MINISTERO DELLA GIUSTIZIA

DECRETO 24 maggio 2001

Regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia
(Pubblicato sulla GU n. 128 del 5/6/2001)

IL MINISTRO DELLA GIUSTIZIA

Vista la legge 2 dicembre 1991, n. 399, recante "Delegificazione delle norme concernenti i registri che devono essere tenuti presso gli uffici giudiziari e l'amministrazione penitenziaria";

Visto il decreto legislativo 12 febbraio 1993, n. 39, recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, ai sensi dell'art. 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421";

Visto il decreto del Presidente della Repubblica 28 ottobre 1994, n. 748, recante il regolamento sulle modalita' applicative del decreto legislativo 12 febbraio 1993, n. 39, in relazione all'amministrazione della giustizia;

Visto l'art. 15, comma 2, della legge 15 marzo 1997, n. 59, sulla validita' ed efficacia degli atti e documenti formati con strumenti informatici e telematici;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

Visto il decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato nella Gazzetta Ufficiale del 15 aprile 1999, n. 87, avente per oggetto le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici;

Visto il decreto del Ministro della giustizia 27 marzo 2000, n. 264, pubblicato nella Gazzetta Ufficiale del 26 settembre 2000, n. 225, recante il regolamento sulla tenuta dei registri presso gli uffici giudiziari;

Visto l'art. 1, comma 1, lettera f), del citato decreto n. 264 del 2000, che prevede l'emanazione di regole procedurali;

Visto il parere reso dall'autorita' per l'informatica nella pubblica amministrazione in data 24 aprile 2001;

Consultato il Garante per la protezione dei dati personali;

Decreta:

Art. 1.

1. Il presente decreto stabilisce le regole procedurali di cui all'art. 1, comma 1, lettera f), del decreto ministeriale 27 marzo 2000, n. 264, relative ai registri informatizzati tenuti, a cura delle cancellerie o delle segreterie, presso gli uffici giudiziari, ovvero ai registri previsti da codici, da leggi speciali o da regolamenti, comunque connessi all'espletamento delle attribuzioni e dei servizi svolti dall'amministrazione della giustizia.

2. Per le modalita' di tenuta informatizzata dei registri e per la sottoscrizione con firma digitale dei documenti informatici si tiene conto anche delle regole tecniche emanate ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

3. Le regole procedurali di cui al comma 1 sono riportate nell'allegato al presente decreto.

Roma, 24 maggio 2001

Il Ministro: Fassino

Allegato ex art. 1

REGOLE PROCEDURALI PER LA TENUTA DEI REGISTRI INFORMATIZZATI DEGLI UFFICI

Capo I
Definizioni e principi generali

Art. 1.
Sistema informativo

1. Il sistema informativo e' definito come l'insieme delle risorse umane, delle regole organizzative, delle risorse hardware e software (applicazioni e dati), dei locali e della documentazione (sia in formato cartaceo, sia elettronico) che, nel loro complesso, consentono di acquisire, memorizzare, elaborare, scambiare e trasmettere informazioni inerenti i registri informatizzati degli uffici.

2. Ai fini delle presenti regole procedurali assumono rilevanza particolare le seguenti componenti del sistema informativo:

a) il sottosistema delle risorse umane, cioe' le persone che gestiscono e utilizzano il sistema;

b) il sottosistema dell'infrastruttura logistica, costituito dai locali in cui sono localizzati i sottosistemi di cui alle lettere seguenti;

c) il sottosistema delle postazioni di lavoro, costituito dagli apparati hardware, dal software di base (sistemi operativi) e dal software di accesso alle basi di dati;

d) il sottosistema applicativo, costituito dal software sviluppato specificamente per l'informatizzazione degli uffici nonche' dagli apparati hardware, dal software di base (sistemi operativi) e dal software di gestione delle basi di dati;

e) il sottosistema dei dati, costituito dall'insieme delle basi di dati e dei file in cui sono conservati i documenti di pertinenza dell'ufficio;

f) il sottosistema di connessione interna o rete locale, costituito dall'hardware e dal software utilizzati per la connessione delle postazioni di lavoro (cablaggio, apparati di rete attivi e passivi, software di gestione rete, ecc.);

g) il sottosistema di connessione con l'esterno, costituito dall'hardware e dal software utilizzati per la connessione della rete locale con il mondo esterno (firewall, router, modem, linea, ecc.);

h) il sottosistema dei servizi di rete, costituito dall'hardware e dal software che tramite la rete realizzano funzioni tese a facilitare lo svolgimento di operazioni comuni o ripetitive tra utenti e utenti, tra utenti e applicazioni nonche' tra applicazioni ed applicazioni (DHCP, DNS, E-MAIL, DMZ, SICAP, ecc.).

3. Le componenti dedicate esclusivamente all'ufficio, specificate al comma 2, lettere c), d), e), insieme con le relative quote di pertinenza dei sottosistemi delle risorse umane e dell'infrastruttura logistica, costituiscono il sistema informativo dell'ufficio.

4. Le risorse condivise, specificate al comma 2, lettere f), g), h), insieme con le relative quote di pertinenza dei sottosistemi delle risorse umane e dell'infrastruttura logistica, costituiscono il sistema informativo di edificio.

Art. 2.
Caratteristiche del sistema informativo

1. Il sistema informativo soddisfa le seguenti proprieta':

a) disponibilita': le informazioni ed i servizi sono a disposizione degli utenti del sistema, compatibilmente con i livelli di servizio prestabiliti;

b) integrita': le informazioni ed i servizi possono essere creati, modificati o cancellati solo dalle persone autorizzate e secondo modalita' predefinite;

c) autenticita': la provenienza dei dati e' garantita e asseverata;

d) controllo degli accessi: le informazioni possono essere fruite solo ed esclusivamente dalle persone autorizzate a compiere tale operazione.

Art. 3.
Responsabile della tenuta dei registri

1. Il dirigente amministrativo dell'ufficio e' il responsabile della tenuta dei registri e provvede alla stesura del piano della sicurezza di cui al successivo art. 7, secondo le indicazioni dell'ufficio del responsabile per i sistemi informativi automatizzati (di seguito URSIA), vigilando sulla sua applicazione.

Art. 4.
Amministratore di sistema

1. L'amministratore di sistema assicura la conduzione operativa del sistema informativo, effettuando tutte le operazioni necessarie a garantire le proprieta' di cui all'art. 2.

2. I compiti dell'amministratore di sistema sono svolti da una o piu' figure professionali del settore della professionalita' informatica a seconda delle dimensioni degli uffici e del numero degli edifici.

3. Un unico soggetto puo' svolgere tali funzioni per piu' uffici o per piu' edifici.

4. L'URSIA provvede a designare i soggetti di cui ai commi 2 e 3 del presente articolo e, qualora riguardi un ufficio giudiziario appartenente ad un distretto, lo individua fra gli esperti informatici del competente coordinamento dei sistemi informativi automatizzati (di seguito CISIA); nel caso in cui non siano disponibili tali risorse, si ricorre a tecnici informatici esterni.

5. Nel caso siano stati individuati piu' soggetti per lo svolgimento delle funzioni di amministratore di sistema, l'URSIA designa il coordinatore.

Art. 5.
Utenti interni ed esterni

1. L'insieme degli utenti interni e' costituito dal personale dell'ufficio abilitato all'accesso al sistema informativo.

2. Gli utenti interni operano secondo le prescrizioni indicate, nel capo V e nel manuale per l'utente di cui all'art. 22, comma 2.

3. L'insieme degli utenti esterni e' costituito dai soggetti, non appartenenti al personale dell'ufficio stesso, i quali sono abilitati da norme di legge e di regolamento all'utilizzo dei servizi telematici dell'ufficio .

Capo II
Misure di tipo organizzativo

Art. 6.
Identificazione delle componenti del sistema informativo

1. E' cura del responsabile della tenuta dei registri, con l'ausilio dell'amministratore di sistema, produrre e mantenere aggiornato un dettagliato inventario di tutti gli elementi facenti parte del sistema informativo di sua competenza.

2. Nel caso di piu' uffici nello stesso edificio i capi degli uffici interessati indicheranno il responsabile della tenuta dei registri che dovra' curare l'inventario delle risorse condivise.

3. L'inventario di cui al comma 1 e' aggiornato ogni qualvolta si verifica una variazione qualsiasi nel sistema informativo dell'ufficio o dell'edificio e la sua corrispondenza con la situazione reale e' verificata con cadenza almeno trimestrale. In ogni caso, l'inventario e' gestito in modo tale da risultare sempre aggiornato e corrispondente alla situazione reale.

Art. 7.
Piano per la sicurezza del sistema informativo dell'ufficio e dell'edificio

1. Il responsabile della tenuta dei registri, con la collaborazione dell'amministratore di sistema, provvede alla stesura e all'aggiornamento periodico di un piano per la sicurezza del sistema informativo dell'ufficio, secondo gli standard definiti dall'URSIA.

2. Nel caso di piu' uffici che condividano lo stesso edificio, il piano per la sicurezza e' stilato con la collaborazione, per quanto di competenza, dei responsabili della tenuta dei registri dei singoli uffici.

3. Il piano per la sicurezza contiene almeno le seguenti informazioni:

a) inventario delle risorse, di cui all'art. 6;

b) misure adottate per la protezione fisica delle aree e dei locali interessati, di cui al capo III;

c) misure adottate per il controllo degli accessi, di cui agli articoli 8, 13 e 17;

d) misure di monitoraggio del sistema, di cui all'art. 9;

e) misure adottate per garantire l'integrita' e la disponibilita' dei dati, di cui all'art. 10;

f) misure adottate per garantire la continuita' degli applicativi relativi ai registri informatizzati nel caso in cui si verifichi un mal funzionamento dei server interessati;

g) piano di adeguamento degli applicativi, di cui all'art. 19, comma 9;

h) la frequenza e le modalita' delle procedure di archiviazione ottica e di copia storica dei dati, coerentemente con le indicazioni di cui all'art. 12 del decreto del Ministro della giustizia 27 marzo 2000, n. 264.

4. Il piano per la sicurezza contiene indicazioni circa la necessita' di avere impianti ridondati e con elevata tolleranza ai guasti.

5. Il piano per la sicurezza prevede misure conformi, per quanto attiene al trattamento dei dati personali, a quanto prescritto dal regolamento di cui all'art. 15, comma 2, della legge 31 dicembre 1996, n. 675.

6. La vigilanza sulla predisposizione e sull'applicazione dei piani di sicurezza e' esercitata dai capi degli uffici, secondo le rispettive competenze, avvalendosi anche di un esperto informatico designato dall'URSIA.

Art. 8.
Politica di gestione degli accessi

1. Ai sensi dell'art. 5 del decreto del Ministro della giustizia 27 marzo 2000, n. 264 la procedura di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo, rispetto alle risorse del sistema informatico.

2. Attraverso la procedura di autenticazione si individua un insieme di gruppi di utenti a livello di sistema, a livello di database management system ed a livello di applicativo. A ciascun gruppo di utenti e' associato uno ed un solo profilo mentre a ciascun utente puo' essere assegnato uno o piu' profili.

3. A livello di sistema deve essere definito almeno un gruppo per ciascuna delle figure previste dagli articoli 3, 4 e 5 delle presenti regole procedurali. In corrispondenza di ciascun gruppo e' definito un profilo tale da assegnare a ciascun utente appartenente al gruppo solo ed esclusivamente i privilegi di accesso ed utilizzo strettamente necessari per l'espletamento delle attivita' di propria competenza.

4. Per ciascuna base di dati sono definiti almeno un gruppo amministratori ed un gruppo utenti a livello di database management system. In corrispondenza di ciascun gruppo e' definito un profilo tale da assegnare a ciascun utente appartenente al gruppo solo ed esclusivamente i privilegi di accesso ed utilizzo delle risorse gestite tramite il database management system strettamente necessari per l'espletamento delle attivita' di propria competenza.

5. Per ciascun applicativo e' definito almeno un gruppo per ciascuna delle diverse tipologie di utenza previste da ogni specifico applicativo.

6. La definizione di gruppi aggiuntivi puo' essere decisa dal capo dell'ufficio.

Art. 9.

Monitoraggio del sistema

1. Tutte le attivita' relative all'utilizzo e alla gestione del sistema informativo sono sottoposte ad un processo continuo di controllo e verifica della loro corretta e completa esecuzione. Tale processo trova attuazione innanzitutto attraverso l'utilizzo di appositi strumenti di controllo a livello di sistema, di database management system e di applicativo.

2. Il sistema consente le seguenti misure minime di monitoraggio a garanzia dell'autenticita' e integrita' dei dati:

a) la registrazione di tutti i tentativi di accesso effettuati, riusciti o falliti, a livello di sistema, di database management system e di applicativo;

b) gli accessi in lettura e scrittura effettuati direttamente attraverso il database management system;

c) tutti gli accessi in lettura e scrittura.

3. E' cura dell'amministratore di sistema controllare periodicamente le registrazioni di cui al comma 3, lettere a) e b), allo scopo di rilevare eventuali anomalie e conservare le registrazioni dei log provvedendo alla trascrizione settimanale su supporti non riscrivibili da conservare unitamente ai backup dei registri.

Art. 10.

Disponibilita' dei dati

1. Presso ciascun ufficio sono previste idonee politiche e procedure per il salvataggio (backup) e per il recupero (recovery) dei dati, sia a livello di sistema, sia a livello di database management system.

2. Nell'ambito delle politiche di cui al comma 1 e' prevista la frequenza del salvataggio dei dati che non puo' essere superiore alla settimana.

3. Le procedure di backup consentono di conservare i dati per il tempo previsto dal decreto del Presidente della Repubblica 30 settembre 1963, n. 1409 e mediante l'utilizzo di supporti non riscrivibili, rinnovati a scadenze prestabilite e secondo le regole tecniche emanate dall'autorita' per l'informatica nella pubblica amministrazione a norma dell'art. 6, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

4. Le procedure di backup consentono di effettuare, con frequenza almeno triennale, una copia storica dei dati, che dovra' essere conservata secondo le modalita' di cui al comma 3. Eseguita tale operazione, dal registro in uso possono essere eliminati i dati relativi agli affari esauriti da almeno due anni.

Capo III
Misure di tipo fisico e logico

Art. 11.
Infrastruttura logistica

1. Le macchine server sono collocate in un apposito locale (sala server), dotato di impianto elettrico ed impianto di condizionamento opportunamente dimensionati e adeguatamente protetto dai rischi di incendio e allagamento.

2. L'accesso alla sala server e' consentito sotto la responsabilita' dell'amministratore di sistema.

3. Tutti i server sono asserviti a gruppi di continuita'.

4. I supporti di backup sono custoditi in armadi blindati e ignifughi, posti in locali diversi dalla sala server.

Art. 12.
Software

1. Presso l'ufficio e' possibile installare ed utilizzare esclusivamente software appartenente ad una delle tre seguenti categorie:

a) software commerciale;

b) applicativi di rilevanza nazionale;

c) applicativi realizzati a livello locale.

2. L'installazione di software diverso da quello indicato alle lettere a) e b) del comma 1 e' autorizzata dal capo dell'ufficio nel rispetto di quanto previsto dall'art. 18, commi 4 e 5.

3. E' possibile installare ed utilizzare software commerciale solo se munito di idonea licenza d'uso, ovvero se fornito, nell'ambito di accordi-quadro a livello nazionale, dall'URSIA.

4. Relativamente agli applicativi realizzati a livello locale e' possibile installare ed utilizzare solo quelli dei quali sia stata verificata la conformita' secondo le procedure di cui all'art. 18.

5. Il software e' installato solo ed esclusivamente a partire da supporti fisici originali, ovvero da supporti fisici per i quali sia nota e sicura la provenienza.

Art. 13.
D a t i

1. Gli archivi informatici sono gestiti tramite software per la gestione di basi di dati (database management system).

2. Il piano per la sicurezza indica una strategia di adeguamento degli eventuali software diversi da quello indicato al comma 1.

3. L'accesso ai dati degli archivi informatici avviene solo ed esclusivamente per il tramite degli applicativi appartenenti al sottosistema applicativo, fatta eccezione per gli amministratori delle basi di dati relative all'archivio stesso, per i quali vale quanto prescritto dal comma 4.

4. L'accesso ai dati degli archivi informatici, da parte degli amministratori di basi di dati, avviene solo ed esclusivamente per il tramite degli strumenti messi a disposizione dal relativo database management system. Tutte le operazioni effettuate, da parte degli amministratori delle basi di dati sono soggette a registrazione, secondo quanto previsto all'art. 9, comma 1, lettera a). Le registrazioni di tali operazioni sono salvate su supporto fisico contestualmente alle ordinarie operazioni di backup e conservate per un periodo non inferiore a due anni.

Art. 14.
Gestione delle utenze

1. L'amministratore di sistema e i suoi collaboratori, ciascuno per quanto di competenza, effettuano le seguenti operazioni:

a) creazione delle utenze e dei gruppi, secondo quanto previsto agli articoli 8 e 19;

b) assegnazione di nome utente e parola chiave a ciascun utente;

c) mantenimento di un elenco completo dei gruppi e delle utenze. Per ciascun gruppo sono indicati almeno l'identificativo, la data di creazione, la lista dei privilegi e l'eventuale data di disabilitazione; per ciascun gruppo sono indicati almeno il nome e il cognome, i gruppi di appartenenza, la data di creazione e la data di disabilitazione.

2. Le utenze non possono essere cancellate, ma solo disabilitate.

3. Le politiche per l'aggiornamento delle parole chiave sono definite nel piano per la sicurezza.

Art. 15.
Backup e recovery

1. Nel piano per la sicurezza vengono individuati i dati da sottoporre a backup, nonche' le modalita' e la frequenza della procedura.

2. I dati oggetto di backup sono classificati in dati di sistema (necessari per il corretto funzionamento del sistema operativo, del software di base, del database management

system, delle applicazioni installate, ecc.) e dati utente (documenti, fogli elettronici, archivi di posta elettronica, ecc.).

3. L'amministratore di sistema mette a disposizione di ciascun utente un'opportuna quota di spazio su disco disponibile per il backup dei dati utente. L'accesso a ciascuna quota e' tale da consentire l'accesso in lettura e scrittura solo ed esclusivamente all'utente proprietario e l'accesso in sola lettura all'amministratore di sistema. E' cura di ciascun utente provvedere a copiare sulla propria quota di spazio i file che desidera sottoporre a backup.

4. L'amministratore di sistema, secondo quanto indicato nel piano per la sicurezza:

a) garantisce l'effettiva messa in opera delle procedure di backup;

b) verifica l'avvenuta esecuzione dei backup;

c) mantiene un elenco delle operazioni di backup effettuate;

d) archivia i supporti fisici;

e) effettua, in caso di mal funzionamento, le procedure di recovery;

f) effettua verifiche periodiche delle procedure di recovery, secondo quanto disposto dal piano per la sicurezza;

g) mantiene un elenco dei problemi verificatisi e delle operazioni di recovery effettuate.

Art. 16.
Archiviazione ottica

1. Il sistema informatico e' dotato di almeno un sistema per la scrittura di supporti ottici, le cui caratteristiche siano conformi alle regole tecniche emanate dall'autorita' per l'informatica nella pubblica amministrazione a norma dell'art. 6, comma 2, del decreto del Presidente della Repubblica n. 445, del 2000.

2. Le applicazioni consentono l'archiviazione dei documenti in almeno uno dei formati indicati nelle regole tecniche di cui al comma 1.

3. Il sistema di archiviazione consente la generazione dei file di controllo e di chiusura, secondo le regole tecniche di cui al comma 1.

4. L'amministratore di sistema ottempera agli obblighi stabiliti dalle regole tecniche di cui al comma 1.

Art. 17.
Antivirus

1. L'URSIA provvede alla distribuzione periodica a tutti gli uffici di un software antivirus e al suo costante aggiornamento.

2. Il piano per la sicurezza stabilisce le modalita' di

aggiornamento del software antivirus sulle postazioni di lavoro.

Capo IV
Misure relative agli applicativi

Art. 18.
Utilizzo degli applicativi

1. Per la gestione informatizzata dei registri e' possibile utilizzare applicativi di rilevanza nazionale o applicativi realizzati a livello locale.

2. Gli applicativi di rilevanza nazionale sono rilasciati dall'URSIA, che ne certifica la conformita' ai sensi dell'art. 3 del decreto del Ministro della giustizia 27 marzo 2000, n. 264.

3. Nessuna modifica o personalizzazione di applicativi di rilevanza nazionale e' consentita da parte di soggetti diversi dall'URSIA.

4. Gli applicativi realizzati nell'ambito di iniziative locali sono conformi alle regole tecniche ed alle presenti regole procedurali.

5. La conformita' dei programmi alle caratteristiche previste nel presente capo viene certificata dall'URSIA.

Art. 19.
Caratteristiche degli applicativi

1. Gli applicativi di cui all'art. 12, comma 1, lettere b) e c), sono sviluppati da societa' dotate di certificato di qualita' EN ISO 9001, relativo ai servizi di sviluppo di prodotti software (CPV 77207721-7723).

2. Gli applicativi che gestiscono i registri consentono l'estrazione e la stampa dei dati, ai sensi dell'art. 6, comma 3, del decreto del Ministro della giustizia 27 marzo 2000, n. 264.

3. L'applicativo consente, come misura minima relativa all'autenticazione degli utenti, l'accesso ai dati con un meccanismo di autenticazione basato sulla conoscenza di una coppia (username, password).

4. L'autenticazione di cui al comma 3 e' effettuata tramite un meccanismo a sfida che non richieda il transito della password sulla rete.

5. L'autenticazione puo' essere effettuata una sola volta al momento dell'accesso al sistema informatico, oppure essere ripetuta al momento dell'accesso a ciascun programma.

6. L'applicativo fornisce un meccanismo di gestione degli accessi che consente di applicare quanto disposto dagli articoli 8 e 14.

7. L'accesso agli archivi informatici da parte degli utenti e' consentito solo ed esclusivamente tramite le componenti del sottosistema applicativo.

8. L'accesso alle basi di dati da parte degli amministratori di basi di dati e' consentito solo ed esclusivamente tramite l'utilizzo degli opportuni strumenti software di amministrazione.

9. Il piano per la sicurezza indica una strategia di adeguamento degli applicativi che non soddisfino i requisiti di cui ai precedenti commi.

Art. 20.
Documentazione

1. L'applicativo e' accompagnato da apposita documentazione di utilizzo, costituita da un manuale di amministrazione ed un manuale di utilizzo, e disponibile sia in forma cartacea che in forma elettronica.

2. La documentazione elettronica soddisfa i seguenti requisiti:

a) essere consultabile con modalita' del tutto compatibili con quelle disponibili nel sistema operativo utilizzato;

b) consentire una navigazione ipertestuale rispetto a termini e argomenti chiave;

c) permettere di effettuare ricerche per sommario, indice e testo libero;

d) rendere disponibile una modalita' di consultazione dipendente dal contesto, in modo tale da attivare le pagine relative all'argomento corrispondente alla funzionalita' correntemente utilizzata.

3. Il manuale di amministrazione contiene almeno le seguenti informazioni:

a) requisiti hardware e software;

b) procedura di installazione;

c) gestione dei gruppi e degli utenti;

d) procedure operative;

e) procedure di aggiornamento;

f) procedure di backup e recovery;

g) gestione dei mal funzionamenti.

4. Il manuale di utilizzo contiene almeno le seguenti informazioni:

a) descrizione generale dell'applicativo;

b) descrizione della procedura di accesso e di uscita dall'applicativo;

c) modalita' di utilizzo;

d) elenco di tutte le funzionalita';

e) elenco dei possibili messaggi di errore e guida alla risoluzione dei problemi;

f) glossario dei termini.

5. Per ciascuna funzionalita' di cui al comma 4, lettera d), il manuale di utilizzo contiene le seguenti informazioni:

a) finalita' della funzione;

b) modalita' di accesso;

c) prerequisiti per l'utilizzo;

d) descrizione delle maschere che compaiono sul video;

e) dati richiesti dall'applicativo per l'esecuzione.

6. L'applicativo e' corredato dal codice sorgente e da tutta la documentazione tecnica, sia in formato elettronico che cartaceo, prodotta durante l'intero ciclo di vita del software, coerentemente con le norme di qualita' di cui all'art. 19, comma 1.

Art. 21.
Servizi accessori

1. L'applicativo e' corredato da idoneo servizio di manutenzione correttiva ed evolutiva, nonche' da idoneo servizio di assistenza tecnica.

Capo V
Comportamento dell'utente

Art. 22.
Manuale per l'utente

1. L'utente del sistema informativo dell'ufficio e' tenuto ad osservare comportamenti atti a ridurre al minimo i rischi di perdita, danneggiamento o diffusione non autorizzata dei dati a garanzia della integrita' e autenticita' degli stessi.

2. I comportamenti di cui al comma 1 sono descritti negli articoli 23, 24, 25 mentre i comportamenti di maggior dettaglio sono riportati in un apposito manuale per l'utente, da stilare, a cura dell'amministratore di sistema, sulla base delle presenti regole procedurali e del piano per la sicurezza.

Art. 23.
Regole di tipo fisico

1. L'utente e' tenuto, ove sia possibile, a chiudere a chiave la porta del proprio ufficio e a tenere sotto chiave i propri documenti, indipendentemente dal supporto fisico utilizzato.

2. L'utente e' tenuto, allontanandosi momentaneamente dalla postazione di lavoro, a chiudere le applicazioni attive o a proteggerla tramite password del salvaschermo.

3. L'utente e' tenuto, al termine della giornata di lavoro, a spegnere la postazione.

4. L'utente e' tenuto ad assicurarsi dell'identita' e delle autorizzazioni di personale che debba installare il nuovo software o hardware sulla propria postazione di lavoro.

5. L'utente e' tenuto a non utilizzare, su postazioni di lavoro collegate alla rete locale dell'ufficio, modem o altri strumenti di connessione con l'esterno.

Art. 24.
Regole di tipo logico

1. L'utente e' tenuto a non installare sulla propria postazione di lavoro alcun programma non preventivamente autorizzato dal capo dell'ufficio.

2. L'utente puo', qualora lo reputi necessario, configurare o richiedere la configurazione della propria postazione di lavoro in modo che venga richiesta una password all'accensione.

3. Il capo dell'ufficio puo' assegnare all'utente un programma per la cifratura dei dati sul disco rigido, su motivata richiesta scritta di quest'ultimo o per espresse esigenze di ufficio.

4. L'amministratore di sistema, su incarico del responsabile della tenuta dei registri, stabilisce le procedure di utilizzo dei programmi di cui al comma 3.

5. L'utente che utilizzi, per le proprie necessita' di lavoro, un computer portatile:

a) risponde personalmente dei dati sul portatile in dotazione;

b) e' motivato a effettuare la richiesta di cui al comma 3;

c) puo' richiedere all'amministratore di sistema l'assegnazione di una quota disco, di cui all'art. 15, comma 3, per il backup dei dati del portatile;

6. L'utente e' tenuto a non diffondere messaggi di posta elettrnica di provenienza dubbia ed a non partecipare alle cosiddette "catene di S. Antonio" o simili.

Art. 25.
Gestione delle password

1. L'utente e' tenuto:

a) a non rivelare a terzi la propria password;

b) a non scrivere la password in punti facilmente visibili;

c) a digitare la password al riparo da sguardi indiscreti.

2. L'utente sceglie la propria password:

a) diversa dal proprio username;

b) non costituita da una semplice parola rintracciabile in un dizionario;

c) non legata alla propria vita personale;

d) con una lunghezza non inferiore a sei caratteri;

e) contenente almeno un simbolo diverso da una lettera, oppure un misto di lettere maiuscole e minuscole.

3. La password e' cambiata con frequenza almeno annuale.

4. L'amministratore di sistema ha facolta' di stabilire una frequenza di cambio della password superiore a quanto stabilito nel comma 3, nonche' di configurare il sistema e gli applicativi in modo da forzare l'utente al cambio allo scadere del termine fissato.

Capo VI
Disposizioni finali

Art. 26.
Tempi di attuazione

1. I tempi di attuazione delle presenti regole procedurali sono i seguenti, con decorrenza dalla data della loro pubblicazione:

a) entro sei mesi e' preparato il piano di adeguamento degli applicativi di cui all'art. 19, comma 9;

b) entro dodici mesi e' completata la prima versione del piano per la sicurezza di cui all'art. 7;

c) entro diciotto mesi sono adottate presso l'ufficio tutte le prescrizioni relative all'infrastruttura tecnologica di cui al capo III e all'infrastruttura logistica di cui al capo IV;

d) entro tre anni, tutti gli applicativi in uso sono adeguati alle prescrizioni del capo IV e dell'art. 16.