Secondo rapporto sullo stato della sicurezza ICT delle PAC

Indice

Indice **2**

Indice delle Figure **3**

Indice delle Tabelle **3**

1 Premessa **5**

1.1 Considerazioni preliminari *5*

1.2 Sintesi dei risultati della rilevazione *6*
1.2.1 Metodologia 6
1.2.2 Campione della rilevazione 7
1.2.3 Considerazioni 7

2 Struttura ed Obiettivi del questionario **9**

2.1 Obiettivi del questionario *9*

2.2 Elementi di novità dell'edizione 2007 ..... *9*

3 Presentazione della metodologia applicata **10**

3.1 Raccolta e Valutazione dei dati *10*

3.2 Gli indicatori rilevati *11*
3.2.1 KPI1: Sicurezza logica 12
3.2.2 KPI2: Sicurezza dell'infrastruttura 12
3.2.3 KPI3: Sicurezza dei servizi 13
3.2.4 KPI4: Sicurezza dell'organizzazione 13

3.3 Le soglie utilizzate ed i valori minimi attesi *14*

4 Presentazione dei risultati **15**

4.1 KPI1: Sicurezza logica *16*

4.2 KPI2: Sicurezza dell'infrastruttura *18*

4.3 KPI3: Sicurezza dei servizi *21*

4.4 KPI4: Sicurezza dell'organizzazione *24*

5 Considerazioni conclusive **27**

5.1 Risultati complessivi *27*

5.2 Tendenze rispetto alle rilevazioni precedenti *27*

Indice delle Figure

Figura 1: "Distribuzione delle Amministrazioni rispetto al numero di dipendenti"..... 11
Figura 2: "Andamento dei 4 KPI medi rispetto alle dimensioni delle Amministrazioni" 14
Figura 3: "Classificazione dei risultati complessivi relativo al KPI1" 17
Figura 4: "Risultati per quesito relativi al KPI1"" 17
Figura 5: "Classificazione dei risultati complessivi relativo al KPI2" 19
Figura 6: "Risultati per quesito relativi al KPI2" 19
Figura 7: "Grafico del numero di incidenti o di attività ostili rilevate negli ultimi 7 anni sulla RUPA" 22
Figura 8: "Grafico del numero di Hit rilevati negli ultimi 7 anni sulla RUPA in miliardi / anno" ... 22
Figura 9: "Grafico del numero di virus (in milioni) rilevati all'interno di E-Mail in transito sulla RUPA negli ultimi 7 anni" 22
Figura 10: "Grafico del numero di E-Mail transitate attraverso la RUPA negli ultimi 7 anni"..... 22
Figura 11: "Classificazione dei risultati complessivi relativo al KPI3" 23
Figura 12: "Risultati per quesito relativi al KPI3" 23
Figura 13: "Classificazione dei risultati complessivi relativo al KPI4" 25
Figura 14: "Risultati per quesito relativi al KPI4" 25

Indice delle Tabelle

Tabella 1: "Analisi della distribuzione dei 4 KPI nel campione rispetto alle dimensioni"..... 15
Tabella 2: "Quesiti e risultati relativi al KPI1" 17
Tabella 3: "Quesiti e risultati relativi al KPI2" 20
Tabella 4: "Quesiti e risultati relativi al KPI3" 23
Tabella 5: "Quesiti e risultati relativi al KPI4" 25
Tabella 6: "Confronto dei risultati complessivi per i 4 KPI negli ultimi 3 anni" 28

Contenuti del documento (executive summary)

Il documento fa riferimento ai dati del questionario per la rilevazione dello stato della sicurezza ICT delle PAC nell'anno 2007 ed è composto da quattro paragrafi, oltre a questa premessa:

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

Il primo paragrafo "Struttura ed Obiettivi del questionario" 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 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 2007 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 del CNIPA.

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 si 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.

1 Premessa

Da alcuni anni, seguendo un interesse crescente da parte di tutta la comunità ICT (operatori e utenti) non solo appartenente alla pubblica amministrazione, il CNIPA ha iniziato un'attività di monitoraggio sul tema della Sicurezza ICT.

L'occasione di poter raccogliere i dati necessari alle elaborazioni che consentano di conoscere e valutare lo stato della sicurezza, nella prospettiva di interventi adeguati, è stata data dalle rilevazioni annuali che il CNIPA svolge presso le Amministrazioni centrali per la produzione della relazione sullo stato dell'ICT della PAC. Come è noto, questa rilevazione si avvale sia di dati descrittivi forniti dalle Amministrazioni, sia di dati desunti da domande presentate alle Amministrazioni sotto forma di questionario online.

Nel 2006 è stata effettuata anche la rilevazione delle infrastrutture ICT della PAC; questa rilevazione, che ha permesso, partendo dalle impostazioni più semplici e meno strutturate impiegate nelle rilevazioni degli anni precedenti, di ampliare il numero di indicatori rilevati e, soprattutto, di definire un modello di riferimento per la relazione sullo stato della sicurezza. A conclusione dell'attività di rilevazione per la razionalizzazione, venne prodotto un documento "Rapporto sullo stato di sicurezza ICT", distribuito e presentato alle Amministrazioni. Di quel documento il presente lavoro è una rielaborata prosecuzione.

E'importante sottolineare come il modello citato si sia rivelato pertinente e sia stato quindi mantenuto in occasione della rilevazione dei dati per l'anno 2007.

Come in occasione della raccolta dati per l'anno 2006, nella raccolta dati per l'anno 2007, oltre a mantenere l'ampiezza degli elementi rilevati, gli stessi dati sono stati presentati classificati secondo un preciso modello. E' questo un importante risultato, che permette di delineare un modello di riferimento per gli aspetti operativi della sicurezza ICT delle Amministrazioni.

Questo documento è destinato primariamente alle Amministrazioni, come contributo conoscitivo dello stato della sicurezza ICT della loro area di attività, al CNIPA, come supporto alla determinazione degli interventi da fare per migliorare lo stato della sicurezza, ma anche all'intera comunità nazionale come aiuto informativo e, più ancora, metodologico in tema di sicurezza ICT.

1.1 Considerazioni preliminari

Si ritiene opportuno, per una corretta interpretazione dei risultati presentati, premettere anche alcune considerazioni generali emerse nel corso della stesura di questo rapporto.

E' importante premettere che il questionario presentato discende in maniera diretta dal "*modello comune per la sicurezza*" che il CNIPA ha definito ed affinato negli anni per offrire un riferimento comune a tutte le Amministrazioni della PAC, stabile nel tempo, in modo tale da poter monitorare i risultati degli sforzi e dei progetti condotti dalle Amministrazioni rispetto al tema della Sicurezza ICT. Questo indispensabile sforzo purtroppo risulta ancora non uniforme all'interno della PAC anche perché, a meno di alcune indicazioni spesso troppo generiche, manca ancora un preciso riferimento normativo.

Riflettendo la sempre crescente attenzione delle comunità internazionali nei confronti del tema Sicurezza ICT, è infatti opinione diffusa che ogni nazione dovrebbe dotarsi di un organismo centrale in grado di garantire un approccio comune al problema della Sicurezza e dell'evoluzione dei sistemi informativi nella Pubblica Amministrazione. Tali agenzie devono essere in grado di predisporre soluzioni già testate e collaudate ancor prima che il problema emerga. Il Federal Office for Information Security (BSI) in Germania

(http://www.bsi.de/english/index.htm) costituisce uno dei più validi esempi di un simile approccio. La struttura tedesca infatti centralizza forti competenze sul tema sicurezza, mettendole a fattor comune per tutte le strutture pubbliche governative e non, guidando così i processi di innovazione senza introdurre debolezze o rischi non calcolati. Tutto il discorso è basato su di una equazione del tipo: "*più si evolvono i sistemi informativi in uso, più si accentua la dipendenza da questi. All'aumentare di questa dipendenza, cresce in maniera esponenziale la criticità degli stessi sistemi e quindi il problema Sicurezza ICT*."

Più in generale, centralizzando gli sforzi sarebbe possibile anche produrre delle grosse economie di scala come accade spesso in contesti analoghi.

Disporre di un modello comune per la sicurezza consente anche un puntuale monitoraggio dell'utenza che, attraverso le rilevazioni annuali, potranno ricevere indicazioni precise sui risultati dei progetti interni applicando eventuali misure correttive in grado di correggere tempestivamente eventuali scostamenti dal modello atteso.

Il modello proposto viene sottoposto ad un processo di revisione anno per anno in funzione dei risultati delle rilevazioni precedenti, delle norme esistenti e delle indicazioni che i vari organismi internazionali emanano. Tutto ciò, ovviamente, viene elaborato, in funzione della profonda conoscenza della Pubblica Amministrazione, che il CNIPA ha acquisito nel corso degli anni, ottenendo un risultato estremamente coerente con le realtà a cui si rivolge.

Tuttavia tale processo di revisione preserva sempre la struttura complessiva del questionario garantendo la confrontabilità dei risultati conseguiti da ciascuna Amministrazione attraverso le varie edizioni. Questo è particolarmente utile per offrire la possibilità di monitorare i risultati dei progetti condotti rispetto all'andamento generale dell'intero campione.

E' stato considerato inoltre che la data ultima per la migrazione ai servizi offerti dal Sistema Pubblico di Connettività (SPC) era stata fissata per il novembre 2007. E' sembrato comunque prematuro rilevare risultati oggettivi di questa importante iniziativa del CNIPA per lasciare alle Amministrazioni il tempo necessario per sperimentare i nuovi servizi e raccogliere qualsiasi tipo di feedback. Tra le altre cose tra i vari lotti previsti da SPC sono stati previsti anche servizi consulenziali per la gestione della sicurezza degli accessi alla rete e per la configurazione degli apparati. Pertanto tra gli indici rilevati non compaiono dati relativi alla "Sicurezza delle comunicazioni" (canali dati ed apparati hardware) mentre è già stata considerata in due quesiti la misurazione del corretto approccio all'outsourcing della sicurezza (attraverso verifiche puntuali e la corretta contrattualizzazione del servizio). Certamente a partire dalla prossima relazione saranno presenti anche dati relativi all'intero insieme di servizi previsti da SPC.

1.2 Sintesi dei risultati della rilevazione

1.2.1 Metodologia

Anche in questa edizione del questionario sono stati mantenuti i quattro indicatori della precedente edizione 2006:

- **KPI 1 - Sicurezza logica**: legata alle scelte passate o future di prodotti software ed hardware atti alla messa in opera della sicurezza ICT.
- **KPI 2 - Sicurezza dell'infrastruttura**: legata alla robustezza fisica della rete ICT e alla presenza di possibili anomalie sintomo di vulnerabilità interne e delle connessioni esterne.
- **KPI 3 - Sicurezza dei servizi**: legata alla robustezza e presenza di anomalie e vulnerabilità introdotte nella rete da alcuni servizi on-line, quali posta elettronica e accesso web, e relative contromisure.

- **KPI 4 - Sicurezza dell'organizzazione**: legata alla corretta applicazione della direttiva del 16 gennaio 2002 "Sicurezza informatica e delle telecomunicazioni nelle PA statali", e del "Modello organizzativo nazionale di sicurezza ICT per la Pubblica Amministrazione".

Il questionario consta complessivamente di 55 quesiti tutti formulati in modo da prevedere solo risposte "chiuse" in un insieme predefinito di casi. Ogni KPI è caratterizzano da un numero di quesiti che intendono rilevare informazioni oggettive sugli aspetti specifici dell'indicatore. Ad ogni quesito (o gruppo di quesiti se logicamente dipendenti) è stato assegnato un punteggio compreso tra 0 e 10 per la valorizzazione delle risposte previste. Per ogni Amministrazione sono stati sommati i punteggi corrispondenti alle risposte relative ai quesiti di ciascun KPI, ottenendo il valore dell'indicatore come media delle risposte raccolte.

1.2.2 Campione della rilevazione

Per il 2007 il numero di Amministrazioni che hanno partecipato alla rilevazione compilando il questionario è stato di 61 in netto aumento rispetto agli anni precedenti (+24,5%). 7 di queste per ragioni di riservatezza non hanno risposto ad un numero sufficiente di quesiti per cui non sono state incluse nel calcolo dei valori medi relativi all'intero campione, mentre tutte le altre hanno compilato interamente il questionario.

1.2.3 Considerazioni finali

Si riportano le principali considerazioni raccolte a valle dell'analisi dei risultati ed alla luce delle interpretazioni degli stessi fornite dal gruppo di lavoro.

- Il primo dato da rilevare è che il modello unico per la sicurezza adottato si è ulteriormente evoluto rispetto all'anno precedente, parallelamente a quanto è avvenuto nella realtà della PAC, confermando la validità della metodologia impiegata per la rilevazione è la maturità raggiunta.
- E' emersa chiara l'esigenza di continuità nella compilazione dei singoli questionari per garantire la qualità dei dati rilevati e l'uniformità di interpretazione da parte degli utenti finali dei quesiti somministrati. Solo in questo modo sarà sempre più significativo il confronto tra i risultati conseguiti anno per anno anche a livello di singola Amministrazione.
- Va ancora una volta rilevato che la carenza normativa in fatto di sicurezza può costituire un alibi se non una reale causa di inefficienze. A tal proposto il CNIPA si propone di supportare nei prossimi anni lo sviluppo di un preciso supporto normativo per fornire tempestivamente un quadro all'interno del quale la PAC possa decidere autonomamente le strategie da adottare. Va qui notato infatti che carenze organizzative in termini di sicurezza possono tradursi in violazioni delle attuali norme a tutela della privacy molto precise e stringenti, pertanto è possibile, ed in qualche caso necessario, tracciare uno stretto parallelo tra il tema della Sicurezza ICT e la corretta custodia dei dati sensibili che ogni Amministrazione possiede. Il termine Sicurezza ICT è qui impiegato per indicare tutte le soluzioni atte a proteggere l'integrità del dato e va quindi esteso, come si vedrà nel seguito della relazione, anche a concetti quali Analisi del Rischio, Continuità Operativa, sicurezza perimetrale e controllo accessi, ecc.
- Altro tema delicato emerso è quello dell'outsourcing a cui sempre più di frequente le Amministrazioni fanno ricorso. Risulta chiaro che prima ancora di poter esternalizzare un servizio così cruciale come la gestione della Sicurezza ICT è indispensabile che l'Amministrazione appaltante possegga forti competenze per gestire il rapporto con l'outsourcer appropriatamente. Pertanto il CNIPA intende intraprendere una attività di

formazione su tali temi per garantire un livello comune di requisiti minimi da stabilire in fase di negoziazione dei contratti.

2 Struttura ed Obiettivi del questionario

2.1 Obiettivi del questionario

I quesiti del questionario sono opportunamente raggruppati in 4 sezioni tematiche in modo da raccogliere indicazioni oggettive su aspetti ritenuti cruciali per misurare lo stato dell'arte delle misure adottate per garantire la sicurezza dei Sistemi Informativi nella Pubblica Amministrazione e conseguentemente la *sensibilità* della Amministrazioni rispetto al tema Sicurezza ICT.

Le risposte a ciascun quesito sono state valorizzate calcolando prima per ciascuna Amministrazione e poi in media per l'intero campione 4 indicatori chiave (nel seguito indicati come Key Performance Indicator) che nel loro complesso ricoprono a 360 gradi tutti gli aspetti connessi al tema Sicurezza ICT.

L'analisi dei dati rilevati fornisce una fotografia puntuale dello stato dell'arte e delle aree di criticità dove è necessario intervenire prestando la massima attenzione. Tali indicazioni permetteranno inoltre attraverso successive analisi di secondo livello di individuare strategie migliorative, laddove necessarie, mirate alle specifiche realtà.

Come per gli anni precedenti, è opportuno chiarire che tali rilevazioni non forniscono una stima della vulnerabilità dei sistemi informatici delle singole Amministrazioni, bensì misurano, in termini oggettivi e globali, la "consapevolezza" raggiunta da ogni singola struttura informatica sugli elementi di criticità introdotti nei processi interni dall'ormai ineluttabile utilizzo massivo dei sistemi informatici.

I risultati globali sono utili, alle Amministrazioni quanto al CNIPA, per tracciare andamenti tendenziali all'interno della PAC e proporre nuove soluzioni riflettendo quelli che vengono ormai considerati i trend più significativi a livello internazionale sempre in stretta relazione con quello che è lo stato corrente di ogni Amministrazione.

2.2 Elementi di novità dell'edizione 2007

Rispetto alle precedenti edizioni il questionario ha subito una serie di aggiornamenti che riflettono gli sviluppi della tecnologia e l'obsolescenza di alcuni temi che nel tempo si sono dimostrati consolidati per la stragrande maggioranza delle Amministrazioni.

Nello specifico sono stati introdotti i seguenti quesiti:

- Per quanto riguarda la sicurezza logica, due quesiti per verificare l'attenzione rispetto al tema protezione dei dati su supporti mobili e corretta conservazione dei supporti di backup.
- Per quanto riguarda la sicurezza fisica, tre quesiti sul controllo accessi, la gestione delle zone protette da firewall e la disponibilità di un log centralizzato per il salvataggio delle informazioni critiche.
- Per quanto riguarda la sicurezza dei servizi sono stati riformulati alcuni quesiti che riguardano la Continuità Operativa dei servizi offerti a testimonianza di un crescente interesse per questo tema.
- Infine per la quanto attiene l'organizzazione per la sicurezza, il numero complessivo di quesiti è stato ridotto, accorpandone alcuni e rendendo più specifico il quesito dedicato alla gestione del rischio informatico.

Oltre all'aggiornamento del questionario, l'edizione 2007 del rapporto introduce una importante novità suddividendo il campione delle Amministrazioni intervistate in 3 fasce in funzione della dimensione della struttura. La dimensione è stata desunta dal numero totale di dipendenti. In questo modo, come verrà illustrato nel paragrafo dedicato alla metodologia di analisi, è stato possibile raccogliere indicazioni più precise rispetto alle reali esigenze di ciascuna Amministrazione. Infatti le problematiche affrontate sono risultate molto più omogenee all'interno di ogni sottoinsieme di Amministrazioni. D'altra parte è naturale che aspetti critici per la sicurezza, quali budget a disposizione o criticità dei servizi offerti dipendono strettamente dalla dimensione complessiva della struttura organizzativa.

3 Presentazione della metodologia applicata

3.1 Raccolta e Valutazione dei dati

Il questionario consta complessivamente di 55 quesiti, di cui 15 di secondo livello o dipendenti[1], tutti formulati in modo da prevedere solo risposte "*chiuse*" in un insieme predefinito di casi. Questo consente di limitare gli errori di interpretazione da parte degli utenti finali e soprattutto rende più oggettiva l'interpretazione dei risultati.

Per la rilevazione dei dati è stata realizzata una procedura fruibile via rete che ha permesso a ciascun utente munito di userID e password di inserire, rivedere e modificare le varie sezioni del questionario. Accanto allo strumento on-line è stato offerto un help-desk di supporto alla corretta interpretazione dei quesiti e compilazione del questionario oltre ad una attività seminariale per condividere contenuti ed obiettivi con i responsabili.

Le tabelle nel paragrafo seguente riportano per ciascun quesito, le risposte ammesse, il punteggio attribuito a ciascuna risposta ed il numero di occorrenze per ciascuna risposta, oltre che in forma percentuale sul totale di risposte raccolte. Ogni quesito riporta anche il numero di Amministrazioni che non hanno fornito risposta indicato tra le risposte come "*N.R.*".

Per consentire l'analisi statistica dei dati rilevati e la realizzazione di un report sintetico per la presentazione dei risultati, è stata adottata la seguente procedura per la normalizzazione dei risultati a partire dai dati inseriti dalle Amministrazioni:

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 positiva, 0 altrimenti. Nel caso di più risposte ammissibili sono stati usati pesi variabili in funzione della tipo di risposta.
2. Si è poi proceduto al *concatenamento logico* di alcuni 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[2]. Al termine di questa fase il numero totale di quesiti è sceso a 40.
3. I quesiti opportunamente raccolti in sottosezioni sono stati associati a 4 "*Key Performance Indicator*" (nel seguito KPI) descritti nei prossimi paragrafi.
4. Per ogni Amministrazione sono stati calcolati i 4 KPI corrispondenti al valore medio dei punteggi ottenuti da ciascuna risposta fornita all'insieme di quesiti che compongono ciascun KPI. Quesiti senza risposta sono stati considerati, laddove applicabile, risposte negative. Pertanto ogni valore medio sarà un numero compreso tra 0 e 10.

[1] La risposta al quesito è ammissibile solo in funzione di una specifica risposta al quesito precedente.
[2] 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.

5. Ad ogni KPI sono state assegnate 3 soglie per dividere il risultato in 4 gruppi. L'ultima soglia, rappresenta il valore al di sotto del quale il risultato è da considerarsi critico per il livello minimo di Sicurezza atteso. In altre parole le Amministrazioni che hanno raggiunto un punteggio inferiore a tale soglia hanno un livello di attenzione agli aspetti di sicurezza troppo basso denunciando delle evidenti criticità e necessitano pertanto di azioni interne e/o coordinate dal CNIPA con alta priorità.
6. Al fine di avere sottoinsiemi omogenei, le 61 Amministrazioni sono state classificate in funzione del numero di dipendenti in 3 fasce (17 *piccole* con meno di 1.000 dipendenti, 28 *medie* con un numero compreso tra 1.000 e 10.000 dipendenti, 9 *grandi* con oltre 10.000 dipendenti.
7. Le restanti 7 Amministrazioni sono state eliminate dal calcolo dei valori medi perché, per ragioni di riservatezza, non hanno risposto almeno al 50% dei quesiti previsti da ciascun KPI. pertanto per non alterare i valori medi con valori anormalmente bassi, si è proceduto alla loro eliminazione dal campione.
8. Per ciascun gruppo di Amministrazioni sono stati calcolati i valori medi di ognuno dei 4 KPI conseguiti. Il risultato è riportato nella Figura 2.
9. Al termine, per avere una visione di maggior dettaglio è stata calcolato anche il valore medio per ciascun quesito ed i 4 KPI per ciascuna Amministrazioni che ha partecipato alla rilevazione per avviare un'indagine conoscitiva delle aree di maggiore criticità.

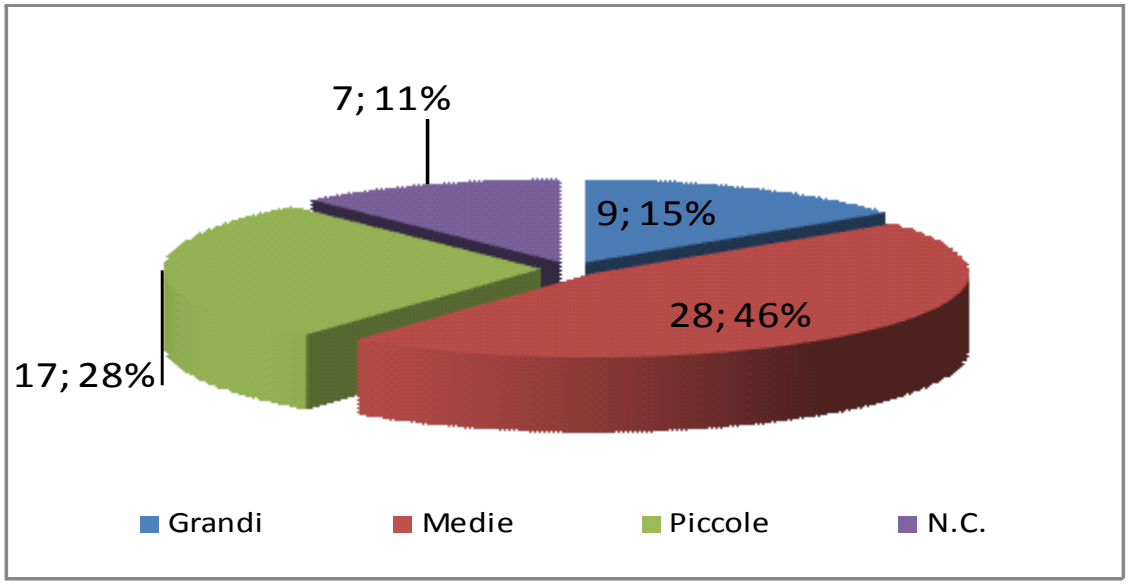

Figura 1: "Distribuzione delle Amministrazioni rispetto al numero di dipendenti"

3.2 Gli indicatori rilevati

Il questionario presentato è stato derivato dal modello di Sicurezza ICT elaborato dal CNIPA negli ultimi anni tenendo conto degli standard internazionali[3] emanati nel settore della sicurezza e coniugando tali standard (che per loro stessa natura devono avere un carattere particolarmente generalista per potersi adattare ad ogni tipo di organizzazione) con la realtà della Pubblica Amministrazione. 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 risultino coerenti con le realtà presenti nelle Amministrazioni intervistate.

[3] Come l'inglese BSS 7799 adottato dall'ISO nella versione ISO 17799 e successivamente confluito nella famiglia di standard ISO 27000 (da 27001 a 27006) tutti dedicati alla sicurezza ed al rischio informatico.

I 4 KPI raccolgono attraverso un insieme di quesiti informazioni su aspetti cruciali per la sicurezza sotto 4 diverse prospettive. Nei prossimi paragrafi sarà quindi descritta l'interpretazione assegnata a ciascuno dei 4 Key Performance Indicator definiti, introducendo così una metrica in grado di coprire a 360 gradi tutti gli aspetti relativi alla sicurezza e consentendo una descrizione estremamente sintetica dei risultati raccolti:

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

Vantaggi principali derivanti dall'uso di Key Performance Indicator è la semplicità di analisi del dato numerico e la capacità di sintesi che così si ottiene. In sostanza una volta individuato il modello e dopo averlo suddiviso in aree omogenee, è stato possibile attraverso i quesiti del questionario estrarre una misura quantitativa per ogni area fotografando così lo stato di ogni singola Amministrazione. Sarà cura del CNIPA mantenere il modello aggiornato e garantire la coerenza e la confrontabilità nel tempo dei KPI.

Il valore medio di ciascun KPI all'interno dei 3 gruppi omogenei di Amministrazioni (raccolti secondo le dimensioni) fornisce anche indicazioni su gli aspetti sui quali investigare o i punti di maggiore criticità su cui intervenire con urgenza.

Nel paragrafo 4 "Presentazione dei risultati" per ogni KPI sarà presentata una tabella che riporta, nella parte sinistra, l'identificativo numerico del quesito, il testo del quesito mentre nella parte destra per ciascun quesito saranno elencate le risposte ammissibili ed i punteggi a queste assegnate.

3.2.1 KPI1: Sicurezza logica

KPI1 raccoglie 14 quesiti di cui 5 dipendenti che prendono in esame tutti gli aspetti connessi alla adozione di strumenti software o soluzioni organizzative atte a garantire un adeguato livello di Sicurezza dei Sistemi Informativi. Tra questi aspetti si citano:

- Implementazione del modello organizzativo per l'amministrazione dei sistemi mediante definizione di procedure o di policy, adozione di certificazioni o standard per la sicurezza.
- Sistemi per l'autenticazione, e controllo accessi.
- Frequenza degli aggiornamenti dei sistemi operativi e sistemi di Software Distribution per le PDL.
- Strumenti e procedure per il Backup e la conservazione dei supporti
- Sicurezza dei dati trasportati all'esterno su supporti o postazioni mobili

Soluzioni adeguate a questi temi rappresentano il corretto punto di partenza per il raggiungimento dei livelli di sicurezza attesi, indipendentemente dalle dimensioni e dalle attività svolte. La Tabella 2: "Quesiti e risultati relativi al KPI1" riporta i quesiti (con identificativo da KPI 1.1 a KPI 1.9) e le risposte ammesse che caratterizzano l'indicatore.

3.2.2 KPI2: Sicurezza dell'infrastruttura

I 12 quesiti (di cui 3 dipendenti) che caratterizzano KPI2 si soffermano sugli aspetti fisici della Sicurezza ed in particolare quelli legati alla infrastruttura di rete, senza però entrare nel merito delle linee dati ed i canali di comunicazione. Complessivamente sono stati raccolte informazioni rispetto ai temi seguenti:

- 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 e contromisure messe in atto per aumentarne la sicurezza.
- Modalità di accesso da remoto e strumenti utilizzati quali VPN.
- Sistemi di log e di accounting centralizzato.

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 utilizzando la tecnologia Wi-Fi in maniera consapevole (proteggendo le comunicazioni radio con protocolli robusti come WPA o WPA2) il punteggio assegnato è 10, per poi scendere in funzione dell'adozione di sistemi di protezione più deboli (4 punti al protocollo WEP con chiavi statiche e 0 punti nel caso di reti wireless non protette).

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 si ottiene solo consentendo accessi da remoto (esigenza molto diffusa) ed impiegando correttamente la tecnologia disponibile (VPN).

La Tabella 3: "Quesiti e risultati relativi al KPI2" riporta i 12 quesiti (da KPI 2.1 a KPI 2.9) e le risposte ammesse con i relativi punteggi assegnati.

3.2.3 KPI3: Sicurezza dei servizi

KPI3 misura l'impegno che le Amministrazioni hanno profuso per rendere affidabili e robusti i servizi offerti. Ovviamente non potendo entrare nel merito dei servizi offerti da ciascuna Amministrazione, si è cercato di individuare un denominatore comune che potesse offrire tale misura prescindendo dalle attività dell'Amministrazione. Pertanto attraverso 11 quesiti (di cui 2 dipendenti) sono stati raccolti dati su temi quali:

- Continuità operativa, procedure da attivare e disponibilità di un piano di disaster recovery
- Servizi centralizzati quali antivirus o antispam sulla posta in transito o sulle PDL
- Protezione dei contenuti e web filtering
- Capacità di rilevare le intrusioni, e/o prevenirle in funzione del tipo di attacchi già subiti

La Tabella 4: "Quesiti e risultati relativi al KPI3" illustra gli 11 quesiti (da KPI 3.1 a KPI 3.9) che caratterizzano KPI3 assieme alla risposte ammesse ed al punteggio assegnato a ciascuna di queste.

3.2.4 KPI4: Sicurezza dell'organizzazione

Ultima area oggetto del questionario è quella relativa all'organizzazione in termini di ruoli e strutture dedicate alla Sicurezza che l'Amministrazione ha messo in atto.

Quest'area riveste particolare importanza perché, in generale, grossi sforzi in termini di realizzazione di soluzioni per migliorare la Sicurezza sono spesso 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 individuare un unico responsabile.

Al contrario soprattutto tra le piccole Amministrazioni tale aspetto viene spesso sottovalutato, tralasciando aspetti rilevanti come la gestione preventiva del rischio o la possibilità di intraprendere iniziative per la formazione e sensibilizzazione del personale interno rispetto ai temi connessi con la Sicurezza.

Pertanto KPI4 mediante i 18 quesiti (di cui 5 dipendenti) riportati nella "Tabella 5: "Quesiti e risultati relativi al KPI4" raccoglie informazioni del tipo:

- 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

3.3 Le soglie utilizzate ed i valori minimi attesi

I risultati per ogni KPI sono stati suddivisi in 4 fasce fissando le seguenti soglie:

$0 \leq KPI < 4$	*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.
$4 \leq KPI < 5$	*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.
$5 \leq KPI < 7$	*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.
$7 \leq KPI \leq 10$	*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.

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. In fatti considerando che ogni KPI è la media di un gruppo di quesiti, un valore basso denuncia che più del 50% dei quesiti ha prodotto risposte contrarie a quelle attese e non può essere considerato come un fenomeno occasionale o una disattenzione. E' chiaro pertanto che in questi casi è certamente necessaria un'indagine di secondo livello per appurare le cause del risultato che non può essere ignorato.

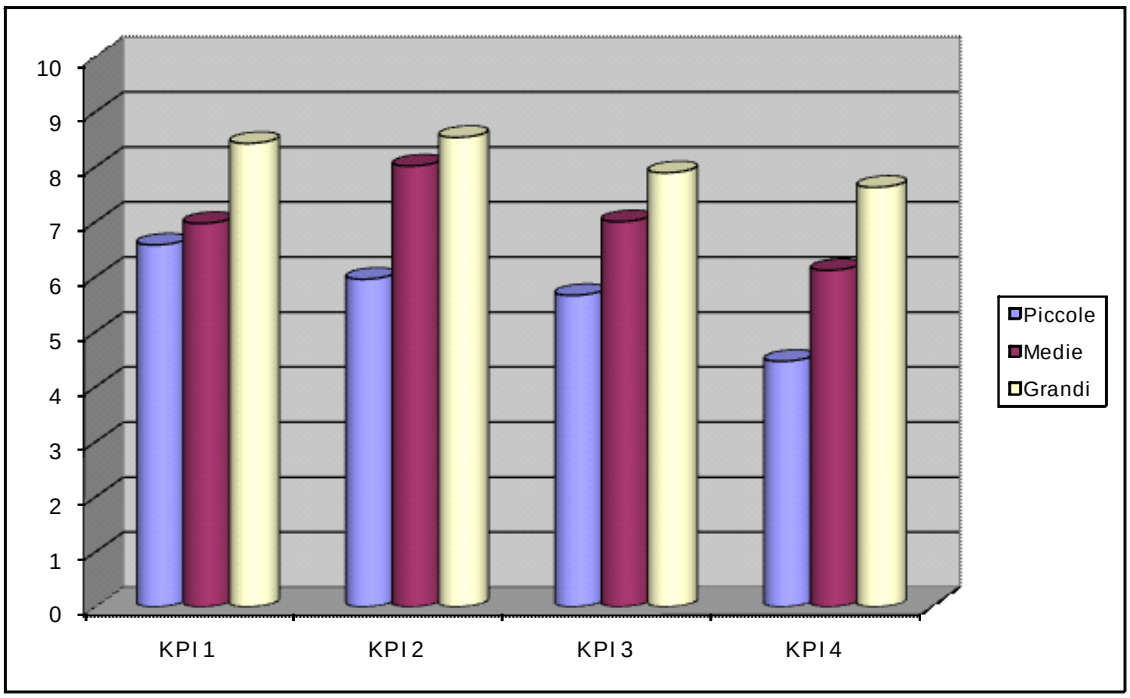

Figura 2: "Andamento dei 4 KPI medi rispetto alle dimensioni delle Amministrazioni"

Categoria	#	KPI 1	KPI 2	KPI 3	KPI 4	Totale
Grandi (> 10.000 dip.)	9	8,42	8,53	7,89	7,62	**8,12**
Medie (tra 1.000 e 10.000)	28	6,97	8,01	7,00	6,12	**7,02**
Piccole (< 1.000 dip.)	17	6,58	5,95	5,66	4,46	**5,66**
Non Classificate	7	1,49	3,06	2,57	1,21	**2,08**
	media	**7,32**	**7,50**	**6,85**	**6,07**	

Tabella 1: "Analisi della distribuzione dei 4 KPI nel campione rispetto alle dimensioni"

4 Presentazione dei risultati

Nei prossimi 4 paragrafi si riportano i dati di dettaglio raccolti attraverso il questionario on-line e le considerazioni scaturite dall'analisi dei risultati secondo la metodologia descritta.

Per una migliore interpretazione dei risultati, si descrivono qui di seguito le convenzioni adottate per la presentazione dei dati. Per ogni indicatore è stata elaborata una tabella, ed ognuna ha la seguente struttura:

1. 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.
2. la seconda colonna riporta il testo del quesito. I quesiti di primo livello sono stampati in grassetto mentre i quesiti di secondo livello, cioè dipendenti dalla risposta precedente secondo la definizione data nel paragrafo 3.1 a pagina 10, sono indentati a destra ed usano un font non in grassetto. Inoltre i quesiti dipendenti sono separati dal precedente da linee orizzontali più sottili;
3. la terza colonna riporta il valore medio sull'intero campione dei punteggi conseguiti dalle Amministrazioni in funzione delle risposte fornite. In questa colonna viene riportato il dato grezzo cioè la media viene calcolata considerando anche le Amministrazioni che hanno fornito un numero di risposte esiguo al di sotto della soglia minima.
4. la quarta colonna riporta l'insieme delle risposte previste per i quesito corrispondete sulla sinistra. Ogni quesito riporta 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;
5. la quinta colonna, con intestazione "Punt." specifica il punteggio assegnato a priori a ciascuna risposta. Per migliorare la leggibilità è stato stampato in italico;
6. la sesta colonna con intestazione "# risp." Indica il numero di Amministrazioni che ha fornito la risposta indicata sulla stessa riga;
7. l'ultima colonna traduce il numero di risposte fornite al quesito in percentuale sul numero totale di Amministrazioni che hanno partecipato al questionario. Va qui notato che, per tutti i quesiti dipendenti, questa percentuale non è riferita all'intero campione ma solo al numero di Amministrazioni che hanno fornito al quesito precedente una risposta che consente di prendere in esame il quesito dipendente.

Oltre alle tabelle descritte, ogni paragrafo riporta anche una prima analisi dei dati scaturiti dall'indicatore complessivo e dalle singole risposte che lo compongono.

4.1 KPI1: Sicurezza logica

L'indicatore KPI1 ha raggiunto un risultato complessivo più che soddisfacente in tutte e tre le categorie di Amministrazioni, piccole, medie e grandi, rispettivamente pari a 6.5, 6.9 e 8.4 ed un indice complessivo di 7.22, ottenuto eliminando dal calcolo della media i risultati delle 7 Amministrazioni che non hanno risposto ad un numero sufficiente di quesiti.

Analizzando i dati nel complesso delle risposte fornite il 53% dell'intero campione, pari a ben 32 Amministrazioni, hanno ottenuto un punteggio per questo indicatore superiore alla soglia ottimale di 7 punti. Analizzando tale risultato nel dettaglio dei singoli quesiti, come evidenzia il grafico in Figura 4: "Risultati per quesito relativi al KPI1" i quesiti che hanno denunciato le maggiori criticità rispetto al campione sono KPI 1.3a, KPI 1.6 e KPI 1.7. Il primo non sorprende riferendosi alla importanza riconosciuta dalle Amministrazioni alle certificazioni per la sicurezza, sia dei prodotti che delle società di servizi. Infatti tra le 40 Amministrazioni che hanno affermato di considerare in fase di selezione le certificazioni per la sicurezza, poi solo poche (una dozzina) in media riconosce tra quelle elencate (ritenute dal CNIPA tra le più significative e utili) quelle effettivamente richieste. Va notato che a tal proposito manca una specifica normativa che prescriva l'adozione di certificazioni da parte delle società fornitrici. Va anche detto che occorrerebbe struttura meglio le autorità adibite al rilascio di tali certificazioni almeno in ambito nazionale.

Per quanto riguarda gli altri due quesiti va notato che KPI 1.7 è stato introdotto quest'anno per la prima volta nel questionario e riveste un carattere particolarmente significativo soprattutto in presenza di dati sensibili. KPI 1.7 riguarda le modalità con cui vengono protetti i dati memorizzati su supporti mobili o computer portatili una volta superato il perimetro fisico della propria sede di lavoro. Molto spesso infatti si è sentito di portatili dimenticati in taxi o rubati all'aeroporto contenenti dati riservati o comunque critici per l'Amministrazione. Anche per questo quesito sarebbe opportuno che ogni Amministrazioni possa regolamentare le dotazioni minime delle postazioni mobili definendo policy per le quali se è previsto che vengano portati all'esterno questi devono essere memorizzati sempre in forma cifrata (supporti con file system cifrato in hardware o software) per cui anche una volta in possesso di male intenzionati, non risulterebbero inutilizzabili.

Per KPI 1.6 vi è stato un peggioramento rispetto all'anno precedente passando da 6,3 a 5,0 o da una percentuale del 67,3% di risposte positive al 50,8%. Questo può essere messo solo in relazione con le Amministrazioni che hanno compilato quest'anno il questionario per la prima volta. Il quesito indaga sulla sensibilità della struttura informatica nel mantenere le postazioni di lavoro sempre aggiornate e quindi protette sia per quanto riguarda il sistema operativo che per quanto riguarda gli applicativi utilizzati. Si auspicava la disponibilità di un sistema totalmente automatizzato per la distribuzione e la verifica della corretta installazione degli aggiornamenti

Inoltre è stato aggiornato il quesito relativo all'esistenza di procedure di backup, aggiungendo il sottoquesito KPI 1.8a che riguarda le modalità di custodia dei supporti utilizzati per il backup. Ovviamente su tali supporti sono presenti tutti i dati dell'Amministrazione necessari per il ripristino in caso di guasti e pertanto è indispensabile che anche questi vengano registrati in forma cifrata e custoditi in armadi ignifughi e blindati per impedire l'accesso indiscriminato ad eventuali malintenzionati, che con pochi nastri avrebbero accesso all'intero patrimonio informativo. A tal proposito da tempo sono già disponibili dispositivi di Backup che provvedono alla cifratura del backup prima di salvare i dati sul supporto esterno. In questo caso la risposta è stata più che positiva, considerando che oltre il 73% delle Amministrazioni che hanno affermato di disporre di procedure di backup hanno dichiarato di utilizzare accorgimenti efficace per la protezione dei supporti di backup. 11 Amministrazioni invece hanno risposto negativamente, e ciò induce ancora una volta alla distribuzione di linee guida che raccolgono le principali norme per la gestione della sicurezza ICT.

Infine rimane da notare che ancora la stragrande maggioranza delle Amministrazioni intervistate utilizzano sistemi di autenticazione, deboli basati su userID e password, pur adottando in generale tutte le precauzioni per irrobustire tale sistema. A tal proposito c'è da segnalare che il

progetto SPC del CNIPA prevede nel lotto "Servizi di interoperabilità evoluta e cooperazione applicativa" anche la fornitura di sistemi avanzati di identificazione/autenticazione basati sull'uso combinato di sistemi biometrici e Smart Card. Tali sistemi inoltre saranno in grado di "federare" le varie autorità ed i domini amministrativi, divenendo così uno strumento abilitante per tutti i servizi di cooperazione applicativa tra Pubblica Amministrazione.

La Tabella 2: "Quesiti e risultati relativi al KPI1" riporta i quesiti è il risultato analitico per ciascun quesito relativo al KPI1

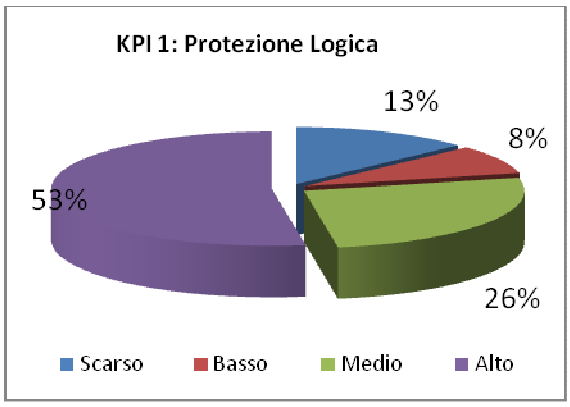

Figura 3: "Classificazione dei risultati complessivi relativo al KPI1"

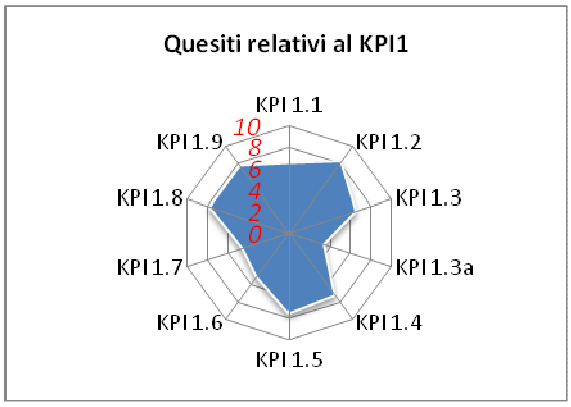

Figura 4: "Risultati per quesito relativi al KPI1""

Tabella 2: "Quesiti e risultati relativi al KPI1"

ID	Quesito	Media Punt.	Risposte	Punt.	# risp	% sul totale
KPI 1.1	**Quale modello di gestione e amministrazione della sicurezza del sistema informativo viene impiegato?**	6,46	Completamente decentralizzato	*10*	1	1,6%
			Parzialmente centralizzato	*8*	33	54,1%
			Completamente centralizzato	*6*	20	32,8%
			Nessuno	*0*	2	3,3%
			N.R.	*0*	5	8,2%
KPI 1.2	**Sono state definite policy per l'uso delle risorse interne da parte degli utenti ?**	8,20	SI	*10*	50	82,0%
			NO	*0*	3	4,9%
			N.R.	*0*	8	13,1%
KPI 1.3	**Nel caso di acquisizione di prodotti o servizi, vengono considerate certificazioni di sicurezza ?**	6,56	SI	*10*	40	65,6%
			NO	*0*	12	19,7%
			N.R.	*0*	9	14,8%
KPI 1.3a	Nel caso vengano considerate certificazioni di sicurezza nell'acquisizione di prodotti o servizi, quali certificazioni sono considerate ?	3,39	CommonCriteria (ISO 15408)	*5*	11	27,5%
			ISO 27001 (ex BS 7799-2)	*5*	15	37,5%
			Certificazioni professionali	*3*	19	47,5%
			Altro	*3*	13	32,5%
KPI 1.4	**Quali criteri/sistemi di autenticazione per l'accesso alla rete interna vengono utilizzati ?**	7,21	UserID/Password	*2*	51	83,6%
			Token di Autenticazione	*6*	0	0,0%
			PKI/Smart Card/PIN	*6*	0	0,0%
			One Time Password	*8*	0	0,0%
			N.R.	*0*	10	16,4%

ID	Quesito	Media Punt.	Risposte	Punt.	# risp	% sul totale
KPI 1.4a	Se si utilizzano UserID e password come sistema di autenticazione, sono state definite regole per la gestione delle password ?		SI	*2*	48	94,1%
KPI 1.4b	Se si utilizzano UserID e password come sistema di autenticazione, è prevista la scadenza automatica di account / password?		SI	*2*	43	84,3%
KPI 1.4c	Se si utilizzano UserID e password come sistema di autenticazione, esiste un controllo preventivo della scelta della password ?		SI	*4*	39	76,5%
KPI 1.5	**Con quale frequenza viene verificata la presenza di aggionamenti dei sistemi operativi dei server ?**	7,51	Automaticamente	*10*	30	49,2%
			Ogni settimana	*10*	10	16,4%
			Ogni mese	*8*	9	14,8%
			Ogni sei mesi	*6*	6	9,8%
			Mai	*0*	0	0,0%
			N.R.	*0*	6	9,8%
KPI 1.6	**Esiste un sistema centralizzato di software distribution per l'aggiornamento automatico delle postazioni di lavoro ?**	5,08	SI	*10*	31	50,8%
			NO	*0*	22	36,1%
			N.R.	*0*	8	13,1%
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?**	4,56	Esistono postazioni mobili o supporti dati rimuovibili con sistemi di prevenzione degli accessi	*10*	20	32,8%
			Esistono postazioni mobili o supporti dati rimuovibili senza sistemi di prevenzione degli accessi	*0*	13	21,3%
			Non esistono postazioni mobili o impiego di supporti dati rimuovibili	*6*	13	21,3%
			N.R.	*0*	15	24,6%
KPI 1.8	**Sono state definite ed adottate tecnologie e procedure per il backup centralizzato ?**	7,77	SI	*6*	53	86,9%
			NO	*0*	2	3,3%
			N.R.	*0*	6	9,8%
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*	39	73,6%
			NO	*0*	11	20,8%
			N.R.	*0*	3	5,7%
KPI 1.9	**Viene utilizzato un sistema di controllo accessi per disciplinare l'accesso alle risorse elaborative ?**	7,70	SI	*10*	47	77,0%
			NO	*0*	7	11,5%
			N.R.	*0*	7	11,5%

4.2 KPI2: Sicurezza dell'infrastruttura

KPI 2, nonostante siano stati modificati 5 quesiti su 9 ha prodotto risultati in linea con gli anni precendenti, ottenendo un punteggio medio di 7.50 ripartito in 8.53 per le grandi Amministrazioni, 8.01 per le medie e 5.95 per le piccole. Anche in questo caso sono state eliminate dal calcolo della media le 7 Amministrazioni che non hanno risposto ad un numero sufficiente di quesiti. Occorre segnalare che storicamente in tutte le precedenti rilevazioni è

sempre emerso il dato che le Amministrazioni tendono a prestare maggiore attenzione agli aspetti della sicurezza esaminati da KPI 2 e cioè dispositivi fisici per la sicurezza, come ad esempio sicurezza perimetrale, controllo accessi fisici. In controtendenza con questo dato il risultato del quesito KPI 2.3, aggiunto quest'anno per la prima volta, che con un punteggio di 4,26 complessivo indica che solo 26 Amministrazioni pari al 42,6% del campione utilizzano un sistema di video sorveglianza per l'accesso ai locali critici, con registrazione H24 delle riprese.

In funzione dell'adozione dei servizi previsti dal progetto SPC (Sistema Pubblico di Connettività) è atteso un sostanziale miglioramento dei sistemi di connessione alla rete pubblica producendo un livellamento verso l'alto dei servizi di connettività, includendo tra questi anche servizi professionali per la configurazione e la definizione di policy interne.

Altro quesito da osservare attentamente nel dettaglio è KPI 2.5. Questo fornisce una istantanea relativa al fenomeno delle reti wireless in ampia diffusione, ma ancora una volta senza specifiche norme di riferimento o indicazioni sul corretto utilizzo. Il valore complessivo di 5.31 denuncia che non viene dedicata abbastanza attenzione a questo tema dalle Amministrazioni che decidono di installare una o più reti wireless. Infatti delle 25 Amministrazioni (pari 41%) che dichiarano di utilizzare reti Wi-Fi solo 10 hanno configurato correttamente il sistema di protezione dei dati scambiati in etere impiegando l'unico standard che garantisce un livello di sicurezza adeguato (WPA o meglio ancora WPA2). Al contrario 11 affermano di utilizzare lo standard WEP che negli anni si è rivelato estremamente debole e facile da aggirare. In questa direzione sarebbe auspicabile una campagna di formazione mirata a fornire indicazioni precise sulle debolezze di questi sistemi e sulle contromisure che devono essere messe in atto per evitare di introdurre punti deboli nell'intero sistema.

Infine, anche quest'anno come negli anni precedenti, altro punto debole dell'indicatore KPI 2 è risultato il quesito KPI 2.8 dedicato alla diffusione dei sistemi di rilevazione e prevenzione delle intrusioni. Con un valore medio di 6.02, appena sufficiente, permette di misurare un diffusione ancora inferiore alle aspettative di tali sistemi all'interno della Pubblica Amministrazione nonostante il già citato progetto SPC che suggerisce l'adozione sistematica di sistemi antintrusione in cooperazione con centri di gestione che ne gestiscono i risultati e gli eventuali allarmi. Infatti solo 37 Amministrazioni pari al 60.7% hanno già adottato tali tecnologie per la sicurezza della rete interna.

Tra i dati positivi, in netto miglioramento rispetto agli anni precedenti, c'è un netto aumento degli accessi dall'esterno attraverso VPN (ben 35 pari al 57,4% di cui ben 29 pari al 82.9% utilizzano VPN), denunciando maggiore consapevolezza e attenzione da parte di tutte le Amministrazioni anche quelle di piccole dimensioni.

Tutti i risultati relativi ai quesiti dell'indicatore KPI2 sono riportati nella Tabella 3: "Quesiti e risultati relativi al KPI2".

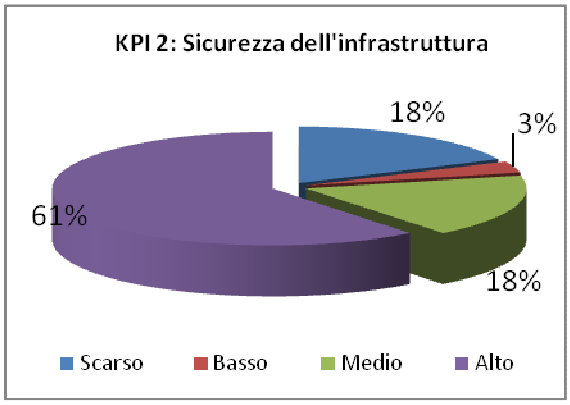

Figura 5: "Classificazione dei risultati complessivi relativo al KPI2"

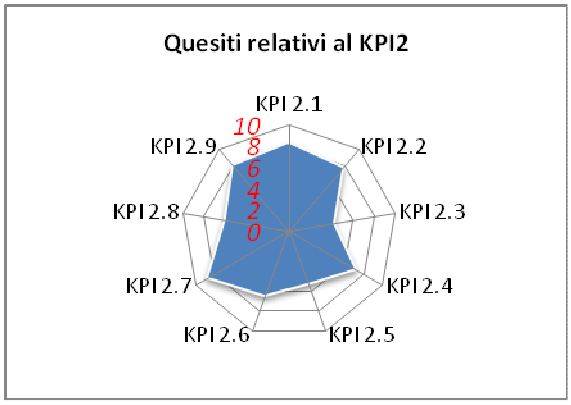

Figura 6: "Risultati per quesito relativi al KPI2"

Tabella 3: "Quesiti e risultati relativi al KPI2"

ID	Quesiti	Media Punt.	Risposte	Punt.	# risp	% sul totale
KPI 2.1	**Esistono barriere fisiche per limitare e perimetrare l'accesso alle risorse elaborative e alla rete interna ?**	8,36	SI	*10*	51	83,6%
			NO	*0*	5	8,2%
			N.R.	*0*	5	8,2%
KPI 2.2	**Esiste un sistema di controllo dell'accesso fisico ai locali dove si trovano gli elaboratori e gli apparati di rete ?**	7,87	SI	*10*	48	78,7%
			NO	*0*	7	11,5%
			N.R.	*0*	6	9,8%
KPI 2.3	**Se l'accesso ai locali critici è ristretto, esiste un sistema di videosorveglianza con registrazione delle riprese H24 ?**	4,26	SI	*10*	26	42,6%
			NO	*0*	19	31,1%
			N.R.	*0*	16	26,2%
KPI 2.4	**Quali di queste protezioni di rete vengono utilizzate?**	7,21	firewall	*5*	55	90,2%
			IDS/IPS	*5*	33	54,1%
			nessuna	*0*	1	1,6%
KPI 2.5	**Sono presenti sottoreti wireless?**	5,31	SI	*0*	25	41,0%
			NO	*6*	30	49,2%
			N.R.	*0*	6	9,8%
KPI 2.5a	Se si utilizzano reti Wi-Fi quali sistemi di protezione vengono utilizzati?		WEP	*4*	11	44,0%
			WPA	*10*	10	40,0%
			Nessuno	*0*	0	0,0%
			N.R.	*0*	4	16,0%
KPI 2.6	**Sono consentiti gli accessi alla rete interna da remoto ?**	6,52	SI	*0*	35	57,4%
			NO	*6*	18	29,5%
			N.R.	*0*	8	13,1%
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*	6	17,1%
			Accesso remoto mediante VPN	*10*	29	82,9%
			N.R.	*0*	0	0,0%
KPI 2.7	**Viene utilizzato un firewall per la protezione delle connessioni alla rete pubblica?**	8,79	SI	*6*	56	91,8%
			NO	*0*	2	3,3%
			N.R.	*0*	3	4,9%
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*	50	89,3%
			NO	*0*	1	1,8%
			N.R.	*0*	5	8,9%
KPI 2.8	**Viene utilizzato un IDS/IPS per la protezione delle connessioni alla rete pubblica?**	6,07	SI	*10*	37	60,7%
			NO	*0*	14	23,0%
			N.R.	*0*	10	16,4%
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?**	8,13	Sì, centralizzato	*10*	46	75,4%
			Sì, non centralizzato	*6*	6	9,8%
			NO	*0*	9	14,8%
			N.R.	*0*	0	0,0%

4.3 KPI3: Sicurezza dei servizi

Come per gli anni precedenti per l'indicatore KPI3 sono emerse grosse differenze all'interno del campione. Infatti il valore complessivo di 6.85, più che soddisfacente, varia da 7.89 per le grandi Amministrazioni, a 5.66 per le piccole Amministrazioni.

Se si considera che KPI3 misura l'attenzione delle Amministrazioni per la robustezza dei servizi offerti si conferma l'idea che mentre le grandi Amministrazioni (Enti Previdenziali ad esempio) hanno già investito su temi quali la continuità operativa per garantire servizi affidabili e stabili nel tempo, le piccole investono anche in virtù della tipologia dei servizi offerti.

Ovviamente anche per KPI3 è stata applicata la stessa metodologia per cui queste valutazioni valgono per il caso medio delle Amministrazioni intervistate.

Scendendo ad un maggior livello di dettaglio, i primi 3 quesiti KPI 3.1, KPI 3.2 e KPI 3.3 hanno prodotto i risultati peggiori ben al di sotto della soglia di criticità spingendo tutti ad una riflessione collettiva su come possono essere affrontati temi quali : Continuità Operativa e Disaster Recovery.

KPI 3.1 con un punteggio medio di 3.44 riflette il fatto che solo 21 Amministrazioni (pari al 34.4% del campione) hanno formalizzato un piano per la Continuità Operativa definendo un piano ben formalizzato. In linea con il risultato precedente, KPI 3.2 (valore medio 4.36) indica la scarsa propensione delle Amministrazioni a definire sistematicamente delle procedure da adottare in caso di indisponibilità anche parziale dei servizi erogati. Infatti solo 11 Amministrazioni (18%) hanno affermato di possedere procedure da attivare in caso di caduta di un qualsiasi servizio (copertura totale). A queste si aggiungono altre 26 Amministrazioni (42,6%) se si considera la copertura solo dei servizi più importanti raggiungendo un complessivo 60,6% del campione. Il dato diventa ancora più allarmante se si considera KPI 3.3 che si è fermato ad un valore medio complessivo di 2.56. In questo caso, solo 6 Amministrazioni (6,8%) affermano di aver redatto un piano per il Disaster Recovery in grado di garantire il ripristino di tutti i servizi in tempi ragionevoli, mentre altre 16 (26.2%) hanno predisposto un piano con copertura parziale limitata alle procedure più importanti.

In questo caso il questionario ha evidenziato un dato estremamente rilevante e diffuso ad oltre il 50% del campione intervistato, richiedendo che vengano intraprese contromisure adeguate nel breve tempo. E' chiaro comunque che il tema della Continuità Operativa non viene ancora avvertito come un fattore di cruciale importanza all'interno di queste Amministrazioni.

Tutti gli altri quesiti, quasi a voler ribilanciare la situazione hanno ottenuto risultati ottimali, mostrando l'ormai diffusa attitudine delle Amministrazioni ad erogare servizi fondamentali quali la posta elettronica o la gestione di siti web e portali pubblicati su Internet.

L'andamento di questi ultimi dati è stato riscontrato con i dati statistici raccolti dall'esercizio della RUPA (Rete Unitaria della Pubblica Amministrazione) che effettivamente confermano i dati rilevati attraverso il questionario e cioè da un lato la crescita costante del numero di servizi offerti dalla PA attraverso la rete pubblica e dall'altro l'alto grado di diffusione dei moderni sistemi Antivirus sulla mail.

I 4 grafici seguenti infatti riportano per gli ultimi 7 anni a sinistra l'andamento del numero di attacchi (numero complessivo di incidenti gestiti o di attività ostili rilevate sulla rete) e di virus rilevati all'interno di messaggi di posta elettronica e a destra la crescita dell'utilizzo della rete rappresentato attraverso il numero di hit http ed il numero di messaggi di posta elettronica scambiati attraverso la RUPA.

Come si vede, nella colonna di destra vi è una costante crescita del traffico, mentre il numero dei virus dopo il picco rilevato a cavallo tra il 2004 ed il 2005 si è poi radicalmente ridotto ed analogamente il numero di incidenti è andato sempre calando negli anni.

L'ultimo quesito KPI 3.9, dedicato al tema gestione degli incidenti ed alla capacità di rilevare tentativi di intrusione, non ha prodotto i risultati attesi ma gli effetti della disponibilità di servizi di gestione degli incidenti offerti da CERT-SPC ad esempio potrebbe migliorare di molto la situazione e la consapevolezza degli utenti rispetto a tale tema. Infatti, nonostante il risultato

complessivo di 8.02 sia più che buono, il numero di incidenti rilevati è troppo basso rispetto ai a quanto rilevato dalle statistiche della RUPA per cui il dato sembra far emergere piuttosto una scarsa consapevolezza rispetto alla effettiva capacità delle Amministrazioni di prevenire intrusioni. Pertanto in futuro sarà dedicata maggiore attenzione alle capacità di rilevare e monitorare il fenomeno delle singole amministrazioni e dei provider del servizio di trasporto.

La Tabella 4: "Quesiti e risultati relativi al KPI3" riporta i risultati relativi ai quesiti dell'indicatore KPI3.

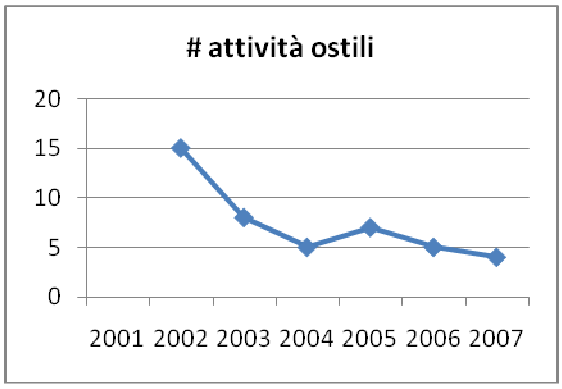

Figura 7: "Grafico del numero di incidenti o di attività ostili rilevate negli ultimi 7 anni sulla RUPA"

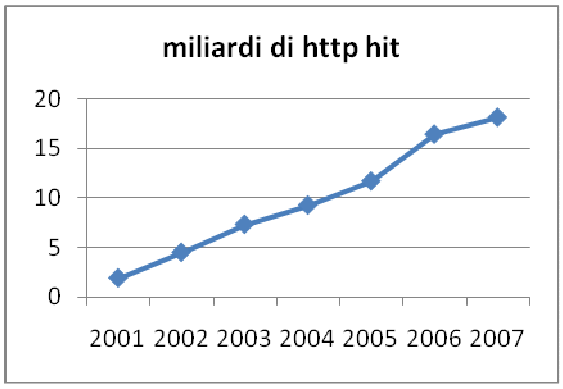

Figura 8: "Grafico del numero di Hit rilevati negli ultimi 7 anni sulla RUPA in miliardi / anno"

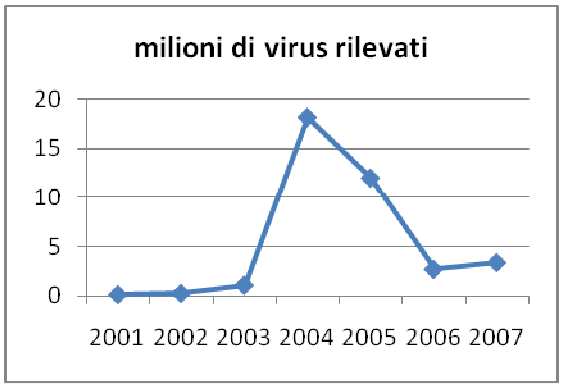

Figura 9: "Grafico del numero di virus (in milioni) rilevati all'interno di E-Mail in transito sulla RUPA negli ultimi 7 anni"

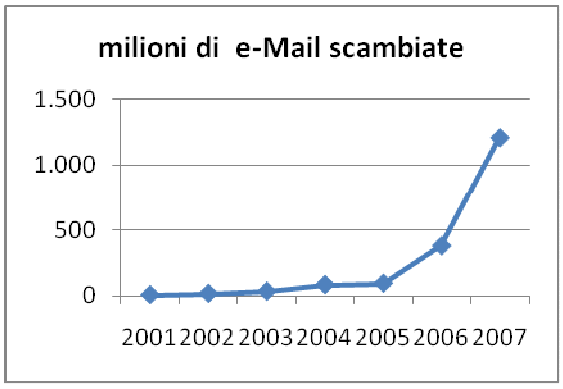

Figura 10: "Grafico del numero di E-Mail transitate attraverso la RUPA negli ultimi 7 anni"

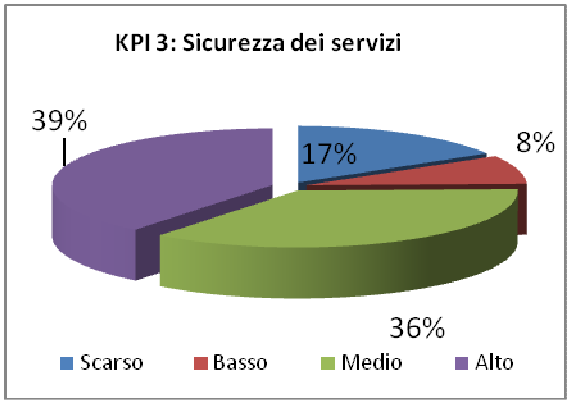

Figura 11: "Classificazione dei risultati complessivi relativo al KPI3"

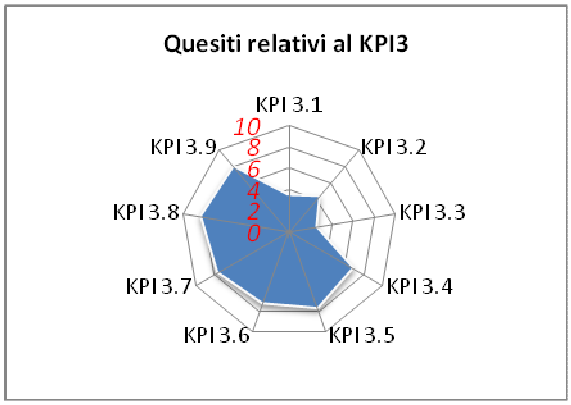

Figura 12: "Risultati per quesito relativi al KPI3"

Tabella 4: "Quesiti e risultati relativi al KPI3"

ID	Quesiti	Media Punt.	Risposte	Punt.	# risp	% sul totale
KPI 3.1	Esiste un piano formalizzato per la continuità operativa ?	3,44	SI	*10*	21	34,4%
			NO	*0*	32	52,5%
			N.R.	*0*	8	13,1%
KPI 3.2	Esistono procedure operative da attivare in caso di indisponibilità parziale dei servizi applicativi ?	4,36	Sì, senza specificazione della copertura	*10*	11	18,0%
			Sì, solo per le applicazioni più importanti	*6*	26	42,6%
			NO	*0*	15	24,6%
			N.R.	*0*	9	14,8%
KPI 3.3	E' stato definito in modo formale il piano di disaster recovery ?	2,56	Sì, senza specificazione della copertura	*10*	6	9,8%
			Sì, solo per le applicazioni più importanti	*6*	16	26,2%
			NO	*0*	31	50,8%
			N.R.	*0*	8	13,1%
KPI 3.4	Nello sviluppo di applicazioni, vengono seguiti dei criteri per ridurre la vulnerabilità del software ?	6,89	SI	*10*	42	68,9%
			NO	*0*	10	16,4%
			N.R.	*0*	9	14,8%
KPI 3.5	Se esiste un server di posta elettronica interno, esiste un filtro antivirus sul server di posta locale ?	7,70	SI	*10*	47	77,0%
			NO	*0*	5	8,2%
			N.R.	*0*	9	14,8%
KPI 3.6	Se esiste un server di posta elettronica interno, esiste un filtro anti-spam sul server locale ?	7,21	SI	*10*	44	72,1%
			NO	*0*	8	13,1%
			N.R.	*0*	9	14,8%
KPI 3.7	Viene utilizzato il protocollo HTTPS per proteggere i contenuti sensibili ?	7,70	SI	*10*	47	77,0%
			NO	*0*	6	9,8%
			N.R.	*0*	8	13,1%
KPI 3.8	Esiste un sistema di protezione antivirus centralizzato ?	8,36	SI	*10*	51	83,6%
			NO	*0*	2	3,3%
			N.R.	*0*	8	13,1%

ID	Quesiti	Media Punt.	Risposte	Punt.	# risp	% sul totale
KPI 3.9	**Sono state rilevate intrusioni riuscite negli ultimi 24 mesi ?**	8,02	NO	*10*	44	72,1%
			SI	*0*	9	14,8%
			N.R.	*0*	8	13,1%
KPI 3.9a	Se sono state rilevate intrusioni riuscite, quante ?		Rilevate < 10	*2*	9	100,0%
			Rilevate > 10	*0*	0	0,0%
KPI 3.9b	Se sono state rilevate intrusioni riuscite di che tipo sono state ?		Denial Of Service	*4*	2	22,2%
			Utilizzo di risorse protette	*2*	0	0,0%
			Accesso a dati riservati	*0*	0	0,0%
			Altro tipo	*1*	7	77,8%

4.4 KPI4: Sicurezza dell'organizzazione

Per KPI4 si accentua ulteriormente il fenomeno rilevato per KPI3. Infatti con un valore medio di 6.07 vicinissimo alla sufficienza ma distribuito tra 7.62 per le grandi, 6.12 per le medie e solo 4.46 per le piccole Amministrazioni evidenzia una distribuzione non uniforme dei risultati legati all'organizzazione dedicata alla Sicurezza.

Il primo dato da sottolineare è che rispetto a questo indicatore, sempre critico negli anni precedenti, vi è stato un netto miglioramento rispetto all'anno 2006 passando da 5.41 a 6.07.

Analizzando le risposte fornite ai singoli quesiti che compongono l'indicatore KPI4 si è potuto percepire con chiarezza come il problema di investire anche in termini organizzativi per affrontare il tema sicurezza, sia ormai percepito dalle grandi organizzazioni e sistematicamente disatteso dalle più piccole.

A confermare questa teoria, arriva il risultato del quesito KPI 4.10 che ha totalizzato un punteggio di soli 2.20. Infatti alla domanda "Esiste un budget dedicato alla sicurezza" solo 20[4] Amministrazioni, pari al 33.9% dell'intero campione, hanno risposto positivamente, ma nessuna di queste ha affermato di dedicare alla sicurezza ICT una percentuale maggiore del 10% del budget complessivo ICT.

In realtà le criticità emerse grazie a KPI4 sono di diversa natura.

In primo luogo si rileva ancora un sostanziale ritardo nell'applicazione concreta del Decreto Ministeriale del 16 Gennaio 2002 per l'attribuzione dei ruoli previsti. Solo 9 Amministrazioni hanno ricoperto tutti i ruoli mentre altre 26 hanno ricoperto i ruoli solo parzialmente. KPI 4.3 con un valore medio 4.03 conferma proprio questo dato e questa criticità.

Occorre però considerare che una cattiva organizzazione interna può vanificare tutti gli sforzi spesi sul piano degli investimenti effettuati in strumenti o procedure, pregiudicando così i risultati positivi conseguiti da KPI1 e KPI2.

A conferma di quanto precedentemente affermato per KPI3, i quesiti KPI 4.4 e KPI 4.5 entrambi con valori al di sotto della sufficienza (5.41 e 5.08) stabiliscono inequivocabilmente che quasi la metà delle Amministrazioni non dedicano sufficiente attenzione alla gestione e prevenzione degli incidenti informatici, rafforzando l'idea alla base CERT-SPC di distribuire attraverso un centro comune tali competenze.

Per altro KPI 4.9, con un valore medio di 7.08 e ben 12 Amministrazioni che affermano di ricorrere a personale misto, indica un deciso miglioramento rispetto alla gestione della sicurezza in outsourcing ed alla capacità delle Amministrazioni di gestire attraverso contratti appropriati l'outsourcer.

Altra nota dolente è la propensione ad effettuare una accurata analisi dei rischi come indicato da KPI 4.11, con valore medio 5.64. Ben 10 Amministrazioni infatti affermano di non aver

[4] Si ricorda che vi sono complessivamente 37 Amministrazioni classificate tra "grandi" e "medie"

effettuato alcuna analisi. 7 hanno effettuato un'analisi dei rischi con copertura minima e 19 con copertura parziale mentre le restanti 15, quasi tutte di grandi e medie dimensioni, hanno effettuato un'analisi con copertura totale. Anche in questo caso è chiaro che, a dispetto della disomogeneità del campione, è necessario che tutte le Amministrazioni acquisiscano l'esigenza di valutazione preventiva del rischio informatico.

Infine, quasi a confermare quanto finora analizzato, emerge in maniera preoccupante la carenza di formazione interna finalizzata alla sensibilizzazione sul tema sicurezza ICT. Infatti KPI 4.13, con un punteggio medio di soli 3.28, testimonia la scarsa propensione ad effettuare formazione al personale interno. Solo 13 Amministrazioni, pari al 22%, hanno redatto e formalizzato un piano di formazione e tra queste solo 7 hanno previsto una partecipazione superiore al 50% del proprio personale.

Anche in questo caso la soluzione a simili problemi passa attraverso la realizzazione di progetti esplicitamente dedicati alla formazione di base per la sicurezza, che mettendo a fattor comune precise competenze ed un modello comune per la sicurezza, possano rapidamente introdurre e diffondere la cultura della sicurezza all'interno della Pubblica Amministrazione.

La Tabella 5: "Quesiti e risultati relativi al KPI4" riporta i risultati rilevati per tale indicatore.

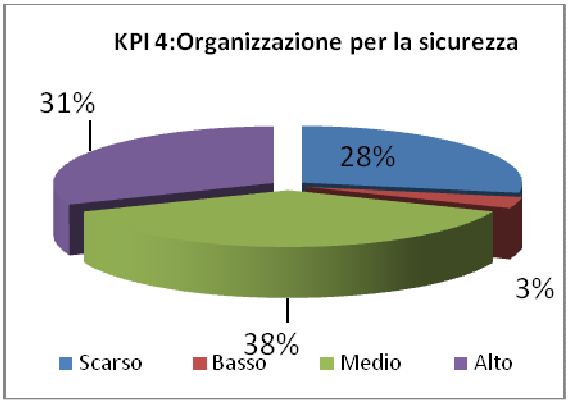

Figura 13: "Classificazione dei risultati complessivi relativo al KPI4"

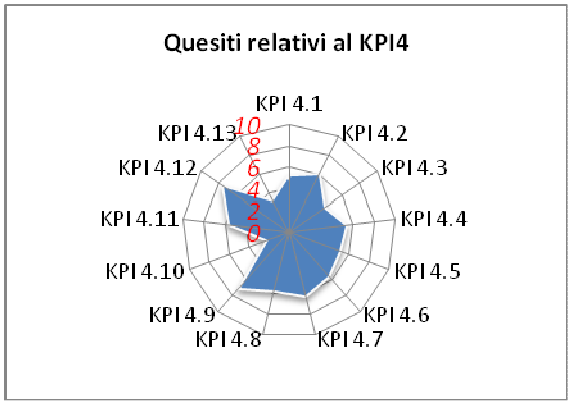

Figura 14: "Risultati per quesito relativi al KPI4"

Tabella 5: "Quesiti e risultati relativi al KPI4"

ID	Quesiti	Media Punt.	Risposte	Punt.	# risp	% sul totale
KPI 4.1	E' stato formalmente definito ed approvato il piano della sicurezza ICT ?	5,25	SI	10	32	54,2%
			NO	0	20	33,9%
			N.R.	0	7	11,9%
KPI 4.2	Esiste la definizione formale di una policy di sicurezza ICT ?	6,07	SI	10	37	62,7%
			NO	0	15	25,4%
			N.R.	0	7	11,9%
KPI 4.3	Sono stati attribuiti i ruoli e le responsabilità secondo quanto previsto dal DM 16-01-2002?	4,03	Sì, tutti	10	9	15,3%
			Sì, alcuni	6	26	44,1%
			NO	0	10	16,9%
			N.R.	0	14	23,7%
KPI 4.4	Esiste ed è attivo un centro di gestione ed amministrazione della sicurezza ICT ?	5,41	SI	10	33	55,9%
			NO	0	21	35,6%
			N.R.	0	5	8,5%
KPI 4.5	Esiste ed è attivo un gruppo di gestione degli incidenti ?	5,08	SI	10	31	52,5%
			NO	0	24	40,7%
			N.R.	0	4	6,8%

ID	Quesiti	Media Punt.	Risposte	Punt.	# risp	% sul totale
KPI 4.6	**Esiste la figura di 'Responsabile protezione dati personali' ?**	5,57	SI	*10*	34	57,6%
			NO	*0*	14	23,7%
			N.R.	*0*	11	18,6%
KPI 4.7	**Esistono una o più procedure di gestione dei log ?**	6,23	SI	*10*	38	64,4%
			NO	*0*	14	23,7%
			N.R.	*0*	7	11,9%
KPI 4.8	**Esiste un responsabile per la gestione ed attuazione delle policy di backup/restore?**	5,70	SI	*6*	34	57,6%
			NO	*0*	17	28,8%
			N.R.	*0*	8	13,6%
KPI 4.8a	La procedura di backup è documentata?		La procedura è ben documentata	*4*	36	61,0%
			No	*0*	12	20,3%
			N.R.	*0*	11	18,6%
KPI 4.9	**Che tipo di personale viene impiegato per la gestione e l'amministrazione della sicurezza del sistema informativo ?**	7,08	Solo personale interno	*10*	36	61,0%
			Personale misto	*6*	12	20,3%
			Outsourcing per la gestione sicurezza	*0*	0	0,0%
			N.R.	*0*	11	18,6%
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*	4	33,3%
			Non previsto audit	*0*	8	66,7%
			N.R.	*0*	0	0,0%
KPI 4.9b	Se è previsto l'audit della gestione della sicurezza dell'outsourcer, l'audit viene effettuato con regolarità ?		SI	*5*	4	33,3%
			NO	*0*	0	0,0%
			N.R.	*0*	8	66,7%
KPI 4.10	**Esiste una previsione di spesa dedicata specificatamente alla sicurezza ?**	2,20	SI	*4*	20	33,9%
			NO	*0*	31	52,5%
			N.R.	*0*	8	13,6%
KPI 4.10a	Se esiste una previsione di spesa dedicata alla sicurezza quale è la percentuale sul budget IT complessivo ?		Inferiore al 5 %	*2*	7	35,0%
			Compresa tra 5 % e 10%	*4*	10	50,0%
			Maggiore del 10%	*6*	0	0,0%
			N.R.	*0*	3	15,0%
KPI 4.11	**E' stata effettuata un'analisi dei rischi connessi alla sicurezza ICT ?**	5,64	Sì	*4*	0	0,0%
			No	*0*	10	16,9%
			Sì, con copertura analisi rischi totale	*10*	15	25,4%
			Sì, con copertura analisi rischi parziale	*8*	19	32,2%
			Sì, con copertura analisi rischi minima	*6*	7	11,9%
			N.R.	*0*	8	13,6%
KPI 4.12	**Sono state prese iniziative per la sensibilizzazione alla Sicurezza ICT rivolte a tutto il personale dell'amministrazione ?**	7,54	SI	*10*	46	78,0%
			NO	*0*	9	15,3%
			N.R.	*0*	4	6,8%
KPI 4.13	**E' stato già redatto ed approvato un piano di formazione e sensibilizzazzione per la sicurezza ICT ?**	3,28	SI	*4*	13	22,0%
			NO	*0*	35	59,3%
			N.R.	*0*	11	18,6%
KPI 4.13a	Se sì quale percentuale di addetti al S.I. ne ha usufruito ?		Inferiore al 10 %	*2*	5	38,5%
			Compresa tra il 10 % e il 30 %	*4*	1	7,7%
			Compresa tra il 30 % e il 50 %	*6*	0	0,0%
			maggiore del 50%	*8*	7	53,8%
			N.R.	*0*	0	0,0%

5 Considerazioni conclusive

5.1 Risultati complessivi

Analizzando i dati relativi ai valori medi per l'intero campione il risultato della rilevazione 2007 sono da considerarsi più che soddisfacenti per tutti gli indicatori. La sicurezza dell'organizzazione rimane il punto debole dell'intera catena.

Per i primi due KPI (Sicurezza logica e Sicurezza dell'Infrastruttura) si conferma la maggiore sensibilità delle Amministrazioni rispetto a temi quali la Continuità Operativa (Sicurezza dei Servizi) o in maniera più diffusa tutta l'Organizzazione per la Sicurezza. Evidentemente devono essere citati anche gli aspetti positivi per i quali sono stati raggiunti risultati ottimali in maniera diffusa, come:

- L'impiego di sistemi di backup / restore centralizzati (anche se poi solo il 57% ha previsto nella propria organizzazione un responsabile dei Backup e gestisce le politiche di backup attraverso procedure ben documentate.)
- buona la diffusione e l'impiego di sistemi per l'identificazione del personale che accede alla sala macchine (77%). Ancora migliore il risultato relativo alla sicurezza perimetrale (83%).
- Ottima la diffusione di firewall che raggiunge quasi il 100% del campione.
- Altrettanto buono l'impiego di sistemi centralizzati per il salvataggio di informazioni critiche, indispensabili per alimentare i sistemi di rilevazione e prevenzione delle intrusioni (event correlation).
- Buona la diffusione, vicina al 77%, di sistemi antivirus centralizzati, o di filtri sulla posta elettronica per la rilevazione di virus o di messaggi non sollecitati.

D'altra parte, sintetizzando quanto già esposto in precedenza, tutte le criticità emerse convergono, secondo l'esperienza del CNIPA, verso tre linee di attività da intraprendere con particolare urgenza:

- Definizione di un piano di formazione dedicato alla sicurezza ICT, sia per gli utenti finali che per i responsabili della Sicurezza. Particolare attenzione nella redazione del piano deve essere dedicata a soluzioni da mettere in atto per colmare le carenze organizzative già rilevate e soprattutto per garantire la massima affidabilità (Continuità Operativa) dei servizi.
- Attivazione di procedure per l'esecuzione di "*penetration test*" standard in grado di valutare oggettivamente il rischio intrusione nei sistemi informativi, e supporto a procedure di *assessment* per la definizione della sicurezza di ogni singola Amministrazione.
- Centralizzazione di competenze per la gestione degli incidenti e la raccolta di statistiche reali in grado di guidare l'evoluzione di ogni sistema informativo in funzione delle caratteristiche specifiche di ogni Amministrazione.

A tal fine è già stata pianificata una rimodulazione del questionario per dettagliare maggiormente questi aspetti ed investigare le pratiche attualmente in uso.

5.2 Tendenze rispetto alle rilevazioni precedenti

Alla luce delle modifiche apportate al questionario ed al numero di Amministrazioni che hanno partecipato alla rilevazione (da 49 a 61) un confronto diretto tra i risultati medi raggiunti dai vari KPI è ancora poco significativo. Al contrario a livello di singola Amministrazione il dato risulta sempre confrontabile ed è stato possibile tracciare delle linee di tendenza.

In ogni caso, con l'obiettivo di disporre sempre di dati reali di alta qualità, il CNIPA ritiene che sia molto importante dare continuità alla compilazione del questionario, facendo in modo, laddove possibile, che siano sempre le stesse persone a produrre i dati da inserire. Infatti in alcuni casi esaminati, i dati hanno prodotto un trend negativo ed in particolare la risposta allo stesso quesito è peggiorata con il passare del tempo, cosa non accettabile, visto che si tratta di risultati stabili nel tempo che non possono regredire. Evidentemente una delle due risposte doveva essere sbagliata oppure sono state date interpretazioni diverse allo stesso quesito da parte di chi ha compilato il questionario nelle due edizioni.

Sul piano squisitamente numerico, i risultati riportati nella Tabella 6: "Confronto dei risultati complessivi per i 4 KPI negli ultimi 3 anni" confermano una tendenza positiva ed una maggiore sensibilità nei confronti del tema Sicurezza ICT.

In questa analisi occorre considerare che solo quest'anno il dato medio è stato calcolato eliminando le Amministrazioni che non hanno risposto almeno al 50% dei quesiti. D'altra parte sono stati eliminati dal questionario tutti i quesiti che hanno prodotto risultati consolidati negli anni precedenti.

Tutto ciò considerato, i due indicatori KPI1 e KPI2 sono rimasti stabili nel tempo, mostrando tra l'altro una buona crescita per le Amministrazioni medio piccole.

La sicurezza dei servizi è cresciuta in maniera sostanziale con un +25% colmando il risultato critico che aveva maturato nella relazione precedente anche alla luce dei progetti in corso censiti nell'anno 2006.

Pur crescendo del 12%, KPI4 rimane sempre molto vicino alla soglia di guardia, confermando così la necessità di attività di formazione e la necessità di norme precise a riguardo della organizzazione di cui si devono dotare tutte le Amministrazioni per gestire adeguatamente la Sicurezza ICT. Di fatto in passato, opportunamente stimolate, le Amministrazioni hanno fornito una ottima risposta ad attività di tipo seminariale o divulgativo.

Tabella 6: "Confronto dei risultati complessivi per i 4 KPI negli ultimi 3 anni"

	2005	2006	Δ'	2007	Δ''
KPI1	4,90	7,33	49,6%	7,32	-0,1%
KPI2	5,90	7,08	20,0%	7,50	5,9%
KPI3	6,80	5,47	-19,6%	6,85	25,2%
KPI4	4,65	5,41	16,3%	6,07	12,1%