grossa criticità, dalla quale discendono molti dei comportamenti errati rilevati, è la mancanza di piani di formazione per la sensibilizzazione dei dipendenti della PAC. Benché fortemente correlati, emerge con chiarezza una dicotomia tra il tema trattamento dei dati sensibili e quello della Sicurezza più in generale. Infatti, mentre la normativa relativa al primo punto (D.L.vo n. 196 del 27 Giugno 2003) è stata largamente recepita anche con risultati oltre le aspettative, il tema Sicurezza ICT ancora stenta a trovare stabili radici nei responsabili della PAC. D’altra parte è facile intuire come una intrusione in un sistema informativo della PAC possa mettere a repentaglio una immensa quantità di dati sensibili. A tal proposito DigitPA ritiene che sia giusto forzare l’adozione di policy, anche attraverso un opportuno quadro normativo, in grado di stimolare maggiore attenzione nei confronti della sicurezza legando in maniera indissolubile il trattamento dei dati sensibili e la sicurezza dell’intero sistema informativo.

# Finalità della rilevazione

## Obiettivi

Obiettivo primario della rilevazione annuale è quello di disporre di dati oggettivi ed aggiornati che possano consentire a DigitPA di tracciare un quadro organico sullo stato della Sicurezza ICT all’interno della PAC. Tali dati, infatti, vengono raccolti ed elaborati ogni anno per avere una misura della *sensibilità* che ogni singola Amministrazione, e nel complesso l’intera PAC, ha sviluppato rispetto al tema della Sicurezza Informatica.

Da questo obiettivo primario derivano 2 sotto obiettivi altrettanto importanti:

* Sviluppare un modello unico e condiviso di Sicurezza ICT per tutta la PAC
* Fornire a tutte le Amministrazioni che annualmente collaborano per la raccolta dati un’indicazione precisa e puntuale sulle prestazioni raggiunte rispetto al modello atteso ed eventuali contromisure da mettere in atto in presenza di forti criticità.

Rispetto al primo punto DigitPA da tempo ha iniziato a sviluppare un modello comune per sicurezza coniugando i più recenti risultati emanati dagli organismi internazionali deputati a definire standard e metriche per la Sicurezza ICT con una profonda conoscenza dei processi interni e delle problematiche tipiche del mondo della PA che DigitPA ha acquisito nel corso degli anni. Tale modello, nel corso degli ultimi 5 anni è stato costantemente aggiornato utilizzando gli stessi risultati raccolti nelle precedenti rilevazioni per determinare l’esigenza di svecchiare alcuni quesiti o di aggiungerne di nuovi.

I due sotto obiettivi sono fortemente correlati, infatti, solo disponendo di un modello comune per la sicurezza, sarà possibile effettuare il monitoraggio puntuale dell’utenza, ed eventualmente fornire agli utenti stessi indicazioni precise su quanto si sta realizzando attraverso progetti interni e quanto rimane da fare per correggere eventuali scostamenti dal modello atteso.

Il fine ultimo, quindi, non è quello di stilare graduatorie di merito bensì quello di raccogliere dati oggettivi per governare un tema così delicato, prevenendo ogni situazione di rischio e garantendo la crescita omogenea, anche per le piccole Amministrazioni. Si auspica infatti che tutte le Amministrazioni devono tendere verso standard di Sicurezza sufficienti per affrontare le inevitabili falle nei propri sistemi che potrebbero causare gravi danni all’intero sistema incidendo negativamente sui servizi offerti ai cittadini. E’ pertanto indispensabile che tutte le strutture informatiche della PAC raggiungano la stessa “maturità e consapevolezza” su ogni possibile elemento di criticità presente nei propri sistemi informativi.

Ultima opportunità offerta dalla rilevazione è quella di poter identificare e successivamente avviare, attraverso i dati raccolti, azioni specifiche atte a ridurre il gap rispetto al modello atteso laddove si dovessero evidenziare criticità diffuse all’interno di un sottoinsieme delle Amministrazioni che hanno partecipato.

In particolare per le amministrazioni i cui risultati ricadono al di sotto della soglia di criticità prefissata saranno fornite indicazioni puntuali sulle criticità riscontrate ed eventualmente le contromisure da mettere in atto per ribaltare il risultato negativo. A tal fine quest’anno saranno redatte schede sintetiche per ciascuna amministrazione e sono stati pianificati cicli di incontri con le Amministrazioni per approfondimenti di secondo livello.

## Struttura del questionario

Per meglio raggiungere gli obiettivi della rilevazione esposti nel precedente paragrafo è stato realizzato e aggiornato negli anni un questionario on-line impiegato come strumento principale per la raccolta dei dati oggetto della rilevazione annuale. Tale questionario discende direttamente dal modello comune per la Sicurezza ICT che DigitPA ha messo a punto. Il questionario è stato strutturato in 4 sezioni ognuna dedicata ad una particolare prospettiva sul tema complessivo della Sicurezza. Le 4 sezioni hanno ereditato il titolo dal KPI corrispondente ed ognuna di queste presenta il set di quesiti individuato per il calcolo del Key Performance Indicator. Ogni KPI esprime infatti numericamente, in maniera estremamente sintetica, un indice prestazionale oggettivamente rilevabile attraverso la metodologia descritta nel prossima paragrafo. L’insieme di tutti i quesiti presenti nel questionario di fatto ricopre a 360 gradi tutti gli aspetti connessi al tema Sicurezza ICT, spaziando dalle dotazioni hardware/software alla organizzazione dedicata alla sicurezza. Per evitare duplicazioni dei dati disponibili è stato stralciato dal questionario il tema connettività ed attrezzature di rete poiché da qualche anno tutte la Pubblica Amministrazione dispone di soluzioni standard che offrono ottimi livelli di sicurezza attraverso il listino del Sistema Pubblico di Connettività.

## Elementi di novità

Ad ulteriore testimonianza del livello di maturità raggiunto dal modello adottato per la Sicurezza ICT, come per l’anno precedente non è stato necessario apportare alcuna modifica al questionario, alle risposte previste ed ai pesi assegnati a queste rispetto alle ultime due rilevazioni. Da ciò deriva anche il vantaggio di poter analizzare insieme ai dati puntuali dell’anno corrente anche le linee di tendenza che il campione ha assunto negli ultimi anni. Anche a livello di singola Amministrazione sarà possibile effettuare raffronti diretti nel tempo ottenendo preziose indicazioni in grado di correlare le prestazioni con il periodo in cui queste sono state conseguite.

A tal fine è stato aggiunto un paragrafo che illustra appunto le linee di tendenza per ciascuna classe di Amministrazioni che hanno partecipato. Inoltre è stato aggiornato il formato delle tabelle per aggiungere le serie storiche per ogni quesito inserendo i valori medi negli ultimi 3 anni e le differenze anno per anno. Quest’ultime sono state espresse in percentuale per dare una migliore indicazione rispetto al numero di partecipanti che può cambiare di anno in anno.

Eventuali miglioramenti sono evidenziati colorando la cella in verde, mentre al contrario regressioni superiori al -3% colorano le cella di rosso, indicando situazioni anomale di potenziale rischio.

Anche l’analisi per dimensioni omogenee (piccole, medie e grandi amministrazioni) in funzione del numero complessivo di dipendenti introdotta per la prima volta con la rilevazione 2007, è stata mantenuta, confermando le stesse soglie utilizzate l’anno precedente. Rispetto alle dinamiche interne al campione della PAC (soppressione o accorpamenti di enti, ridenominazione dell’Ente, ecc.) si precisa che, per quanto possibile, è stata mantenuto un unico identificativo per tutte le amministrazioni censite, indipendentemente da ogni cambio di nome. Le tabelle riportano solo i risultati delle amministrazioni che hanno risposto al questionario identificandole con i dati forniti nell’anagrafica dai responsabili della compilazione.

Per tutte le Amministrazioni che ne faranno richiesta saranno compilate schede di sintesi che riporteranno i dati puntuali quesito per quesito, raffrontati alla media del campione di dimensioni analoghe. Per quelle che sono ricadute sotto la soglia di criticità, saranno fornite indicazioni specifiche e raccomandazioni molto puntuali, con azioni correttive definite in funzione delle risposte che fornite ai quesiti si sono discostate dal modello atteso.

Infine, è noto che nel periodo di riferimento il progetto SPC è andato pienamente a regime e la quasi totalità delle amministrazioni intervistate ormai dispone di una connessione e dei servizi previsti dal contratto SPC. Ciò ha modificato radicalmente la configurazione della rete della Pubblica Amministrazione, e facendo in modo che la connettività geografica venga considerata sempre più come una commodity, basata su pratiche ben consolidate e con pochi spazi di miglioramento dal punto di vista della sicurezza, pertanto il questionario continuerà a non trattare esplicitamente tali argomenti.

# Presentazione della metodologia applicata

## Raccolta e Valutazione dei dati

Come negli anni precedenti il questionario è stato compilato dai responsabili delle Amministrazioni appartenenti al campione individuato attraverso strumenti on-line raccogliendo direttamente le risposte fornite in una base dati per poter essere successivamente elaborati. Per ridurre il più possibile errori di interpretazione tutti i quesiti sono stati proposti nella formula “scelta singola in un insieme chiuso di risposte”.

Il questionario nella revisione attuale è composto da 55 quesiti. 15 di questi sono definiti di secondo livello, cioè sono attivi solo in presenza di una determinata risposta al quesito precedente che li include in un’unica valutazione.

Prima di avviare la raccolta dei dati sono stati tenuti seminari divulgativi per chiarire direttamente ai responsabili gli obiettivi e le modalità di compilazione. E’ stato anche attivato un help-desk per fornire ulteriori chiarimenti sui quesiti presentati. Infine ogni utente ha ricevuto le proprie credenziali per accedere al questionario on-line ed attraverso un sito web appositamente allestito ogni utente ha potuto inserire le risposte relative alla propria organizzazione. La stessa procedura consentiva fino alla chiusura definitiva di rivedere e modificare i dati inseriti per riflettere eventuali evoluzioni intervenute nel periodo di inserimento dati. Per non condizionare le risposte, durante l’inserimento dei dati non è stata fornita nessuna indicazione agli utenti sulla interpretazione della risposta fornita né sul risultato complessivo per ogni indicatore.

Nei paragrafi successivi per ogni indicatore sarà fornita una tabella complessiva che riporta l’insieme di quesiti che ne fanno parte e per ognuno di questi le risposte ammesse con i relativi punteggi. Accanto ad ogni quesito si indicheranno i tre valori medi relativi al risultato dell’anno corrente e ai due anni precedenti per consentire una migliore analisi dei trend osservati da campione.

Sotto ad ogni quesito sono poi state riportate le risposte attese e per ognuna di queste le tabelle riportano il punteggio assegnato a ciascuna risposta, la % di amministrazioni che nell'anno corrente ha fornito la specifica risposta e sempre per analizzare i trend scostamento e % delle risposte nei due anni precedenti (2008-2009). Il dato viene fornito in percentuale perché il numero di amministrazioni che hanno partecipato alla rilevazione è cambiato nel corso degli ultimi due anni.

Ovviamente per ogni quesito sono state contate anche i casi in cui la risposta non è stata fornita, nella riga indicata come “N.R.” (non risponde). Ad ogni risposta non fornita il punteggio assegnato è stato 0 e ciò evidentemente si ripercuote sulla media complessiva per il calcolo dell’indicatore.

Per avere risultati più oggettivi e facili da interpretare in un report basato sui 4 indici individuati è stata adottata la stessa procedura degli anni precedenti descritta nel seguito per la normalizzazione dei risultati ed il calcolo dei valori numerici dei 4 indici:

1. Ad ogni quesito (o gruppo di quesiti nel caso di quesiti dipendenti) è stato assegnato un peso totale pari a 10 punti se la risposta è coerente rispetto al modello atteso o altrimenti un punteggio decrescente fino a 0 nel caso si allontani dal modello scelto.
2. Laddove previsto si è poi proceduto al *concatenamento logico* dei quesiti scomposti in più quesiti perché complessivamente possano rappresentare un unico risultato (con valore complessivo comunque compreso tra 0 e 10). Questo è necessario ad esempio per i quesiti dipendenti[[1]](#footnote-1) o per tutti quelli che ammettevano risposte multiple come ad esempio la lista delle certificazioni per la sicurezza riconosciute. Al termine di questa fase il numero totale di quesiti si è ridotto a 40.
3. L’insieme dei quesiti previsti per il questionario, opportunamente raccolti in 4 sotto insiemi distinti, sono stati associati a 4 indici prestazionali, nel seguito indicati come “*Key Performance Indicator*” o per brevità KPI, descritti nei prossimi paragrafi.
4. Per ogni Amministrazione sono stati calcolati i 4 KPI corrispondenti al valore medio dei punteggi ottenuti per ciascun quesito appartenente all’insieme individuato dal KPI. Quesiti senza risposta sono stati considerati risposte negative. Pertanto ogni valore medio sarà un numero compreso tra 0 e 10.
5. Successivamente sono state assegnate 3 soglie per raccogliere i risultati nelle 4 fasce: *ottima*, *buona*, *accettabile*, *scarsa*. L’ultima soglia, rappresenta il valore minimo al di sotto del quale il risultato è da considerarsi assolutamente critico rispetto al livello minimo di Sicurezza atteso. In altre parole le Amministrazioni che si posizioneranno al di sotto di tale soglia hanno un livello di criticità tale da richiedere l’avvio di azioni interne e/o coordinate da DigitPA con alta priorità. La Figura 2: Distribuzione dei **4 KPI medi rispetto alle 3 soglie** riporta questo tipo di risultato di massima sintesi.
6. Prima di procedere al calcolo dei valori medi del campione analizzato, per aumentare il livello di significatività del dato, l’intero insieme delle Amministrazioni (46 in totale) è stato suddiviso in 4 sottoinsiemi. Dapprima, per non influenzare negativamente i valori medi, sono state eliminate dal campione tutte le Amministrazioni che, per diversi motivi o per ragioni di riservatezza, non hanno completato il questionario lasciando senza risposta più del 50% dei quesiti di almeno un KPI[[2]](#footnote-2). Infine le restanti sono state ripartite in funzione del numero di dipendenti e precisamente 9 *piccole* con meno di 1.000 dipendenti, 30 *medie* con un numero compreso tra 1.000 e 10.000 dipendenti, 6 *grandi* con oltre 10.000 dipendenti (cf. Figura 1: Distribuzione delle Amministrazioni rispetto al numero di dipendenti).
7. Per ciascun gruppo di Amministrazioni sono stati calcolati i valori medi di ognuno dei 4 KPI conseguiti. Il risultato è riportato nella .
8. Oltre al dato di sintesi rappresentato dai valori medi per ciascun campione è stato calcolato il valore medio sull’intero campione dei punteggi ottenuti per ciascun quesito. Tale valore viene riportato nelle tabelle seguenti per avere una buona indicazioni delle specifiche criticità da affrontare.
9. Al termine di tale procedura sono stati raccolti i 4 KPI ottenuti da ciascuna amministrazione nelle ultime tre rilevazioni per poterne analizzare il trend e soprattutto per poter raccogliere maggiori indicazioni ed elaborare schede individuali.
10. Con la stessa tecnica, confrontando la coerenza delle risposte fornite nella rilevazione 2010 con quelle raccolte negli ultimi due anni, sono state rilevate tutte le situazioni anomale, probabilmente generate da una scarsa attenzione in fase di compilazione, sia per disporre solo di dati significativi in fase di analisi che per avviare procedure di richiamo ed evitare che si possa ripetere negli anni a venire.

Figura 1: Distribuzione delle Amministrazioni rispetto al numero di dipendenti

## Gli indicatori rilevati

I 4 indici prestazionali (KPI) individuati, e di conseguenza i quesiti del questionario utilizzato per la rilevazione dei dati, riflettano direttamente il modello di Sicurezza ICT elaborato da DigitPA negli ultimi anni. Tale modello è stato elaborato a partire dagli standard internazionali[[3]](#footnote-3) più riconosciuti nel settore della Sicurezza ICT. Successivamente, tali standard che per loro stessa natura devono avere un carattere generalista per potersi adattare ad ogni tipo di organizzazione, sono stati coniugati tenendo conto delle specifiche realtà presenti nella Pubblica Amministrazione italiana. In alcuni casi sono state operate delle semplificazioni eliminando controlli inutili o già gestiti da altre normative (come quelli sulla sicurezza e la gestione del personale ad esempio), in altri sono stati semplicemente adattati in modo che i quesiti presentati coerenti possano essere facilmente ricondotti alle realtà presenti nelle Amministrazioni intervistate.

In sostanza i 4 KPI raccolgono in maniera esaustiva, attraverso un insieme di quesiti del questionario, informazioni su aspetti cruciali per la sicurezza sotto 4 diverse prospettive la cui interpretazione sarà descritta nei prossimi paragrafi. Disponendo di un indice numerico è stato possibile di esprimere in maniera estremamente sintetica i dati raccolti. Inoltre a partire dai dati numerici si è potuto effettuare confronti diretti tra i risultati raccolti anno per anno e tracciare linee di tendenza che hanno notevolmente semplificato l’interpretazione dei risultati. Ad ognuno dei 4 indici seguenti sarà dedicato un paragrafo per descriverne i contenuti ed una dettagliata interpretazione semantica:

* KPI1: Sicurezza logica
* KPI2: Sicurezza dell'infrastruttura
* KPI3: Sicurezza dei servizi
* KPI4: Sicurezza dell’organizzazione

Ovviamente in funzione della rapidità con cui si evolve il settore Sicurezza ed in generale il mondo ICT saranno necessari costanti aggiornamenti al modello per la Sicurezza ed al questionario per mantenere sempre aggiornato l’insieme degli oggetti di controllo ed evitare di raccogliere dati su questioni ormai obsolete o definitivamente superate. Nel riconoscere la validità dello strumento adottato, DigitPA si farà cura di tali aggiornamenti, garantendo nel contempo la coerenza e la confrontabilità nel tempo dei 4 KPI.

Attraverso il KPI medio si individuano gli ambiti (tema) o le amministrazioni su cui occorre concentrare l’attenzione. Successivamente attraverso l’analisi dei risultati dei singoli quesiti e quindi dei corrispondenti oggetti di controllo, si individuano in maniera puntuale gli aspetti sui quali investigare o i punti di maggiore criticità su cui intervenire con urgenza.

### KPI1: Sicurezza logica

KPI1 è costituito da 14 quesiti di cui 5 dipendenti da KPI1.1 a KPI1.9 che investigano gli aspetti connessi agli strumenti software ed alle procedure adottate a supporto della Sicurezza del Sistema Informativo. Tra queste si citano:

* Capacità di strutturare i processi per l’amministrazione dei sistemi informavi attraverso strumenti e procedure, ad esempio, per l’autenticazione degli utenti, la definizione di policy centralizzate per l’assegnazione dei privilegi assegnati a ciascun utente, l’ adozione di software o procedure certificate per la sicurezza.
* Sistemi per il controllo accessi.
* Le procedure per l’aggiornamenti dei sistemi operativi e sistemi di Software Distribution per le PDL, favorendo quelle che garantiscono aggiornamenti automatici in maniera *non presidiata* ed almeno con frequenza giornaliera.
* Strumenti per la protezione del dato fisico, quali dischi RAID e procedure per il Backup inclusa la modalità di conservazione dei supporti
* Sicurezza dei dati trasportati all’esterno dell’organizzazione attraverso supporti o postazioni mobili

Soluzioni adeguate a questi temi rappresentano sicuramente il corretto punto di partenza per il raggiungimento dei livelli di sicurezza attesi, indipendentemente dalle dimensioni della struttura, dalle attività svolte e dai servizi erogati. La Tabella 4: Quesiti e risultati relativi al KPI1 riporta l’elenco completo dei quesiti, le risposte ammesse che caratterizzano l’indicatore ed i punteggi assegnati ad ognuna.

### KPI2: Sicurezza dell'infrastruttura

L’indice KPI2 è dedicato agli aspetti fisici della Sicurezza ed in particolare ai dispositivi hardware dedicati alla protezione delle infrastrutture di rete. Consta di 12 quesiti di cui 3 dipendenti che vanno da KPI2.1 a KPI2.9. Come già indicato in precedenza, non vengono esaminati gli aspetti già affrontati dal progetto SPC, quali canali per la trasmissione dati.

In particolare KPI2 esprime la media dei valori ottenuti rispetti i seguenti temi:

* Sicurezza perimetrale, protezione degli accessi ai locali tecnici, sistemi di videosorveglianza.
* Apparati attivi per la sicurezza degli accessi quali firewall, sistemi per la rilevazione delle intrusioni o per la prevenzione.
* Presenza di reti wireless con adeguati sistemi di protezione per garantire la privatezza dei dati trasmessi via radio ed impedire accessi non autorizzati.
* Eventuali servizi di accesso remoto e modalità seguite per proteggere le connessioni quali VPN.
* Sistemi di log e di accounting centralizzato in grado di garantire l’integrità delle informazioni custodite.

Occorre notare che nel caso specifico del quesito KPI 2.5 “*Sono presenti sottoreti wireless* ?” è stato assegnato un punteggio di 6 punti a chi ha risposto “NO”. D’altra parte la tecnologia Wi‑Fi negli ultimi anni ha raggiunto un sufficiente grado di maturità tale da garantire livelli di sicurezza equivalenti ed in qualche caso maggiori delle reti cablate. Pertanto utilizzando tali tecnologie in maniera consapevole, cioè proteggendo le comunicazioni radio con protocolli robusti come WPA o WPA2, il punteggio assegnato è 10. Utilizzando sistemi di protezione non sufficientemente robusti viene assegnato un punteggio via via decrescente. Ad esempio 4 punti se viene impiegato il protocollo WEP con chiavi statiche e 0 punti nel caso di reti wireless non protette, cosa ritenuta estremamente pericolosa.

Analogamente laddove non sono consentiti accessi remoti (quesito KPI 2.6) il punteggio assegnato corrisponde alla sufficienza ma, anche in questo caso, il punteggio massimo di 10 punti viene assegnato alle amministrazioni che consentono accesso remoto o servizi di telelavoro (esigenza molto diffusa) ed impiegano correttamente le tecnologie disponibili (VPN).

La Tabella 5: Quesiti e risultati relativi al KPI2 riporta i 12 quesiti, le risposte ammesse ed i relativi punteggi assegnati.

### KPI3: Sicurezza dei servizi

Assumendo che ogni amministrazione offre almeno i 3 servizi essenziali quali posta elettronica, siti web su intranet o rete pubblica ed antivirus, l’indice KPI3 intende misurare l’impegno che ogni Amministrazione ha dedicato per rendere più affidabili e robusti tali servizi. Ovviamente non potendo entrare nel merito dei servizi specifici offerti da ciascuna Amministrazione, si è individuato questi 3 servizi come comune denominatore comune per poter rilevare tale informazione prescindendo dalle attività dell’Amministrazione. Quindi attraverso 11 quesiti di cui 2 dipendenti, sono stati raccolti dati su temi rilevanti quali:

* Sensibilità rispetto al tema Continuità operativa, espressa dalla presenza di procedure da attivare in caso di eventi disastrosi e disponibilità di un piano di disaster recovery
* Modalità di erogazione di servizi centralizzati quali antivirus ed antispam sulla posta in transito o per la protezione delle PDL
* Protezione dei contenuti e web filtering
* Capacità di rilevare le intrusioni, e/o prevenirle in funzione del tipo di attacchi già subiti, oltre alla capacità di individuare eventuali attacchi, riconoscendone la tipologia rispetto alle classificazioni più diffuse

La Tabella 6: Quesiti e risultati relativi al KPI3 elenca gli 11 quesiti che caratterizzano KPI3 assieme alle risposte ammesse ed al punteggio assegnato a ciascuna di queste.

### KPI4: Sicurezza dell’organizzazione

Ultima area oggetto del questionario, ma sicuramente la più rilevante rispetto all’impatto prodotto sulla sicurezza dei sistemi informativi, è quella che confronta l’organizzazione interna in termini di ruoli e strutture dedicate alla Sicurezza che ogni amministrazione ha scelto rispetto alle soluzioni, ormai consolidate anche attraverso norme, che il modello comune per la sicurezza ritiene necessarie.

E’ estremamente importante, infatti, che ogni struttura informatica, disponga di un’adeguata organizzazione, altrimenti grossi sforzi per mettere in atto soluzioni tecniche per migliorare i livelli di Sicurezza rischiano spesso di essere vanificati da una organizzazione carente. Ad esempio, disporre di un sistema di autenticazione basato su smart card e certificati digitali non comporta alcun beneficio se il ruolo di Certification Authority non è svolto con sufficiente cura ed in maniera da poter ripercorrere la lista di responsabili per l’emissione dei certificati.

Al contrario, purtroppo già da anni si localizzano proprio in questa area le maggiori debolezze soprattutto tra le piccole Amministrazioni, dimostrando che tali aspetti vengono spesso sottovalutati, tralasciando temi rilevanti come: gestione preventiva del rischio, corretta gestione dei contratti di outsourcing o possibilità di intraprendere iniziative per la formazione e sensibilizzazione del personale.

L’indice KPI4 raccoglie i dati proprio in tale direzione attraverso i 18 quesiti di cui 5 dipendenti riportati nella Tabella 7: Quesiti e risultati relativi al KPI4. Più in dettaglio KPI4 affronta temi relativi a:

* Copertura dei ruoli previsti dal DM del 16/02/2002, e tutte le figure critiche già individuate nell’ambito della sicurezza
* Gestione degli incidenti e capacità di intervento in condizioni critiche
* Sensibilità rispetto al tema Sicurezza per una corretta gestione dell’Outsourcing della Sicurezza o disponibilità di un budget esplicitamente dedicato alla sicurezza
* Analisi preventiva del rischio
* Gestione amministrativa della sicurezza, percentuale del bilancio espressamente dedicata alla sicurezza oltre che capacità di pianificare formazione interna per sensibilizzare l’utenza sul tema sicurezza.

# Presentazione dei risultati

## Risultati di sintesi e linee di tendenza

Prima di iniziare il lavoro di analisi sono state confermate le 3 soglie adottate negli anni precedenti che suddividono i valori ottenuti per ciascun KPI in 4 fasce denominate: *ottima*, *buona*, *accettabile* e *scarsa* a secondo dei valori riportati nella tabella seguente:

|  |  |  |
| --- | --- | --- |
| 0 ≤ KPI < 4 | scarsa | Valori medi dei KPI al di sotto di questa soglia sono da considerarsi critici. Di fatto a fronte di tali risultati occorrerebbe pianificare con urgenza un intervento strutturato per evitare situazioni critiche. |
| 4 ≤ KPI < 5 | accettabile | Valori medi dei KPI all’interno di questa fascia indicano situazioni non critiche che devono essere riportate alla norma con interventi mirati e puntuali frutto di analisi ulteriori. |
| 5 ≤ KPI < 7 | buona | Valori medi dei KPI all’interno di questa fascia sono da considerarsi già positivi ma è necessario identificare gli spazi di miglioramento per raggiungere prestazioni ottimali. |
| 7 ≤ KPI ≤ 10 | ottima | Valori medi dei KPI al di sopra della soglia fissata rappresentano l’obiettivo che tutte le Amministrazioni dovrebbero conseguire capitalizzando gli sforzi già spesi nel campo della Sicurezza ICT. |

Tabella 1: Soglie numeriche per la interpretazione dei risultati complessivi

La scelta di queste soglie è stata effettuata in maniera arbitraria sulla base di un’evidenza sperimentale riconoscendo, nelle Amministrazioni che hanno ottenuto valori degli indicatori nella fascia “scarsa”, un sostanziale disinteresse nei confronti del tema sicurezza palesato da numerose (più del 50% dell’insieme di quesiti relativi al KPI) risposte in controtendenza rispetto ai valori attesi. E’ chiaro pertanto che se un Amministrazione ottiene per un KPI un punteggio inferiore a 4 questo non può essere considerato come un fenomeno occasionale o una banale disattenzione bensì si dovranno necessariamente avviare indagini di secondo livello volte a determinare le cause e le contromisure da mettere in atto nel breve periodo.

Un importante risultato di questa attività di monitoraggio è costituito proprio dalle indicazioni puntuali che gli esperti di DigitPA ottengono per individuare con precisione il gruppo di Amministrazioni che si colloca al di sotto di questa fascia, per poi avviare in funzione di questi dati interventi mirati. Con gli stessi dati è anche possibile stabilire politiche comuni di intervento, individuando con precisione i punti deboli analizzando i quesiti che hanno prodotto i risultati peggiori.

Successivamente è stata elaborata la che rappresenta il massimo momento di sintesi dei dati raccolti. Infatti sono state classificate tutte le Amministrazioni in funzione del valore ottenuto per ciascun KPI rispetto alle 3 soglie citate in precedenza. La dimensione delle bolle è proporzionale al numero di Amministrazioni il cui risultato ricade nell’intervallo prestabilito. Sono state quindi collocate nell’area verde tutte le bolle (Amministrazioni) che hanno raggiunto un ottimo livello di sicurezza, nell’area gialla quelle che comunque si sono assestate su un livello accettabile di sicurezza e al di sotto nell’area gradatamente più rossa, tutte le Amministrazioni che assolutamente necessitano di una serie di interventi per aumentare la sensibilità nei confronti del tema Sicurezza ICT. Come si vede la grande maggioranza delle amministrazioni si colloca nella parte alta del grafico in particolare 44 su 46 per KPI1 e 41 per KPI2. Per KPI3 e KPI4 al contrario alcune di queste si collocano nella zona critica 7 per KPI3 e ben 12 per KPI4. Per quest’ultimo KPI il dato in percentuale è rilevante rappresentando oltre il 26 % del campione. Occorre però notare un deciso miglioramento anche in questo settore poiché si è passati 32% dell’anno 2008 al 39% del 2009, al 26% del 2010).

Figura 2: Distribuzione dei 4 KPI medi rispetto alle 3 soglie

Ne consegue quindi un primo risultato che vede le maggiori criticità concentrarsi proprio nell’area organizzativa (fotografata da KPI4) dove insieme alle carenze più diffuse si nascondono anche molte delle cause che hanno prodotto i casi maggiormente critici osservati all’interno del campione.

I tre grafici seguenti riportano l’andamento dei valori medi dei 4 KPI nelle ultime 4 rilevazioni suddivisi per le tre classi di Amministrazioni, evidenziando miglioramenti e arretramenti conseguiti nel settore sicurezza oltre che i valori medi complessivamente sopra la sufficienza.

Dai grafici è possibile da notare un complessivo andamento positivo per le Grandi Amministrazioni, che in valore assoluto mostrano valori molto alti per tutti i KPI e sufficientemente stabili per l’intero periodo di osservazione.

|  |  |
| --- | --- |
| Figura 3: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le grandi amministrazioni  Figura 4: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le medie amministrazioni  Figura 5: Andamento dei 4 KPI nelle ultime 4 rilevazioni per le piccole amministrazioni | Nel contempo si nota in maniera altrettanto evidente il netto peggioramento nell’ultimo anno delle prestazioni delle piccole amministrazioni rispetto a KPI1 e, in maniera ancor più evidente di KPI2. Nel contempo sempre le piccole amministrazioni hanno mostrato un netto miglioramento rispetto a KPI3 e KPI4 che nell’anno precedente erano finiti in media sotto la soglia ammissibile. Per motivare l’andamento negativo dei primi due KPI occorre considerare che le riduzioni dei bilanci subiti da molte Amministrazioni negli anni 2009-2010 ha contribuito in maniera rilevante a dirottare risorse economiche verso altre attività ritenute maggiormente critiche riducendo gli investimenti (Hw e Sw) per la sicurezza.  Oltre alla conferma del dato, piuttosto naturale, che le grandi organizzazioni mostrano una maggiore sensibilità rispetto al tema Sicurezza ICT il dato che emerge è quello che vede il primo indice KPI1 sostanzialmente indipendente dalla dimensione delle Amministrazioni, mentre tutti gli altri mostrano una forte dipendenza funzionale dalle dimensioni dell’Amministrazione che comunque cominciano ad assestarsi intorno a valori ormai consolidati e superiori alla soglia di ammissibilità.  Successivamente è stata effettuata una ulteriore verifica incrociando i due dati (cf. la Figura 1 e la Tabella 2) ed è risultato che delle 12 Amministrazioni sotto la soglia di criticità citate nella Figura 1 una volta eliminate quelle che non hanno risposto ad un numero sufficiente di quesiti (1) tutte quelle rimanenti (11) sono tutte concentrate nella categorie delle *medie*. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

2

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **2007** | **2008** | **2009** | **2010** | **Δ 2008** | **Δ 2009** | **Δ 2010** | **Δ% 2008** | **Δ% 2009** | **Δ% 2010** |
| Grandi | KPI 1 | 8,42 | 7,33 | 8,40 | 8,50 | -1,09 | 1,07 | 0,10 | -13,0% | 14,6% | 1,2% |
| KPI 2 | 8,53 | 8,29 | 8,77 | 8,56 | -0,25 | 0,48 | -0,21 | -2,9% | 5,8% | -2,4% |
| KPI 3 | 7,89 | 7,48 | 8,40 | 8,04 | -0,41 | 0,92 | -0,36 | -5,2% | 12,3% | -4,3% |
| KPI 4 | 7,62 | 7,76 | 8,05 | 8,23 | 0,13 | 0,29 | 0,18 | 1,8% | 3,8% | 2,2% |
| Medie | KPI 1 | 6,97 | 7,29 | 7,22 | 7,57 | 0,32 | -0,07 | 0,34 | 4,6% | -0,9% | 4,8% |
| KPI 2 | 8,01 | 8,21 | 8,44 | 8,51 | 0,19 | 0,23 | 0,07 | 2,4% | 2,9% | 0,8% |
| KPI 3 | 7,00 | 7,05 | 6,65 | 7,03 | 0,05 | -0,40 | 0,38 | 0,7% | -5,7% | 5,7% |
| KPI 4 | 6,12 | 6,21 | 5,00 | 5,78 | 0,09 | -1,21 | 0,78 | 1,5% | -19,4% | 15,6% |
| Piccole | KPI 1 | 6,58 | 7,32 | 7,53 | 7,09 | 0,75 | 0,20 | -0,44 | 11,4% | 2,8% | -5,8% |
| KPI 2 | 5,95 | 6,62 | 7,42 | 6,48 | 0,67 | 0,80 | -0,94 | 11,2% | 12,1% | -12,7% |
| KPI 3 | 5,66 | 6,05 | 4,78 | 6,31 | 0,39 | -1,27 | 1,53 | 6,9% | -21,0% | 32,0% |
| KPI 4 | 4,46 | 5,17 | 5,10 | 6,58 | 0,71 | -0,07 | 1,48 | 15,9% | -1,3% | 28,9% |
| Tutte | KPI1 | 7,32 | 7,31 | 7,72 | 7,72 | -0,01 | 0,40 | 0,00 | -0,1% | 5,5% | 0,0% |
| KPI2 | 7,50 | 7,70 | 8,21 | 7,85 | 0,21 | 0,50 | -0,36 | 2,7% | 6,6% | -4,4% |
| KPI3 | 6,85 | 6,86 | 6,61 | 7,13 | 0,01 | -0,25 | 0,52 | 0,1% | -3,7% | 7,8% |
| KPI4 | 6,07 | 6,38 | 6,05 | 6,86 | 0,31 | -0,33 | 0,81 | 5,1% | -5,1% | 13,4% |

Tabella 3: Andamento nelle ultime 3 rilevazioni dei KPI rispetto alle dimensioni delle amministrazioni



Questo dato fornisce una precisa indicazione sul fatto che occorre dedicare maggiore attenzione alle piccole e medie organizzazioni ed in particolare sviluppare una maggiore consapevolezza sugli sforzi da mettere in atto per migliorare l’organizzazione interna e renderla più sicura.

Sempre dalla tabella 2 per KPI3 si evince che le piccole Amministrazioni prestano minore attenzione rispetto alle altre al tema “Robustezza dei Servizi” (Continuità Operativa) con ben 7 Amministrazioni (su 11) sotto la soglia della sufficienza.

Figura 9: Risultati dei 4 KPI suddivisi tra le 3 classi di Amministrazioni

Nei 4 paragrafi che seguono, per ogni KPI si presentano i risultati elaborati secondo la metodologia descritta e, attraverso altrettante tabelle si riportano i dati di dettaglio (grezzi) per ogni quesito raccolti attraverso il questionario on-line. Per ogni indicatore vengono analizzate le risposte raccolte, fornendo anche una possibile interpretazione del fenomeno così come appare dai dati statistici.

La struttura delle tabelle necessaria per rappresentare tutti i dati raccolti incluse le serie storiche risulta piuttosto complessa e per agevolarne la lettura si riporta di seguito una descrizione delle convenzioni adottate per la presentazione dei dati. Per ogni indicatore è stata elaborata una tabella costituita da 11 colonne.

La prima colonna riporta il l’identificativo del quesito con il quale sarà citato nel resto del rapporto. Ogni ID è del tipo KPI X.Y, laddove X specifica il KPI in questione e Y la posizione del quesito nel gruppo di quesiti dell’indicatore X. Eventualmente per i quesiti dipendenti viene aggiunto un indice letterale.

A destra dell’identificativo, per ogni quesito su una riga separata ed evidenziata da un font di dimensioni maggiori si riporta il testo proposto dal questionario e, nelle ultime 3 colonne, i valori medi sull’intero campione ottenuti dal corrispondente quesito negli ultimi 3 anni. Va qui notato che questo è un dato grezzo e la media viene calcolata considerando tutte le Amministrazioni che hanno partecipato alla rilevazione incluse quelle che hanno fornito un numero di risposte esiguo al di sotto della soglia minima;

I quesiti di secondo livello, cioè dipendenti dalla risposta precedente secondo la definizione data nel paragrafo 3.1 a pagina 7 saranno racchiusi nello stesso box del quesito principale e separati da questo da linee orizzontali più sottili;

Di seguito per ogni risposta prevista vi è una riga con 10 colonne con la seguente struttura:

1. La seconda colonna, con intestazione “*Risposta*”, riporta l’insieme delle risposte previste (una per linea) per i quesito corrispondete in testa. Ogni quesito prevede il caso “N.R.” (non rispondono) che conteggia le Amministrazioni che non hanno riposto al quesito. In questo caso viene assegnato un punteggio pari a zero, corrispondente alla riposta peggiore;
2. la terza colonna, con intestazione “*Punt*.” specifica il punteggio assegnato a priori a ciascuna risposta. Per migliorare la leggibilità i dati in questa colonna sono stati inseriti in italico;
3. la quarta, la sesta e la ottava colonna con intestazioni *“%2010%,* *“% 2009*” e*“% 2008*” riportano rispettivamente per l’anno corrente, il 2009 ed il 2008, la percentuale sull’intero campione di Amministrazioni che hanno fornito la risposta citata sulla stessa riga;
4. la quinta e la settima, con intestazioni “Δ '10/'09” e “Δ '09/'08” riportano rispettivamente le differenze rispetto all’anno precedente e le differenze tra gli ultimi due anni. Eventuali variazioni in diminuzione per valori superiori al -3% saranno evidenziate in rosso ed in verde variazioni in aumento superiori al +3%;
5. le ultime 3 colonne, rispettivamente “# Risp. 2010”, “*# Risp. 2009*” e “*# Risp. 2008*”, forniscono il numero (valore assoluto) di Amministrazioni che hanno fornito la risposta corrispondente negli ultimi 3 anni. E’ evidente che in funzione delle differente numero di Amministrazioni che hanno partecipato alla rilevazione nel corso degli anni non è possibile confrontare direttamente tali valori (nel 2009 erano 46, mentre nel 2008 erano 56). Vengono ugualmente qui riportate per fornire una misura esatta di quante Amministrazioni possono aver bisogno di interventi puntuali sulla base dei contenuti specifici di un singolo quesito;

## KPI1: Sicurezza logica

La Tabella 2 mostra che KPI1 è l’unico indice che presenta valori ottimali per tutte le tre classi di Amministrazioni, con valori medi che vanno da 8,5 per le grandi Amministrazioni a 7,09 per le piccole Amministrazioni. Le medie hanno ottenuto un valore medio di 7,57 producendo un risultato complessivo più che soddisfacente.

Volendo comunque approfondire la ricerca delle aree per un possibile ulteriore miglioramento si nota che i quesiti che hanno prodotto i valori più bassi sono: KPI1.3a e KPI1.7 e saranno analizzati nel seguito.

Analizzando nello specifico i quesiti che compongono l’indicatore KPI1 si nota un diffuso miglioramento delle prestazioni rispetto a questo indice anche se le piccole amministrazioni sono complessivamente arretrate passando dal 7,53 del 2009 all’attuale 7,09. Ciò testimonia comunque i progressi conseguiti dalle Amministrazioni della PAC in termini di cultura della Sicurezza nell’ultimo anno. Come riportato nella Tabella 4 quasi tutti i quesiti evidenziano un trend in miglioramento costante anno per anno. Unica eccezione è rappresentata dal valore del quesito KPI1.3 “Nel caso di acquisizione di prodotti o servizi, vengono considerate certificazioni di sicurezza ?“ che ha ottenuto un lieve arretramento (da 7,39 a 7,17) riducendo del 2,2% il numero delle Amministrazioni che hanno dichiarato di considerare al momento dell’acquisto le certificazioni per la sicurezza delle ditte fornitrici. Al contrario migliorano il dato è in miglioramento se si analizzano le risposte fornite al sotto quesito KPI1.3a per il quale aumenta del +15,9% (13 su 33 rispetto a 8 su 34) il numero delle amministrazioni che richiedono certificazioni Common Criteria (ISO 15408) e del +10,8% (22 su 33 rispetto 19 su 34) quelle che richiedono la certificazione ISO 27001, riflettendo anche nei numeri il crescente interesse rivolto verso le certificazioni per la sicurezza dei prodotti. Di conseguenza diminuiscono le amministrazioni che considerano “Altre certificazioni” meno riconosciute, confermando così l’esigenza di avere norme precise in proposito.

D’altra parte, nonostante i miglioramenti rilevati il valore medio ottenuto per KPI1.3a (4,70, 4,22 e 3,8) resta sotto la soglia di accettabilità denunciando che vi è ancora molto da fare per diffondere la cultura della Sicurezza in maniera capillare tra tutti gli utenti.

|  |  |
| --- | --- |
|  |  |
| Figura 10: Distribuzione dei risultati relativi al KPI1 rispetto alle 3 soglie | Figura 11: Valori medi delle risposte ai quesiti relativi al KPI1 |

KPI1.6 tende a misurare la capacità delle strutture informatiche di tenere sempre aggiornato ed efficiente il software di base delle postazioni di lavoro attraverso l’installazione di procedure automatiche di aggiornamento capaci, senza richiedere interventi esterni, di provvedere ad applicare almeno gli aggiornamenti più critici per la sicurezza. Da rilevare il consistente miglioramento (+10,9%) del valore medio per KPI1.6 che passa da 5,87 a 6,96 superando abbondantemente la soglia della sufficienza.

Secondo tema rispetto alle criticità emerse dall’analisi di KPI1 è quello della sicurezza dei dati presenti su dispositivi mobili quali computer portatili o semplicemente dischi/pen drive USB. Infatti è già accaduto in più occasioni che, per furto o semplicemente per smarrimento dei dispositivi, notevoli moli di dati sensibili venissero perse o finissero nelle mani di terzi per scopi fraudolenti. KPI1.7 riflette appunto l’attenzione rispetto a questi temi ed ha ottenuto valori medi piuttosto bassi vicini alla soglia minima di accettabilità (4,96 rispetto al 4,52 del 2009 e 4,18 del 2008). Infatti, nonostante il miglioramento conseguito nell’ultimo ano (+4,3%) solo 18 Amministrazioni (su 46) hanno dichiarato di utilizzare dispositivi mobili dotati di adeguati sistemi per la protezione (cifratura) dei dati residenti prevenendo così il furto di dati. Ancora 13 Amministrazioni (+6,5% rispetto al 2009) hanno dichiarato invece di non adottare nessuna contromisura per proteggere i dati su dispositivi mobili mentre 8 dichiarano di non usare alcun dispositivo per trasportare i dati oltre il perimetro aziendale.

Sembra invece ormai definitivamente consolidato il dato relativo all’esigenza di proteggere i propri dati (disaster recovery) adottando le adeguate strategie per il backup centralizzato (KPI1.8). A fronte dei miglioramenti conseguiti negli anni precedenti, nell’ultima rilevazione si è potuto osservare un netto ulteriore miglioramento (+10,5%) che ha portato il dato complessivo ad un valore medio di 8,96 (rispetto all’8,04 ed al 7,64 degli anni precedenti). Tecnicamente la quasi totalità del campione (44 su 46 amministrazioni) ha dischiarato di possedere ed utilizzare strumenti per il backup centralizzato dei dati. Tra queste l’84,1% ha dichiarato di aver formalizzato le più note best practices in materia di backup e conservazione dei supporti come procedure per l’attuazione.

Infine relativamente a KPI1.4 cioè ai sistemi di autenticazione impiegati nella PAC si nota che, nonostante il dato complessivamente positivo con un valore oltre la soglia dell’ottimo (9,30), permane un largo uso di sistemi basati su username/password (95,7% con un +4,3 nell’ultimo anno) che, benché gestito da corrette policy di expire e verifica proattiva della password, risultano secondo il modello di DigitPA deboli e complessi da gestire, quindi vulnerabili nella pratica quotidiana. Sarebbe pertanto auspicabile avviare per tutte le Amministrazioni una concreta opera di sensibilizzazione volta alla introduzione di sistemi di autenticazione più robusti basati su Smart Card e/o sistemi biometrici, tali da garantire in maniera assoluta l’identità dell’utente che accede ai sistemi ed alla risorse della Amministrazione.

La tabella seguente riporta nel dettaglio i dati presentati relativi a KPI1.

| **ID** | **Risposta** | **Punt.** | **% 2010** | **Δ '10/'09** | **% 2009** | **Δ '09/'08** | **% 2008** | **# risp. 2010** | **# risp. 2009** | **# risp. 2008** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| KPI 1.1 | Quale modello di gestione e amministrazione della sicurezza del sistema informativo viene impiegato? | | | | | | | 6,78 | 6,61 | 6,29 |
| Completamente decentralizzato | *10* | 4,3% | -2,2% | 6,5% | 3,0% | 3,6% | 2 | 3 | 2 |
| Parzialmente centralizzato | *8* | 37,0% | 0,0% | 37,0% | -2,3% | 39,3% | 17 | 17 | 22 |
| Completamente centralizzato | *6* | 56,5% | 6,5% | 50,0% | 3,6% | 46,4% | 26 | 23 | 26 |
| Nessuno | *0* | 0,0% | 0,0% | 0,0% | -3,6% | 3,6% | 0 | 0 | 2 |
| N.R. | *0* | 2,2% | -4,3% | 6,5% | -0,6% | 7,1% | 1 | 3 | 4 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 1.2 | Sono state definite policy per l'uso delle risorse interne da parte degli utenti ? | | | | | | | 9,13 | 8,70 | 8,04 |
| SI | *10* | 91,3% | 4,3% | 87,0% | 6,6% | 80,4% | 42 | 40 | 45 |
| NO | *0* | 6,5% | 0,0% | 6,5% | -0,6% | 7,1% | 3 | 3 | 4 |
| N.R. | *0* | 2,2% | -4,3% | 6,5% | -6,0% | 12,5% | 1 | 3 | 7 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 1.3 | Nel caso di acquisizione di prodotti o servizi, vengono considerate certificazioni di sicurezza ? | | | | | | | 7,17 | 7,39 | 6,96 |
| SI | *10* | 71,7% | -2,2% | 73,9% | 4,3% | 69,6% | 33 | 34 | 39 |
| NO | *0* | 13,0% | 0,0% | 13,0% | -4,8% | 17,9% | 6 | 6 | 10 |
| N.R. | *0* | 15,2% | 2,2% | 13,0% | 0,5% | 12,5% | 7 | 6 | 7 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
| KPI 1.3a | Nel caso vengano considerate certificazioni di sicurezza nell'acquisizione di prodotti o servizi, quali certificazioni sono considerate ? | | | | | | | 4,70 | 4,22 | 3,80 |
| CommonCriteria (ISO 15408) | *5* | 39,4% | 15,9% | 23,5% | 3,0% | 20,5% | 13 | 8 | 8 |
| ISO 27001 (ex BS 7799-2) | *5* | 66,7% | 10,8% | 55,9% | 2,0% | 53,8% | 22 | 19 | 21 |
| Certificazioni professionali | *3* | 48,5% | -7,4% | 55,9% | 2,0% | 53,8% | 16 | 19 | 21 |
| Altro | *3* | 9,1% | -2,7% | 11,8% | 1,5% | 10,3% | 3 | 4 | 4 |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 1.4 | Quali criteri/sistemi di autenticazione per l'accesso alla rete interna vengono utilizzati ? | | | | | | | 9,30 | 8,17 | 7,89 |
| USERID/PASSWORD | *2* | 95,7% | 4,3% | 91,3% | 3,8% | 87,5% | 44 | 42 | 49 |
| TOKEN DI AUTENTICAZIONE | *6* | 2,2% | 2,2% | 0,0% | 0,0% | 0,0% | 1 | 0 | 0 |
| PKI/SMART CARD/PIN | *6* | 0,0% | 0,0% | 0,0% | -1,8% | 1,8% | 0 | 0 | 1 |
| ONE TIME PASSWORD | *8* | 0,0% | 0,0% | 0,0% | 0,0% | 0,0% | 0 | 0 | 0 |
| N.R. | *0* | 2,2% | -6,5% | 8,7% | -2,0% | 10,7% | 1 | 4 | 6 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
| KPI 1.4a | Se si utilizzano UserID e password come sistema di autenticazione, sono state definite regole per la gestione delle password ? | | | | | | |  |  |  |
| Utilizzo di policy per password | *2* | 100,0% | 4,8% | 95,2% | 1,4% | 93,9% | 44 | 40 | 46 |
| KPI 1.4b | E' prevista la scadenza automatica di un account/password ? | | | | | | |  |  |  |
| Expire automatico password | *2* | 93,2% | 7,5% | 85,7% | 2,0% | 83,7% | 41 | 36 | 41 |
| KPI 1.4c | Esiste un controllo preventivo della scelta della password ? | | | | | | |  |  |  |
| Controllo proattivo password | *4* | 93,2% | 9,8% | 83,3% | -0,3% | 83,7% | 41 | 35 | 41 |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 1.5 | Con quale frequenza viene verificata la presenza di aggiornamenti dei sistemi operativi dei server ? | | | | | | | 7,87 | 7,52 | 7,25 |
| AUTOMATICAMENTE | *10* | 47,8% | -2,2% | 50,0% | 1,8% | 48,2% | 22 | 23 | 27 |
| OGNI SETTIMANA | *10* | 17,4% | 4,3% | 13,0% | -4,8% | 17,9% | 8 | 6 | 10 |
| OGNI MESE | *8* | 23,9% | 2,2% | 21,7% | 11,0% | 10,7% | 11 | 10 | 6 |
| OGNI SEI MESI | *6* | 6,5% | 2,2% | 4,3% | -4,6% | 8,9% | 3 | 2 | 5 |
| MAI | *0* | 0,0% | -2,2% | 2,2% | 0,4% | 1,8% | 0 | 1 | 1 |
| N.R. | *0* | 4,3% | -4,3% | 8,7% | -3,8% | 12,5% | 2 | 4 | 7 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 1.6 | Esiste un sistema centralizzato di software distribution per l'aggiornamento automatico delle postazioni di lavoro ? | | | | | | | 6,96 | 5,87 | 5,71 |
| SI | *10* | 69,6% | 10,9% | 58,7% | 1,6% | 57,1% | 32 | 27 | 32 |
| NO | *0* | 26,1% | -6,5% | 32,6% | 2,3% | 30,4% | 12 | 15 | 17 |
| N.R. | *0* | 4,3% | -4,3% | 8,7% | -3,8% | 12,5% | 2 | 4 | 7 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 1.7 | Se esistono postazioni mobili o supporti dati che vengono trasportati oltre i confini del luogo di lavoro dell'amministrazione, vengono adottati sistemi software per impedire l'accesso ai dati da parte di persone non autorizzate? | | | | | | | 4,96 | 4,52 | 4,18 |
| Esistono postazioni mobili o supporti dati rimuovibili con sistemi di prevenzione degli accessi | *10* | 39,1% | 4,3% | 34,8% | 2,6% | 32,1% | 18 | 16 | 18 |
| Esistono postazioni mobili o supporti dati rimuovibili senza sistemi di prevenzione degli accessi | *0* | 28,3% | 6,5% | 21,7% | -6,8% | 28,6% | 13 | 10 | 16 |
| Non esistono postazioni mobili o impiego di supporti dati rimuovibili | *6* | 17,4% | 0,0% | 17,4% | 1,3% | 16,1% | 8 | 8 | 9 |
| N.R. | *0* | 15,2% | -10,9% | 26,1% | 2,9% | 23,2% | 7 | 12 | 13 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 1.8 | Sono state definite ed adottate tecnologie e procedure per il backup centralizzato ? | | | | | | | 8,96 | 8,04 | 7,64 |
| SI | *6* | 95,7% | 10,9% | 84,8% | 2,6% | 82,1% | 44 | 39 | 46 |
| NO | *0* | 2,2% | -4,3% | 6,5% | 1,2% | 5,4% | 1 | 3 | 3 |
| N.R. | *0* | 2,2% | -6,5% | 8,7% | -3,8% | 12,5% | 1 | 4 | 7 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
| KPI 1.8a | Se si effettuano regolarmente backup dei sistemi, i supporti usati per il backup vengono custoditi in un locale diverso dalla sala macchine o in un armadio ignifugo? | | | | | | |  |  |  |
| SI | *4* | 84,1% | -3,1% | 87,2% | 4,6% | 82,6% | 37 | 34 | 38 |
| NO | *0* | 9,1% | 1,4% | 7,7% | -5,4% | 13,0% | 4 | 3 | 6 |
| N.R. | *0* | 6,8% | 1,7% | 5,1% | 0,8% | 4,3% | 3 | 2 | 2 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **44** | **39** | **46** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 1.9 | Viene utilizzato un sistema di controllo accessi per disciplinare l'accesso alle risorse elaborative ? | | | | | | | 8,48 | 8,70 | 8,21 |
| SI | *10* | 84,8% | -2,2% | 87,0% | 4,8% | 82,1% | 39 | 40 | 46 |
| NO | *0* | 10,9% | 8,7% | 2,2% | -5,0% | 7,1% | 5 | 1 | 4 |
| N.R. | *0* | 4,3% | -6,5% | 10,9% | 0,2% | 10,7% | 2 | 5 | 6 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |

Tabella 4: Quesiti e risultati relativi al KPI1

## KPI2: Sicurezza dell'infrastruttura

Rispetto alla protezione fisica della infrastruttura, gli alti punteggi medi conseguiti dalle Amministrazioni per KPI2, 8,56 per le grandi, 8,51 per le medie e 6,48 per le piccole confermano la naturale propensione ad investire in termini di dispositivi hardware per la protezione delle proprie dotazioni informatiche. Rispetto al modello adottato occorre anche notare che il valore medio per le piccole Amministrazioni, nettamente inferiore rispetto alle altre classi ed arretrato rispetto all’anno precedente (7,42 nel 2009 pari a -12,7%), è sicuramente sintomatico di una minore sensibilità rivolta alla Sicurezza ICT ma potrebbe anche riflettere una minore di disponibilità di risorse economiche.

Grazie alle iniziative intraprese per la diffusione del modello adottato, cresce nettamente rispetto all’anno precedente il risultato per i 3 quesiti: KPI2.1, KPI2.2 e KPI2.3.

Infatti il valore medio di 9,13 per KPI2.1, ulteriormente migliorato (+4,3%) rispetto agli anni precedenti, conferma che ormai la quasi totalità del campione (91,3% pari a 42 su 44 amministrazioni) ha adottato barriere fisiche per limitare e controllare l’accesso alle risorse elaborative. Analogamente per KPI2.2 con un valore di 8,91 (+8,7%) dimostra che ormai il 89,1% del campione utilizza sistemi per il controllo degli accessi per i locali critici. Infine, anche KPI2.3 (utilizzo di telecamere a circuito chiuso), storicamente il più critico dei tre KPI, cresce nettamente rispetto all’anno precedente (+13,0%) raggiungendo il valore medio di 6,96. Nonostante il miglioramento, rimane ancora basso il numero delle Amministrazioni che hanno installato un sistema di videosorveglianza H24 per il controllo accessi alla sala macchine (32 su 46). Questo dato indica che occorre insistere con le attività per la formazione continua sulle best practice in tema di sicurezza ICT quali ad esempio l’utilizzo di sistemi di videosorveglianza per proteggere il CED da accessi fraudolenti.

KPI2.4 con un valore medio di 7,72 (rispetto a 7,61 e 7,05 degli anni precedenti) conferma che il passaggio ad SPC ha consentito una larga diffusione degli strumenti per la sicurezza perimetrale della rete come l’impiego di un firewall (raggiungendo una percentuale di adozione superiore al 93,5% come confermato anche dal quesito di controllo KPI2.7), mentre l’utilizzo di sistemi IDS/IPS rimane ancora piuttosto limitato (60,9% pari a 28 su 46) e tipicamente confinato alle grandi Amministrazioni. Il dato raccolto è stato ampiamente confermato dal quesito di controllo KPI2.8.

Dopo anni di lavoro svolto da DigitPA per la protezione delle reti wireless, ritenuto un fattore estremamente critico in passato, il dato fotografato da KPI2.5 si è ormai assestato su valori meno allarmanti. Infatti, diminuisce il numero delle reti wireless installate (solo il 41,3% pari a 19 su 46 amministrazioni dichiarano di utilizzare la tecnologia Wi-Fi all’interno delle proprie organizzazioni). L’utilizzo di WEP (Wired Equivalent Protection) come sistema di protezione permane per solo 4 di queste, mentre 12 correttamente configurano WPA (Wireless Protected Access in versione 1 o 2) per la protezione dei dati trasmessi via radio. E’ scomparsa del tutto la presenza di reti non protette. Più critica invece è la presenza di 3 amministrazioni che non hanno saputo o voluto rispondere al quesito sul tipo di protezioni adottato per le reti wireless.

Migliora infine il dato relativo a KPI2.6 che raggiunge il valore medio di 7,78 con oltre il 76% di amministrazioni che offrono servizi per l’accesso remoto ai propri sistemi opportunamente protetti da VPN o da infrastrutture equivalenti. ulteriormente del 2,26,1 (35 su 46),tra queste (31 su 35) che correttamente installa una VPN per proteggere la propria rete da accessi fraudolenti.

Anche il dato relativo alla disponibilità di adeguati sistemi di logging (KPI2.9) è molto incoraggiante ed in costante aumento. Infatti l’80% del campione (37 su 46) dichiara di utilizzare un sistema di log centralizzato, 7 usano un sistema di log locale evidentemente più vulnerabile e solo 2 non utilizzato sistemi per la registrazione degli eventi critici.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |  | | |
| Figura 12: Distribuzione dei risultati relativi al KPI2 rispetto alle 3 soglie | | Figura 13: Valori medi delle risposte ai quesiti relativi al KPI2 |

La tabella seguente riporta nel dettaglio i dati relativi a KPI2.

| **ID** | **Risposta** | **Punt.** | **% 2010** | **Δ '10/'09** | **% 2009** | **Δ '09/'08** | **% 2008** | **# risp. 2010** | **# risp. 2009** | **# risp. 2008** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| KPI 2.1 | Esistono barriere fisiche per limitare e perimetrare l'accesso alle risorse elaborative e alla rete interna ? | | | | | | | 9,13 | 8,70 | 8,57 |
| SI | *10* | 91,3% | 4,3% | 87,0% | 1,2% | 85,7% | 42 | 40 | 48 |
| NO | *0* | 6,5% | 0,0% | 6,5% | 3,0% | 3,6% | 3 | 3 | 2 |
| N.R. | *0* | 2,2% | -4,3% | 6,5% | -4,2% | 10,7% | 1 | 3 | 6 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 2.2 | Esiste un sistema di controllo dell'accesso fisico ai locali dove si trovano gli elaboratori e gli apparati di rete ? | | | | | | | 8,91 | 8,04 | 7,50 |
| SI | *10* | 89,1% | 8,7% | 80,4% | 5,4% | 75,0% | 41 | 37 | 42 |
| NO | *0* | 8,7% | -4,3% | 13,0% | -1,2% | 14,3% | 4 | 6 | 8 |
| N.R. | *0* | 2,2% | -4,3% | 6,5% | -4,2% | 10,7% | 1 | 3 | 6 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 2.3 | Se l'accesso ai locali critici è ristretto, esiste un sistema di videosorveglianza con registrazione delle riprese H24 ? | | | | | | | 6,96 | 5,65 | 4,46 |
| SI | *10* | 69,6% | 13,0% | 56,5% | 11,9% | 44,6% | 32 | 26 | 25 |
| NO | *0* | 15,2% | -8,7% | 23,9% | -1,1% | 25,0% | 7 | 11 | 14 |
| N.R. | *0* | 15,2% | -4,3% | 19,6% | -10,8% | 30,4% | 7 | 9 | 17 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 2.4 | Quali di queste protezioni di rete vengono utilizzate? | | | | | | | 7,72 | 7,61 | 7,05 |
| firewall | *5* | 93,5% | 2,2% | 91,3% | 2,0% | 89,3% | 43 | 42 | 50 |
| IDS/IPS | *5* | 60,9% | 0,0% | 60,9% | 9,1% | 51,8% | 28 | 28 | 29 |
| nessuna | *0* | 0,0% | 0,0% | 0,0% | -1,8% | 1,8% | 0 | 0 | 1 |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 2.5 | Sono presenti sottoreti wireless? | | | | | | | 5,57 | 6,52 | 5,68 |
| SI | *0* | 41,3% | -8,7% | 50,0% | 7,1% | 42,9% | 19 | 23 | 24 |
| NO | *6* | 43,5% | 0,0% | 43,5% | -3,0% | 46,4% | 20 | 20 | 26 |
| N.R. | *0* | 15,2% | 8,7% | 6,5% | -4,2% | 10,7% | 7 | 3 | 6 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
| KPI 2.5a | Se si utilizzano reti Wi-Fi quali sistemi di protezione vengono utilizzati? | | | | | | |  |  |  |
| WEP | *4* | 21,1% | -0,7% | 21,7% | -11,6% | 33,3% | 4 | 5 | 8 |
| WPA | *10* | 63,2% | -6,4% | 69,6% | 15,4% | 54,2% | 12 | 16 | 13 |
| NESSUNO | *0* | 0,0% | 0,0% | 0,0% | 0,0% | 0,0% | 0 | 0 | 0 |
| N.R. | *0* | 15,8% | 7,1% | 8,7% | -3,8% | 12,5% | 3 | 2 | 3 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **19** | **23** | **24** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 2.6 | Sono consentiti gli accessi alla rete interna da remoto ? | | | | | | | 7,78 | 7,70 | 6,29 |
| SI | *0* | 76,1% | 2,2% | 73,9% | 16,8% | 57,1% | 35 | 34 | 32 |
| NO | *6* | 17,4% | -2,2% | 19,6% | -10,8% | 30,4% | 8 | 9 | 17 |
| N.R. | *0* | 6,5% | 0,0% | 6,5% | -6,0% | 12,5% | 3 | 3 | 7 |
| **Totale** |  | 100,0% | 0,0% | 100,0% | 0,0% | 100,0% | **46** | **46** | **56** |
| KPI 2.6a | Nel caso sia consentito l'accesso alla rete interna da remoto, la modalità di connessione utilizza VPN ? | | | | | | |  |  |  |
| Accesso remoto senza VPN | *0* | 5,7% | -6,1% | 11,8% | -10,1% | 21,9% | 2 | 4 | 7 |
| Accesso remoto mediante VPN | *10* | 88,6% | 0,3% | 88,2% | 10,1% | 78,1% | 31 | 30 | 25 |
| N.R. | *0* | 5,7% | 5,7% | 0,0% | 0,0% | 0,0% | 2 | 0 | 0 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **35** | **34** | **32** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 2.7 | Viene utilizzato un firewall per la protezione delle connessioni alla rete pubblica? | | | | | | | 9,22 | 9,13 | 8,82 |
| SI | *6* | 95,7% | 0,0% | 95,7% | 4,6% | 91,1% | 44 | 44 | 51 |
| NO | *0* | 0,0% | 0,0% | 0,0% | 0,0% | 0,0% | 0 | 0 | 0 |
| N.R. | *0* | 4,3% | 0,0% | 4,3% | -4,6% | 8,9% | 2 | 2 | 5 |
| **Totale** |  | 100,0% | 0,0% | 100,0% | 0,0% | 100,0% | **46** | **46** | **56** |
| KPI 2.7a | Nel caso vengano utilizzati firewall, la configurazione dei firewall per l'accesso alla rete pubblica prevede una o più DMZ (Demilitarized Zone) per il posizionamento dei server direttamente accessibilità da internet? | | | | | | |  |  |  |
| SI | *4* | 90,9% | 2,3% | 88,6% | -3,5% | 92,2% | 40 | 39 | 47 |
| NO | *0* | 4,5% | -2,3% | 6,8% | 0,9% | 5,9% | 2 | 3 | 3 |
| N.R. | *0* | 4,5% | 0,0% | 4,5% | 2,6% | 2,0% | 2 | 2 | 1 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **44** | **44** | **51** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 2.8 | Viene utilizzato un IDS/IPS per la protezione delle connessioni alla rete pubblica? | | | | | | | 7,39 | 7,17 | 6,61 |
| SI | *10* | 73,9% | 2,2% | 71,7% | 5,7% | 66,1% | 34 | 33 | 37 |
| NO | *0* | 10,9% | -6,5% | 17,4% | -4,0% | 21,4% | 5 | 8 | 12 |
| N.R. | *0* | 15,2% | 4,3% | 10,9% | -1,6% | 12,5% | 7 | 5 | 7 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 2.9 | Esiste un sistema centralizzato per la raccolta ed il salvataggio delle informazioni critiche (system log, accounting, autorizzazione, autenticazione, tracciamento,IDS) quali accesso ai sistemi, alla rete, alle procedure, ai dati, ecc? | | | | | | | 8,96 | 8,78 | 7,93 |
| Sì, centralizzato | *10* | 80,4% | 4,3% | 76,1% | 6,4% | 69,6% | 37 | 35 | 39 |
| Sì, non centralizzato | *6* | 15,2% | -4,3% | 19,6% | 3,5% | 16,1% | 7 | 9 | 9 |
| NO | *0* | 4,3% | 0,0% | 4,3% | -8,2% | 12,5% | 2 | 2 | 7 |
| N.R. | *0* | 0,0% | 0,0% | 0,0% | -1,8% | 1,8% | 0 | 0 | 1 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **46** | **56** |

Tabella 5: Quesiti e risultati relativi al KPI2

## KPI3: Sicurezza dei servizi

L’indice KPI3 intende misurare l’attenzione rivolta dalle Amministrazioni alla robustezza ed alla affidabilità dei servizi che erogano. Nell’edizione 2010 KPI3 ha mostrato buoni risultati (8,04 le grandi amministrazioni, 7,03 le medie e 6,31 le piccole) superando anche le criticità emerse nella precedente rilevazione per le piccole amministrazioni (4,78 nel 2009). Rimane una sostanziale disomogeneità tra le tre classi di Amministrazioni ma in ogni caso sono sparite le evidenti aree grigie che pesavano su questo indicatore. Ancora una volta le maggiori debolezze si sono concentrate tra le Amministrazioni più piccole e quindi con minore dotazioni, ma non per questo meno critiche rispetto all’intero sistema paese.

Il primo dato che emerge con chiarezza è che, nonostante siano state intraprese già da tempo da DigitPA iniziative atte a promuovere e a sensibilizzare gli utenti rispetto ai temi trattati da questo KPI, permane negli anni un sostanziale disinteresse delle Amministrazioni rispetto al tema “Continuità Operativa”. Infatti, a dispetto di un aumento del +6,3%, KPI3.1 rivela che solo il 43,5% del campione (pari a 20 su 46) dichiara di aver formalizzato un piano per la Continuità Operativa producendo quindi come risultato un valore medio di 4,35 ben al di sotto della soglia di criticità.

Sempre sullo stesso tema, il risultato migliora nel caso di KPI3.2 (*Esistono procedure operative da attivare in caso di indisponibilità parziale dei servizi applicativi ?*) per il quale quasi il 73,9% del campione ha dichiarato di aver predisposto procedure operative da attivare in caso di indisponibilità parziale dei servizi operativi. Il dato di dettaglio vede il 21,7% (+7,8%) delle Amministrazioni con una copertura totale dei servizi ed il 52,2% (-8,3%) con una copertura parziale limitata solo alle procedure più importanti. Da ciò si evince che le amministrazioni che hanno avviato un progetto per la continuità operativa nel 2009 avevano copertura limitata alle procedure più importanti e successivamente hanno esteso la copertura a tutte le procedure nell’anno successivo. Molte altre amministrazioni (20 su 46) invece hanno ignorato il problema.

Il quadro sollevato dai risultati dei precedenti KPI è completato e confermato da KPI3.3 che, con un valore medio di 4,0, ha prodotto il risultato peggiore dell’intero KPI. KPI3.3 intende affrontare tema disaster recovery e da questo, il dato che emerge è che solo il’15,2%, pari a 7 su 19, (nonostante un ulteriore miglioramento del +3,6% rispetto al 2009) del campione dichiara di possedere un piano di disaster recovery con copertura totale ed il 41,3% con un piano limitato alle applicazioni più importanti. Il valore medio resta in linea con gli anni precedenti (2,98 nel 2009 e 2,43 nel 2008) dimostra nella fredda logica dei numeri, quanto siano urgenti ed indispensabili interventi del governo centrale mirati ad individuare una soluzione globale per l’intero campione e definitiva nel tempo per la maggioranza delle Amministrazioni della PAC.

Dall’osservazione dei trend è anche possibile rilevare che gli sforzi per introdurre e sensibilizzare gli utenti sul tema stanno costantemente producendo i risultati attesi ma ancora molto, è chiaro, che ancora molto rimane da fare ed occorre intervenire in fretta se non si vogliono prendere rischi rilevanti. Purtroppo il tema Continuità Operativa viene troppo spesso percepito come un aggravio di costi senza ricadute nel breve periodo. D’altra parte è possibile, mettendo in atto iniziative condivise tra più amministrazioni, ridurre notevolmente l’impegno economico e facilitare la definizione e l’adozione di piani di *disaster* *recovery* utilizzando template preelaborati per la PAC.

D’altra parte è purtroppo evidente che crescendo il livello di informatizzazione della PA aumentano anche la dipendenza e quindi l’esposizione al rischio di subire danni derivanti dalla indisponibilità, seppur temporanea, dei servizi offerti.

Tutti gli altri quesiti che compongono questo indicatore hanno prodotto risultati stabili rispetto all’anno precedente e sostanzialmente positivi. Nella quasi totalità dei casi le amministrazioni hanno mostrato di adottare tutte le corrette soluzioni tecnologiche per garantire il corretto funzionamento e la stabilità dei propri servizi quali gestione delle posta elettronica e siti web (interni o pubblici). Anche l’adozione di sistemi centralizzati per l’aggiornamento degli antivirus (KPI3.8) è una pratica ormai consolidata e oltre l’93,5% del campione afferma di averne implementato uno all’interno della propria organizzazione.

Il dato relativo a KPI3.4, in merito alla vulnerabilità del software ed ai criteri da adottare per limitare la presenza di malware all’interno dei sistemi della PA, rimane estremamente stabile nel tempo (6,52 nel 2010, 6,05 nel 2009, 6,07 nel 2008) indicando da un lato soluzioni consolidate per circa il 60% del campione e dall’altro la mancanza di iniziative in tale direzione volte ad estendere il numero delle Amministrazioni che adottano soluzioni adeguate.

Per quanto riguarda la robustezza dei servizi di base (antivirus ed antispam per la posta elettronica KPI3.5 e KPI3.6, sito Web istituzionale KPI3.7 e servizi centralizzati per rilevazione dei virus informatici KPI3.8), al contrario dei primi tre quesiti di KPI3, vi è una situazione ottimale, con percentuali che vanno dal 78% fino al 93% di Amministrazioni che affermano di aver implementato la soluzione auspicata dal modello.

Infine, rispetto al tema delle intrusioni e degli attacchi informatici (KPI3.9) si nota un aumento della consapevolezza dei rischi e della capacità di percepire gli inevitabili attacchi a cui la rete pubblica espone le amministrazioni. Questo è un dato molto confortante perché laddove c’è questa consapevolezza ci sarà anche la capacità di mettere in atto costantemente le necessarie contromisure.

Laddove è impensabile disporre di una rete in grado di filtrare tutti gli attacchi è sicuramente possibile mettere tutte le amministrazioni in condizioni tale da riuscire a controllare il rischio e garantire comunque la continuità dei propri servizi. Resta comunque forte l’esigenza di disporre di un centro dedicato alla Pubblica Amministrazione per l’allerting precoce di minacce note o possibili attacchi. Un tale servizio consentirebbe anche la segnalazione proattiva di vulnerabilità man mano che queste saranno rese note.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |  | | |
| Figura 14: Distribuzione dei risultati relativi al KPI3 rispetto alle 3 soglie | | Figura 15: Valori medi delle risposte ai quesiti relativi al KPI3 |

La tabella seguente riporta i dati di dettaglio relativi al KPI3:

| **ID** | **Risposta** | **Punt.** | **% 2010** | **Δ '10/'09** | **% 2009** | **Δ '09/'08** | **% 2008** | **# risp. 2010** | **# risp. 2009** | **# risp. 2008** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| KPI 3.1 | Esiste un piano formalizzato per la continuità operativa ? | | | | | | | 4,35 | 3,72 | 3,21 |
| SI | *10* | 43,5% | 6,3% | 37,2% | 5,1% | 32,1% | 20 | 16 | 18 |
| NO | *0* | 47,8% | -5,7% | 53,5% | 5,3% | 48,2% | 22 | 23 | 27 |
| N.R. | *0* | 8,7% | -0,6% | 9,3% | -10,3% | 19,6% | 4 | 4 | 11 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 3.2 | Esistono procedure operative da attivare in caso di indisponibilità parziale dei servizi applicativi ? | | | | | | | 5,30 | 5,02 | 4,29 |
| Sì, senza specificazione della copertura | *10* | 21,7% | 7,8% | 14,0% | -2,1% | 16,1% | 10 | 6 | 9 |
| Sì, solo per le applicazioni più importanti | *6* | 52,2% | -8,3% | 60,5% | 15,8% | 44,6% | 24 | 26 | 25 |
| NO | *0* | 13,0% | -3,2% | 16,3% | -6,9% | 23,2% | 6 | 7 | 13 |
| N.R. | *0* | 13,0% | 3,7% | 9,3% | -6,8% | 16,1% | 6 | 4 | 9 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 3.3 | E' stato definito in modo formale il piano di disaster recovery ? | | | | | | | 4,00 | 2,98 | 2,43 |
| Sì, senza specificazione della copertura | *10* | 15,2% | 3,6% | 11,6% | 4,5% | 7,1% | 7 | 5 | 4 |
| Sì, solo per le applicazioni più importanti | *6* | 41,3% | 11,1% | 30,2% | 1,7% | 28,6% | 19 | 13 | 16 |
| NO | *0* | 30,4% | -11,4% | 41,9% | -2,8% | 44,6% | 14 | 18 | 25 |
| N.R. | *0* | 13,0% | -3,2% | 16,3% | -3,4% | 19,6% | 6 | 7 | 11 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 3.4 | Nello sviluppo di applicazioni, vengono seguiti dei criteri per ridurre la vulnerabilità del software ? | | | | | | | 6,52 | 6,05 | 6,07 |
| SI | *10* | 65,2% | 4,8% | 60,5% | -0,2% | 60,7% | 30 | 26 | 34 |
| NO | *0* | 19,6% | -3,7% | 23,3% | 1,8% | 21,4% | 9 | 10 | 12 |
| N.R. | *0* | 15,2% | -1,1% | 16,3% | -1,6% | 17,9% | 7 | 7 | 10 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 3.5 | Se esiste un server di posta elettronica interno, esiste un filtro antivirus sul server di posta locale ? | | | | | | | 8,04 | 7,91 | 7,50 |
| SI | *10* | 80,4% | 1,4% | 79,1% | 4,1% | 75,0% | 37 | 34 | 42 |
| NO | *0* | 2,2% | -2,5% | 4,7% | 2,9% | 1,8% | 1 | 2 | 1 |
| N.R. | *0* | 17,4% | 1,1% | 16,3% | -6,9% | 23,2% | 8 | 7 | 13 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 3.6 | Se esiste un server di posta elettronica interno, esiste un filtro anti-spam sul server locale ? | | | | | | | 7,83 | 7,67 | 7,32 |
| SI | *10* | 78,3% | 1,5% | 76,7% | 3,5% | 73,2% | 36 | 33 | 41 |
| NO | *0* | 6,5% | -0,5% | 7,0% | 3,4% | 3,6% | 3 | 3 | 2 |
| N.R. | *0* | 15,2% | -1,1% | 16,3% | -6,9% | 23,2% | 7 | 7 | 13 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 3.7 | Viene utilizzato il protocollo HTTPS per proteggere i contenuti sensibili ? | | | | | | | 8,48 | 8,14 | 8,04 |
| SI | *10* | 84,8% | 3,4% | 81,4% | 1,0% | 80,4% | 39 | 35 | 45 |
| NO | *0* | 4,3% | -0,3% | 4,7% | 2,9% | 1,8% | 2 | 2 | 1 |
| N.R. | *0* | 10,9% | -3,1% | 14,0% | -3,9% | 17,9% | 5 | 6 | 10 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 3.8 | Esiste un sistema di protezione antivirus centralizzato ? | | | | | | | 9,35 | 9,07 | 8,57 |
| SI | *10* | 93,5% | 2,8% | 90,7% | 5,0% | 85,7% | 43 | 39 | 48 |
| NO | *0* | 4,3% | 4,3% | 0,0% | -1,8% | 1,8% | 2 | 0 | 1 |
| N.R. | *0* | 2,2% | -7,1% | 9,3% | -3,2% | 12,5% | 1 | 4 | 7 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  |  |  |  |  |  |  |  |  |  |
| KPI 3.9 | Sono state rilevate intrusioni riuscite negli ultimi 24 mesi ? | | | | | | | 8,00 | 7,24 | 7,43 |
| NO | *10* | 71,7% | 4,3% | 67,4% | 4,9% | 62,5% | 33 | 29 | 35 |
| SI | *0* | 19,6% | -3,7% | 23,3% | 0,0% | 23,2% | 9 | 10 | 13 |
| N.R. | *0* | 8,7% | -0,6% | 9,3% | -5,0% | 14,3% | 4 | 4 | 8 |
| **Totale** |  | 100,0% |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
| KPI 3.9a | Se sono state rilevate intrusioni riuscite, quante ? | | | | | | |  |  |  |
| Rilevate < 10 | *2* | 100,0% | 0,0% | 100,0% | 0,0% | 100,0% | 9 | 10 | 13 |
| Rilevate > 10 | *0* | 0,0% | 0,0% | 0,0% | 0,0% | 0,0% | 0 | 0 | 0 |
| KPI 3.9b | Se sono state rilevate intrusioni riuscite di che tipo sono state ? | | | | | | |  |  |  |
| Denial Of Service | *4* | 11,1% | -8,9% | 20,0% | -18,5% | 38,5% | 1 | 2 | 5 |
| Utilizzo di risorse protette | *2* | 0,0% | 0,0% | 0,0% | 0,0% | 0,0% | 0 | 0 | 0 |
| Accesso a dati riservati | *0* | 0,0% | 0,0% | 0,0% | 0,0% | 0,0% | 0 | 0 | 0 |
| Altro tipo | *1* | 88,9% | 18,9% | 70,0% | 8,5% | 61,5% | 8 | 7 | 8 |

Tabella 6: Quesiti e risultati relativi al KPI3

## KPI4: Sicurezza dell’organizzazione

KPI4 è sicuramente l’indice prestazionale più complesso da interpretare anche perché è viene calcolato in funzione del maggior numero di oggetti di controllo, tutti dedicati alla rilevazione della capacità di un’amministrazione di realizzare una organizzazione in grado di sostenere e promuovere la propria sicurezza informatica. Questa sicuramente rappresenta l’area in cui è possibile ottenere i margini di miglioramento più ampi soprattutto implementando soluzioni condivise facilmente adottabili da tutte le amministrazioni ma capaci di imprimere un grosso impatto sul livello di Sicurezza ICT globale della PAC.

Nell’analisi di questo indice storicamente sono emerse numerose criticità in modo diffuso sull’intero campione e su numerosi oggetti di controllo individuati da questo indicatore. Nell’edizione 2010 il valore medio KPI4 si è assestato comunque sopra la soglia della sufficienza (8,23 per le grandi, 5,78 per le medie e 6,58 per le piccole). I notevoli scarti tra i tre valori in funzione delle dimensioni dell’Amministrazione spingono ad intervenire con iniziative specifiche opportunamente declinate in funzione della dimensione dell’amministrazione.

D’altra parte sono numerosi gli indicatori che sono rimasti sotto la sogli di criticità, di seguito descritti:

Analizzando le serie storiche di osserva che se da un lato le grandi amministrazioni sono costantemente cresciute rispetto al tema organizzazione per la sicurezza raggiungendo valori ottimali (7,62 nel 2007, 7,76 nel 2008, 8,05 nel 2009 e 8.23 nel 2010) dall’altro le medie hanno avuto un allarmante regresso passando dai valori già bassi iniziali (6,12 del 2007 e 6,21 nel 2008) ai valori critici osservati negli ultimi due anni (5,00 del 2009 e 5,78 del 2010) e le piccole amministrazioni hanno invece tenuto un andamento più regolare e costante nel tempo rimanendo sempre intorno ai valori di sufficienza (6,07 nel 2007, 6,38 nel 2008, 6,05 nel 2009 e 6,86 nel 2010).



Vista l’ampiezza del dato rilevato sembrerebbe che il tema organizzazione per la sicurezza venga sistematicamente disatteso per molteplici motivi. E’ sicuramente opportuno citare che dai dati raccolti emerge che ancora oggi le amministrazioni difficilmente riconoscono il ruolo determinante che l’organizzazione riveste rispetto al risultato finale atteso in termini di sicurezza complessiva del sistema. A questo problema si sommano gli effetti collaterali prodotti da fattori completamente estranei alla sicurezza quali la scarsa sensibilità negli investimenti in termini di risorse umane allocate alla copertura dei ruoli previsti, già rilevata negli anni precedenti, la scarsa volontà di gestire opportunamente il ricorso all’outsourcing e di governarne i rischi ed infine gli scarsi sforzi messi in atto per garantire adeguati livelli di formazione agli utenti interni.

I dati analizzati con la rilevazione 2010 confermando le tesi esposte, spingono ad individuare in queste aree i temi su cui investire per il miglioramento e per prevenire situazioni critiche.

Analizzando nello specifico i quesiti che hanno pesato maggiormente sullo scarso risultato di questo indicatore si notano:

* KPI4.1 (Disponibilità di un piano per la sicurezza ICT), con valore medio di 5,43 (rispetto al valore di 4,42 dell’anno precedente e 4,64 nel 2008), riflette il fatto che ben 14 amministrazioni hanno dichiarato di non averlo definito (oltre a 7 che non hanno risposto), dato di per se molto significativo anche alla lunce delle recenti norme emanate in materia di sicurezza.
* KPI4.2 (definizione formale di policy per la sicurezza), con valore medio di 6,30 (rispetto a 5,35 del 2009 e al 4,82 del 2008) denuncia che nonostante il miglioramento consistente +9,6% quasi il 37% del campione ancora non dispone di policy formalmente definite per la sicurezza ICT.
* KPI4.3 (copertura dei ruoli previsti dal DM 16/2/2002) analogamente ha disatteso nella media le aspettative del modello (basate sui riferimenti normativi) producendo un valore medio di 4,35, sotto la soglia di criticità e molto vicino a quello degli anni precedenti (5,51 nel 2009 e 4,21 nel 2008). Il dato conferma il ridotto numero di amministrazioni (su 46 amministrazioni 14 hanno ricoperto tutti i ruoli, 10 solo parzialmente, mentre ben 22 non hanno ottemperato alla norma).
* KPI4.10 (budget dedicato alla sicurezza) con una valore medio di 2,78 abbondantemente sotto la soglia di criticità denuncia che solo poche (19 su 46) amministrazioni dedicano una voce separata del proprio bilancio alla sicurezza e tra queste tutte si attestano ad una % inferiore al 10%. D’altra parte non è possibile addebitare questo risultato ai tagli al bilancio prodotti dalla crisi poiché il dato è perfettamente in linea con quelli rilevati negli ultimi 5 anni.
* KPI4.13 (formazione agli utenti sul tema sicurezza ICT). Analogamente a quanto è accaduto per il quesito precedente, anche per questo il risultato di 3,91 (3,70 nel 2009 e 3,25 nel 2008) è particolarmente basso e per questo richiede una più accurata analisi. Questo risultato riflette il fatto che all’interno del campione solo una stretta minoranza delle amministrazioni (14 su 46) ha investito nel corso del 2010 definendo un piano di formazione dedicato alla sicurezza per il proprio personale interno. Senza entrare nel merito dei piani di formazione, il dato peggiora ancora se si considera che tra queste solo 8 hanno avuto come target una percentuale di dipendenti superiore al 30%. Risulta pertanto evidente la grande opportunità per il governo centrale rappresentata dalla possibilità di attivare iniziative congiunte volte alla definizione di piani di formazione standard per classi medie di utenti ed alla loro attuazione, conseguendo da un lato un notevole risparmio e dall’altro garantendo il pieno governo dei contenuti necessari e così una maggiore consapevolezza da parte degli utenti finali in termini di sicurezza ICT.

Tutti gli altri quesiti per KPI4 si sono attestati su valori superiori alla sufficienza. Questo di per se non rappresenta un risultato entusiasmante perché, seppur misurato su basi reali, implica che resta almeno un 40% delle amministrazioni del campione su cui investire sia per una crescita qualitativa delle strategie per la sicurezza sia per promuovere una crescita quantitativa che garantisca la copertura competa del campione rispetto al tema affrontato da KPI4.

Va inoltre segnalata il notevole miglioramento del risultato relativo al quesito KPI4.6 (*Esiste la figura di 'Responsabile protezione dati personali' ?*) che ha raggiunto il valore medio di 7,61 (+17,9%) mentre negli anni precedenti si ea sempre attestato sotto la sufficienza (5,81 nel 2009 e 5,89 nel 2008). E’ evidente che finalmente una buona parte delle amministrazioni del campione (76%) hanno ricoperto il ruolo previsto dal garante della privacy in accordo con l’ormai consolidato Decreto per la Sicurezza.

Analogo risultato per KPI4.7 (*Esistono una o più procedure di gestione dei log ?*)che con un valore medio di 7,83 (+1,5%) si attesta ben al di sopra della sufficienza consolidando il risultato degli anni precedenti.

Anche KPI4.8 (*politiche di backup/restore*) con valore medio di 7,52 conferma che ormai il tema della salvaguardia del dati è stato percepito da tutte le amministrazioni come cruciale e determinante per la vita del proprio CED. In accordo con il quesito analogo proposto da KPI1 oltre il 76% del campione dispone di strumenti e procedure per il backup/restore garantendo la completa protezione dei dati maneggiati nel ciclo di vita delle procedure interne.

migliora rispetto all’anno precedente passando da un valore medio di 5,7 del 2007 a 6,22 rilevando un aumento complessivo del 14,5% del numero di amministrazioni che hanno nominato un responsabile delle politiche di backup (dal 57,6% al 72,1%). Non si è avuto malauguratamente lo stesso miglioramento anche sul numero di amministrazioni che hanno formalizzato e depositato la documentazione relativa alle procedure di loro competenza (KPI4.8a) e pertanto solo 25 delle 31 amministrazioni (pari al 58,1%) che gestiscono procedure di backup/restore hanno approcciato correttamente definendo e documentando le politiche da adottare.

Resta ancora molto ristretto il numero delle amministrazioni che hanno effettuato un’analisi dei rischi connessi alla propria infrastruttura ICT. Infatti secondo KPI4.11 solo 9 amministrazioni su 46 (19,6%) hanno effettuato una analisi dei rischi con copertura totale, 18 con copertura parziale, 5 con copertura minima e quindi ben 14 amministrazioni non hanno preso in considerazione l’opportunità di valutare a priori i rischi derivanti dai processi interni frutto di procedure informatizzate. Ovviamente solo conoscendo i rischi e le aree ove questi di annidano sarà possibile gestire o mitigare il rischio complessivo evitando di creare situazioni estremamente critiche. Sulla scorta di una tale valutazione si auspica che tutte le amministrazioni del campione possano procedere ad una valutazione del rischio con copertura totale perché è solo in questo caso che la stima potrà essere accurata valutando probabilità congiunte di eventi che altrimenti non sarebbero prese in considerazione da analisi parziali

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |  | | |
| Figura 16: Distribuzione dei risultati relativi al KPI4 rispetto alle 3 soglie | | Figura 17: Valori medi delle risposte ai quesiti relativi al KPI4 |

La seguente tabella riporta i risultati rilevati per l’indicatore KPI4.

| **ID** | **Risposta** | **Punt.** | | **% 2010** | | **Δ '10/'09** | | **% 2009** | **Δ '09/'08** | **% 2008** | **# risp. 2010** | **# risp. 2009** | **# risp. 2008** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| KPI 4.1 | E' stato formalmente definito ed approvato il piano della sicurezza ICT ? | | | | | | | | | | 5,43 | 4,42 | 4,64 |
| SI | | *10* | | 54,3% | | 10,2% | 44,2% | -2,2% | 46,4% | 25 | 19 | 26 |
| NO | | *0* | | 30,4% | | -6,8% | 37,2% | 3,3% | 33,9% | 14 | 16 | 19 |
| N.R. | | *0* | | 15,2% | | -3,4% | 18,6% | -1,0% | 19,6% | 7 | 8 | 11 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.2 | Esiste la definizione formale di una policy di sicurezza ICT ? | | | | | | | | | | 6,30 | 5,35 | 4,82 |
| SI | | *10* | | 63,0% | | 9,6% | 53,5% | 5,3% | 48,2% | 29 | 23 | 27 |
| NO | | *0* | | 21,7% | | -6,2% | 27,9% | -0,7% | 28,6% | 10 | 12 | 16 |
| N.R. | | *0* | | 15,2% | | -3,4% | 18,6% | -4,6% | 23,2% | 7 | 8 | 13 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.3 | Sono stati attribuiti i ruoli e le responsabilità secondo quanto previsto dal DM 16-2-02? | | | | | | | | | | 4,35 | 4,51 | 4,21 |
| Sì, tutti | | *10* | | 30,4% | | 4,9% | 25,6% | 5,9% | 19,6% | 14 | 11 | 11 |
| Sì, alcuni | | *6* | | 21,7% | | -10,8% | 32,6% | -4,9% | 37,5% | 10 | 14 | 21 |
| NO | | *0* | | 15,2% | | 3,6% | 11,6% | -4,4% | 16,1% | 7 | 5 | 9 |
| N.R. | | *0* | | 32,6% | | 2,4% | 30,2% | 3,4% | 26,8% | 15 | 13 | 15 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.4 | Esiste ed è attivo un centro di gestione ed amministrazione della sicurezza ICT ? | | | | | | | | | | 6,96 | 6,28 | 5,36 |
| SI | | *10* | | 69,6% | | 6,8% | 62,8% | 9,2% | 53,6% | 32 | 27 | 30 |
| NO | | *0* | | 15,2% | | -3,4% | 18,6% | -6,4% | 25,0% | 7 | 8 | 14 |
| N.R. | | *0* | | 15,2% | | -3,4% | 18,6% | -2,8% | 21,4% | 7 | 8 | 12 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.5 | Esiste ed è attivo un gruppo di gestione degli incidenti ? | | | | | | | | | | 6,52 | 6,05 | 6,07 |
| SI | | *10* | | 65,2% | | 4,8% | 60,5% | -0,2% | 60,7% | 30 | 26 | 34 |
| NO | | *0* | | 19,6% | | 1,0% | 18,6% | -1,0% | 19,6% | 9 | 8 | 11 |
| N.R. | | *0* | | 15,2% | | -5,7% | 20,9% | 1,3% | 19,6% | 7 | 9 | 11 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.6 | Esiste la figura di 'Responsabile protezione dati personali' ? | | | | | | | | | | 7,61 | 5,81 | 5,89 |
| SI | | *10* | | 76,1% | | 17,9% | 58,1% | -0,8% | 58,9% | 35 | 25 | 33 |
| NO | | *0* | | 13,0% | | -7,9% | 20,9% | -0,5% | 21,4% | 6 | 9 | 12 |
| N.R. | | *0* | | 10,9% | | -10,1% | 20,9% | 1,3% | 19,6% | 5 | 9 | 11 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.7 | Esistono una o più procedure di gestione dei log ? | | | | | | | | | | 7,83 | 7,67 | 5,89 |
| SI | | *10* | | 78,3% | | 1,5% | 76,7% | 17,8% | 58,9% | 36 | 33 | 33 |
| NO | | *0* | | 4,3% | | -7,3% | 11,6% | -11,6% | 23,2% | 2 | 5 | 13 |
| N.R. | | *0* | | 17,4% | | 5,8% | 11,6% | -6,2% | 17,9% | 8 | 5 | 10 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.8 | Esiste un responsabile per la gestione ed attuazione delle policy di backup / restore ? | | | | | | | | | | 7,52 | 6,22 | 6,14 |
| SI | | *6* | | 76,1% | | 4,0% | 72,1% | 11,4% | 60,7% | 35 | 31 | 34 |
| NO | | *0* | | 10,9% | | -3,1% | 14,0% | -7,5% | 21,4% | 5 | 6 | 12 |
| N.R. | | *0* | | 13,0% | | -0,9% | 14,0% | -3,9% | 17,9% | 6 | 6 | 10 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
| KPI 4.8a | La procedura di backup è documentata? | | | | | | | | | |  |  |  |
| La procedura è ben documentata | | *4* | | 73,9% | | 15,8% | 58,1% | -4,4% | 62,5% | 34 | 25 | 35 |
| No | | *0* | | 10,9% | | -5,4% | 16,3% | -1,6% | 17,9% | 5 | 7 | 10 |
| N.R. | | *0* | | 15,2% | | -10,4% | 25,6% | 5,9% | 19,6% | 7 | 11 | 11 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.9 | Che tipo di personale viene impiegato per la gestione e l'amministrazione della sicurezza del sistema informativo ? | | | | | | | | | | 8,04 | 6,43 | 7,32 |
| Solo personale interno | | *10* | | 73,9% | | 15,8% | 58,1% | -4,4% | 62,5% | 34 | 25 | 35 |
| Personale misto | | *6* | | 10,9% | | -5,4% | 16,3% | -1,6% | 17,9% | 5 | 7 | 10 |
| Outsourcing per la gestione sicurezza | | *0* | | 0,0% | | 0,0% | 0,0% | 0,0% | 0,0% | 0 | 0 | 0 |
| N.R. | | *0* | | 15,2% | | -10,4% | 25,6% | 5,9% | 19,6% | 7 | 11 | 11 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
| KPI 4.9a | Se esiste un contratto di outsourcing, il contratto prevede che l'amministrazione appaltante effettui verifiche su come è gestita la sicurezza ? | | | | | | | | | |  |  |  |
| Previsto audit | | *5* | | 20,0% | | -22,9% | 42,9% | 32,9% | 10,0% | 1 | 3 | 1 |
| Non previsto audit | | *0* | | 60,0% | | 2,9% | 57,1% | -2,9% | 60,0% | 3 | 4 | 6 |
| N.R. | | *0* | | 20,0% | | 20,0% | 0,0% | -30,0% | 30,0% | 1 | 0 | 3 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **5** | **7** | **10** |
| KPI 4.9b | Se è previsto l'audit della gestione della sicurezza dell'outsourcer, l'audit viene effettuato con regolarità ? | | | | | | | | | |  |  |  |
| SI | | *5* | | 0,0% | | -14,3% | 14,3% | 14,3% | 0,0% | 0 | 1 | 0 |
| NO | | *0* | | 40,0% | | -2,9% | 42,9% | 42,9% | 0,0% | 2 | 3 | 1 |
| N.R. | | *0* | | 60,0% | | 17,1% | 42,9% | -23,8% | 66,7% | 3 | 3 | 10 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 66,7% | **5** | **7** | **11** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.10 | Esiste una previsione di spesa dedicata specificatamente alla sicurezza ? | | | | | | | | | | 2,78 | 2,57 | 2,11 |
| SI | | *4* | | 41,3% | | 1,8% | 39,5% | 7,4% | 32,1% | 19 | 17 | 18 |
| NO | | *0* | | 37,0% | | -2,6% | 39,5% | -10,5% | 50,0% | 17 | 17 | 28 |
| N.R. | | *0* | | 21,7% | | 0,8% | 20,9% | 3,1% | 17,9% | 10 | 9 | 10 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
| KPI 4.10a | Se esiste una previsione di spesa dedicata alla sicurezza quale è la percentuale sul budget IT complessivo ? | | | | | | | | | |  |  |  |
| Inferiore al 5 % | | *2* | | 36,8% | | 7,4% | 29,4% | -31,7% | 61,1% | 7 | 5 | 11 |
| Compresa tra 5 % e 10% | | *4* | | 42,1% | | -16,7% | 58,8% | 25,5% | 33,3% | 8 | 10 | 6 |
| Maggiore del 10% | | *6* | | 5,3% | | 5,3% | 0,0% | 0,0% | 0,0% | 1 | 0 | 0 |
| N.R. | | *0* | | 15,8% | | 4,0% | 11,8% | 6,2% | 5,6% | 3 | 2 | 1 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **19** | **17** | **18** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.11 | E' stata effettuata un'analisi dei rischi connessi alla sicurezza ICT ? | | | | | | | | | | 5,74 | 5,44 | 5,29 |
| Sì | | *4* | | 0,0% | | 0,0% | 0,0% | 0,0% | 0,0% | 0 | 0 | 0 |
| No | | *0* | | 17,4% | | 5,8% | 11,6% | -8,0% | 19,6% | 8 | 5 | 11 |
| Sì, con copertura analisi rischi totale | | *10* | | 19,6% | | 3,3% | 16,3% | -6,9% | 23,2% | 9 | 7 | 13 |
| Sì, con copertura analisi rischi parziale | | *8* | | 39,1% | | 1,9% | 37,2% | 6,9% | 30,4% | 18 | 16 | 17 |
| Sì, con copertura analisi rischi minima | | *6* | | 10,9% | | -3,1% | 14,0% | 5,0% | 8,9% | 5 | 6 | 5 |
| N.R. | | *0* | | 13,0% | | -7,9% | 20,9% | 3,1% | 17,9% | 6 | 9 | 10 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.12 | Sono state prese iniziative per la sensibilizzazione alla sicurezza informatica rivolte a tutto il personale dell'amministrazione ? | | | | | | | | | | 6,74 | 6,51 | 7,50 |
| SI | | *10* | | 67,4% | | 2,3% | 65,1% | -9,9% | 75,0% | 31 | 28 | 42 |
| NO | | *0* | | 17,4% | | -3,5% | 20,9% | 10,2% | 10,7% | 8 | 9 | 6 |
| N.R. | | *0* | | 15,2% | | 1,3% | 14,0% | -0,3% | 14,3% | 7 | 6 | 8 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
|  |  | |  | |  | |  |  |  |  |  |  |  |
| KPI 4.13 | E' stato già redatto ed approvato un piano di formazione e sensibilizzazione per la sicurezza ICT ? | | | | | | | | | | 3,91 | 3,70 | 3,25 |
| SI | | *4* | | 30,4% | | 0,2% | 30,2% | 8,8% | 21,4% | 14 | 13 | 12 |
| NO | | *0* | | 50,0% | | -3,5% | 53,5% | -0,1% | 53,6% | 23 | 23 | 30 |
| N.R. | | *0* | | 19,6% | | 3,3% | 16,3% | -8,7% | 25,0% | 9 | 7 | 14 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **46** | **43** | **56** |
| KPI 4.13a | Se sì quale percentuale di addetti al S.I. ne ha usufruito ? | | | | | | | | | |  |  |  |
| Inferiore al 10 % | | *2* | | 28,6% | | 5,5% | 23,1% | 6,4% | 16,7% | 4 | 3 | 2 |
| Compresa tra il 10 % e il 30 % | | *4* | | 7,1% | | -23,6% | 30,8% | 30,8% | 0,0% | 1 | 4 | 0 |
| Compresa tra il 30 % e il 50 % | | *6* | | 21,4% | | 13,7% | 7,7% | 7,7% | 0,0% | 3 | 1 | 0 |
| maggiore del 50% | | *8* | | 35,7% | | -2,7% | 38,5% | -19,9% | 58,3% | 5 | 5 | 7 |
| N.R. | | *0* | | 7,1% | | 7,1% | 0,0% | -25,0% | 25,0% | 1 | 0 | 3 |
| **Totale** | |  | | 100,0% | |  | 100,0% |  | 100,0% | **14** | **13** | **12** |

Tabella 7: Quesiti e risultati relativi al KPI4

# Considerazioni conclusive (TBD)

Per le conclusioni mi orienterei verso qualcosa di molto soft del tipo:

Anche con questa rilevazione si sono visti l’utilità dei dati raccolti e la ricaduta in termini di crescita culturale degli utenti sul tema sicurezza ottenuta dalle edizioni precedenti.

Le rilevazioni effettuate dimostrano inconfutabilmente che la PAC è cresciuta significativamente negli ultimi 5 anni ma ancora resta da completare il cammino intrapreso.

Il modello va svecchiato, adeguandolo alle nuove norme ed alle tecnologie.

E’ importante misurare ma per farlo occorrono le metriche adatte ed un modello a cui tendere

E’ importante integrare il modello a tendere con gli obiettivi dell’agenda digitale italiana e soprattutto fornire alle amministrazioni oltre al modello il necessario supporto (cloud computing ???)

Il tema sicurezza è sempre più variegato ed investe aree sempre più significative come la CO ed ovviamente il disaster recovery … occorre avere una visione integrata di tuti questi aspetti.

1. Ad Esempio i quesiti relativi alle procedure adottate per la gestione delle password hanno senso solo se l’Amministrazione utilizza username e password come sistema di autenticazione. In questo caso il punteggio penalizza chi usa un sistema debole come username e password ma viene incrementato fino ad un massimo di 4 punti se questo viene gestito correttamente. [↑](#footnote-ref-1)
2. Solo un'amministrazione nell'edizione 2010 è stata esclusa dal campione per aver risposto ad un numero insufficiente di quesiti [↑](#footnote-ref-2)
3. Come la famiglia di standard ISO 27000 , tutti dedicati alla sicurezza ed al rischio informatico. [↑](#footnote-ref-3)