Risultano in lieve calo i DBMS su piattaforma distribuita o distribuita e replicata la cui quota, complessivamente, passa dal 30,7% del 2003 al 29,5% del 2004;

- la principale piattaforma elaborativa su cui risiede la maggior parte delle basi dati, è quella dipartimentale, sia a livello centrale sia periferico.

Tra le iniziative effettuate o in corso delle amministrazioni, si rileva che:

- il Ministero della giustizia, nell'ambito del portale Normeinrete, ha completato il progetto per la consultazione del patrimonio normativo (normativa statale a partire dal 1948, si prevede di indicizzare e rendere accessibile la normativa dal 1904). Per quanto riguarda, invece, il portale ItalGiure web, sono stati resi disponibili gratuitamente (disposizione di cui all'art. 2 del DPR 17 giugno 2004 n. 195), i documenti contenuti negli archivi normativi della banca dati del Centro elettronico di documentazione della Corte Suprema di Cassazione. È in corso il progetto Sistema Informatico Procure e Prefetture dell'Italia Meridionale che prevede la realizzazione di una banca dati relativa ai beni sequestrati o confiscati in materia di criminalità organizzata. Il sistema verrà alimentato dai costituendi registri informatizzati delle misure di prevenzione, oltre che dalle altre Amministrazioni interessate (Interno, Agenzia del demanio ed Economia e finanze), che condivideranno il patrimonio informativo attraverso una piattaforma di interoperabilità;
- i Carabinieri, nell'ambito del progetto di automazione del Sistema d'Indagine del Comando CC e tutela dell'ambiente, prevedono la costituzione di un sistema di elaborazione e di gestione delle informazioni. Tra le attività, è prevista: la realizzazione di una Banca Dati multimediale costituita da archivi contenenti dati alfanumerici, quadri cartografici e topografici, mappe statiche, modelli digitali del terreno, fotogrammetriche satellitari, ecc.; la costituzione di una rete di trasmissione dati ad alta velocità, che consenta il collegamento tra le diverse utenze del sistema;
- il Ministero dell'interno da settembre 2004 sta sperimentando in provincia di Milano, Cernusco sul Naviglio, l'automazione verbali/multe per le pattuglie della Polizia Stradale. Tale progetto riguarda lo sviluppo di un'applicazione, basata sulla tecnologia "penna ANOTO", che consente di trasferire su un PC/Server tutto ciò che la penna digitale scrive su appositi moduli cartacei, e convertire il testo manoscritto in caratteri digitali per l'automatico inserimento in banca dati;
- l'Inail, ha completato, per la Consulenza statistico-attuariale, la realizzazione della nuova Banca Dati Statistica, ristrutturata integralmente rispetto alla precedente, che fornisce informazioni articolate nelle seguenti aree tematiche: datori di lavoro, infortuni e malattie professionali, rendite, rischio. È in corso la realizzazione dell'area tematica lavoratori. A tale realizzazione sono strettamente collegate le ristrutturazioni di "Banca Dati al femminile" e quella delle pubblicazioni statistiche. È stata completata la realizzazione e rilasciata in esercizio la nuova versione relativa alla Banca Dati Disabili più dinamica e dettagliata rispetto alla precedente versione;
- il Territorio, nell'ambito della costituzione dell'Anagrafe dei beni immobiliari, ha acquisito e riversato in base informativa i dati dei soggetti di circa 3 milioni di note ottiche della Conservatoria, e ha avviato le procedure di gara per l'acquisizione di ulteriori 3,2 milioni di note per il completamento dell'informatizzazione degli atti di almeno venti anni per tutti gli uffici. È proseguita l'attività di completamento della banca dati cartografica nell'ambito del progetto per la dematerializzazione dei documenti.

5.2.2 Datawarehouse e Decision Support System

Continua lo sviluppo del datawarehouse come strumento di supporto al processo di valutazione e controllo strategico dell'amministrazione. Nel 2004 si sono avuti circa 218mila utenti utilizzatori. In particolare, rispetto al 2003, il numero dei sistemi è cresciuto di 132 unità per l'Arma dei Carabinieri, di cinque unità per il comparto finanziario e per l'Istat, di tre unità per l'Aci e di uno per il Corpo forestale dello Stato e per l'UNIRE.

L'uso di un datawarehouse comporta diversi vantaggi tra i quali:

- il raggruppamento di dati decisionali per aree o temi di interesse e l'orientamento degli stessi rispetto all'utilizzazione finale;
- la salvaguardia del patrimonio informativo e l'incremento della qualità dei dati;
- la disponibilità di elementi informativi di sintesi utili al processo di valutazione e controllo strategico dell'amministrazione, ottenuti integrando i dati dei sistemi operazionali e gestionali;
- la disponibilità di un orizzonte temporale ampio, che garantisce il mantenimento di informazioni storiche, in modo da poter favorire le attività di analisi comparative su diversi periodi temporali;
- la risposta tempestiva e corretta a problemi decisionali, legati alle attività istituzionali dell'amministrazione, garantendo migliori risultati in termini di efficacia ed efficienza.

In particolare, L'Agenzia delle entrate ha avviato la realizzazione di un datawarehouse per monitorare la spesa sanitaria italiana, con l'obiettivo di fornire agli organi di Governo un supporto nelle fasi di individuazione delle politiche e degli interventi più idonei per una gestione più ottimale della spesa stessa.

Il Ministero dell'economia e delle finanze ha integrato nel "Nuovo Sistema Entrate in ambiente distribuito" i sistemi di supporto alle decisioni, e ha predisposto l'utilizzo di strumenti conoscitivi, per effettuare l'analisi delle informazioni in entrata.

L'Ipost utilizza le funzionalità rese disponibili dalla piattaforma SAP (Business Information Warehouse), che consentono di integrare i modelli di contabilità finanziaria, contabilità economico-patrimoniale e il controllo, per ottenere un sistema in grado di fornire dati analitici e di sintesi sulle attività dell'Ente. Ha avviato, inoltre, la realizzazione del sistema direzionale per misurare la gestione del personale, la contabilità, il ciclo degli acquisti e la gestione della corrispondenza. Per i servizi istituzionali, è stato rilasciato, in particolare, un prototipo completo, che include un "cruscotto direzionale".

Il Cnr ha consolidato gli attuali strumenti decisionali finalizzati al controllo di gestione e ha incrementato la produzione di reportistica per i diversi organi e servizi dell'Ente.

5.2.3 Qualità dei dati

Cresce l'attenzione sul problema della qualità dei dati e di conseguenza sulla valorizzazione dell'ingente patrimonio informativo detenuto e gestito dalle amministrazioni pubbliche.

Nel 2004 dieci amministrazioni (tre amministrazioni in più rispetto al 2003) dichiarano di avere nominato un responsabile della qualità dei dati, mentre ventiquattro sono quelle che hanno effettuato attività di miglioramento (quattro in più rispetto al 2003). Soltanto undici dichiarano di aver definito degli standard per la qualità dei dati.

Tra le iniziative in corso ricordiamo quella:

- dell'Aci, che ha avviato la reingegnerizzazione delle applicazioni PRA e delle procedure relative alle tasse automobilistiche, anche in un'ottica di miglioramento della qualità dei dati, sia in ingresso, sia in erogazione;
- dell'Inpdap, che ha realizzato per i mutui un sistema per monitorare la qualità dei dati attraverso opportuni indicatori;
- del Ministero dell'economia e delle finanze, che nell'ambito delle attività mirate al consolidamento del sistema nazionale di monitoraggio dei fondi strutturali UE, ha definito e reso condivisibile una metodologia unica per il controllo della qualità dei dati, attraverso la standardizzazione dei prospetti utilizzati nelle sedi istituzionali centrali e periferiche. Inoltre, nel corso del 2004, l'amministrazione ha avviato una sperimentazione finalizzata alla verifica della completezza e della qualità delle informazioni presenti nel sistema per il controllo di gestione;
- dell'Interno, che nell'ambito del servizio di polizia scientifica, ha acquistato apparecchiature specializzate per le attività di fotosegnalamento digitale, che consentiranno di migliorare notevolmente la qualità dei dati acquisiti.

6. Sicurezza ICT

La Relazione annuale 2004 presenta per la prima volta un ampio insieme di informazioni sullo stato della sicurezza ICT nelle amministrazioni. Le informazioni sono state strutturate in cinque aree: organizzazione, pianificazione, tecnologie, gestione e continuità di servizio.

I dati esaminati sono stati forniti da 51 amministrazioni; le risposte non date a specifici quesiti sono state considerate risposte negative.

L'analisi dei dati evidenzia che il tema della sicurezza è generalmente piuttosto avvertito dalle amministrazioni.

Va però sottolineato come, a fronte di una predisposizione in termini tecnologici relativamente elevata (le Amministrazioni che dichiarano di disporre di sistemi antivirus sono il 96% e quelle che dichiarano di disporre di sistemi di *firewalling* sono l'86%), si evidenziano lacune per gli aspetti organizzativi, per quelli attinenti alla pianificazione, alla formazione ed alla gestione.

A distanza di tre anni da quanto raccomandato dalla Direttiva del 16 gennaio 2002 infatti solo il 43% delle Amministrazioni dichiara di avere nominato un responsabile della sicurezza ICT, solo il 37% delle Amministrazioni dichiara di avere definito formalmente una *policy* della sicurezza, solo il 53% delle Amministrazioni dichiara di avere avviato un piano di formazione e sensibilizzazione, solo il 22% delle stesse dichiara di disporre di un gruppo di gestione degli incidenti (CERT-AM).

Si rileva, infine, una qualche confusione circa gli aspetti inerenti analisi del rischio, *business continuity* e *disaster recovery*, temi che pur indicando aspetti differenti del problema generale della continuità operativa delle infrastrutture informatiche, sono comunque tra loro correlati: tra le Amministrazioni che dichiarano di disporre di un piano formalizzato per la continuità operativa, il 31,6% non ha effettuato l'analisi dei rischi.

6.1 Organizzazione

Di seguito nella tabella è riportato il numero di amministrazioni che affermano di avere definito, nella propria organizzazione interna, specifici ruoli e responsabilità destinati alla sicurezza ICT.

Complessivamente i dati evidenziano, sugli aspetti organizzativi, una realtà che desta molte preoccupazioni. Infatti, dal punto di vista normativo, si evince che la direttiva del 16 gennaio 2002 è stata ampiamente disattesa e che i dati suggeriscono inoltre che due amministrazioni su tre non rispettano quanto prescritto nel "Codice per la protezione dei dati personali". Passando poi dagli aspetti normativi a quelli sostanziali, la mancata individuazione del responsabile della sicurezza ICT da parte di 29 amministrazioni dimostra l'assenza di una figura essenziale per la definizione e il coordinamento di tutti gli interventi in materia di sicurezza ICT, fatto che induce a ritenere che gli interventi metodologici, tecnologici e procedurali effettuati, in corso di effettuazione o pianificati non siano frutto della necessaria visione di insieme.

Tabella 42 – Stato dell'organizzazione della sicurezza, anno 2004

Quesiti	Numero amministrazioni (SI)	%
Consigliere tecnico sicurezza ICT[34]	7	14
– nominativo comunicato al CNIPA	*7*	*14*

(segue)

[34] Il consulente strategico del Ministro, interfaccia il Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni e il titolare del Dicastero.

Comitato sicurezza ICT[35]	11	22
Responsabile sicurezza ICT[36]	22	43
– nominativo comunicato al CNIPA	*14*	*27*
Responsabile protezione dati	18	35
Responsabile infrastrutture e controllo accessi[37]	16	31

6.2 Piano di sicurezza

Di seguito è riportato nella tabella il numero di amministrazioni che hanno risposto affermativamente al quesito sull'esistenza di un piano di sicurezza con particolare riguardo ai seguenti punti: analisi dei rischi, policy di sicurezza, piano di interventi per misure e contromisure di carattere logico e fisico, formazione e sensibilizzazione.

Tabella 43 – Stato del Piano di sicurezza, anno 2004

QUESITI	NUMERO AMMINISTRAZIONI (SI)	%
Definizione formale di un piano di sicurezza	25	49
Effettuata un' analisi dei rischi[38]	36	71
– copertura analisi rischi totale	*7*	*14*
– copertura analisi rischi parziale	*16*	*31*
– copertura analisi rischi minima	*13*	*25*
Definizione formale di una policy di sicurezza	19	37
Definizione piano di interventi per la sicurezza logica[39]	28	55
Interventi tecnico – procedurali per la sicurezza logica	26	51
– interventi effettuati	*9*	*18*
– interventi pianificati	*2*	*4*
– interventi in corso	*9*	*18*
– interventi effettuati - in corso – pianificati	*5*	*10*

(segue)

[35] Il Comitato formula le proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT), al fine del raggiungimento di un livello di sicurezza nelle informazioni conforme a criteri standard internazionali e per garantire integrità e affidabilità dell'informazione.

[36] Il Responsabile della sicurezza ICT definisce le soluzioni tattiche, ossia sceglie i mezzi e le azioni idonee dirette all'attuazione delle direttive impartite dal Ministro e/o dal Comitato.

[37] La persona nominata che controlla l'accesso fisico nelle zone in cui si trovano risorse informatiche hw e sw, apparati di rete, linee dati, dispositivi di backup, documenti, impianti elettrici, ecc.

[38] Per analizzare e gestire correttamente il rischio si dovrebbe stilare l'elenco dei beni da proteggere e, in corrispondenza di ciascun bene, porre: una stima del loro valore (che è pari al *danno* derivante dalla perdita del bene); l'elenco delle potenziali minacce; l'elenco delle vulnerabilità del sistema; l'elenco dei precedenti controlli.
In genere, ad ogni minaccia viene assegnato: un *rischio* (ossia un parametro di gravità), una probabilità (detto fattore di attuabilità) e un *danno* (che si pone pari al valore del bene colpito). Per valutare il rischio si utilizza la relazione: *Rischio= Danno*Fattore di attuabilità*. La *gestione del rischio* ha lo scopo di ridurre il rischio fino ad un valore considerato accettabile mediante la scelta di opportune contromisure.

[39] Una delle componenti della sicurezza logica riguarda l'accesso degli utenti alle informazioni e alle risorse del sistema informatico. Così come per l'accesso fisico, l'accesso logico va regolato da precise procedure in quanto non tutti gli utenti possono accedere a tutte le informazioni o servizi disponibili o eseguire tutti i programmi implementati nel sistema.

– interventi effettuati - in corso	*1*	*2*
Definizione di un piano di interventi per la sicurezza fisica	26	51
Interventi tecnico - procedurali per la sicurezza fisica	26	51
– interventi effettuati	*7*	*14*
– interventi pianificati	*3*	*6*
– interventi in corso	*9*	*18*
– interventi effettuati - in corso – pianificati	*4*	*8*
– interventi effettuati - in corso	*1*	*2*
– interventi in corso – pianificati	*1*	*2*
– interventi effettuati – pianificati	*1*	*2*
Avvio di un piano di formazione e sensibilizzazione	27	53
Attività di formazione e sensibilizzazione	25	49
– attività di formazione effettuate	*4*	*8*
– attività di formazione pianificate	*7*	*14*
– attività di formazione in corso	*5*	*10*
– attività di formazione effettuate - in corso - pianificate	*4*	*8*
– attività di formazione effettuate - in corso	*2*	*4*
– interventi in corso – pianificati	*2*	*4*
– attività di formazione effettuate – pianificate	*1*	*2*

Anche per quanto attiene agli aspetti di pianificazione la situazione che traspare dalle risposte fornite dalle amministrazioni non è confortante.

Più di una amministrazione su due non ha ancora definito un piano di sicurezza e pertanto, coerentemente, non ha definito un piano di interventi; risulta inoltre particolarmente basso il numero delle amministrazioni che ha già redatto in modo formale una politica di sicurezza (una su tre).

Ricordiamo che il Cnipa ha emanato in proposito il documento "Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione", dove le amministrazioni possono rinvenire utili suggerimenti in materia di pianificazione.

È da rimarcare inoltre che quasi una amministrazione su due si è attivata in materia di formazione e sensibilizzazione sulla sicurezza ICT, aspetto essenziale per la realizzazione di un efficace sistema di sicurezza, come dimostrato, ad esempio, dai casi più gravi registrati nel 2004 relativi ad epidemie "virali" tutte causate di *worm* di tipo *mass mailing* (Netsky, Mydoom, Beagle) e tutte innescate ed alimentate da azioni degli utenti.

6.3 Sicurezza logica

Nella tabella seguente sono riportate il numero di amministrazioni che hanno realizzato misure e contromisure nell'ambito della sicurezza.

Tabella 44 – Stato della sicurezza logica, anno 2004

QUESITI	NUMERO AMMINISTRAZIONI (SI)	%
Esistenza di un sistema di protezione antivirus	49	96
– protezione dai virus totale	*35*	*69*
– protezione dai virus parziale	*14*	*27*
Utilizzo di sistemi di firewallig almeno come difesa perimetrale	44	86
Firewall posizionati su tutti i punti di accesso alla rete interna	41	80
Utilizzo di sistemi di intrusion detection o protection[40]	27	53
Utilizzo di sistemi di autenticazione per l'accesso alla rete interna (password, token card, smart card, ecc.)	45	88
Utilizzo di sistemi di autenticazione e di autorizzazione nominativi per l'accesso alle applicazioni[41]	49	96
– per accesso a tutte le applicazioni	*30*	*59*
– per accesso solo alle applicazioni più critiche	*19*	*37*
Esistenza di misure di protezione dei dati	47	92
Sono state attuate misure di autorizzazione all'accesso ai dati	46	90
Sono state definite ed adottate tecnologie e procedure backup	47	92

Note positive arrivano invece dall'utilizzo di tecnologie per la sicurezza ICT.

In particolare i dati raccolti indicano che 35 amministrazioni dispongono di sistemi per la protezione dai virus informatici con copertura totale e 14 con copertura parziale; a questo proposito non si può però fare a meno di notare che questa basilare misura di protezione dovrebbe ormai essere un corredo "standard" di qualsiasi piattaforma informatica anche in conformità a quanto previsto dal "Codice per la protezione dei dati personali".

L'introduzione e l'utilizzo di sistemi di *firewalling* ha raggiunto un buon livello di penetrazione nei sistemi informatici delle amministrazioni; anche questa misura di protezione è da considerarsi basilare e se ne auspica un incremento, ricordando che una definizione ed un aggiornamento poco accurato della configurazione di questi dispositivi, così come un insufficiente controllo dei log, ne compromette facilmente l'efficacia.

Desta qualche perplessità il dato relativo alle modalità di accesso alle applicazioni, che, pur globalmente confortante (96%), mostra che ben 19 amministrazioni utilizzano sistemi di autenticazione ed autorizzazione nominativi solo per le applicazioni che considerano più critiche.

Va infine rimarcato che quattro amministrazioni non hanno ancora definito ed adottato tecnologie e procedure per il backup di dati e sono quindi particolarmente esposte a danni ingenti in caso di incidenti che colpiscano l'integrità e la disponibilità dei dati gestiti nei loro sistemi.

6.3.1 Procedure di accesso ai servizi on-line

Dall'analisi dei servizi on-line risulta che su 205 servizi erogati da 36 amministrazioni il 56% (in termini assoluti 95) richiede una qualche forma di autenticazione dell'utente. Le principali modali-

[40] Sistemi utilizzati per il monitoraggio delle reti e dei server critici, allo scopo di identificare segnali di attacchi o intrusioni e di intraprendere immediate azioni correttive.

[41] Meccanismi utilizzati per la verifica dell'identità e la limitazione ed il controllo dei livelli di accesso ai programmi e/o alle funzioni che fanno parte del sistema informativo automatizzato tramite utenze riconducibili a singoli individui.

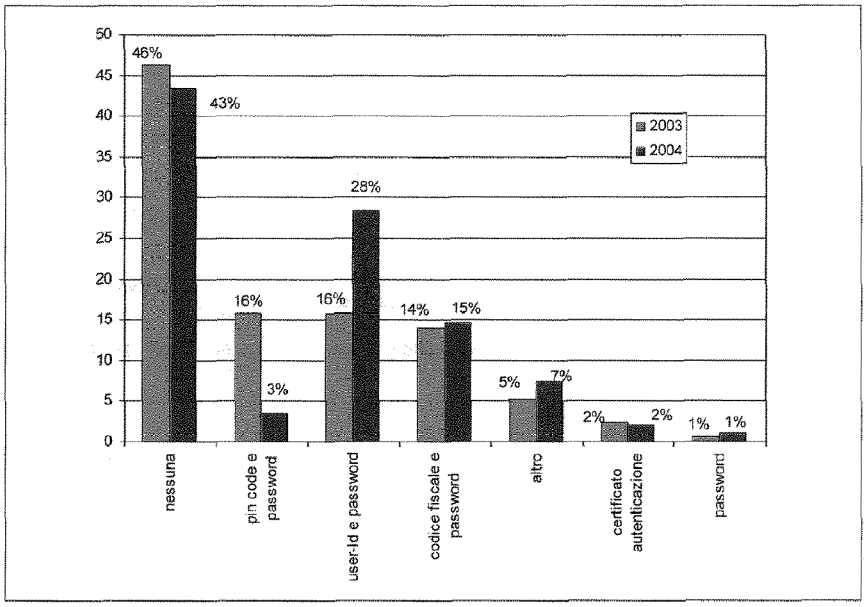
tà di autenticazione e certificazione sono la User-Id e password (28%), il codice fiscale e password (15%) e il PIN code e password (3%). Tra le amministrazioni, la modalità "User-id e password" è utilizzata principalmente dall'Inail (22 servizi) e da Entrate (11); "Codice fiscale e password" da Entrate (21) e Inps (4); "PIN code e password" dall'Inps (5).

La diversità di codici e di password, per modalità di accesso e per amministrazione, rimane una delle principali criticità alla diffusione dei servizi on-line. Questa criticità potrà essere notevolmente ridotta con la diffusione della Carta nazionale dei servizi.

Tabella 45 – Procedure di accesso ai servizi on-line per amministrazione, anni 2003 e 2004

Amministrazione	Totale servizi		Nessuna		Pin code e password		User-Id e password		Codice fiscale e password		Altro		Certificato autent.ne		Password	
	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004
ACI	12	14	7	7	–	–	–	2	–	–	5	5	–	–	–	–
AGEA	1	1	–	–	–	–	1	1	–	–	–	–	–	–	–	–
Ambiente	1	1	1	1	–	–	–	–	–	–	–	–	–	–	–	–
Attività produttive	3	4	3	3	–	–	–	–	–	–	–	1	–	–	–	–
Beni culturali	5	6	5	6	–	–	–	–	–	–	–	–	–	–	–	–
CFS	1	1	1	1	–	–	–	–	–	–	–	–	–	–	–	–
Consiglio di Stato	1	1	1	1	–	–	–	–	–	–	–	–	–	–	–	–
Corte dei conti	2	2	2	2	–	–	–	–	–	–	–	–	–	–	–	–
Difesa	–	3	–	2	–	–	–	–	–	–	–	1	–	–	–	–
Dogane	1	1	–	–	–	–	1	1	–	–	–	–	–	–	–	–
ENEA	1	1	1	1	–	–	–	–	–	–	–	–	–	–	–	–
ENPALS	4	3	1	–	2	1	–	–	1	2	–	–	–	–	–	–
Entrate	31	39	3	6	10	–	–	11	17	21	–	–	1	1	–	–
Giustizia	2	2	1	1	–	–	1	1	–	–	–	–	–	–	–	–
ICE	14	11	7	9	7	–	–	–	–	1	–	1	–	–	–	–
IIMS	1	1	1	1	–	–	–	–	–	–	–	–	–	–	–	–
INAIL	17	27	2	5	–	–	11	22	–	–	3	–	1	–	–	–
INEA	2	3	–	1	–	–	2	1	–	–	–	1	–	–	–	–
Infrastrutture	2	1	2	1	–	–	–	–	–	–	–	–	–	–	–	–
INPDAP	3	2	–	–	2	1	–	–	–	–	–	–	1	1	–	–
INPS	21	22	9	7	5	5	1	1	4	4	1	4	1	1	–	–
Interno	3	7	2	4	–	–	1	3	–	–	–	–	–	–	–	–
IPOST	–	1	–	–	–	–	–	–	–	–	–	–	–	1	–	–
IPSEMA	3	3	–	–	–	–	3	3	–	–	–	–	–	–	–	–
ISPESL	1	1	1	1	–	–	–	–	–	–	–	–	–	–	–	–
ISS	10	11	8	8	–	–	2	3	–	–	–	–	–	–	–	–
ISTAT	4	4	4	3	–	–	–	–	–	–	–	–	–	–	–	1
Istruzione	7	9	4	4	–	–	3	5	–	–	–	–	–	–	–	–
Politiche agricole	3	3	3	3	–	–	–	–	–	–	–	–	–	–	–	–
Politiche fiscali	4	5	3	3	–	–	–	–	–	–	–	1	–	–	1	1
Presidenza	1	3	1	1	–	–	–	1	–	–	–	1	–	–	–	–
Salute	4	1	3	–	1	–	–	1	–	–	–	–	–	–	–	–
SSPA	3	3	2	2	–	–	1	1	–	–	–	–	–	–	–	–
Territorio	2	2	–	–	–	–	–	–	2	2	–	–	–	–	–	–
Tesoro	1	6	1	5	–	–	–	1	–	–	–	–	–	–	–	–
Totale	**171**	**205**	**79**	**89**	**27**	**7**	**27**	**58**	**24**	**30**	**9**	**15**	**4**	**4**	**1**	**2**

Figura 8 – Diffusione delle diverse procedure di accesso ai servizi on-line, anni 2003 e 2004 (in percentuale)



6.4 Amministrazione e gestione

Il paragrafo descrive il sistema adottato dalle amministrazioni per l'amministrazione e la gestione della sicurezza ICT. Nella tabella è riportato il numero di amministrazioni che hanno risposto affermativamente al quesito su un totale di 51.

Tabella 46 – Stato dell'amministrazione e gestione della sicurezza, anno 2004

QUESITI	NUMERO AMMINISTRAZIONI (SI)	%
Esistenza ed operatività dei centri di gestione ed amministrazione della sicurezza ICT[42]	27	53
Tipo di gestione ed amministrazione della sicurezza del sistema informativo	49	96
– parzialmente decentralizzata	*23*	*45*
– completamente decentralizzata	*26*	*51*
Tipo di personale per la gestione e l'amministrazione della sicurezza del sistema informativo	45	88
– personale misto	*25*	*49*
– personale interno	*20*	*39*
Esistenza di un contratto di outsourcing per la gestione e l'amministrazione della sicurezza	14	27
– con clausole che consentano all'amministrazione di effettuare un audit di sicurezza[43]	*11*	*22*
Esistenza ed operatività di un gruppo di gestione degli incidenti - CERT-AM della direttiva 16/1/2002[44]	11	22

[42] Il centro di gestione della sicurezza si occupa di gestire ed amministrare la sicurezza ICT.

[43] Esistenza di una procedura che consenta di verificare le policy di sicurezza e il livello di sicurezza forniti dalla terza parte.

[44] Esistenza nell'organizzazione informatica (formale o informale) di un gruppo operativo che ha il compito di prevenire gli incidenti informatici e di minimizzarne l'impatto ed i tempi di ripristino.

I sistemi informativi sono per loro natura sistemi non statici, in particolare se li si osserva dal punto di vista della sicurezza; sono molti i parametri soggetti a continua variazione, uno per tutti la continua presenza di nuove minacce provenienti dalla rete.

L'amministrazione e la gestione sono quindi processi fondamentali per il mantenimento di un sistema di sicurezza.

Dalle risposte ricevute si constata che 49 amministrazioni su 51 effettuano attività di amministrazione e gestione della sicurezza anche se solo 27 di esse dispongono di un centro dedicato a tali attività. Inoltre 20 amministrazioni utilizzano solo personale interno a fronte delle 25 che si avvalgono anche di collaboratori esterni.

Solo una amministrazione su quattro ha affidato la gestione della sicurezza ad una terza parte; a questo proposito va però rilevato con preoccupazione che tre di queste non hanno previsto contrattualmente clausole che permettano loro di effettuare attività di verifica (audit di sicurezza).

Va infine rilevato che solo una amministrazione su cinque ha dato vita ad una unità locale di gestione degli incidenti (CERT-AM) come raccomandato dalla direttiva 16 gennaio 2002 e, soprattutto, come suggerito dall'elevato numero di vulnerabilità su prodotti commerciali scoperte negli ultimi anni (più di 2500 solo nel 2004) e dal crescente numero di minacce (20.000 nuovi *malicious code* solo nel 2004).

6.5 Continuità operativa (Business continuity)

Di seguito nella tabella sono descritte le modalità previste dalle amministrazioni per garantire la continuità operativa in caso di incidenti, che pregiudichino la disponibilità del sistema informativo.

Tabella 47 – Stato della continuità operativa (business continuity), anno 2004

QUESITI	NUMERO AMMINISTRAZIONI (SI)	%
Esistenza di un piano formalizzato per la continuità operativa[45]	19	37
Esistenza di procedure operative da attivare in caso di indisponibilità parziale dei servizi applicativi	38	75
– senza specificazione della copertura	*24*	*47*
– solo per le applicazioni più importanti	*14*	*27*
Esistenza di un piano di disaster recovery	29	57
– senza specificazione della copertura	*16*	*31*
– solo per le applicazioni più importanti	*13*	*25*

Come detto nelle considerazioni iniziali, i dati inerenti gli aspetti della continuità operativa delle infrastrutture informatiche, anche se percepiti generalmente nella loro corretta importanza (questo è rilevato non solo dai dati di consuntivo qui presentati, ma anche in altri contesti comunicativi e formativi proposti dal Cnipa) presentano qualche elemento contraddittorio. Il dato rilevante è che il 75% delle Amministrazioni dichiara di avere procedure da attivare in caso di indisponibilità, anche parziale, dei servizi applicativi. Ma, come pure detto, il 31,6% di queste Amministrazioni non dichiara di avere effettuato un'analisi dei rischi, così come non lo dichiara il 34,5% delle Amministrazioni che afferma la presenza di un piano di *disaster recovery*. Questa situazione porta a considerare necessaria un'opera di sostegno e supporto organizzativo e formativo, ancora prima che strettamente tecnico, alle amministrazioni.

[45] Insieme di piani, procedure, organizzazione, risorse hw, sw e di rete, che hanno lo scopo di contrastare le interruzioni ai processi (almeno quelli critici) di business che derivano dagli effetti negativi di gravi guasti/malfunzionamenti/eventi disastrosi.

7. Organizzazione e processi per l'ICT

La collocazione organizzativa della struttura, preposta allo sviluppo dei sistemi informativi automatizzati, continua a rimanere inadeguata in molte amministrazioni. Questa struttura in alcune di esse ha un ruolo gestionale e in altre ancora un ruolo strumentale, mentre, in nessuna amministrazione ha un evidente ruolo di supporto alle strategie.

Dopo alcuni anni di stasi riprende la crescita del numero degli addetti ICT, anche se in molte amministrazioni si registra ancora una carenza di personale informatico capace d'indirizzare, governare e controllare gli interventi sui sistemi informativi e di raccordarli con le trasformazioni organizzative. Questa carenza non è facilmente colmabile, stante la difficoltà delle amministrazioni di acquisire nuove risorse dall'esterno in maniera permanente. Se si aggiunge anche la carenza di formazione funzionale alla creazione di nuove competenze specialistiche, il quadro complessivo permane piuttosto critico. Nell'anno la formazione ha coinvolto principalmente i nuovi addetti all'ICT in quanto registra un aumento della percentuale di tempo dedicata alla formazione, una diminuzione degli allievi coinvolti e una riduzione della spesa.

7.1 Struttura organizzativa per l'ICT

Nelle amministrazioni la collocazione organizzativa della struttura preposta allo sviluppo dei sistemi informativi automatizzati indica indirettamente la funzione che questa struttura ha all'interno dell'amministrazione. In particolare, tale struttura ha una funzione di supporto alle strategie nel caso in cui si collochi tra la parte di indirizzo e la struttura operativa dell'amministrazione, mentre riveste un rilevante ruolo gestionale operativo quando si trovi tra le unità organizzative di primo livello. D'altra parte, la collocazione tra le unità organizzative di secondo livello, la porta ad assumere funzioni tipicamente strumentali.

Di seguito si riportano alcuni esempi di diversa collocazione di questa struttura e casi di modifiche organizzative apportate nel corso dell'anno.

Nel corso del 2004 è stato definito il nuovo assetto organizzativo e la nuova dotazione organica dell'Inpdap. Per la parte informatica è stata creata una struttura denominata "Area Organizzazione, Formazione e Sistemi Informativi" che accorpa la Direzione sistemi informativi e telecomunicazioni e la Direzione centrale organizzazione e formazione.

L'attuale struttura organizzativa del Lavoro, il cui riassetto è iniziato nel 2003, definisce le Direzioni Generali come Unità organizzative di primo livello coordinate dal Segretario Generale. La struttura per l'informatica è inserita nella Direzione Generale delle reti informative e dell'Osservatorio del mercato del lavoro e dal 2001 si articola in quattro divisioni (pianificazione e sviluppo; gestione; reti di comunicazione; sicurezza).

È denominata "Coordinamento, Organizzazione e Sistemi" in Enac la struttura organizzativa per l'informatica, che è suddivisa in tre settori (servizio sviluppo; ufficio gestione sistemi informatici e telematici; ufficio metodi, procedure, processi e flussi documentali) a questi va aggiunto il Responsabile del Coordinamento, coadiuvato da una risorsa con compiti amministrativi/segretariali.

Per l'Enea, vista la specificità dell'Ente, sono presenti due macro strutture, l'Unità programmatica calcolo e modellistica e il Servizio centralizzato informatica e reti, per supportare le unità organizzative dell'Ente. Alcune di queste unità, in funzione della loro complessità e di specifiche attività programmatiche, sono dotate di propri nuclei di supporto.

Nelle amministrazioni particolarmente complesse per dimensione, numero di unità organizzative e presenza territoriale (Beni culturali, Amministrazione finanziaria, Giustizia, Infrastrutture, Difesa, Interno, ecc.) e in quelle dove sono presenti entità dotate di un ampio grado d'autonomia (Agenzie, Dipartimenti, Soprintendenze, ecc.) per la struttura organizzativa, preposta allo sviluppo dei sistemi informativi automatizzata, si rilevano difficoltà di coordinamento o di integrazione

rispetto all'unicità del sistema. Difficoltà di integrazione e di coordinamento si manifestano, a maggior ragione, nei Ministeri che sono stati accorpati nel 2001. In questi Ministeri, i preesistenti sistemi informativi automatizzati, rimangono ancora separati e gestiti in modo autonomo rispetto al nuovo sistema organizzativo. La mancata integrazione produce ovviamente difficoltà operative, ridondanze e diseconomie di gestione. Si tratta dei casi dei seguenti Dicasteri, quali:

- le Attività produttive, che hanno accorpato le attività dell' Ex-Ministero dell'industria, commercio ed artigianato e dell'Ex-Ministero del commercio estero nonché di interi settori di altre amministrazioni. L'attuale struttura per l'informatica è inserita nella Direzione Generale Servizi Interni[46] ed è articolata in tre uffici ("Mercato, reti e Gabinetto", "Imprese" e "Internazionalizzazione"). Benché sia trascorso oltre un anno, non è stato ancora nominato il Responsabile per i sistemi informativi automatizzati;
- le Infrastrutture, che hanno accorpato l'ex-Ministero dei trasporti e della navigazione e l'ex-Ministero dei lavori pubblici. La struttura preposta all'informatica è inserita nella Direzione Generale[47] "Sistemi informativi e statistica", che a sua volta comprende cinque divisioni (Affari generali personale e controllo di gestione; Pianificazione, organizzazione, servizi Internet e Intranet; Sviluppo sistemi informativi e reti informatiche; Gestione approvvigionamenti; Servizi statistici dell'amministrazione). Per garantire il governo unitario dei processi di innovazione e il coordinamento delle attività a livello interdipartimentale si sta istituendo il "Comitato per la Digitalizzazione dei Processi".

7.2 Dimensioni, attività e capacità di governo

Il numero degli addetti ICT registra un incremento del 12% rispetto al 2003, così come il rapporto con il numero dei dipendenti informatizzabili che passa dal 4,6% del 2003 al 5,1% del 2004.

Tabella 48 – Addetti ICT, numerosità e percentuale su dipendenti informatizzabili, anni 2003 e 2004

Amministrazioni	Addetti ICT		Addetti ICT su dipendenti informatizzabili (%)	
	2003	2004	2003	2004
Amministrazioni centrali	21.998	23.939	4,8	5,2
Enti	2.335	3.328	3,3	4,2
Tutte	**24.333**	**27.267**	**4,6**	**5,1**

Seppur in maniera contenuta, cresce anche il rapporto tra gli addetti *Full Time Equivalent* (FTE)[48] e il numero dei dipendenti informatizzabili (da 3,1% del 2003 al 3,2% del 2004). Questo rapporto, distinto per le unità organizzative centrali e per quelle periferiche, è più elevato al centro (7%) che in periferia (2,5%). La differenza tra centro e periferia, e tra gli addetti ICT e quelli FTE è dovuta spesso, specie nelle amministrazioni con ampia articolazione territoriale, alla necessità di avere un punto di riferimento (*focal point*) in periferia sia per le attività di "problem management", sia per quelle di "change management".

[46] L'attuale struttura del Ministero è articolata in dodici centri di costo, corrispondenti ad altrettante Unità Organizzative Centrali (undici Direzioni Generali oltre gli Uffici di Gabinetto e di diretta collaborazione del Ministro).

[47] Questa direzione è inserita in uno dei quattro dipartimenti in cui è diviso il Ministero. Diciannove sono complessivamente le direzioni generali.

[48] Un addetto Full Time Equivalent (FTE) è un addetto che dedica tutto il suo tempo lavorativo disponibile ad una sola attività. Il tempo disponibile è 7 ore e 12 minuti per un giorno di lavoro (giorno persona) e di 220 giorni per un anno di lavoro (anno persona).

Tabella 49 – Addetti ICT, anni persona e percentuale su dipendenti informatizzabili, anno 2004

Amministrazioni	Addetti ICT (anni persona)			Addetti ICT (anni persona) su dipendenti informatizzabili (%)		
	Centro	Periferia	Totale	Centro	Periferia	Totale
Amministrazioni centrali	4.532	10.154	14.686	6,8	2,6	3,2
Enti	1.204	1.325	2.529	7,9	2,1	3,2
Tutte	**5.736**	**11.479**	**17.215**	**7,0**	**2,5**	**3,2**

La distribuzione percentuale per tipologia di attività, distinte tra centro e periferia, evidenzia come al centro prevalgano le attività di governo del sistema (inteso come coordinamento, pianificazione e controllo, e gestione progetti e contratti dei sistemi) e quelle rivolte alla realizzazione di progetti (inteso come studio e progettazione, sviluppo software e avviamento e messa in produzione). Mentre, in periferia prevalgono le attività di gestione e conduzione dei sistemi (gestione sistemi, gestione reti, acquisizione dati, assistenza utenti).

Tabella 50 – Attività degli addetti ICT, anni 2003 e 2004 (distribuzione percentuale)

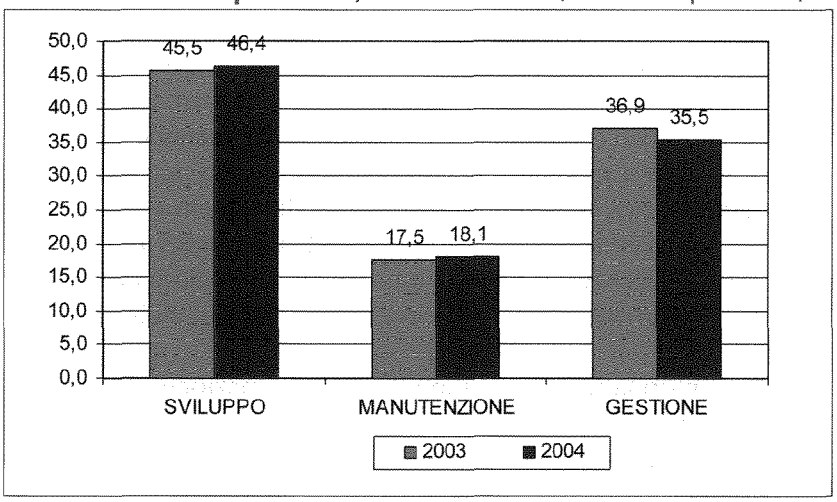
Attività	Amministrazioni centrali				Enti				Tutte			
	Centro		Periferia		Centro		Periferia		Centro		Periferia	
	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004
Studi e progettazione	13	12	3	4	11	11	3	4	13	12	3	4
Sviluppo software	8	8	3	3	14	13	16	12	9	9	5	4
Avviamento e messa in produzione	7	5	5	2	5	5	4	8	7	5	5	2
Manutenzione hardware	3	5	8	14	1	1	–	–	3	4	7	13
Manutenzione software di base e ambiente	7	5	7	5	4	4	–	–	6	4	6	5
Manutenzione adeguativa correttiva del software ad hoc	6	5	4	3	11	9	16	11	7	6	5	4
Gestione sistemi	14	14	11	22	17	16	35	25	15	14	14	23
Gestione reti	10	10	17	12	8	9	7	4	9	10	16	11
Acquisizione dati	4	4	25	8	1	1	–	14	3	3	21	8
Assistenza utenti	9	10	10	17	8	9	15	18	9	10	11	17
Totale attività di sviluppo, gestione e manutenzione	**81**	**78**	**91**	**91**	**80**	**79**	**96**	**96**	**81**	**78**	**92**	**91**
Attività di governo del sistema	**19**	**22**	**9**	**9**	**20**	**21**	**4**	**4**	**19**	**22**	**8**	**9**
Totale attività	**100**	**100**	**100**	**100**	**100**	**100**	**100**	**100**	**100**	**100**	**100**	**100**

Nelle amministrazioni alla carenza di addetti ICT si supplisce con l'acquisizione di risorse professionali dall'esterno. Il grafico seguente mette in evidenza la percentuale di risorse professionali esterne dedicate alle attività di sviluppo, manutenzione e gestione. Per effettuare la stima è stato applicato alla spesa per l'acquisizione di risorse professionali un fattore di correzione sulla base del mix di figure professionali presenti nelle varie attività[49]. Da un'attenta analisi emerge che le amministrazioni registrano una lieve crescita delle risorse esterne destinate alle attività di sviluppo

[49] Le spese dichiarate dalle amministrazioni sono state normalizzate, ossia divise per un fattore proporzionale relativo all'impiego di tre tipi di risorse esterne: il programmatore, l'analista e il capo progetto. Le spese di sviluppo sono normalizzate secondo un fattore 120 relativo alla figura dell'analista. Le spese per attività di manutenzione secondo un fattore 100 relativo alla figura del programmatore e le spese di gestione per un fattore 105 relativo ad un mix di figure. L'ultimo fattore si ottiene considerando che per le attività di gestione sono impiegate sia risorse Capo progetto relative alle attività di governo e coordinamento dei sistemi sia risorse di profilo normale per le attività di gestione.

(dal 45,5% del 2003 al 46,4% di quest'anno), mentre diminuiscono quelle destinate alle attività di gestione (dal 36,9% del 2003 al 35,5%).

Figura 9 – Stima delle risorse esterne per attività, anni 2003 e 2004 (distribuzione percentuale)



Il livello di informatizzazione e, di conseguenza il livello di standardizzazione delle procedure a supporto delle attività di governo del sistema informativo automatizzato forniscono un'indicazione della maturità organizzativa. Il ricorso parziale (o nullo) a strumenti gestionali di pianificazione e controllo causa spesso una gestione del sistema informatico non efficace.
Nell'ultimo anno sono aumentate le amministrazioni che utilizzano strumenti di supporto automatizzati per la pianificazione (dall'82% nel 2003 all'84% del 2004) e per l'*asset management* (dal 73% nel 2003 al 76% del 2004) e cresce il livello di informatizzazione (da parziale a elevato) per tutte le procedure.

Tabella 51 – Livello di informatizzazione procedure a supporto delle attività di governo del sistema, anni 2003 e 2004

Amministrazioni	Pianificazione				Asset management				Misurazione e controllo attività				Project management			
	Parziale		Elevata		Parziale		Elevata		Parziale		Elevata		Parziale		Elevata	
	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004
Amministrazioni centrali	17	16	6	7	15	14	6	7	15	16	7	7	18	17	5	5
Enti	17	16	2	4	15	15	1	3	13	10	2	4	15	15	2	3
Tutte	**34**	**32**	**8**	**11**	**30**	**29**	**7**	**10**	**28**	**26**	**9**	**11**	**33**	**32**	**7**	**8**

A titolo esplicativo si riportano le attività effettuate dagli addetti ICT di tre amministrazioni.

Per la Corte dei conti gli addetti svolgono prevalentemente attività di gestione dei progetti e dei relativi contratti. Predispongono, inoltre, studi di fattibilità e capitolati tecnici, in vista delle relative gare d'appalto. Nelle sedi periferiche i referenti informatici sono coinvolti prevalentemente in attività di avviamento e messa in produzione dei sistemi e loro gestione minimale.

Per il Cnr gli addetti sono coinvolti prevalentemente nella fascia alta del processo di sviluppo, ed in particolare nella progettazione, nella pianificazione delle soluzioni, nella gestione e nel coordinamento sia delle attività di sviluppo che delle attività di *testing* nelle diverse fasi di rilascio.

Per l'Ipost gli addetti svolgono principalmente attività di interfacciamento con il fornitore esterno e con i servizi interni.

7.3 Formazione

Dopo una flessione registrata nel 2003, aumenta lievemente la percentuale di tempo dedicata alla formazione degli addetti ICT[50], che passa da 1,1% a 1,2%, in particolare: per le amministrazioni centrali l'impegno è stato dell'1,1% (circa 2,5 giornate di formazione per addetto), mentre per gli enti è stato dell'1,8% (circa 4 giornate), nel 2003 la formazione per addetto era stata complessivamente di circa 2 giornate per le amministrazioni centrali e di circa 5 giornate per gli enti. Nel 2004 cresce, peraltro, la formazione per addetto presso l'Ambiente (di 14 giornate sul 2003), presso il Consiglio di Stato (di 6 giornate) e presso l'Inps (di circa 4,5 giornate) mentre diminuisce alle Comunicazioni (di circa 3 giornate), all'Aci (di circa 17,5 giornate), all'Inail (di circa 5 giornate) e all' Ipost (di 3 giornate).

Il numero degli allievi informatici coinvolti in attività di formazione, diminuisce del 14,5%, passando da 10.821 individui nel 2003 a 9.252 individui nel 2004. Anche la spesa per la formazione degli addetti ICT diminuisce complessivamente del 32,5%, passando dai 3,8 milioni di euro del 2003 ai 2,6 milioni del 2004.

Tabella 52 – Impegno degli addetti ICT in formazione, anni 2003 e 2004

Amministrazioni	Impegno degli addetti ICT in formazione (%)	
	2003	2004
Amministrazioni centrali	1,0	1,1
Enti	2,4	1,8
Tutte	**1,1**	**1,2**

7.4 Rapporti con gli utenti interni[51]

I rapporti di cooperazione e di comunicazione tra gli utenti del sistema e il settore ICT possono considerarsi soddisfacenti.

Durante lo sviluppo progettuale, trentasei amministrazioni utilizzano procedure formalizzate (+1 rispetto al 2003) per coinvolgere l'utente almeno nelle fasi di definizione dei requisiti funzionali e di qualità nonché di verifica della rispondenza del prodotto sviluppato alle specifiche definite.

Trentanove amministrazioni su 51 (due in più rispetto al 2003) dichiarano di avere canali "formalizzati" di comunicazione con gli utenti.

La struttura di assistenza utenti (help desk) esiste in quasi tutte le amministrazioni (48 su 51). Rispetto al 2003, si estendono le strutture che offrono assistenza a tutte le procedure (da 30 nel 2003 a 32 nel 2004). A titolo di esempio si riportano le funzioni della struttura di help desk centralizzato della Corte dei conti. Il servizio, affidato in outsourcing, fornisce assistenza sistemistica e assistenza di primo livello sugli applicativi in esercizio (Sisp, Protocollo Informatico, Pegaso, Biblioteca, ecc.).

[50] Tale valore è calcolato dividendo il numero delle giornate allievo con la disponibilità complessiva degli addetti ICT, calcolata moltiplicando il numero di addetti ICT per 220 giorni lavorativi.

[51] Per utenti si intende l'insieme dei dipendenti informatizzabili meno il numero degli addetti all'ICT-FTE.

Tabella 53 – Procedure di rapporto con gli utenti, anni 2003 e 2004

Amministrazioni	Meccanismi di coinvolgimento nello sviluppo		Canali comunicazione dedicati		Struttura per l'assistenza utenti (help-desk)			
	2003	2004	2003	2004	2003		2004	
					parziale	elevata	parziale	elevata
Amministrazioni centrali	19	19	20	20	7	19	6	19
Enti	16	17	17	19	11	11	10	13
Tutte	**35**	**36**	**37**	**39**	**18**	**30**	**16**	**32**

Diminuisce la percentuale di tempo dedicata alla formazione da parte degli utenti, che passa da circa quattro ore e mezza del 2003 a circa quattro ore del 2004, anche se aumenta il numero complessivo di utenti coinvolti nella formazione, passando da 76.857 a 89.671 (+16,7% rispetto al 2003). Questo numero complessivo di utenti coinvolti nella formazione rappresenta circa il 16,5% dei dipendenti informatizzabili. Appare ancora sottodimensionato il numero delle giornate allievo a causa della mancata valorizzazione delle ore di formazione fruite dagli utenti in modalità e-learning.

La spesa destinata alla formazione degli utenti rimane nel complesso stazionaria (6,69 milioni di euro del 2003, 6,72 milioni di euro nel 2004) anche se in molti casi sottostimata. Questa sottostima deriva:

- dalla difficoltà di scorporare la componente formazione e addestramento utenti dai contratti per l'acquisizione di beni e servizi;
- dall'esistenza in molte amministrazioni di un'unità organizzativa interna preposta alla formazione, che determina un centro di costo diverso da quello per l'informatica (ad es. per l'Inail, l'Inps e il Dpf);
- dai costi sostenuti da organismi pubblici esterni (ad es. il Cnipa).

A titolo di esempio sulla formazione, si riporta il caso dell'Ipost, il cui contratto per la realizzazione del nuovo sistema informativo prevede la formazione specifica per ciascuna delle componenti applicative realizzate. Inoltre, l'Istituto ha stipulato un contratto con una società per la fornitura di servizi di formazione basati sia su corsi tradizionali in aula, sia su forme innovative di formazione interattiva multimediale. In questo ambito sono stati realizzati corsi multimediali basati su internet streaming per l'informatica individuale, mentre per le principali funzionalità applicative sono stati realizzati corsi *Web-Based Training* e sono stati messi a disposizione di tutti gli utenti sulla intranet.

Tabella 54 – La formazione degli utenti, anni 2003 e 2004

Amministrazioni	Tempo dedicato (%)	
	2003	2004
Amministrazioni centrali	0,26	0,21
Enti	0,20	0,26
Tutte	**0,25**	**0,22**

8. Introduzione delle tecnologie emergenti

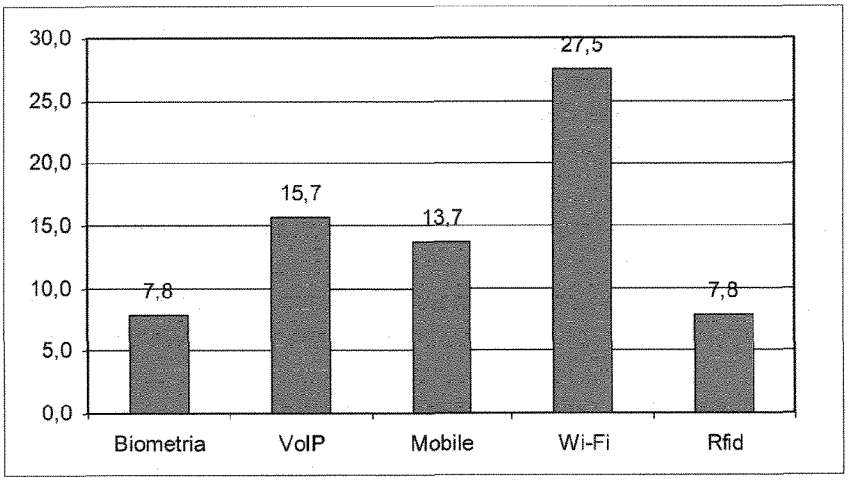
Nella rilevazione annuale sullo stato dell'informatizzazione della pubblica amministrazione centrale è stato inserito un nuovo modulo denominato "Nuove tecnologie". Tale inserimento è volto a verificare l'effettivo stato di penetrazione e l'interesse delle amministrazioni rispetto ad alcune tecnologie emergenti.

Di seguito sono riportati i risultati dell'indagine effettuata su 51 amministrazioni.

I grafici riportati evidenziano in valore percentuale il numero delle amministrazioni che hanno risposto affermativamente ai quesiti proposti. In particolare, i primi tre grafici evidenziano in un'ottica di breve periodo quale sia attualmente il livello di penetrazione delle varie tecnologie.

In particolare, il primo mostra che la tecnologia più utilizzata dalle amministrazioni è il Wi-Fi (27,5%) seguita da VoIP e dal Mobile.

Figura 10 – Percentuale di amministrazioni che utilizzano queste tecnologie, anno 2004



Il secondo grafico mostra in valore percentuale il numero di amministrazioni che hanno in corso di realizzazione progetti riguardanti principalmente la tecnologia Wi-Fi (23,5%), e quella VoIP e *Mobile.*

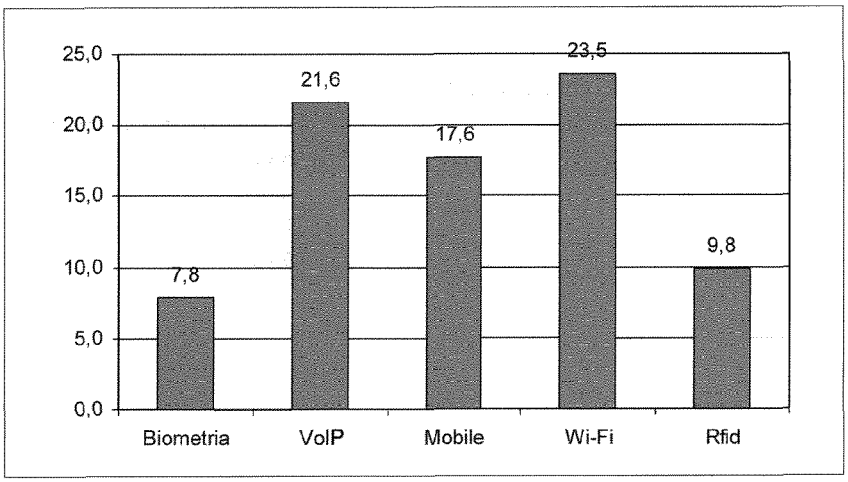



Figura 11 – Percentuale di amministrazioni che hanno progetti in corso, anno 2004