CNIPA
Centro Nazionale per l'Informatica
nella Pubblica Amministrazione

Primo Rapporto sullo Stato della Sicurezza ICT delle PAC
Anno 2006

Primo rapporto sullo stato della sicurezza ICT delle PAC

SOMMARIO

Indice delle figure

Indice delle tabelle

Introduzione

Il CNIPA da qualche anno pianifica i propri interventi nel campo della sicurezza informatica delle pubbliche amministrazioni in modo sempre più sistematico.

A questa sistematicità hanno fortemente contribuito le indicazioni che il Comitato tecnico per la sicurezza ICT ha fornito e che hanno portato, già nel corso del 2005, alla costituzione presso il CNIPA di una unità di prevenzione e supporto alla PA centrale per le problematiche connesse alla gestione degli attacchi e degli incidenti informatici, denominata "GovCERT".

Quale contributo alla definizione di una visione organica e operativa della sicurezza ICT delle pubbliche amministrazioni, il CNIPA ha poi redatto le linee guida per la sicurezza ICT delle Pubbliche Amministrazioni, comprendenti le proposte relative alla predisposizione del Piano nazionale della sicurezza ICT e del relativo Modello organizzativo.

Si tratta ora di rendere questo percorso ancora più definito, al fine di favorire iniziative organiche e normative che possano consentire un intervento decisivo e profondo per la difesa dei servizi di e-governement e del patrimonio di dati dello Stato, patrimonio ancora più importante oggi, se possibile, nell'attuale fase di evoluzione della Pubblica Amministrazione.

Questo documento rappresenta un passo in questa direzione. Benché nel 2006 fosse stata prodotta una prima rilevazione strutturata della sicurezza ICT nell'ambito delle attività per la razionalizzazione delle infrastrutture ICT della PAC, in occasione della raccolta di dati per l'annuale relazione del CNIPA sullo stato dell'ICT della PAC si è proceduto a predisporre un sistema di rilevazione più completo e definito. Il presente documento è il risultato di questa attività, il primo di un appuntamento che il CNIPA ha deciso avere cadenza annuale. Questo strumento, che verrà ulteriormente affinato con l'aggiunta di altri dati da rilevare, a cominciare da quelli relativi al SPC, intende avvalersi anche dell'auspicabile contributo delle stesse pubbliche amministrazioni e cercherà di estendersi, su base volontaria, anche alla raccolta di dati di amministrazioni locali e di concessionarie pubbliche. Tale obiettivo, se raggiunto, aumenterà il già alto interesse di questi dati e fornirà un prezioso e unico riferimento sullo stato della sicurezza ICT del settore pubblico.

Un particolare ringraziamento viene rivolto per il lavoro svolto, per l'estrema competenza e per l'impegno dimostrati all'Ing. Gianfranco Pontevolte, al Dott. Giovanni Rellini Lerz del Centro Nazionale per l'Informatica nella Pubblica Amministrazione ed al Prof. Giuseppe Cattaneo, dell'Università di Salerno.

Claudio Manganelli
Componente del Collegio del Cnipa

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 informatica.

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.

A queste occasioni, si è affiancata nel 2006 la rilevazione nell'ambito della razionalizzazione delle infrastrutture ICT della PAC; questa rilevazione, che ha mutuato dalle rilevazioni annuali l'uso di un questionario online, ha rappresentato una opportunità estremamente favorevole 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. 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 2006.

Nel corso di questa ultima rilevazione, utilizzando ancora il questionario online, oltre a mantenere l'ampiezza degli elementi rilevati come confezionata in occasione della rilevazione per la razionalizzazione, gli stessi dati sono stati presentati classificati secondo il modello. Tramite una attività di informazione specifica alle Amministrazioni, si è richiesto che i dati sulla sicurezza provenienti in formato libero dalle Amministrazioni stesse, fossero presentati con la medesima classificazione. Già questo è stato un primo importante risultato utile per verificare che la maggioranza delle Amministrazioni che hanno ritenuto opportuno specificare attività per la sicurezza ICT svolte nel corso del 2006, ha fatto propria questa indicazione. Questo apre la strada sia all'analisi sinottica dei vari contesti delle pubbliche amministrazioni, sia alla possibilità di condividere un linguaggio comune sul tema.

Al termine della rilevazione 2006, la quantità di dati rilevati si è dimostrata più grande di quanto strettamente necessario alle considerazioni da inserire nel documento finale per la rilevazione Ict del 2006. Questo ha dato la possibilità di elaborare i dati ottenuti in modo tale da produrre un rapporto completo sullo stato dell'ICT delle PAC, assimilabile quindi nei contenuti a quello prodotto per la razionalizzazione e sopra richiamato.

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 Contenuti del documento

Il documento fa riferimento ai dati del questionario per la rilevazione dello stato dell'ICT delle PAC nell'anno 2006 ed è composto da quattro paragrafi, oltre alla 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. Il paragrafo successivo "Presentazione della metodologia applicata" presenta la metodologia utilizzata per tradurre i dati rilevati sinteticamente in coefficienti che possano attribuire un significato oggettivo ai quattro *Key Performance Indicator* individuati. Il paragrafo "Presentazione dei risultati" infine illustrerà i risultati ottenuti sia intermini statistici che in termini di motivazioni dei fenomeni osservati o quali quesiti hanno fatto emergere indicazioni utili sulle linee guida da fornire come feedback del questionario.

Il questionario, come negli anni precedenti, non ha rilevato elementi relativi alla sicurezza delle reti geografiche, ma la sua evoluzione prevede sicuramente di inserire anche questi dati, ancora più importanti col diffondersi, dal corrente anno 2007, del Sistema Pubblico di Connettività.

1.2 Considerazioni generali

Di seguito si riportano alcune considerazioni di carattere generale messe a fattor comune per una corretta interpretazione dei risultati.

Il questionario riporta nei paragrafi seguenti specifici riferimenti ad un "modello comune per la sicurezza". Tale modello rappresenta il risultato degli sforzi che il CNIPA ha prodotto negli ultimi anni per supportare un tema così delicato. D'altra parte tutte le Amministrazioni operano ancora in assenza di un preciso riferimento normativo a meno di alcune indicazioni ancora troppo generiche. Il modello proposto, attualmente in fase di perfezionamento, tiene conto dei risultati delle rilevazioni precedenti, delle norme esistenti e delle indicazioni che i vari organismi internazionali hanno finora emanato, opportunamente calate nella realtà della Pubblica Amministrazione.

Infine, a valle dell'analisi dei dati riportati nel questionario, è possibile affermare che la sensibilità da parte delle Amministrazioni rispetto al tema "Sicurezza Informatica" è in crescita e che da più parti questa maggiore sensibilità ha favorito integrazione e razionalizzazione dei processi interni. L'ultimo paragrafo del documento (§ 1.15 Iniziative delle Amministrazioni) è interamente dedicato alla presentazione dei progetti attivi che sono stati rilevati attraverso il questionario ed alle motivazioni che li hanno generati.

2. Struttura ed Obiettivi del questionario

2.1 Obiettivi del questionario

Il questionario, nella sua versione corrente, è costituito da 49 quesiti che riprendono quelli predisposti nella sezione sicurezza del questionario elaborato nell'ambito del progetto per la razionalizzazione della PAC. In tal modo si è inteso salvaguardare la possibilità di confrontare dei dati rilevati tra le diverse edizioni.

Anche il processo di rilevazione dei dati è rimasto pressoché invariato. Tali dati nel loro insieme forniscono una misura della *sensibilità* di ogni singola Amministrazione, nel complesso dell'intera PAC, rispetto al tema Sicurezza Informatica. I quesiti sono stati raccolti in 4 sottosezioni che permettono di valorizzare 4 indicatori chiave (nel seguito indicati come Key Performance Indicator) che nel loro complesso riflettono tutti gli aspetti che coinvolgono il tema Sicurezza all'interno di un'organizzazione. Pertanto a valle dell'analisi dei dati rilevati sarà possibile conoscere statisticamente fino a che punto il tema sia stato affrontato, ma soprattutto sarà possibile individuare le aree dove è più opportuno intervenire con iniziative puntuali o comuni a più Amministrazioni.

Con questa rilevazione, più che conoscere e stimare la vulnerabilità dei sistemi informatici delle singole Amministrazioni, si è cercato di misurare la "consapevolezza" raggiunta da ogni singola struttura informatica sugli elementi di criticità introdotti nei processi interni dall'ormai ineluttabile utilizzo massivo dei sistemi informatici.

Obiettivo primario del questionario è stato quindi quello di rilevare i valori specifici riferiti agli indicatori individuati per fornire una misura realistica sullo stato della PAC rispetto al tema Sicurezza Informatica. Il campione individuato include un insieme di 49 Amministrazioni e per la sua natura stessa sarà stabile negli anni. In ogni caso è stato escluso a priori ogni meccanismo di competizione tra le Amministrazioni intervistate o di classificazione delle stesse in base ai risultati conseguiti.

2.2 Struttura del questionario

La struttura del questionario riflette direttamente la suddivisione del tema Sicurezza in 4 aree. Come meglio specificato nel seguito, ogni sezione del questionario ha raccolto un numero variabile di quesiti tesi a misurare gli obiettivi principali dell'area della Sicurezza in questione.

La prima sezione è dedicata alla sicurezza logica e rileva quindi la presenza di soluzioni e strumenti ritenuti indispensabili in tutti i sistemi informatici del campione analizzato e per questo ritenuti particolarmente significativi (ad esempio sistemi per l'autenticazione, controllo accessi, aggiornamento delle postazioni di lavoro, ecc.).

La seconda sezione riguarda l'infrastruttura fisica e le misure che ogni Amministrazione ha adottato per garantirne il corretto funzionamento. Intende quindi rilevare la presenza di un insieme di apparati fisici atti a garantire la sicurezza del CED e soprattutto dell'infrastruttura di rete dati interna (intranet) ed esterna (extranet).

La terza sezione è connessa con la sicurezza dei servizi elementari (posta elettronica, antivirus, ecc.) ed essenzialmente viene rilevata per misurare l'attenzione dedicata alla sicurezza dei servizi ICT, nelle varie forme che spaziano dai sistemi di disaster recovery fino alla contromisure elementari ma indispensabili come antivirus ed antispam.

L'ultima sezione del questionario riguarda l'organizzazione interna che l'Amministrazione ha saputo / voluto darsi per gestire adeguatamente le problematiche connesse con la Sicurezza. La sezione raccoglie indicazioni sulle principali strutture e ruoli presenti all'interno dell'organizzazione in risposta a precisi adempimenti legislativi o in risposta a problematiche specifiche.

Al termine di ogni sezione è stata lasciata la possibilità ad ogni Amministrazione di aggiungere delle note alla compilazione del questionario. Attraverso questo meccanismo sono stati raccolti numerosi spunti estremamente interessanti sia per la corretta interpretazione dei dati, sia per rilevare tutto quello che non può essere espresso semplicemente con risposte chiuse.

3. Presentazione della metodologia applicata

3.1 Raccolta e valutazione dei dati

Il questionario consta di 36 quesiti e 13 sottoquesiti[1], cioè la risposta è applicabile solo in funzione della risposta data al quesito principale. Tutti i quesiti del questionario sono stati concepiti per avere risposte "*chiuse*" in un insieme predefinito di valori per limitare gli errori di interpretazione delle risposte.

Tutti i dati descrittivi hanno fornito un ulteriore riscontro analitico a quanto ipotizzato attraverso gli indicatori. In sostanza, laddove gli indicatori hanno rilevato una buon livello di interesse sul tema Sicurezza da parte dell'Amministrazione, nelle descrizioni delle attività correnti è sempre emersa la propensione ad affrontare tematiche di rilevante interesse tecnico sempre sul piano della sicurezza.

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 la rilevazione dei dati è stata realizzata una procedura fruibile via rete che ha permesso a ciascun utente munito di username e password di inserire, rivedere e modificare le varie sezioni del questionario.

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:

a) sono stati eliminati tutti i dati puramente descrittivi;
b) ad ogni quesito restante è stato assegnato un peso 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;
c) si è poi proceduto al *concatenamento logico* di alcuni quesiti perché complessivamente possano rappresentare un unico risultato sul tema specifico (con valore complessivo comunque compreso tra 0 e 10). Questo è avvenuto quasi sempre in presenza di domande condizionate[2]. Al termine di questo lavoro il numero totale di quesiti da valutare si è ridotto a 36;
d) i quesiti opportunamente raccolti in sottosezioni sono stati associati a 4 "*Key Performance Indicator*" (nel seguito KPI) descritti nei prossimi paragrafi;
e) per ogni Amministrazione sono stati calcolati i 4 KPI sommando il valore ottenuto da ciascun quesito in funzione delle risposte fornite. Quesiti senza risposta sono stati considerati, laddove applicabile, risposte negative;
f) la somma ottenuta è stata normalizzata a un punteggio compreso tra 0 e 10, dividendo per il numero di quesiti che compongono ciascun KPI;
g) 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 mini-

[1] Il quesito è ammissibile solo in funzione della risposta 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.

mo 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;

h) al termine, traslando i risultati ottenuti, è stata calcolata la media per ciascun quesito e per ciascun KPI su tutte le Amministrazioni che hanno partecipato al questionario per conoscere le aree di maggiore criticità. Va qui precisato che hanno risposto al questionario 49 Amministrazioni, ma due di queste hanno risposto rispettivamente solo a 2 e a 6 quesiti per ragioni di riservatezza dei dati trattati.

3.2 Il modello di sicurezza atteso

Il questionario presentato riflette un modello di sicurezza elaborato dal CNIPA negli ultimi anni che da un lato tiene conto degli standard internazionali emergenti nel settore della sicurezza dall'altro mira a calare tali standard (che per loro stessa natura devono avere un carattere particolarmente generalista per potersi adattare ad ogni tipo di azienda) nella realtà della Pubblica Amministrazione. In tale modo sono state possibili alcune semplificazioni eliminando controlli inutili o già gestiti da altre normative (come quelli sulla sicurezza e la gestione del personale) e facendo in modo che i quesiti presentati riflettano da vicino le realtà delle Amministrazioni intervistate.

3.3 Gli indicatori rilevati

Coerentemente con il modello tracciato, i 4 KPI riflettono le risposte relative ai quesiti corrispondenti ai raggruppamenti individuati. Nei prossimi paragrafi sarà quindi descritta l'interpretazione assegnata a ciascuno dei 4 Key Performance Indicator utilizzati, 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

Ognuno di questi raccoglie un numero variabile di quesiti del questionario, coerentemente aggregati attorno ad una specifica area del tema Sicurezza.

Vantaggi principali derivanti dall'uso di Key Performance Indicator è la semplicità di analisi del dato numerico e la capacità di sintesi che 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 indicativa dello stato di ogni singola amministrazione sommando i risultati ottenuti per ciascun quesito che compone il KPI ed ottenendo un unico dato molto rappresentativo nel tempo. Analogamente, per ciascun KPI, è stato possibile calcolare la media tra tutte le Amministrazioni, ottenendo un dato complessivo dello stato della Sicurezza nella PAC espresso dai 4 KPI medi.

Nel paragrafo "Presentazione dei risultati" per ogni KPI sarà presente 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.

3.3.1 KPI1: Sicurezza logica

KPI1 prende in esame tutti gli aspetti connessi alla adozione di strumenti software o soluzioni organizzative per affrontare il tema sicurezza, quali:

- Modello organizzativo per l'amministrazione dei sistemi, definizione di policy, controllo degli accessi alle risorse e certificazioni richieste.
- Sistemi per l'autenticazione,
- Aggiornamento S.O. dei server e Software Distribution per le PDL,
- Strumenti per il Backup/Restore

Per questa edizione del questionario è stato individuato un insieme minimale di soluzioni ritenute indispensabili per qualsiasi Amministrazione a prescindere dalle sue dimensioni e dalle attività svolte. La Tabella 1: "Quesiti e risultati relativi al KPI1" riporta gli 8 quesiti (con identificativo da 1 a 8) e le risposte ammesse che compongono l'indicatore.

3.3.2 KPI2: Sicurezza dell'infrastruttura

KPI2 tende a fotografare gli aspetti più fisici connessi con la sicurezza dell'impianto ed in particolare quelli legati alla infrastruttura di rete, senza però entrare nel merito delle linee dati ed i canali di comunicazione. Complessivamente 5 quesiti sono serviti per raccogliere informazioni rispetto ai temi seguenti:

- Sicurezza fisica
- Sicurezza perimetrale e controllo accessi ai locali tecnici
- Apparati attivi per la sicurezza degli accessi quali firewall, sistemi per la rilevazione delle intrusioni o per la prevenzione
- Reti wireless e contromisure per aumentare la sicurezza delle reti wireless.
- Modalità di accesso da remoto e strumenti utilizzati quali VPN

Nel caso specifico del quesito 11 "Sono presenti sottoreti wireless?" è stato assegnato un punteggio di 6 punti a chi ha risposto "NO". Mentre utilizzando la tecnologia Wi-Fi in maniera consapevole (proteggendo le comunicazioni radio con protocolli robusti come WPA) il punteggio assegnato è 10, per poi scendere in funzione delle protezioni adottate (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 il punteggio assegnato corrisponde alla sufficienza ma, anche in questo caso, il punteggio massimo di 10 punti si ottiene consentendo accessi ed impiegando la tecnologia disponibile (VPN).

La Tabella 2: "Quesiti e risultati relativi al KPI2" riporta i 6 quesiti (dal 9 al 14) e le risposte ammesse con i relativi punteggi assegnati.

3.3.3 KPI3: Sicurezza dei servizi

Passando all'area della sicurezza relativa ai servizi erogati, sono stati individuati alcuni quesiti che rappresentano un naturale denominatore comune tra tutte le Amministrazioni che hanno partecipato.

KPI3 fotografa la sensibilità dell'amministrazione nel rendere affidabili e robusti i servizi offerti. In particolare affronta 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 3: "Quesiti e risultati relativi al KPI3" illustra i 9 quesiti (dal 15 al 23) che compongono KPI3 assieme alla risposte ammesse ed al punteggio assegnato a ciascuna di queste.

3.3.4 KPI4: Sicurezza dell'organizzazione

Ultima area oggetto della rilevazione è quella relativa all'organizzazione presente nell'Amministrazione in termini di ruoli e strutture dedicate alla Sicurezza.

Quest'area riveste particolare importanza perché, in generale, tra i vari approcci viene spesso sottovalutata, sia in termini di gestione preventiva del rischio, sia in termini di iniziative per la formazione e sensibilizzazione del personale interno rispetto ai temi connessi con la Sicurezza.
KPI4 mediante 13 quesiti riportati nella "Tabella 4: "Quesiti e risultati relativi al KPI4", intende rilevare la cura delle Amministrazioni nel:

- Ricoprire i ruoli previsti dal DM del 16/02/2002, e tutti i ruoli "noti" nell'ambito della sicurezza
- Gestire adeguatamente gli incidenti
- Definire policy e curare un budget esplicitamente dedicato alla sicurezza.
- Gestire adeguatamente le eventuali risorse esterne per la gestione della sicurezza
- Avviare iniziative per garantire sviluppi futuri su questi temi.

3.4 Le soglie utilizzate ed i valori minimi attesi

I risultati per ogni KPI sono stati raccolti in 4 fasce alle quali sono stati attribuiti i seguenti significati:

$0 \leq KPI < 4$	scarsa	Valori critici, che nella media stabiliscono un sostanziale disinteresse rispetto al tema Sicurezza
$4 \leq KPI < 5$	accettabile	Valori mediocri per molti quesiti, è possibile con sforzi non rilevanti ottenere buoni margini di miglioramento.
$5 \leq KPI < 7$	buona	Valori positivi, con interventi mirati sono possibili ulteriori miglioramenti
$7 \leq KPI \leq 10$	ottima	Valori medi accettabili per gli attuali requisiti in termini di sicurezza per i quesiti che compongono il KPI.

Risulta evidente come in questo caso l'uso di KPI come aggregati di più quesiti inserisce un ulteriore elemento di appiattimento dei risultati, essendo questi mediati sull'insieme di quesiti. In sostanza in questo modo si è voluto filtrare tutto il rumore che può nascere per cattive interpretazione dei quesiti o per inadeguatezza del quesito al caso specifico. Pertanto un KPI nella fascia "*scarsa*" va ricondotto ad un comportamento di carattere generale rispetto all'area ricoperta dal KPI e non può essere considerato come un fenomeno occasionale. In questi casi è certamente necessaria un'indagine di secondo livello per appurare le cause del risultato che non può essere ignorato.

4. Presentazione dei risultati

Le tabelle nei prossimi 4 paragrafi riportano l'elaborazione dei risultati raccolti attraverso il questionario, dopo aver applicato la metodologia descritta. La parte destra di ciascuna tabella, accanto ad ogni quesito elenca le risposte ammissibili, il peso assegnato a ciascuna risposta, il numero di strutture informatiche che hanno fornito la specifica risposta e la percentuale sul totale di risposte per ciascuna categoria. Laddove applicabile, è stato fornito anche il numero di strutture informatiche che non hanno risposto al quesito, con la descrizione "N.R." (non rispondono). In questo caso il punteggio assegnato è 0 corrispondente alla risposta peggiore.

Insieme al puro dato statistico è stata anche aggiunta una possibile interpretazione del fenomeno ed in alcuni casi sono anche state proposte le necessarie contromisure da adottare per raggiungere il risultato atteso.

4.1 KPI1: Sicurezza logica

L'indicatore KPI1 ha raggiunto un risultato complessivo più che soddisfacente pari a 7.33, ottenuto mediando i risultati delle Amministrazioni che hanno compilato il questionario. In concreto il 65% del campione, ben 32 Amministrazioni, hanno ottenuto un punteggio superiore alla soglia ottimale (7 punti). Analizzando tale risultato più nel dettaglio, come evidenzia il grafico in Figura 2: "Risultati per quesito relativi al KPI1" gli unici punti di debolezza dell'indicatore, nel suo complesso, sono rappresentati dai quesiti 3 e 4 relativi, il primo ai criteri utilizzati nell'acquisizione del software o servizi ed il secondo agli strumenti impiegati per l'autenticazione degli utenti. Nel primo caso occorre dire che i meccanismi di certificazione del software sono ancora poco diffusi.

Nel secondo caso una possibile motivazione risiede nella mancanza di un vero standard in grado di garantire piena interoperabilità tra sistemi operativi diversi garantendo al tempo stesso meccanismi robusti per l'autenticazione in ogni ambiente.

Per tutti gli altri quesiti che compongono questo indicatore i risultati mostrano un andamento ottimale, se si considera che le uniche Amministrazioni che hanno ottenuto un punteggio sotto la soglia di criticità hanno scelto, dichiarandolo, di non rispondere alla stragrande maggioranza dei quesiti che compongono l'indicatore per questioni di riservatezza dei dati trattati.

Figura 1: "Classificazione dei risultati complessivi relativo al KPI1"

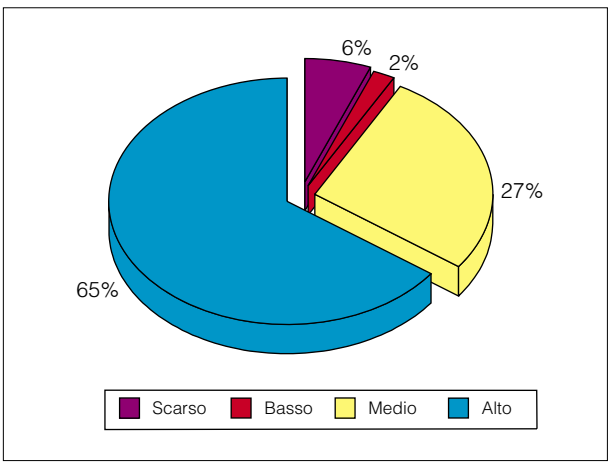
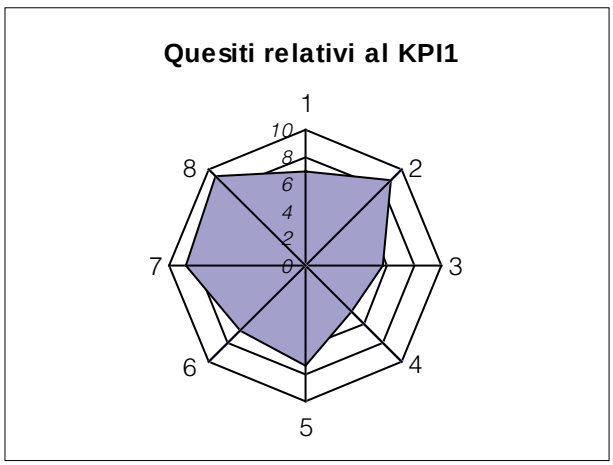


Figura 2: "Risultati per quesito relativi al KPI1"



La Tabella 1: "Quesiti e risultati relativi al KPI1" riporta i quesiti è il risultato analitico per ciascun quesito relativo al KPI1

Tabella 1: "Quesiti e risultati relativi al KPI1"

ID	QUESITI	RISPOSTE	PUNT.	# RISP	% SUL TOTALE
1	Quale modello di gestione ed amministrazione della sicurezza del sistema informativo viene impiegato ?	N.R. Completamente decentralizzato Parzialmente centralizzato Completamente centralizzato Nessuno	*0* *10* *8* *6* *0*	2 2 27 17 1	4,1% 4,1% 55,1% 34,7% 2,0%
2	Sono state definite policy centralizzate per l'uso delle risorse interne da parte degli utenti ?	N.R. SI NO	*0* *10* *0*	3 44 2	6,1% 89,8% 4,1%
3	Nel caso di acquisizione di prodotti o servizi, vengono considerate certificazioni di sicurezza?	N.R. SI NO	*0* *4* *0*	3 30 16	6,1% 61,2% 32,7%
3a	Se vengono considerate certificazioni di sicurezza nell'acquisizione di prodotti o servizi, quali certificazioni sono considerate?	Common Criteria (ISO 15408) ISO27001 (ex BS7799-2) Certificazioni Professionali Altre	*4* *4* *2* *2*	13 15 16 7	43,3%[3] 50,0%[3] 53,3%[3] 23,3%[3]
4	Quali criteri/sistemi di autenticazione per l'accesso alla rete interna vengono utilizzati?	N.R. UserID/password Token di autenticazione Smart Card Radium SSO Altro	*0* *2* *6* *6* *7* *8* *4*	2 47 0 0 0 0 0	4,1% 95,9% 0,0% 0,0% 0,0% 0,0% 0,0%
4a	Se si utilizzano UserID e password come sistema di autenticazione, sono state definite regole per la gestione delle password ?	SI NO	*1* *0*	43 4	91,5%[4] 8,5%[4]
4b	Se si utilizzano UserID e password come sistema di autenticazione, è prevista la scadenza automatica di un account / password?	SI NO	*1* *0*	37 10	78,7%[4] 21,3%[4]
4c	Se si utilizzano UserID e password come sistema di autenticazione, esiste un controllo preventivo della scelta della password ?	SI NO	*2* *0*	31 16	66,0%[4] 34,0%[4]

[3] La percentuale relativa al quesito 3a è stata calcolata sulle 30 Amministrazioni che hanno risposto SI al quesito precedente. Ovviamente le 4 risposte consentite non sono esclusive e pertanto le percentuali non sommano a 100 riflettendo il fatto che la stessa Amministrazione può considerare più certificazioni.

[4] Le percentuali relative ai 3 sottoquesiti 4a, 4b, 4c sono state calcolate sulla base delle 47 amministrazioni che hanno affermato di utilizzare Username/Password come sistema primario per l'autenticazione degli utenti.

***Segue:* Tabella 1: "Quesiti e risultati relativi al KPI1"**

ID	Quesiti	Risposte	Punt.	# risp	% sul totale
5	Con che frequenza viene verificata la presenza di aggiornamenti dei sistemi operativi dei server?	N.R. Automaticamente Ogni settimana Ogni mese Mai	*0* *10* *8* *6* *0*	4 25 7 9 4	8,2% 51,0% 14,3% 18,4% 8,2%
6	Esiste un sistema centralizzato di software distribution per l'aggiornamento automatico delle postazioni di lavoro ?	N.R. SI NO	*0* *10* *0*	3 33 13	6,1% 67,3% 26,5%
7	Sono state definite ed adottate tecnologie e procedure per il backup centralizzato ?	N.R. SI NO	*0* *10* *0*	2 43 4	4,1% 87,8% 8,2%
8	Viene utilizzato un sistema di controllo accessi per disciplinare l'accesso alle risorse elaborative?	N.R. SI NO	*0* *10* *0*	2 46 1	4,1% 93,9% 2,0%

4.2 KPI2: Sicurezza dell'infrastruttura

Anche in questo caso il KPI2 ha ottenuto risultati molto incoraggianti con un punteggio medio di 7.08, incluse anche le 2 Amministrazioni che non hanno risposto alla maggior parte dei quesiti per le già citate ragioni di riservatezza. Storicamente KPI2 riguarda argomenti rispetto ai quali le Amministrazioni hanno sempre rivolto la massima attenzione, come ad esempio le dotazioni per la sicurezza perimetrale, la sicurezza del controllo accessi fisici e le reti in genere, investendo coerentemente sforzi e risorse.

In tal senso occorre anche considerare gli effetti del progetto SPC (Sistema Pubblico di Connettività) che comincia a produrre i risultati attesi standardizzando e livellando verso l'alto i servizi di connettività, includendo tra questi anche servizi professionali per la sicurezza. Alcuni quesiti relativi a KPI2 riguardano infatti dotazioni standard la cui fornitura rientra tra i vari lotti del progetto SPC. Ad esempio praticamente tutte le Amministrazioni sono ormai dotate di uno o più firewall opportunamente collocati per garantire la sicurezza della reti dati interna.

A dispetto di tali risultati estremamente incoraggianti, va però rilevata la presenza di 4 Amministrazioni (oltre le 2 che hanno scelto di non rispondere) con un punteggio al di sotto della soglia critica che asseriscono di non utilizzare alcuna protezione nella connessione alla rete pubblica. Tutti questi casi andrebbero analizzati con maggiore cura, anche in funzione delle diverse dimensioni delle Amministrazioni che compongono il campione analizzato. Comunque va rilevato che nella definizione di modello della PA sempre più basato su sistemi distribuiti ed interoperabili, la robustezza del sistema complessivo può essere messa seriamente in discussione dall'anello più debole della catena. Anche se nessuno dei quesiti che compongo il KPI ha ottenuto valori medi al di sotto della soglia dell'accettabilità (5.00, cf. Figura 4: "Risultati per quesito relativi al KPI2") particolare attenzione deve essere ancora rivolta al tema reti wireless il cui quesito (ID=11) ha ottenuto un valore medio di 5.63 denunciando ancora la presenza di alcune reti protette da sistemi inadeguati.

Anche rispetto l'utilizzo di sistemi per la rilevazione o prevenzione delle intrusioni (quesito 14) si rileva un utilizzo ancora non abbastanza diffuso, risultando in uso solo presso 25 Amministrazioni pari al 51% del campione.

Tutti i risultati relativi ai quesiti dell'indicatore KPI2 sono riportati nella Tabella 2: "Quesiti e risultati relativi al KPI2".

Figura 3: "Classificazione dei risultati complessivi relativo al KPI2"

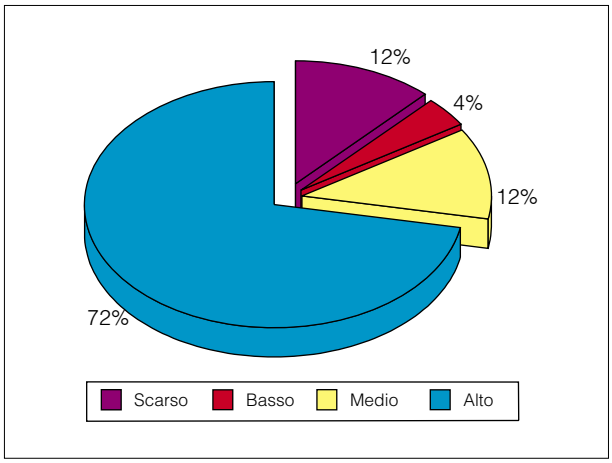


Figura 4: "Risultati per quesito relativi al KPI2"

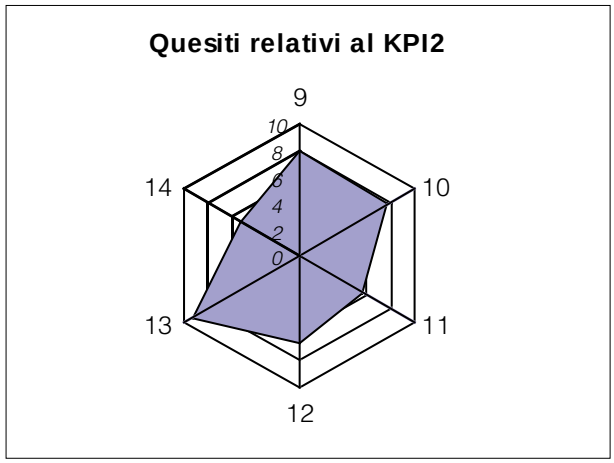


Tabella 2: "Quesiti e risultati relativi al KPI2"

ID	QUESITI	RISPOSTE	PUNT.	# RISP	% SUL TOTALE
9	Esistono predisposizioni fisiche per limitare e perimetrare l'accesso alle risorse elaborative e alla rete interna?	N.R. SI NO	*0* *10* *0*	3 39 7	6,1% 79,6% 14,3%
10	Esiste un sistema di controllo dell'accesso fisico ai locali dove si trovano gli elaboratori e gli apparati di rete?	N.R. SI NO	*0* *10* *0*	3 44 2	6,1% 89,8% 4,1%
11	Sono presenti sottoreti wireless (Wi-Fi) ?	N.R. SI NO	*0* *0* *6*	4 18 27	8,2% 36,7% 55,1%
11a	Se si utilizzano reti Wi-Fi quali sistemi di protezione utilizzano ?	Sistema di protezione WEP Sistema di protezione WPA Nessun sistema di protezione	*4* *10* *0*	11 7 0	61,1%[5] 38,9%[5] 0,0%[5]

[5] Le percentuali relative al quesito 11a sono state calcolate sulla base delle 18 Amministrazioni che hanno affermato di utilizzare reti senza filo Wi-Fi

***Segue:* Tabella 2: "Quesiti e risultati relativi al KPI2"**

ID	Quesiti	Risposte	Punt.	# risp	% sul totale
12	Sono consentiti gli accessi alla rete interna da remoto ?	N.R. SI NO	*0* *0* *6*	4 29 16	8,2% 59,2% 32,7%
12a	Nel caso sia consentito l'accesso alla rete interna da remoto la modalità di connessione utilizza VPN ?	N.R. SI - Accesso remoto mediante VPN NO - Accesso remoto senza VPN	*0* *10* *0*	4 23 2	13,8%[6] 79,3%[6] 6,9%[6]
13	Viene utilizzato un Firewall per la protezione delle connessioni alla rete pubblica?	N.R. SI NO	*0* *10* *0*	1 46 2	 93,9% 7,1%
14	Viene utilizzato un IDS/IPS per la protezione delle connessioni alla rete pubblica?	N.R. SI NO	*0* *10* *0*	1 25 13	 51,0% 7,1%

4.3 KPI3: Sicurezza dei servizi

I risultati raccolti dall'indicatore KPI3 mostrano una sostanziale disomogeneità dei dati raccolti sia tra i diversi quesiti della sezione sia tra le diverse Amministrazioni che hanno partecipato. Infatti la varianza all'interno del campione ha raggiunto il valori sensibilmente maggiori, vicino al doppio, rispetto agli altri 3 indicatori.

Il risultato complessivo ha raggiunto il valore medio di 5,47 molto vicino alla soglia limite inferiore per l'accettabilità.

Analizzando i singoli quesiti, i peggiori risultati sono stati ottenuti sul tema Continuità Operativa (quesiti 15, 16 e 17), evidentemente non ancora avvertito come un fattore cruciale per la robustezza dell'intero impianto e per la qualità dei servizi offerti.

I risultati sono stati altrettanto scadenti per quanto attiene alla capacità delle Amministrazioni di rilevare intrusioni o attacchi, attività certamente inevitabile per qualsiasi sistema connesso ad internet per prendere le necessarie contromisure ed evitare accessi non autorizzati (quesito 23).

Rispetto invece alla distribuzione dell'indicatore KPI3 tra le varie Amministrazioni occorre notare che ben 15 tra queste, pari al 36% del campione, hanno ottenuto un punteggio inferiore a 4,00. Un numero così rilevante è sicuramente indicativo della esigenza di avviare una serie di iniziative volte ad aumentare la sensibilità delle Amministrazioni su tutti gli obiettivi raccolti in di questa sezione del questionario e ad individuare misure opportune per aumentare la robustezza e la sicurezza dei servizi erogati.

La Tabella 3: "Quesiti e risultati relativi al KPI3" riporta i risultati relativi ai quesiti dell'indicatore KPI3.

[6] Le percentuali relative al quesito 12.a sono state calcolate sulla base del totale di 29 Amministrazioni che hanno affermato di consentire accessi da remoto alla propria rete interna.

Figura 5: "Classificazione dei risultati complessivi relativo al KPI3"

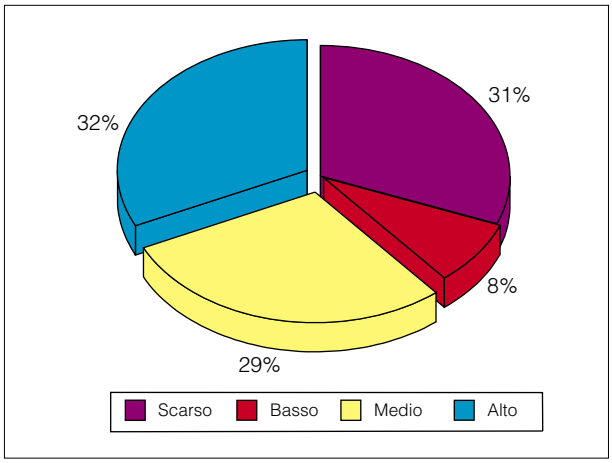


Figura 6: "Risultati per quesito relativi al KPI3"

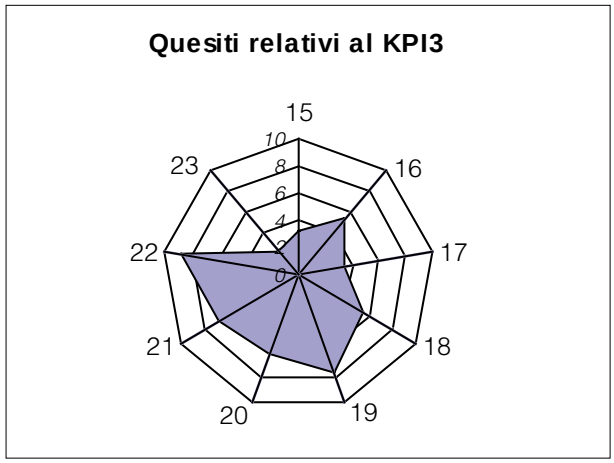


Tabella 3: "Quesiti e risultati relativi al KPI3"

ID	QUESITI	RISPOSTE	PUNT.	# RISP	% SUL TOTALE
15	Esiste un piano formalizzato per la continuità operativa ?	N.R. SI NO	*0* *10* *0*	4 16 29	8,2% 32,7% 59,2%
16	Esistono procedure operative da attivare in caso di indisponibilità parziale dei servizi applicativi ?	N.R. SI - Senza spec. della copertura SI - Solo per le appl. più importanti NO	*0* *10* *7* *0*	4 8 26 11	8,2% 16,3% 53,1% 22,4%
17	E' stato definito in modo formale il piano di disaster recovery ?	N.R. SI - Senza spec. della copertura SI - Solo per le appl. più importanti NO	*0* *10* *7* *0*	4 7 14 24	8,2% 14,3% 28,6% 49,0%
18	Vengono adottate soluzioni per limitare gli attacchi che sfruttano la vulnerabilità delle applicazioni?	N.R. SI NO	*0* *10* *0*	7 27 15	14,3% 55,1% 30,6%
19	Se esiste un server di posta elettronico interno, esiste un filtro antivirus sul server di posta locale?	N.R. SI NO	*0* *10* *0*	10 38 1	20,4% 77,6% 2,0%
20	Se esiste un server di posta elettronico interno, esiste un filtro anti-spam sul server locale?	N.R. SI NO	*0* *10* *0*	10 30 9	20,4% 61,2% 18,4%
21	Se esiste un web server, viene utilizzato il protocollo HTTPS per proteggere i contenuti sensibili?	N.R. SI NO	*0* *10* *0*	7 33 9	14,3% 67,3% 18,4%

***Segue:* Tabella 3: "Quesiti e risultati relativi al KPI3"**

ID	Quesiti	Risposte	Punt.	# risp	% sul totale
22	Esiste un sistema di protezione antivirus centralizzato ?	N.R. SI NO	*0* *10* *0*	3 43 3	6,1% 87,8% 6,1%
23	Sono state rilevate intrusioni riuscite negli ultimi 24 mesi ?	N.R. SI NO	*0* *0* *10*	6 13 30	12,2% 26,5% 61,2%
23a	Se sono state rilevate intrusioni riuscite, quante ?	Rilevate < 10 Rilevate > 10	*4* *2*	12 1	92,3%[7] 7,7%[7]
23b	Se sono state rilevate intrusioni riuscite di che tipo sono state ?	Se rilevate, tipo Denial of Service Se rilevate utilizzo di risorse prot. Se rilevate accesso a dati riservati Se rilevate altro tipo	*4* *2* *0* *1*	7 2 0 8	53,8%[7] 15,4%[7] 0,0%[7] 61,5%[7]

4.4 KPI4: Sicurezza dell'organizzazione

Anche il KPI4 ha prodotto risultati simili al KPI3 con un valore medio di 5,41. In questo caso però in maniera molto più uniforme tra le varie Amministrazioni è emersa un serie di risultati i che testimoniano altrettante criticità. Tipicamente, anche quest'anno, si è riscontrata una propensione molto maggiore ad attuare piani per la sicurezza fisica e logica rispetto a dedicare energie per adeguare la propria organizzazione. E' evidente infatti che una cattiva organizzazione interna può vanificare tutti gli sforzi spesi sul piano degli strumenti adottati, rappresentando inoltre una diseconomia.

Dall'analisi dei singoli quesiti, i peggiori risultati sono stati rilevati per il quesito 33 in base al quale più della metà delle Amministrazioni (25) non hanno una voce in bilancio dedicata alla Sicurezza e, in maniera ancora più preoccupante per il quesito 36 in base al quali più del 61% del campione (31 Amministrazioni) non ha mai approntato o previsto un piano di formazione volto a stimolare negli utenti dei sistemi informativi una maggiore sensibilità al tema Sicurezza ed una maggiore capacità di affrontare consapevolmente condizioni critiche.

Anche il tema dell'analisi del rischio informatico è risultato piuttosto scoperto, a dispetto della grande rilevanza che questo tema ha avuto negli ultimi anni soprattutto nel privato. Ben 10 Amministrazioni affermano che non hanno mai effettuato un'analisi dei rischi connessi alla Sicurezza informatica.

Infine con un valore medio inferiore al 6,00 si è rilevato che ancora oggi il D.M. del 16 Gennaio 2002 resta in parte disatteso con 4 Amministrazioni che non hanno risposto, 11 che afferma-

[7] Le percentuali relative ai quesiti 23a e 23b sono state calcolate sulla base del numero totale di Amministrazioni (13) che hanno affermato di aver rilevato un tentativo di intrusione. Ovviamente nel caso delle risposte relative al quesito 23b sono state consentite risposte multiple, cioè non possono essere sommate perché è realistico che vi siano Amministrazioni che hanno subito diverse tipologie di attacchi.

no di non aver ricoperto alcun ruolo previsto dal decreto ed ancora ben 21 che ne hanno adeguato solo parzialmente la propria organizzazione.

La Tabella 4: "Quesiti e risultati relativi al KPI4" riporta i risultati rilevati per l'indicatore KPI4.

Figura 7: "Classificazione dei risultati complessivi relativo al KPI4"

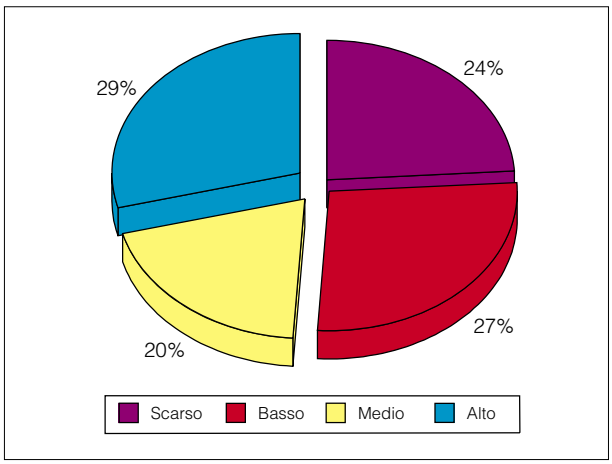


Figura 8: "Risultati per quesito relativi al KPI4"

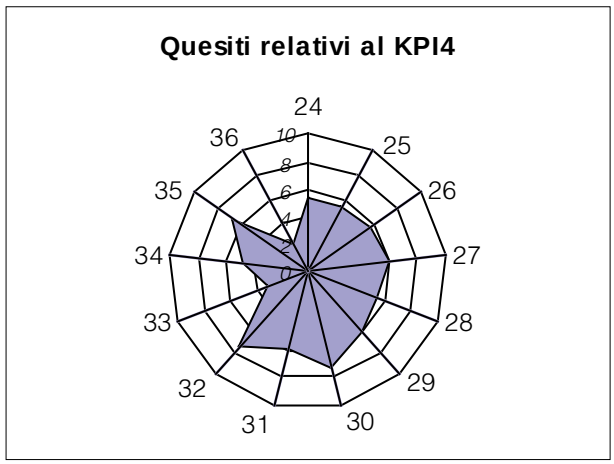


Tabella 4: "Quesiti e risultati relativi al KPI4"

ID	QUESITI	RISPOSTE	PUNT.	# RISP	% SUL TOTALE
24	E' stato formalmente definito ed approvato il piano della sicurezza ICT ?	N.R. SI NO	*0* *10* *0*	2 26 21	4,1% 53,1% 42,9%
25	Esiste la definizione formale di una policy di sicurezza ICT ?	N.R. SI NO	*0* *10* *0*	3 44 2	6,1% 89,8% 4,1%
26	Sono stati attribuiti i ruoli e le responsabilità secondo quanto previsto dal DM 16-1-2002?	N.R. SI - Tutti Si - Alcuni NO	*0* *10* *7* *0*	4 12 22 11	8,2% 24,5% 44,9% 22,4%
27	Esiste ed è attivo un centro di gestione ed amministrazione della sicurezza ICT ?	N.R. SI NO	*0* *10* *0*	1 29 19	2,0% 59,2% 38,8%
28	Esiste ed è attivo un gruppo di gestione degli incidenti?	N.R. SI NO	*0* *10* *0*	1 26 22	2,0% 53,1% 44,9%
29	Esiste la figura di "Responsabile protezione dati personali" ?	N.R. SI NO	*0* *10* *0*	3 29 17	6,1% 59,2% 34,7%

***Segue:* Tabella 4: "Quesiti e risultati relativi al KPI4"**

ID	Quesiti	Risposte	Punt.	# risp	% sul totale
30	Esistono una o più procedure di gestione dei log?	N.R.	*0*	3	6,1%
		SI	*10*	35	71,4%
		NO	*0*	11	22,4%
31	Esiste un responsabile per la gestione ed attuazione delle policy di backup/restore ?	N.R.	*0*	2	4,1%
		SI	*5*	30	61,2%
		NO	*0*	17	34,7%
31a	La procedura di backup è documentata ?	N.R.	*0*	0	0,0%[8]
		SI	*5*	26	86,7%[8]
		NO	*0*	4	13,3%[8]
32	Che tipo di personale viene impiegato per la gestione e l'amministrazione della sicurezza del sistema informativo ?	N.R.	*0*	2	4,1%
		Solo personale interno	*10*	14	28,6%
		Personale misto	*6*	27	55,1%
		Outsourcing per la gestione della sicurezza	*4*	6	12,2%
32a	Se esiste un contratto di outsourcing, il contratto prevede che l'amministrazione appaltante effettui modifiche su come è gestita la sicurezza ?	SI - Sono previste modifiche al contratto	*4*	4	66,7%[9]
		NO -.Il contratto non prevede modifiche	*0*	2	33,3%[9]
32b	Se esiste un contratto di outsourcing ed è previsto l'audit della gestione della sicurezza dell'outsourcing, l'audit viene effettuato con regolarità ?	Si - Audit effettuato con regolarità	*2*	2	33,3%[9]
		No - Audit NON effettuato regolarmente	*0*	2	33,3%[9]
33	Esiste una previsione di spesa dedicata specificatamente alla sicurezza ?	N.R.	*0*	2	4,1%
		SI	*4*	22	44,9%
		NO	*0*	25	51,0%
33a	Se esiste una voce dedicata alla sicurezza quale è la percentuale sul budget IT complessivo ?	N.R.	*0*	3	13,6%[10]
		Inferiore al 5%	*2*	9	40,9%[10]
		Compreso tra il 5% ed il 10%	*4*	10	45,5%[10]
		Maggiore di 10%	*6*	0	0,0%[10]
34	E' stata effettuata un'analisi dei rischi connessi alla sicurezza ICT ?	N.R.	*0*	3	6,1%
		SI	*5*	18	36,7%
		NO	*0*	10	20,4%
		SI con copertura analisi risichi totale	*10*	2	4,1%
		SI con copertura analisi risichi parziale	*8*	11	22,4%
		SI con copertura analisi rischi minima	*6*	5	10,2%

[8] Le percentuali relative al quesito 31a sono state calcolate sul totale di 30 Amministrazioni che hanno risposto "SI" al quesito 31 affermando di avere un responsabile dell'attuazione delle politiche di Backup/Restore

[9] Le percentuali relative ai quesiti 32a e 32b sono state calcolate sulla base del totale di 6 Amministrazioni che hanno affermato di ricorrere a contratti di Outsourcing per la gestione della sicurezza.

[10] Le percentuali relative al quesito 33a sono state calcolate sulla base del totale di 22 Amministrazioni che hanno affermato di avere una previsione di spesa relativa alla sicurezza

***Segue:* Tabella 4: "Quesiti e risultati relativi al KPI4"**

ID	QUESITI	RISPOSTE	PUNT.	# RISP	% SUL TOTALE
35	Sono state prese iniziative per la sensibilizzazione alla sicurezza informatica rivolte a tutto il personale dell'amministrazione?	N.R. SI NO	*0* *10* *0*	2 33 14	4,1% 67,3% 28,6%
36	E' stato già redatto ed approvato un piano di formazione e sensibilizzazione per la sicurezza ICT ?	N.R. SI NO	*0* *5* *0*	4 14 31	8,2% 28,6% 63,3%
36a	Se è stato già redatto un piano di formazione, quale percentuale di addetti al Sistema Informativo ne ha usufruito ?	Inferiore al 10% Compreso tra il 10% ed il 30% Compreso tra il 30% ed il 50% Maggiore del 50%	*1* *2* *4* *5*	2 1 6 2	14,3%[11] 7,1% 42,9% 14,3%

[11] Le percentuali relative al quesito 36a sono state calcolate sulla base del totale di 14 Amministrazioni che hanno affermato di aver già redatto ed approvato un piano di formazione e sensibilizzazione per la sicurezza ICT

5. Considerazioni conclusive

5.1 Risultati complessivi

Sulla scorta dei risultati ottenuti mediando sull'intero campione analizzato, per i primi due KPI (Sicurezza logica e Sicurezza dell'Infrastruttura) i risultati sono complessivamente più che soddisfacenti. Su queste due aree si è potuto osservare tra l'altro un netto miglioramento rispetto al passato.

Sarebbe comunque necessario ricorrere, in maniera molto puntuale, ad indagini di secondo livello per migliorare ulteriormente il risultato complessivo intervenendo specificamente sulle cause che hanno portato a risultati critici per alcuni quesiti dei due KPI.

Al contrario sugli indicatori KPI3 e KPI4 è evidente che è necessario un intervento specifico ed urgente per raggiungere quella soglia minima di accettabilità. Sulla parte dei servizi, sempre in generale, è certamente possibile individuare strategie comuni che possano consentire la centralizzazione dei servizi critici, realizzando ad esempio, strumenti comuni per l'analisi dei dati raccolti da strumenti per la rilevazione delle intrusioni.

Analogamente si potrebbero concentrare sforzi ed esigenze per realizzare modelli di piani per la Continuità Operativa fruibili dalle Amministrazioni, così come predisporre centri comuni di backup che consentirebbero grosse economie di scale riducendo tra l'altro tutti i rischi di progetto. A tal proposito il DPCM del 31/05/2005 prevede che il CNIPA tra i suoi ruoli istituzionali offra un servizio di questo tipo, mettendo a fattor comune esperienze e risultati per la realizzazione di funzioni così critiche ed importanti.

Analogamente sul piano dell'organizzazione interna è importante notare che ancora rimangono disattese le norme emanate da tempo e che in generale la cultura della sicurezza è rimasta appannaggio degli addetti ai lavori, ma i piani di formazione e sensibilizzazione sul tema sono ancora poco diffusi, mentre è auspicio di tutti che queste iniziative possano avere la massima diffusione raggiungendo tutti gli utenti anche in periferie remote.

Va comunque sottolineato, a conferma della metodologia utilizzata, che tutte le Amministrazioni che hanno ottenuto un buon punteggio ad uno qualsiasi del KPI, si sono posizionate altrettanto bene in tutti gli altri KPI. Questa nota prova che laddove un'Amministrazione ha sviluppato una particolare attenzione rispetto al tema Sicurezza, questa viene perseguita a 360 gradi, confermando i forti fattori di correlazione che vi sono tra le varie aree individuate.

5.2 Tendenze rispetto alle rilevazioni precedenti

I risultati riportati nella Tabella 5: "Confronto dei risultati complessivi per i 4 KPI negli ultimi 2 anni" confermano quanto accennato nel paragrafo precedente e cioè la tendenza sostanzialmente positiva intrapresa negli ultimi anni dalla Pubblica Amministrazione Centrale rispetto al tema Sicurezza Informatica. I primi due indicatori KPI1 e KPI2 hanno ottenuto un miglioramento sostanziale, passando da un risultato appena accettabile ad uno ottimale, superiore ad ogni aspettativa.

Analizzando i dati e considerando le tendenze mostrate da ogni singola amministrazione, si può notare come siano state proprio le Amministrazioni, che nell'anno precedente avevano avuto i risultati più insoddisfacenti, a produrre il maggior margine di miglioramento.

Ciò conferma da un lato le indicazioni ottenute dalle rilevazioni precedenti, dall'altro la forte volontà delle Amministrazioni, se opportunamente stimolate, ad affrontare il problema sicurezza con tutte le energie necessarie.

Solo per l'indicatore KPI3 apparentemente sembra vi sia stato un peggioramento, ma questo dato è il risultato della completa ristrutturazione e riformulazione dei quesiti che compongono l'indicatore rispetto all'anno precedente. Infatti il precedente questionario contava solo 4 quesiti.

L'ultimo questionario invece proponeva 9 quesiti, tutti sostanzialmente aggiornati rispetto alla precedente edizione per meglio catturare le specificità di ogni Amministrazione rispetto alla Sicurezza, qui intesa come robustezza, affidabilità o resistenza agli attacchi, dei servizi erogati.

Anche l'indicatore KPI4 ha mostrato una tendenza al miglioramento, attestandosi attorno a valori medi vicini alla sufficienza. Anche in questo caso è stato utile osservare quali quesiti hanno prodotto tale miglioramento, rilevando come ancora una volta, in media rispetto all'intero campione, proprio i temi organizzazione e formazione per la sicurezza siano quelli che hanno esibito il più basso fattore di crescita. E' evidente come in questo ambito occorra concentrare ulteriori sforzi.

Va comunque rilevato che l'indicatore è stato rimodulato, riducendo drasticamente il numero di quesiti da 17 a 13 e questo rende poco significativi ogni tentativo di confronto diretto dei risultati.

Tabella 5: "Confronto dei risultati complessivi per i 4 KPI negli ultimi 2 anni"

	2005	2006	
KPI1	4,90	7,33	2,43
KPI2	5,90	7,08	1,16
KPI3	6,80	5,47	-1,37
KPI4	4,65	5,41	0,75

5.3 Iniziative delle Amministrazioni

I dati derivanti dalla rilevazione non sono consistiti solo dalle risposte fornite al questionario ma anche da segnalazioni volontarie di progetti che ogni singola Amministrazione ha eventualmente fornito sul tema Sicurezza. Tali iniziative risultano estremamente coerenti con il modello e le indicazioni rilevate nelle precedenti edizioni. Pertanto questo ultimo paragrafo è interamente dedicato alla analisi delle iniziative più diffuse in corso presso le Amministrazioni. E' stato rilevato infatti un consistente numero di progetti, alcuni in esecuzione altri ancora da avviare, di estremo impatto sul piano della sicurezza i cui risultati potrebbero manifestarsi già nel corso dell'anno corrente.

Come primo tema, ben 8 Amministrazioni hanno dichiarato la loro intenzione di dotarsi di un sistema per il disaster recovery, ed alcune di queste hanno già individuato finanziamenti e strategie per la realizzazione del progetto.

Analogamente sul tema Single Sign On, almeno 5 Amministrazioni, anche di dimensioni notevolmente differenti sul numero di utenti, hanno descritto progetti incorso per la centralizzazione degli account utente e per l'adozione di sistemi SSO.

Molte Amministrazioni hanno realizzato o intendono farlo nel breve, processi di "Vulnerability Assessment".

Infine sempre dalle stesse note è emerso il dato concreto che molto Amministrazioni hanno già emesso o intendono dotarsi in un documento del tipo: "Politiche di Sicurezza dell'Infrastruttura Telematica" attraverso il quale diffondere norme interne relative alla Sicurezza dei sistemi informativi. Su questo punto si intuisce la necessità di individuare un blocco di norme comuni a tutte le Amministrazioni scritte in base ad un modello condiviso ed indipendente dalle dimensioni e dalle funzioni dell'Ente. Questo potrebbe da un lato ridurre gli sforzi mettendo a fattor comune le esperienze interne già disponibili dall'altro garantirebbe una possibilità concreta di successo ad un processo così delicato.

Finito di stampare nel mese di settembre 2007
presso la Stilgrafica S.r.l. - Roma

CNIPA
Centro Nazionale per l'Informatica
nella Pubblica Amministrazione

via Isonzo, 21/b – 00198 Roma
tel. 06 85264.1
www.cnipa.gov.it