3.3.3.1 Riuso del software e dei servizi e la diffusione del software open source

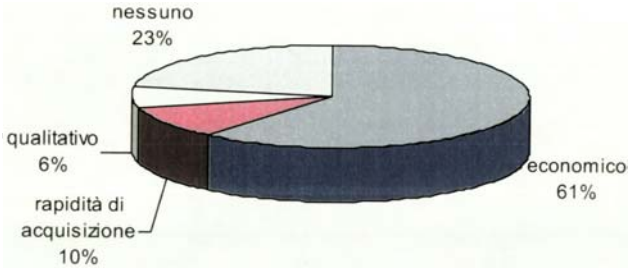
Il riuso del software e dei servizi

Il ricorso al riuso, quale strumento di contenimento della spesa pubblica per l'ICT, è previsto anche dalla normativa che lo ha inteso come uno degli strumenti disponibili per la razionalizzazione ed il recupero di efficienza nei processi di produzione del software. Il ricorso a tale pratica rimane ancora limitato a casi sporadici.

Il ricorso all'open source

Nel 2008 hanno dichiarato il ricorso a soluzioni open source 38 amministrazioni (il 79% del totale). Il dato è stabile rispetto al 2007 e in leggera crescita rispetto al 2006 (circa il 72%). Inoltre le amministrazioni che si sono rivolte a fornitori esterni per servizi di open source sono 21 (lo scorso anno erano 27). Tra le amministrazioni che gestiscono con proprio personale il software open source rientrano gli enti di ricerca (ISTAT e CNR) che stanno attivando propri gruppi di sviluppo specializzati in questi ambienti. I vantaggi che le amministrazioni dichiarano di apprezzare nell'uso dell'open source sono descritti nel grafico seguente.

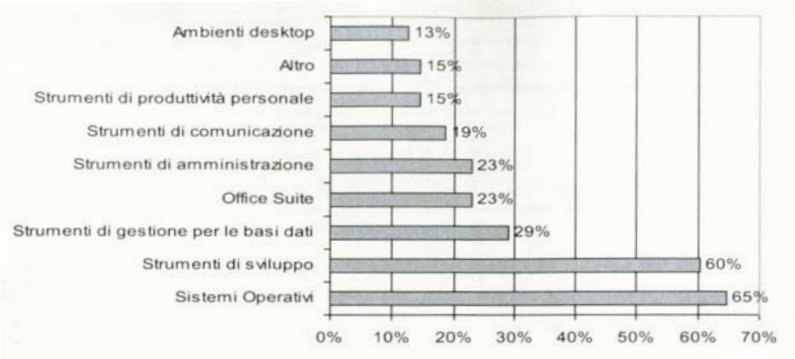
Figura 2 : Vantaggi riscontati nell'utilizzo di soluzioni open source, anno 2008



Rispetto allo scorso anno è pressoché stabile sia la percezione del risparmio economico che l' open source porta con sé sia la valutazione positiva della rapidità di acquisizione, che si confermano come i principali vantaggi per la PA.

Soluzioni open source sono state adottate prevalentemente per i sistemi operativi, per il web, per lo sviluppo. E' evidente, quindi, che si continua a fare uso dell'OS soprattutto sul lato server, mentre l'uso sui desktop sembra dedicato ad una utenza presumibilmente più specializzata (sviluppo).

Figura 3 : Ambito di utilizzo di soluzioni open source, anno 2008



3.3.4 Sicurezza ICT

Nell'ambito della relazione sullo stato di informatizzazione della PA che il CNIPA redige annualmente è stata condotta anche per l'anno 2008 un'indagine specificamente dedicata allo stato della sicurezza ICT della Pubblica Amministrazione Centrale.

Questa iniziativa, giunta già alla quarta edizione, il CNIPA intende da un lato valutare la presenza di particolari criticità sulle quali occorre intervenire con urgenza proponendo i correttivi più appropriati, dall'altro, una volta misurata la sensibilità degli utenti rispetto al tema specifico, proporre comuni modelli evolutivi per guidare l'intera PA verso una visione unitaria della Sicurezza ottenibile solo attraverso sforzi congiunti e condivisione degli obiettivi. Gli obiettivi ovviamente vengono aggiornati costantemente riflettendo le evoluzioni della tecnologia man mano che vanno delineandosi all'orizzonte nel panorama dell'ICT.

Come avviene ormai da anni nei principali stati della Comunità Europea, il CNIPA ha definito un modello di sicurezza costituito da una serie di indicatori oggettivamente rilevabili. Attraverso il questionario e le iniziative di carattere seminariale che si sviluppano attorno a questo, si intende verificare l'effettiva aderenza delle strutture informatiche della PAC a tale modello monitorando i processi di informatizzazione delle amministrazioni coinvolte. In questo modo sarà sempre possibile garantire l'attuazione di strategie comuni, preventivamente testate e messe a punto, anticipando ogni criticità prima ancora che diventi una minaccia per l'intera comunità. Così facendo il tema innovazione tecnologica dei processi interni alla PA potrà essere affrontato serenamente dalle amministrazioni senza introdurre debolezze o rischi imprevisti. E' facile intuire, infatti, che 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 della Sicurezza ICT.

Oltre all'aspetto sicurezza, occorre tenere conto che attraverso un organismo centrale è sempre possibile produrre rilevanti economie di scala, come già è accaduto nel caso del progetto SPC, che possono da sole giustificare i costi dell'intera struttura.

3.3.4.1 Metodologia di analisi

In questo scenario si innesta la metodologia di analisi che il CNIPA ha sviluppato e consolidato anno per anno per fotografare la situazione corrente e per fornire alle Amministrazioni una serie di obiettivi a cui tendere nell'anno successivo. Caratteristica fondamentale della metodologia adottata è stata quella di basarsi solo su dati numerici, oggettivamente riscontrabili nelle diverse realtà, pertanto anche quest'anno l'analisi è stata effettuata attraverso un questionario compilato dai rappresentanti di ogni struttura informatica della Pubblica Amministrazione Centrale. Il questionario è organizzato in 4 sezioni ed ognuna rappresenta una prospettiva specifica del tema Sicurezza ICT espressa da un valore detto Key Performance Indicator (KPI). Ogni KPI è ottenuto attraverso l'attribuzione di punteggi numerici ad ognuno dei quesiti che lo caratterizzano.

Se nelle precedenti edizioni è stato necessario aggiornare l'insieme dei quesiti per riflettere le evoluzioni correnti della tecnologia, quest'anno il questionario è rimasto

completamente inalterato, offrendo l'opportunità considerevole di confrontare direttamente i risultati rilevati con quelli conseguiti dalle Amministrazioni nel corso della relazione 2007 e verificando quindi le ricadute dei progetti realizzati e le linee di tendenza dell'intero campione statistico.

La metodologia di analisi dei dati procede in maniera top-down analizzando dapprima il dato grezzo rappresentato dai valori dei 4 KPI ottenuti come valore medio tra tutte le Amministrazioni che hanno partecipato alla rilevazione. Successivamente il dato viene scomposto in 3 sotto insiemi ottenuti raggruppando tutte le Amministrazioni in funzione delle dimensioni (numero di dipendenti censiti). Infine è possibile valutare in ogni singola Amministrazione il valore dei 4 KPI ed eventualmente, in presenza di particolari criticità, risalire alle effettive motivazioni valutando le risposte ai singoli quesiti del questionario.

In ognuna delle fasi descritte sono state fissate 3 livelli soglia per definire i criteri di ottimalità, accettabilità o criticità elevata. Valori inferiori alla soglia critica richiedono evidentemente interventi urgenti.

La suddivisione in funzione delle dimensioni delle singole Amministrazioni, introdotta per la prima volta nella rilevazione 2007, ha fornito indicazioni molto più precise e puntuali consentendo di distinguere all'interno del campione fortemente disomogeneo, problematiche differenti, frutto di condizioni al contorno completamente diverse. I tre sottoinsiemi: Piccole, fino a 1.000 dipendenti, Medie tra 1000 e 10.000 dipendenti, Grandi oltre i 10.000 dipendenti sono risultati molto più omogenei ed hanno consentito quindi di analizzare ancor meglio i valori medi proponendo soluzioni mirate e specifiche per ogni insieme.

A differenza di quanto è accaduto nella rilevazione 2007, le grandi Amministrazioni hanno ottenuto risultati solo leggermente migliori delle altre di dimensioni più piccole, mostrando come la sensibilità verso il tema Sicurezza si va diffondendo indipendentemente dalle risorse disponibili. D'altra parte analizzando i trend dei 4 KPI la maggiore crescita è stata ottenuta proprio all'intero della classe Amministrazioni di dimensioni "Medie". In realtà un fenomeno di regressione era atteso proprio dalle Amministrazioni di maggiori dimensioni in funzione della situazione congiunturale che ha visto ridurre considerevolmente i bilanci di tali Amministrazioni.

Rispetto al miglioramento dei risultati occorre infine considerare che durante il 2008 si sono misurati anche i vantaggi e le ricadute della migrazione delle Amministrazioni al Sistema Pubblico di Connettività (SPC) che, condividendo il "modello comune per la sicurezza" del CNIPA, nei sui listini ha negoziato anche servizi specifici di consulenza per la Sicurezza, oltre che hardware standard per la sicurezza delle connessioni geografiche e specifici servizi di monitoraggio ed assistenza da parte dei fornitori di connettività.

Nella redazione del questionario, dapprima sono stati definiti tutti gli elementi ritenuti essenziali in termini di sicurezza per la PA, popolando così l'insieme degli oggetti (obiettivi) di controllo sui quali raccogliere i dati statistici. Tale lavoro è stato effettuato tenendo come riferimento le principali norme internazionali come la ISO 27001 e declinando opportunamente il risultato tenendo conto delle specifiche realtà della Pubblica Amministrazione italiana.

Una volta raccolta la lista degli oggetti di controllo questi sono stati raggruppati secondo l'area di pertinenza individuando così i 4 KPI seguenti:

- KPI1 sicurezza logica; valuta la sensibilità dell'Amministrazione rispetto alle scelte effettuate in termini di prodotti software e soluzioni per l'organizzazione della sicurezza logica del CED. I principali temi trattati sono: Autenticazione e controllo accessi, Certificazioni di prodotti e servizi, aggiornamento software delle PdL, sicurezza delle postazioni mobili, backup.
- KPI2 sicurezza dell'infrastruttura; valuta gli aspetti fisici della sicurezza dell'impianto ed in particolare quelli legati alla infrastruttura di rete, raccogliendo informazioni rispetto ai temi seguenti: sicurezza perimetrale e controllo accessi ai locali tecnici, apparati attivi per la sicurezza degli accessi quali firewall, sistemi per la rilevazione delle intrusioni, sicurezza delle reti wireless, modalità di accesso da remoto e VPN.
- KPI3 sicurezza dei servizi; misura sensibilità gli sforzi spesi dalle amministrazioni per incrementare l'affidabilità e la robustezza dei propri servizi ICT. In particolare al centro del KPI vi sono i temi della continuità operativa e del disaster recovery. D'altra parte vi sono anche temi più consolidati quali antivirus o antispam per la posta elettronica, protezione dei contenuti e web filtering, capacità di rilevare le intrusioni, e/o prevenirle in funzione del tipo di attacchi eventualmente subiti.
- KPI4 sicurezza dell'organizzazione; rileva lo sforzo espresso dalle Amministrazioni nell'allocazione di proprie risorse umane per ricoprire i ruoli previsti nell'ambito della sicurezza, gestire adeguatamente gli incidenti, gestire adeguatamente le eventuali risorse esterne gestione dedicate alla sicurezza ed avviare iniziative per garantire ulteriori sviluppi su questi temi.

Successivamente ogni oggetto di controllo è stato tradotto in uno o più quesiti attraverso i quali raccogliere le indicazioni sullo stato dell'arte di ogni singola amministrazione. Ogni quesito ammette un insieme chiuso e predefinito di risposte (documenti descrittivi sono stati raccolti a parte). La risposta attesa è stata sempre valutata con il punteggio massimo di 10, mentre le altre ottengono un punteggio decrescente fino a 0 che corrisponde anche al punteggio assegnato alla risposta non fornita. In questo modo, ogni KPI è stato calcolato come il valore medio dei punteggi assegnati alle risposte fornite all'insieme di quesiti del questionario associato al KPI. In questo modo ogni indicatore raccoglie un insieme di elementi di valutazione in grado di stabilire in maniera sufficientemente oggettiva una metrica per misurare il livello di attenzione di ciascuna Amministrazione intervistata sul tema Sicurezza ICT. I 4 KPI infatti ricoprono il tema Sicurezza ICT in maniera ampia analizzandolo sotto 4 prospettive diverse e forniscono così indicazioni più precise sulle eventuali contromisure da intraprendere in caso di risultati negativi.

Contemporaneamente sono state fissate 3 soglie (alto, medio e basso) per raccogliere tali risultati in 4 fasce, evidenziando quelle che hanno raggiunto un valore al di sotto della soglia di criticità.A questo punto, come accennato in precedenza questi risultati sono stati raccolti in 3 gruppi in funzione della dimensione di ciascuna Amministrazione.

I valori dei KPI rilevati di fatto rappresentano diverse viste sul "modello unico per la sicurezza" che il CNIPA ha prodotto negli ultimi anni. Tale modello si è arricchito ed irrobustito nel corso degli anni risultando sempre più aderente alla realtà cella PAC che intende fotografare, per cui anche in termini statistici, eventuali dissonanze sono subito evidenti e, negli anni precedenti, si è potuto constatare che queste esprimono

effettivamente condizioni di esercizio particolari tali da richiedere indagini di secondo livello per disporre dei necessari approfondimenti.

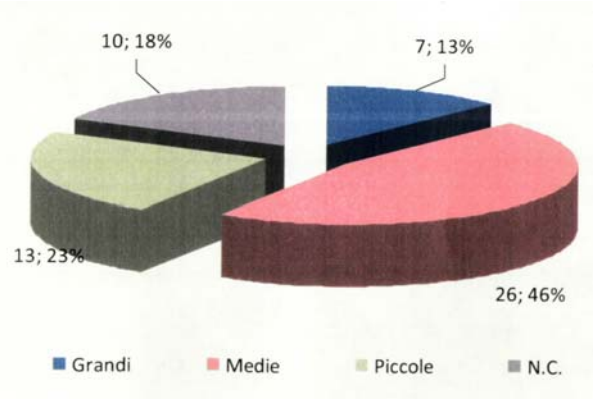
Ovviamente ciò richiede uno sforzo costante per tenere costantemente aggiornato il modello in modo da riflettere le esperienze dirette del CNIPA sul tema Sicurezza ICT e quanto avviene nei vari organismi internazionali opportunamente calati alla realtà della Pubblica Amministrazione Centrale Italiana.

3.3.4.2 Risultati

In questo paragrafo si presenta una ragionevole sintesi dei dati rilevati, rimandando il lettore interessato alla relazione annuale sullo stato delle sicurezza ICT delle pubbliche amministrazioni per l'anno 2008, ancora in fase di elaborazione, che riporterà i dati di dettaglio (risposte ai singoli quesiti) e le relative conclusioni.

Il questionario è stato compilato da 56 unità organizzative centrali complesse (amministrazioni e/o dipartimenti), ma ben 10 di queste sono stati scartate perché incompleti o mancanti di parti rilevanti per ragioni di riservatezza sui dati richiesti. Le rimanenti sono state raccolte in 3 classi in funzione delle dimensioni espresse attraverso il numero di dipendenti. Il risultato è riportato nel diagramma a torta nella figura seguente. 7 "Grandi" con più di 10.000 dipendenti, 26 "Medie" tra 1.000 e 10.000 dipendenti e 13 "Piccole" con meno di 1.000 dipendenti. Ogni classe è evidentemente più omogenea e ciò garantisce al dato statistico una maggiore significatività soprattutto rispetto all'interpretazione dei risultati sulle problematiche comuni da affrontare.

Figura 4: Distribuzione delle amministrazioni in funzione delle dimensioni



I due grafici seguenti riportano quindi i valori dei 4 KPI ottenuti mediando i valori ottenuti da ogni amministrazione all'interno di ciascuna classe. Con lo sfondo azzurro i risultati ottenuti con quest'ultima rilevazione e con lo sfondo verde quelli relativi all'anno precedente.

Figura 5: Risultati dei 4 KPI come valore medio per ciascuna classe nella rilevazione 2008

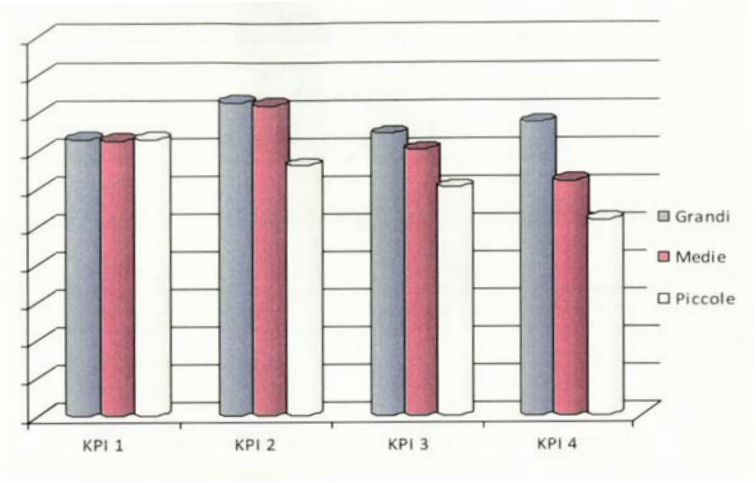
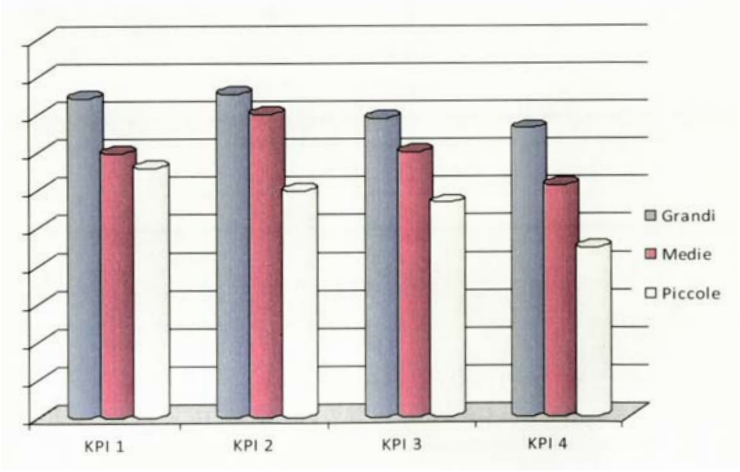


Figura 6: Risultati dei 4 KPI come valore medio per ciascuna classe nella rilevazione precedente 2007



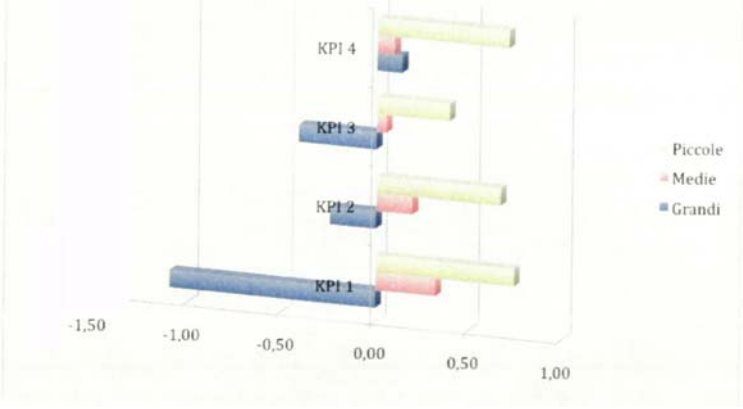
Volendo analizzare quindi le linee di tendenza il risultato indica un buon miglioramento del dato relativo alle due classi di amministrazioni Piccole e Medie mentre le Grandi hanno subito una regressione rispetto al dato dell'anno precedente.

Questo è particolarmente evidente per il KPI1 dove la classe Grandi passa da un valore medio di 8,42 nel 2007 a 7,33 nel 2008. Pur essendo prematura l'interpretazione di questo dato, c'è da osservare che gli effetti della crisi economica si sono avvertiti prima nelle grandi organizzazione, già nel secondo semestre del 2008. A conferma di tale dato si rileva che il KPI1 Sicurezza Logica è più connesso alle dotazione Hardware Software per cui potrebbe aver risentito della riduzione dei budget delle amministrazioni.

Il dato confortante al contrario è il netto miglioramento conseguito dalle altre due classi, Piccole e Medie, soprattutto rispetto al KPI4 dove storicamente si registrava una netto ritardo rispetto a quanto auspicato.

La figura seguente illustra questo dato ed in particolare i miglioramenti ottenuti dalle piccole amministrazioni rispetto ai 4 KPI. Su questo dato sicuramente hanno influito in maniera rilevante i risultati del progetto Sistema Pubblico di Connettività (SPC) e tutte le attività per la sensibilizzazione degli utenti rispetto al tema Sicurezza soprattutto per quanto riguarda l'organizzazione per la sicurezza (KPI4).

Figura 7: Differenze tra i 4 KPI nelle rilevazioni 2007 e 2008



3.3.4.3 Sicurezza logica

Rispetto al KPI1 nelle precedenti rilevazioni sono sempre emersi due dati importanti: a) KPI2 è storicamente l'indicatore che produce i risultati migliori; b) KPI2 risente meno di ogni altro delle differenze in termini di dimensioni tra le varie amministrazioni. Nella rilevazione 2008 il secondo dato è stato pienamente confermato, producendo praticamente valori identici nelle 3 classi, mentre il primo è stato radicalmente disatteso, in funzione del sostanziale arretramento di quasi un 1,2 punti sulla media del campione costituito dalle Grandi amministrazioni. Occorre anche notare che la classe delle Grandi amministrazioni è quella che nella rilevazione 2008 si è ridotta maggiormente passando da 10 a 7 istanze, anche in funzione dei dati scartati perché incompleti.

Analizzando nello specifico il KPI1 si nota subito il netto progresso che la cultura della Sicurezza ha avuto nell'ultimo anno. Infatti sull'intero campione costituito dalle 56 amministrazioni (incluse quindi anche quelle che sono state scartate) è

cresciuto del 4% il numero di quelle che hanno dichiarato di considerare al momento dell'acquisto come rilevanti eventuali certificazioni per la sicurezza delle ditte fornitrici (KPI1.3a). Il dato è maggiormente significativo se si analizzano le risposte fornite al KPI1.3b dove diminuiscono del 7% le amministrazioni che richiedono certificazioni Common Criteria (ISO 15408) ma aumentano del 16% quelle che richiedono la certificazione ISO 27001 (ex BS7799-2), riflettendo la maggiore attualità della seconda rispetto alla prima. Inoltre diminuiscono del 22% le "Altre certificazioni" richieste confermando il carattere di universalità ricoperto dalle prime due. Tutto ciò a riprova del crescente interesse verso il tema certificazioni per la sicurezza, a dispetto dell'ancor debole quadro normativo in materia di certificazioni richieste per le forniture alla PA.

Per quanto riguarda i sistemi di autenticazione, rimangono purtroppo largamente diffusi (87,5%) i sistemi basati su username e password ma sono aumentati del 7% (83,7%) rispetto all'anno precedente i sistemi automatici di controllo proattivo sulla robustezza delle password.

Molto interessante, non solo per il miglioramento mostrato, è il dato relativo al KPI1.6 che vede un aumento del 6% del numero di amministrazioni dotate di un sistema automatico di aggiornamento delle postazioni di lavoro raggiungendo così il 57% dell'intero campione.

Al contrario invece, attraverso il KPI1.7, si è osservato un aumento della diffusione delle postazioni mobili o dei supporti mobili per la memorizzazione dei dati (+ 7,3%), cosa che per altro rispecchia le tendenze del mercato ICT, ma sfortunatamente si rileva che non viene dedicata alcuna attenzione alla sicurezza dei dati trasportati all'esterno della propria organizzazione e per questo più vulnerabili. Coerentemente con i dati di mercato lo stesso KPI1.7 dichiara la diminuzione del 5,2% tra coloro che dichiarano di non utilizzare postazioni mobili.

Contrastante invece il dato sui sistemi per il backup centralizzato (KPI1.8) in quanto diminuisce circa del 5% il numero di amministrazioni che dichiarano di aver implementato un tale sistema (passando dall'87% all'82% che comunque rappresenta una percentuale ragguardevole) ma aumenta significativamente (+9%) la percentuale di coloro che dichiarano di aver formalizzato correttamente una policy per la verifica e la custodia dei supporto che raggiungono ormai l'82% (38 / 46 amministrazioni).

Infine migliora anche il dato relativo alla disponibilità di sistemi per il controllo degli accessi alle risorse elaborative (KPI1.9) passando dal 77% all'82%.

3.3.4.4 Sicurezza dell'infrastruttura

Rispetto alla sicurezza fisica della infrastruttura si conferma la naturale propensione delle amministrazioni, indipendentemente dalle dimensioni, ad investire in termini di dispositivi hardware per la protezione delle proprie dotazioni informatiche.

I primi tre quesiti (KPI2.1, KPI2.2 e KPI2.3) sono rimasti sostanzialmente inalterati rispetto all'anno precedente e testimoniano una buona attenzione delle amministrazioni verso quelle installazioni che possano irrobustire l'intera infrastruttura, come sicurezza perimetrale, controllo accessi alla sala macchine e videosorveglianza. Si conferma quindi il dato che vede installate barriere fisiche quasi nell'80% dei casi (KPI2.1 e KPI2.2) ma meno del 50% (passando dal 42% al 46%) utilizza sistemi di videosorveglianza (KPI2.3).

Sostanzialmente stabile e largamente diffuso l'utilizzo di firewall (attorno al 90%) anche perché imposto da SPC ed in via di diffusione i sistemi IDS/IPS che restano fermi intorno ad una percentuale del 60% di adozione.

Decisamente più incoraggiante il dato relativo alla sicurezza delle reti wireless (KPI2.5), che denuncia un lieve aumento delle reti installate che raggiungono ormai il 43%, ma una decisa diminuzione del numero di reti protette con un protocollo debole come WEP (che calano dal 44% al 33% di coloro che usano reti Wi-Fi) passando al protocollo più sicuro WPA (1 o 2) che cresce del 14%. Anche questo dato rafforza sostanzialmente la tesi che vede una concreta crescita della sensibilità mostrata dal campione analizzato. Se infatti l'utilizzo di WPA viene naturale in una grande organizzazione, occorre considerare che un processo analogo per la messa in sicurezza delle reti wireless è stato avviato anche nelle piccole sedi con pochi dipendenti confermando la crescente attenzione verso la sicurezza.

Infine per quanto riguarda la disponibilità di sistemi di logging (KPI2.9), sembrerebbe che il numero complessivo di installazioni sia rimasto inalterato, ma molte amministrazioni (circa il 7%) sono passate stranamente da un sistema correttamente centralizzato e perciò opportunamente irrobustito, ad un sistema locale, evidentemente più debole.

3.3.4.5 Sicurezza dei servizi

Per quanto riguarda la robustezza dei servizi il primo dato che emerge è che occorre prendere atto della scarsa attenzione rivolta dalle amministrazioni al tema "Continuità Operativa". Infatti i primi tre quesiti KPI3.1, KPI3.2 e KPI3.3, con valori medi rispettivamente di 3,21, 4,29 e 2,43, decisamente al di sotto della sufficienza, testimoniano che è questa l'area in cui si deve investire maggiormente per sensibilizzare gli utenti e promuovere iniziative volte ad incrementare l'impegno delle amministrazioni. Purtroppo il tema Continuità Operativo viene troppo spesso visto come un aggravio di costi senza alcuna ricaduta. D'altra parte è possibile, mettendo in atto iniziative condivise tra più amministrazioni, ridurre notevolmente l'impegno economico e facilitare la definizione e l'adozione di piani di disaster recovery utilizzando template preelaborati per la PA. Passando alle cifre, a tutti e 3 i quesiti citati quasi il 20% dell'intero campione non ha risposto e già questo dato è abbastanza allarmante. Inoltre solo il 32% afferma di disporre di un piano formalizzato per il disaster recovery. Solo il 16% dispone di procedure operative da attivare in caso di indisponibilità dei servizi (con copertura totale dei servizi) ed a questi deve essere sommato il 44,6% che dispone di procedure di recovery solo per alcuni servizi. Infine il dato più eclatante è che oltre al 20% che non risponde ben il 44,6% delle amministrazioni intervistate afferma di non disporre di un piano di disaster recovery.

E' evidente che crescendo il livello di informatizzazione della PA aumentano anche l'esposizione ed il rischio di subire danni derivanti dalla indisponibilità, seppur temporanea, dei servizi offerti.

Tutti gli altri quesiti che compongono questo indicatore hanno prodotto risultati stabili rispetto all'anno precedente e sostanzialmente positivi. Nella quasi totalità dei casi le amministrazioni hanno mostrato di adottare tutte le corrette contromisure per la gestione delle posta elettronica e di siti web (interni o pubblici) anche avvalendosi, nel caso di piccole amministrazioni, dei servizi di consulenza offerti da SPC. Anche l'adozione di sistemi centralizzati per l'aggiornamento degli antivirus è

una pratica consolidata e oltre l'85% del campione afferma di averne implementato uno al proprio interno.

Infine, rispetto al tema delle intrusioni e degli attacchi informatici, c'è da rilevare un aumento del 10% delle amministrazioni che hanno percepito tali minacce. Il dato è da considerarsi in maniera estremamente positiva in quanto testimonia una maggiore consapevolezza degli utenti, ed infatti nonostante il monitoraggio offerto dai centri di servizio dei fornitori di connettività previsto da SPC ben 13 amministrazioni dichiarano di aver riscontrato tentativi di intrusione (che non hanno avuto successo) e 5 hanno anche riconosciuto il tipo di attacco classificandolo tra i "denial of service".

Tutto ciò dimostra che il miglioramento delle amministrazioni nell' affrontare situazioni critiche quali i tentativi di intrusione e gli attacchi informatici. Anche su questo tema rimane molto da fare in termini di diffusione del Know How, ma attraverso il centro di gestione degli incidenti predisposto dai fornitori di connettività si conta di avere un buon ritorno in termini di comunicazione preventiva agli utenti di possibili debolezze dei sistemi oltre che un buon livello di filtraggio a monte e monitoraggio delle attività centralizzato.

Al momento non sono ancora disponibili i report delle attività dei 4 centri di gestione e del centro principale di gestione degli incidenti ma è chiaro che il livello di attacco è ormai elevato e costante uniformemente distribuito su tutta la rete pubblica internet. Pertanto è possibile avere l'esatta percezione di ciò che accade anche analizzando i dati forniti da altri centri di gestione degli incidenti (CERT) che operano a livello mondiale.

3.3.4.6 Sicurezza dell'organizzazione

Ancora una volta KPI4 con un valore medio complessivo di 5,27 è risultato il peggiore tra i 4 KPI, facendo emergere criticità diffuse in quasi tutti i controlli individuati da questo indicatore. Nel contempo Medie e Piccole amministrazioni sono migliorate notevolmente aumentando di quasi un punto il valore medio per ciascuna classe.

Vista l'ampiezza del fenomeno sembrerebbe che il tema organizzazione per la sicurezza venga sistematicamente disatteso per svariati motivi. Tra questi vi è sicuramente la tendenza a sottovalutarne l'importanza rispetto al risultato finale in termini di sicurezza complessiva del sistema, ma anche una scarsa sensibilità negli investimenti in termini di risorse umane allocate alla copertura dei ruoli previsti, la capacità di organizzare il ricorso all'outsourcing e di governarne le insidie ed infine gli sforzi per la formazione degli utenti.

I dati, infatti, riportano in maniera estremamente significativa queste preoccupanti tendenze. Ad esempio si riduce dell'8% il numero delle amministrazioni che dichiarano di avere formalmente definito ed approvato un piano per la sicurezza ICT (KPI4.1) che scendono al 46% del campione. Analogamente si sono ridotte le amministrazioni (-14%) che dispongono di policy formalizzate per la Sicurezza ICT (KPI4.2), anche queste pari al 48% meno della metà del campione. Inoltre, seppur in miglioramento (+4% le amministrazioni che hanno ricoperto tutti ruoli previsti pari al 19%) ben oltre il 42% del campione affermano di non aver totalmente disatteso quanto previsto dal D.M. del 16/2/2002 (evitando di rispondere o dichiarando esplicitamente di non averli assegnati). In linea con questo dato solo il 53% (-2%)

delle amministrazioni dichiara di disporre di un centro per la gestione e l'amministrazione della sicurezza (KPI4.4).

Coerentemente con il passaggio a SPC, che mette a disposizione degli utenti un servizio analogo, si riduce al 60% (-21%) il numero delle amministrazioni che hanno predisposto un centro di gestione degli incidenti (KPI4.5).

Seppur lievemente, migliora il risultato sul numero di amministrazioni che hanno ricoperto il ruolo previsto dal garante della privacy di "Responsabile protezione dei dati personali" che con un +1,3% raggiunge il 58,9% del campione. Su un risultato analogo (60,7%) si assestano le amministrazioni rispetto al tema "responsabile per le politiche di backup/restore", il dato positivo è che tutti questi hanno formalizzato e depositato la documentazione relativa alle procedure di loro competenza (KPI4.8a).

Rispetto al tema outsourcing per la sicurezza ICT solo 10 amministrazioni hanno dichiarato di utilizzare personale misto per la gestione della sicurezza (KPI4.9), ma tra questi solamente un'amministrazione ha previsto nel contratto procedure per l'audit che poi vengono effettuate regolarmente. Risulta pertanto evidente che occorre un grosso contributo esterno sia in termini normativi che in termini di negoziazione con i fornitori per arrivare a rendere meno rischiose le attività gestite in outsourcing.

In linea con la crisi economica che ha visto ridurre le dotazioni delle amministrazioni, rimane stabile attorno al 32% il numero delle amministrazioni che hanno allocato una voce nel proprio bilancio dedicata alla sicurezza ICT, e tra queste si riducono i budget crescendo del 26% il numero che ha allocato a questa voce meno del 5% del proprio budget complessivo. Ciononostante il numero delle amministrazioni che hanno effettuato un'analisi dei rischi è elevato (il 19% dichiara di non averla effettuata ed altrettante non rispondono).

Infine, quasi a voler motivare il dato espresso dal KPI4, il risultato dell'ultimo quesito comprova la scarsa attenzione dedicata alla formazione degli utenti sul tema sicurezza ICT (KPI4.13). Infatti solo il 21% (12) ha dichiarato di aver redatto ed approvato un piano di formazione e sensibilizzazione per la sicurezza ICT (KPI4.13) e tra queste solo il 58% ha coinvolto oltre il 50% degli utenti potenziali mentre per tutte le altre le ricadute sono state ben più limitate.

3.3.4.7 Considerazioni finali

Con la rilevazione 2008 per la prima volta si è potuto procedere ad un confronto puntuale, quesito per quesito, dei dati raccolti con i risultati dell'anno precedente. Ciò ha consentito analisi più approfondite ed interpretazioni più vicine alla realtà delle amministrazioni della PAC.

Grazie alla maturità del modello comune per la sicurezza molte amministrazioni hanno ritrovato la propria situazione interna all'interno dei quesiti e delle risposte previste del questionario, tanto da diventare obiettivi correnti di progetti strategici da attivare nel breve. Ciò ha fatto si che nonostante la crisi economica che certamente non ha facilitato l'avvio di nuovi progetti, vi è stata un sostanziale crescita soprattutto tra le Piccole e Medie amministrazioni. Le Grandi organizzazioni hanno pagato maggiormente il prezzo della crisi, ma, come più volte affermato nelle precedenti relazioni, il questionario ha come primo scopo quello di individuare le principali criticità, maggiormente diffuse all'interno della PAC, sulle quali intervenire in maniera prioritaria, mentre l'eccellenza, a cui naturalmente occorre

tendere, può essere raggiunta solo attraverso impegno costante e strategie comuni condivise mettendo a fattor comune i risultati conseguiti. Pertanto il miglioramento dei valori minimi ottenuti nella precedente edizione costituisce di per se un risultato rilevante ripagando degli sforzi condotti nel corso degli ultimi 4 anni. Questo risultato in se vale molto di più dell'arretramento dei valori massimi raggiunti nelle precedenti edizioni.

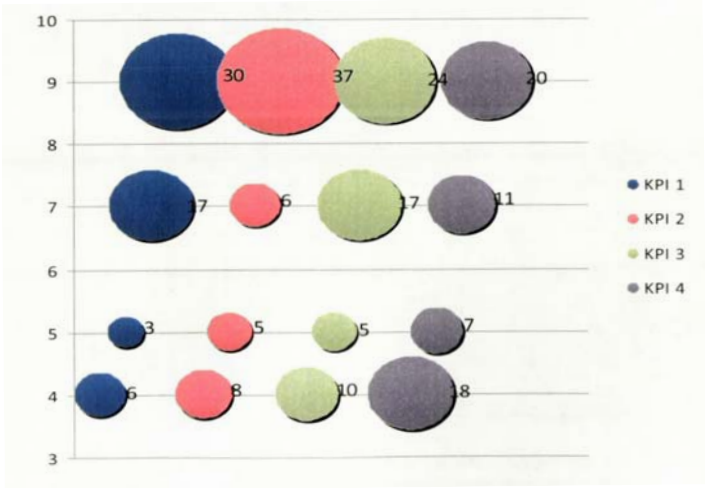
In sostanza la rilevazione annuale mira principalmente ad individuare le amministrazioni posizionate al di sotto della soglia critica, evidenziate nel grafico in

nell'area cerchiata, per fornire loro soluzioni di rapida implementazione e basso impatto organizzativo. D'altra parte, solo grazie all'esperienza maturata in questi anni dal CNIPA attraverso tutte le attività di raccolta dati dalla PA, è possibile proporre linee guida valide per ampie classi di utenti e per le aree di intervento individuate. La

mostra il numero di amministrazioni che ricadono nelle 4 categorie: ottima, per valori maggiori di 7, buona, per valori compresi tra 5 e 7, accettabile, per valori tra 4 e 5 e scarsa per valori inferiori a 4.

La dimensione della sfera indica il numero di amministrazioni che ricadono nella categoria mentre il colore individua il KPI. Pertanto si intuisce come la maggioranza delle amministrazioni ricadono nelle due categorie Ottima e Buona. D'altra parte il numero di amministrazioni al di sotto della soglia di criticità è ancora elevato specialmente per KPI4 (18 amministrazioni pari al 32%) ed è appunto su queste che occorre pianificare gli interventi più urgenti.

Figura 8: Classificazione amministrazioni in funzione del punteggio conseguito per ciascun KPI



Il questionario fornisce anche un accurato monitoraggio delle singole amministrazioni producendo indicazioni molto precise sui punti sui quali occorre intervenire. Quest'anno i punteggi più bassi sono stati ottenuti sui quesiti relativi al tema Continuità Operativa (C.O.), sul quale il CNIPA è impegnato già da tempo. Per risolvere il problema in maniera più radicale occorre attivare progetti più incisivi e

con un maggiore coinvolgimento da parte delle amministrazioni. A titolo esemplificativo, si potrebbero realizzare centri di backup condivisi tra amministrazioni omogenee (per dimensioni e tecnologie impiegate nei propri CED) che oltre a ridurre i costi complessivi, consentirebbero di sviluppare rapidamente competenze tecniche all'interno delle amministrazioni oltre che ad una maggiore consapevolezza sul tema specifico. I partecipanti potrebbero condividere oltre alle attrezzature anche piani preelaborati per la C.O. riducendo i tempi e le incertezze rispetto ad un progetto in house.

Altro tema di carattere generale è proprio quello della diffusione della cultura della sicurezza ICT che ancora non si è radicata adeguatamente tra gli utenti finali. In tale direzione il CNIPA propone di intervenire preconfigurando piani di formazione general purpose, utilizzando anche strumenti come formazione a distanza per limitare gli impatti sull'organizzazione interna.

I risultati del questionario offrono un quadro molto variegato della PAC ben sintetizzato dalla figura precedente. Laddove esistono molti casi di vera eccellenza per i quali non sono necessari interventi urgenti, ne esistono altri in condizioni davvero critiche che richiedono interventi urgenti e ben mirati differenziati in funzione delle Amministrazioni destinatarie. Anche in presenza di una buona sensibilità rispetto al tema sicurezza ICT in taluni casi, anche alla luce delle dimensioni estremamente contenute dell'amministrazione è impensabile che l'obiettivo posto dal modello unico della sicurezza possa essere raggiunto dagli utenti autonomamente senza il contributo di un ente centrale che possa guidare il processo evolutivo garantendone l'esito finale.

Prima di concludere questa breve sintesi, occorre ribadire ancora una volta che la metodologia sottesa dal questionario intende misurare l'attenzione dei responsabile rispetto al tema sicurezza ICT ma in prima battuta non può di rilevare l'esposizione al rischio di ciascuna amministrazione. Questa informazione potrà essere ottenuta attraverso indagini di secondo livello e ricostruendo i dati provenienti dall'osservatorio sugli incidenti di sicurezza del Sistema Pubblico di Connettività, una volta a regime, consentendo di porre in relazione i valori KPI rilevati con la frequenza dei problemi di sicurezza che via via si manifesteranno.

Il i dati raccolti per l'anno 2008 complessivamente hanno prodotto un quadro rassicurante, in netto miglioramento soprattutto per quanto riguarda le maggiori criticità poste dalle piccole e medie amministrazioni che spinge a mantenere l'impegno profuso in questi anni ed a capitalizzare il principale risultato ottenuto, costituito da un modello unico per la sicurezza.

3.3.5 Nuove tecnologie

3.3.5.1 Adozione di tecnologie innovative

L'adozione di tecnologie innovative - VoIP, WI-MAX, WI-FI, Applicazioni di telecomunicazioni mobili, Rfid e Biometrie - porta alle amministrazioni importanti benefici in termini di razionalizzazione della spesa, efficienza ed efficacia dei servizi, funzionamento del back office. Una delle priorità è lo sviluppo del VoIP, la cui adozione nella PA centrale è stata resa obbligatoria dalla Legge finanziaria 2008.

All'indagine sull'utilizzo delle tecnologie emergenti hanno risposto tutte le amministrazioni che hanno inviato i dati.

Da notare che circa il 40% (19 amministrazioni) di esse possiede un'unità organizzativa o una funzione preposta all'osservazione del mercato e delle nuove tecnologie nonché alla loro sperimentazione.

I grafici seguenti evidenziano l'utilizzo attuale e le previsioni di utilizzo nell'immediato futuro e nel prossimo triennio delle tecnologie emergenti.

Figura 9 : Tecnologie emergenti nelle amministrazioni (in numero), anno 2008

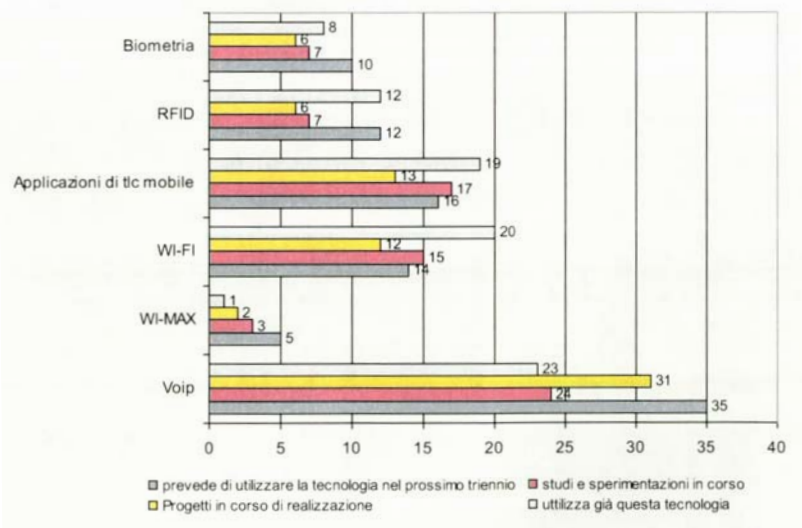
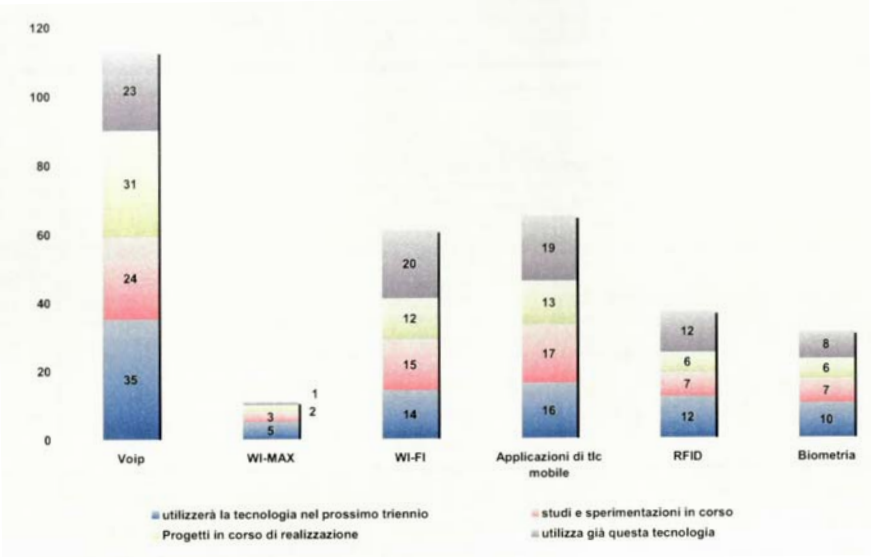


Figura 10 : Numero di amministrazione che utilizzano o utilizzeranno nuove tecnologie, anno 2008



La tecnologia al momento più utilizzata dalle amministrazioni è il VoIP amministrazioni) seguita dal Wi-Fi.

La tecnologia con più studi e sperimentazioni in corso è il VOiP seguito dalle applicazioni di telecomunicazione mobile.

Infine la tecnologia VOiP è quella che ha più progetti in corso di realizzazione ed è quella che si prevede verrà utilizzata maggiormente nel prossimo triennio.

3.3.5.2 Biometria - iniziative delle amministrazioni

Tra le amministrazioni che utilizzano o hanno avviato iniziative per utilizzare questa tecnologia si segnala che:

- Il Dipartimento dell'amministrazione penitenziaria (DAP) della Giustizia utilizza una funzionalità denominata "AFIS-Nuova Matricola"[20] basata sull'utilizzo del Sottosistema Periferico per l'Acquisizione delle Impronte Digitali (SPAID), che consente la rilevazione delle impronte digitali mediante scanner biometrico;

[20] AFIS è un programma approvato e finanziato dall'Unione Europea che coinvolge il servizio di Polizia scientifica del Ministero dell'interno (promotore del progetto) e il DAP, per la creazione e la gestione della banca dati delle impronte digitali situata presso il servizio di Polizia scientifica del Ministero dell'interno. La base dati è costituita da circa 5 milioni di cartellini fotosegnaletici (pari a circa 50 milioni di impronte digitali) redatti dalle diverse Forze di Polizia per fini identificativi. Oltre alle impronte contiene anche elementi desumibili dal cartellino fotosegnaletico (es. fotografie, dati anagrafici e biometrici). Attualmente la banca dati viene alimentata ricorrendo alla classica inchiostrazione che, richiedendo un doppio passaggio prima della trasformazione numerica, rallenta l'intero processo e diminuisce drasticamente la qualità delle immagini.