Allegato “A” - Misure di sicurezza generali

1. MISURE ORGANIZZATIVE COMUNI A TUTTI I TIPI DI TRATTAMENTO

1.1 Disposizioni generali per il trattamento dei dati personali

Ogni trattamento di dati personali è consentito alla Provincia, in quanto soggetto pubblico, qualora sussistano i presupposti previsti dall'articolo 18 del d.lgs. 196/03. Esso deve svolgersi nel rispetto delle seguenti indicazioni:

- va privilegiato, ove possibile, il trattamento di dati anonimi;
- se non è possibile il perseguimento delle finalità istituzionali mediante il trattamento di dati anonimi, va comunque garantita l'osservanza del principio di necessità, pertinenza e non eccedenza rispetto alle finalità del trattamento medesimo, ai sensi degli artt. 3 e 11 del Codice (stretta coerenza con la natura dei compiti da svolgere, minimo utilizzo dei dati personali, adozione di modalità di trattamento il meno lesive possibile).

1.2 I ruoli previsti dalla legge

Nell'ambito della pubblica amministrazione, l'applicazione delle norme del Codice comporta l'attribuzione di compiti e responsabilità in capo alle seguenti figure:

- titolare del trattamento (art. 4, c. 1, lett. f, e art. 28 del Codice);
- responsabile del trattamento (art. 4, c. 1, lett. g, e art. 29 del Codice);
- incaricato del trattamento (art. 4, c. 1, lett. h, e art. 30 del Codice);

Il ruolo di amministratore di sistema non è formalmente previsto dalla legge e nell'ambito del d.lgs. 196/03 dal punto di vista strettamente giuridico va considerato come una forma particolare di responsabile del trattamento. E' tuttavia un ruolo tecnico fondamentale per la gestione di ogni sistema informatico e la definizione dei suoi compiti va cercata nell'ambito della prassi delle tecniche informatiche.

Un altro ruolo fondamentale previsto dalla legge è quello di "interessato al trattamento" che viene definito come "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali".

1.2.1 Il titolare

Il titolare, secondo la definizione del Codice, è il soggetto (persona fisica, giuridica, pubblica amministrazione ecc.) investito del potere decisionale circa le attività di trattamento dei dati personali, cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

La Giunta provinciale, con propria deliberazione n. 3216 del 23-12-2002, ha dato atto che **la Provincia Autonoma di Trento** (come persona giuridica) è titolare del trattamento dei dati personali rispetto ai trattamenti funzionali all'esercizio delle proprie competenze istituzionali.

L'individuazione del titolare fa riferimento all'Amministrazione provinciale unitariamente considerata e non alle competenze dei singoli organi o di chi ne abbia la rappresentanza o ne esprima la volontà (Presidente, giunta, dirigenti), in conformità a quanto previsto dall'articolo 28 del Codice che dispone che quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, **titolare del trattamento è l'entità nel suo complesso** o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Nell'esercizio delle funzioni di titolare del trattamento, la Provincia opererà in concreto (come sempre avviene) attraverso gli **organi** ed i soggetti di volta in volta competenti in base alle

disposizioni ordinamentali (Presidente, con particolare riferimento al potere di rappresentanza, Giunta provinciale per quanto riguarda la competenza ad adottare atti generali di carattere organizzativo e procedurale o direttive, dirigenti con riferimento alle decisioni e alle scelte attinenti all'attività gestionale).

1.2.1.1 Affidamento all'esterno di trattamenti

Quando la Provincia si avvale della collaborazione di soggetti esterni alla propria struttura (sulla base di concessioni, appalti, convenzioni, consulenze, collaborazioni, tirocini) molto spesso nell'ambito di questo rapporto accade che vi sia comunicazione ai soggetti esterni di dati personali in possesso della Provincia. Si tratta di una **comunicazione** ai sensi del Codice anche se vi è una semplice autorizzazione all'accesso alle banche dati.

Per gestire questa problematica è necessario che, nell'ambito delle convenzioni o degli atti che disciplinano il rapporto di collaborazione, venga individuato il **ruolo** da attribuire al soggetto esterno nel trattamento dei dati. Il soggetto esterno può essere nominato:

- autonomo titolare
- responsabile
- incaricato.

Se si intende garantire al soggetto esterno ampia autonomia in ordine al trattamento dei dati personali è opportuno individuarlo quale autonomo **titolare** del trattamento. In questo caso la cessione di dati personali da parte della Provincia al collaboratore esterno, anche nella forma dell'accesso alle proprie banche dati, configura **comunicazione** di dati ed è legittimata solo nelle ipotesi di cui all'art. 19 del Codice (cioè se è prevista da norma di legge o di regolamento). Il collaboratore deve adottare, nel trattamento dei dati personali, le misure e le cautele previste dal Codice.

Tuttavia nella maggior parte dei casi la Provincia deve conservare il potere di decidere in ordine alle finalità e modalità del trattamento. In questi casi si dovrà procedere all'individuazione, in forma espressa, del soggetto esterno quale **responsabile** o **incaricato** del trattamento (in relazione al grado di autonomia decisionale e di responsabilità che al medesimo si vuole demandare) ed impartire allo stesso le necessarie **direttive**. Si ricorda che le persone giuridiche possono essere nominate responsabili ma non incaricati.

Nel caso quindi di nomina ad incaricato o responsabile, la cessione di dati personali da parte della Provincia al collaboratore esterno, anche nella forma dell'accesso alle proprie banche dati, non configura comunicazione di dati personali. Il collaboratore esterno, considerato in tal caso alla stregua di un'articolazione organizzativa della Provincia per il trattamento dei dati personali, è soggetto alle regole previste dal Codice per i soggetti pubblici e deve applicare tutte le disposizioni organizzative in vigore per le strutture provinciali.

1.2.2 Il responsabile

Il responsabile del trattamento, ai sensi del Codice, è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

La nomina di un **responsabile** non è necessaria. Tuttavia è auspicabile nelle organizzazioni complesse quali sono le pubbliche amministrazioni.

Il **responsabile** viene designato dal titolare tra coloro che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

1.2.2.1 Adempimenti in materia di misure di sicurezza

Il responsabile:

- procede al trattamento **attenendosi alle istruzioni** impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni in materia di trattamento e delle proprie istruzioni;
- **non svolge meri compiti esecutivi** (come quelli spettanti all'incaricato) ma traduce in

istruzioni operative le scelte strategiche e le direttive generali impartite dal titolare, dettagliandole e riferendole agli specifici contesti lavorativi e di trattamento.

Con deliberazione della Giunta provinciale 23 dicembre 2002, n. 3216, sono stati nominati responsabili per i trattamenti di dati personali relativi alle materie di rispettiva competenza e alle funzioni di gestione amministrativa, finanziaria e tecnica:

- **i dirigenti generali**, laddove gestiscano a titolo esclusivo determinati trattamenti;
- **i dirigenti**, ivi compresi i dirigenti delle Agenzie comunque denominati;
- la Società "**Informatica Trentina SpA**", responsabile (esterno) dei trattamenti dalla stessa effettuati ai fini della gestione del Sistema Informativo Elettronico Provinciale (S.I.E.P.), di cui alla legge provinciale 6 maggio 1980, n. 10, nell'ambito delle prestazioni stabilite dalla convenzione prevista dall'articolo 5, comma 1, della medesima legge;

E' anche possibile la nomina di un responsabile del **trattamento esterno** alla Provincia (persona fisica o giuridica) nei casi relativi a collaborazioni di soggetti esterni per l'espletamento dei compiti d'istituto (concessioni, appalti, convenzioni, consulenze, collaborazioni, tirocini, ecc.).

1.2.2.2 Altri adempimenti del responsabile del trattamento

In via generale, **il dirigente responsabile del trattamento** deve provvedere ai seguenti adempimenti:

1.2.2.2.1 Verifica dei trattamenti:

il responsabile deve:

- verificare che i trattamenti in corso o da intraprendere presso la struttura siano rispondenti a quanto disposto dal Codice: ove difforme dalla norma, il trattamento deve essere adeguato o cessare;
- provvedere ad un **censimento** dei trattamenti presenti nella propria struttura**.**

1.2.2.2.2 Verifica della adeguatezza delle abilitazioni di accesso:

il responsabile deve:

- individuare i **soggetti abilitati** all'accesso alle risorse di rete protette, in relazione ai compiti svolti dal personale;
- verificare - d'intesa con l'amministratore di sistema - che la configurazione e l'utilizzo delle risorse presenti sul **server di rete** della propria struttura (unità logiche, cartelle) sia atta a garantire la riservatezza e l'accesso selezionato alle banche dati contenenti dati personali; la verifica può essere effettuata sulla base delle informazioni che deve comunicare l'amministratore di sistema sulla composizione dei gruppi di utenti e sulle restrizioni di accesso assegnate alle cartelle di lavoro sul server.

1.2.2.2.3 Nomina degli incaricati del trattamento di dati personali:

il responsabile deve:

- provvedere alla nomina degli incaricati di ciascun trattamento;
- impartire agli incaricati, all'atto della loro nomina le necessarie istruzioni operative.

1.2.2.2.4 Osservanza delle misure di sicurezza

Il responsabile deve:

- garantire che il trattamento, la comunicazione e la diffusione dei dati avvenga nel rispetto delle vigenti disposizioni, ivi comprese quelle relative alla sicurezza;
- rispettare le direttive e le misure generali impartite dalla Giunta provinciale in materia di trattamento dei dati personali e di sicurezza, curare gli adempimenti da essa stabiliti (v. delibere n. 3216/2002, n. 7911/1999, n. 3217/2002 ed eventuali altre disposizioni che verranno adottate),
- ottemperare alle istruzioni operative integrative approvate dal dirigente competente in materia di informatica, ai sensi di quanto disposto dalla deliberazione n. 3217/2002,

adottando, nell'ambito della struttura di competenza, le misure organizzative necessarie.

1.2.3 Incaricato

Ai sensi del Codice (art. 4, lettera h), incaricato del trattamento è la persona fisica autorizzata dal titolare a compiere le operazioni di trattamento di dati personali, attenendosi alle istruzioni impartite dal titolare e dal responsabile. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima (art. 30 del Codice).

Possono essere designati incaricati solo e soltanto persone fisiche.

Gli incaricati del trattamento sono nominati dal responsabile/dirigente, ai sensi della lettera d) dell'allegato A della deliberazione della Giunta provinciale 23 dicembre 2002, n.3216 (si vedano indicazioni per la nomina nel paragrafo 4.3.1.2).

L'incaricato procede al trattamento sotto la diretta autorità del titolare o del responsabile, che devono impartirgli istruzioni e vigilare sul suo operato; svolge, nell'ambito del trattamento, meri compiti esecutivi sulla base delle istruzioni operative impartite dal titolare o dal responsabile.

1.2.3.1 Adempimenti dell'incaricato del trattamento

In via generale, l'incaricato del trattamento deve provvedere ai seguenti adempimenti:

- trattare i dati nel rispetto della normativa in materia di tutela della riservatezza ed in particolare dei principi di legittimità, pertinenza, non eccedenza nonché nel rispetto di quanto individuato nel presente documento;

- procedere all'**informativa** agli interessati ai sensi dell'art. 13 del Codice, e verificare che ciascuna operazione di comunicazione e diffusione dei dati sia conforme alle disposizioni di legge e regolamento;
- osservare le disposizioni organizzative e operative impartite dal dirigente/responsabile;
- attuare le misure e gli **interventi per la sicurezza** del trattamento dei dati nell'esercizio dell'attività cui è preposto.

1.2.4 Informativa

L'informativa va data all'interessato cui i dati si riferiscono, secondo le modalità di cui all'art. 13 del Codice.

L'informativa deve essere completa e contenere, sia pure in modo sintetico, tutte le notizie previste dal Codice:

- le finalità del trattamento;
- le modalità del trattamento (strumenti elettronici o manuali, modalità di organizzazione o di raffronto ed elaborazione particolari, creazione di profili per età, professione o altro);
- se il conferimento dei dati richiesti è obbligatorio o facoltativo relativamente agli scopi dichiarati;
- le conseguenze di un eventuale rifiuto a fornire i dati;
- se i dati possono essere ceduti a terzi, in tal caso identificandoli o quanto meno individuando le categorie dei soggetti destinatari;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti di cui all'articolo 7 del Codice;
- i dati identificativi del titolare del trattamento;
- i dati identificativi del responsabile del trattamento.

Nel caso di trattamento di dati sensibili, l'informativa deve inoltre fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base ai quali è effettuato il trattamento.

- ai sensi dell'art. 48 del d. P. R. 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), è obbligatorio inserire l'informativa nella modulistica per la presentazione delle dichiarazioni sostitutive di certificazione e di atto notorio;
- è opportuno comunque inserire l'informativa in via generale nella modulistica relativa alle istanze da presentare all'Amministrazione provinciale.

1.2.5 Amministratore di sistema

L'amministratore di sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

La Giunta provinciale, con propria deliberazione n. 3217 di data 23 dicembre 2002, ha incaricato di nominare gli amministratori di sistema:

1. **Informatica Trentina SpA** per i sistemi operativi presenti su elaboratori in uso presso le strutture provinciali affidati alla gestione della società medesima;
2. **i dirigenti responsabili del trattamento** per i sistemi operativi non gestiti da Informatica Trentina SpA.

1.2.6 Interessato

L'interessato è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (art. 4 lettera i del Codice). E' il soggetto tutelato dalla normativa in materia di privacy.

Per i trattamenti operati dalla pubblica amministrazione l'interessato non è tenuto ad esprimere alcun consenso, purché sussistano i presupposti per il trattamento previsti dagli articoli 18 e 19 del Codice.

Ai sensi del Codice, sono riconosciuti all'interessato i seguenti diritti:

- diritto di informativa al momento della raccolta dei dati (art.13; si veda paragrafo 4.3.1.3.);
- diritto di accesso (art.7);
- diritto di essere informato circa l'esistenza presso l'amministrazione di dati che lo riguardano;
- diritto di essere informato circa i dati identificativi del titolare e del responsabile del trattamento nonché circa le modalità e le finalità del trattamento (art.13);
- diritto ad ottenerne la cancellazione, la trasformazione in forma anonima, il blocco dei dati raccolti illegittimamente, l'aggiornamento, la rettifica o l'integrazione dei dati inesatti (art. 7);
- diritto di opporsi al trattamento dei dati ai fini di informazione commerciale, pubblicitaria, di vendita diretta o ricerche di mercato (art.7 comma 4 lett. b);
- diritto al risarcimento del danno cagionato per l'effetto del trattamento di dati personali (art.15);
- diritto di ricorrere al Garante per far valere i diritti sopra elencati (art. 145).

La richiesta di accesso ai dati personali che lo riguardano può essere inoltrata dall'interessato al titolare o al responsabile senza formalità, anche verbalmente. Tuttavia il Garante ha predisposto un modello di richiesta informazioni, che si può scaricare dal sito internet www.garanteprivacy.it.

Se l'interessato non ottiene risposta, potrà far valere il proprio diritto con ricorso all'autorità giudiziaria o al Garante. Il ricorso al Garante non può essere proposto qualora, per il medesimo oggetto e tra le stesse parti, sia stata già adita l'autorità giudiziaria.

2. MISURE DI SICUREZZA RELATIVE AI SERVER

I dati personali per cui la legge richiede la tutela con misure idonee vengono memorizzati, nella maggior parte dei casi, sui server di rete. Per questo motivo va riservata una particolare

attenzione alle misure di sicurezza e di protezione relative ai server.

2.1. Misure di sicurezza organizzative

Il **responsabile/dirigente** - d'intesa con l'amministratore di sistema - **verifica** che la configurazione e l'utilizzo delle risorse presenti sul server di rete della propria struttura (unità logiche, cartelle) sia funzionale alle **esigenze di riservatezza** delle banche dati contenenti dati personali.
In particolare verifica che la configurazione preveda l'accesso differenziato, in base ad abilitazioni personali o per gruppi di lavoro e in relazione ai compiti svolti dal personale.

2.2. Misure di sicurezza logistiche

Per un'adeguata collocazione dei server, devono essere adottate le misure logistiche idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso fisico non autorizzato;
- distruzione o perdita dei dati dovuta ad eventi fisici.

L'amministratore di sistema e i tecnici che hanno accesso ai locali del server devono informare il dirigente responsabile del trattamento nel caso in cui riscontrino il mancato rispetto delle misure di sicurezza logistiche qui elencate (ad esempio locali server lasciati aperti o mancata custodia delle chiavi degli stessi).

2.2.1 Protezione del server da accesso fisico non autorizzato

Per tutelare la riservatezza dei dati personali accessibili sul server e per proteggere l'efficienza delle apparecchiature, l'accesso ai locali in cui vi sono uno o più sistemi server è limitato nel seguente modo:

- le apparecchiature server devono essere poste in apposite stanze, destinate a contenere soltanto il server stesso ed eventualmente le apparecchiature di rete;
- ove sia logisticamente difficoltosa l'ubicazione del server in un apposito locale e per le strutture esistenti che non rispondono ai requisiti di cui al punto precedente, vanno cercate soluzioni organizzative alternative (es. armadi chiusi e appositamente allestiti) che offrano le medesime garanzie di sicurezza;
- l'accesso ai locali server è protetto tramite la chiusura a chiave del locale;
- la chiave è custodita da personale incaricato della custodia dal responsabile/ dirigente (normalmente presso le segreterie);
- il personale incaricato della custodia delle chiavi è tenuto a riporle in un luogo non agevolmente accessibile da altri.

2.2.1.1 Accesso di personale interno della struttura

Possono accedere ai locali in cui sono presenti uno o più sistemi server solo:

- il dirigente/responsabile del trattamento;
- l'amministratore del sistema;
- il personale della struttura che deve accedervi per l'espletamento dei compiti propri, per le necessità di gestione e manutenzione dei sistemi (ad es. il personale preposto al cambio giornaliero delle cassette di backup), dei locali e degli impianti nonché per attività di pulizia ed affini ed altre attività comunque indispensabili.

2.2.1.2 Accesso di personale esterno alla struttura

Gli interventi di manutenzione o adeguamento sui server, sui locali che li contengono ed sui relativi impianti, sono richiesti o comunque autorizzati dal dirigente/responsabile. Quando, per l'espletamento di compiti di servizio e per altre attività, è necessario consentire l'accesso a personale esterno o a personale dipendente della Provincia non appartenente alla struttura, vanno osservate le seguenti misure:

- il locale viene aperto dal personale custode delle chiavi;

- ciascun intervento è annotato su un apposito registro conservato nella stanza del server recante data e orario dell'intervento (inizio-fine), tipo di intervento, nome, cognome del tecnico intervenuto/Ditta o struttura, firma;
- al termine dell'intervento, l'incaricato della custodia della chiave provvede alla chiusura dei locali;
- nessun soggetto estraneo può accedere ai sistemi server se non accompagnato dal personale.
- non c'è la necessità di effettuare quotidianamente le operazioni di pulizia nella stanza contenente il server: le giornate in cui il personale addetto alle pulizie accede alla medesima sono programmate, anche al fine dell'apertura del locale;
- è preferibile che le operazioni di pulizia si svolgano quando è presente il personale addetto alla custodia della chiave, che provvede personalmente all'apertura;
- ove non sia possibile la presenza del personale addetto alla custodia della chiave, in quanto l'intervento di pulizia si svolge al di fuori dell'orario di servizio per altre cause ostative, in via eccezionale, il locale rimane aperto al fine di consentire l'ingresso del personale addetto, limitatamente ai periodi in cui è stato programmato l'intervento di pulizia.

2.2.2 Protezione dei dati dal rischio di perdita dovuta ad eventi fisici

Tra gli eventi fisici che possono portare alla perdita dei dati per distruzione delle apparecchiature vengono considerati incendio, surriscaldamento delle apparecchiature, anomalie di alimentazione elettrica e altri eventi (allagamenti, crolli ecc.).

2.2.2.1 Contromisure per il rischio di incendio

Contro l'eventualità che un incendio nei locali in cui sono custoditi i sistemi server possa causare danni irreversibili ai dati sono necessarie le seguenti misure di sicurezza:

- in prossimità del server deve essere installato un dispositivo antincendio; in sede di progettazione e di realizzazione di nuove strutture adibite ad uffici provinciali ovvero in sede di ristrutturazione di edifici esistenti vanno tenute presenti le esigenze di sicurezza, ad es. dotando i locali di impianti di spegnimento automatico degli incendi;
- le cassette di backup devono essere conservate in un armadio ignifugo, chiuso a chiave, dislocato in un locale diverso da quello che ospita il server.

2.2.2.2 Contromisure per le anomalie nell'alimentazione elettrica

Contro l'eventualità che anomalie dell'alimentazione elettrica dei sistemi server possa danneggiare i dati è necessario predisporre un collegamento ad un gruppo statico di continuità.

2.2.2.3 Contromisure per altri eventi (allagamenti, crolli ecc.)

In sede di progettazione e di realizzazione di nuove strutture adibite ad uffici provinciali ovvero in sede di ristrutturazione di edifici esistenti, vanno tenute presenti le esigenze di sicurezza evitando ad es. la collocazione dei locali contenenti i server in scantinati o piani seminterrati (a rischio allagamenti).

2.3 Misure di sicurezza tecniche, informatiche e procedurali

La sicurezza dei server deve essere tutelata con le misure tecniche, informatiche e procedurali illustrate nei seguenti paragrafi, idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso logico non autorizzato o non conforme alle regole;
- distruzione o perdita dei dati dovuta ad attacchi esterni (es.: virus);
- distruzione o perdita dei dati dovuta ad attacchi di malintenzionati;
- perdita accidentale dei dati.

2.3.1 Protezione da accessi logici non autorizzati

Per accesso logico, nel contesto di questo documento, si intende l'accesso ai dati contenuti sul server attraverso l'utilizzo di un computer connesso in rete. Si tratta cioè dell'accesso e dell'utilizzo dei dati personali tramite i PC connessi alla rete a cui è connesso il server o dell'accesso ai dati dalla console del server stesso. L'accesso logico è permesso a chi digita la corretta combinazione di identificativo utente (user-id) e parola chiave (password).

Il sistema operativo Windows XP consente di:

- regolare l'accesso, disponendo di caratteristiche personalizzabili in grado di implementare vari gradi di sicurezza (vedi paragrafo relativo alle "Risorse di rete"), garantendo contro il rischio di utilizzo dei dati da parte di persone non autorizzate;
- mantenere una traccia di tutti gli accessi (*log*), e quindi conoscere quando e che utente si è connesso al sistema e quali utenti hanno cercato di accedere a risorse non autorizzate.

2.3.2 Protezione dai virus

I virus sono particolari programmi predisposti per essere eseguiti all'insaputa dell'utente che possono causare danni ai dati memorizzati sul computer o al sistema operativo del computer stesso. Sui sistemi NT l'amministratore di sistema installa e provvede a mantenere un software antivirus con aggiornamento periodico automatico via Internet che garantisce una protezione idonea ad evitare il verificarsi di danni ai dati causati dai virus informatici.

2.3.2.1 Tipologie di virus

Dal punto di vista tecnico si possono catalogare i virus in varie categorie. Le principali sono le seguenti:

- boot sector virus;
- macro virus;
- network virus;

Una forma particolare di virus sono quelli definiti "cavalli di Troia" (Trojans). Solitamente vengono inviati come allegati a messaggi di posta elettronica e l'utente viene indotto ad eseguirli. Una volta eseguito, il virus "cavallo di Troia" si installa sul computer attaccato rendendosi invisibile e permette di accedere alla macchina da remoto per sottrarre documenti o per usare il computer come punto di partenza per ulteriori attività illegali.

Una tecnica molto pericolosa di attacco informatico è il phishing (da "fishing", pescare). Si tratta del tentativo di ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante messaggi di posta elettronica fasulli. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione o altro.

2.3.3 Protezione da malintenzionati

Ogni computer collegato in rete può essere soggetto di tentativi di connessione effettuati da soggetti che utilizzano altri computer collegati alla rete. Quando il computer è collegato a Internet le intrusioni possono teoricamente essere effettuate da computer connessi a Internet situati in una qualsiasi parte del mondo.

Per fare fronte a questo rischio i posti di lavoro ed i server della struttura sono collegati alla rete Internet attraverso la rete Telpat per cui la protezione dalla distruzione o perdita dei dati dovuta ad attacchi di malintenzionati che agiscono collegandosi dall'esterno via Internet è garantita dai sistemi *firewall* gestiti da Informatica Trentina SpA.

La difesa dagli attacchi di questo tipo è comunque assicurata solo se viene data puntuale applicazione a tutto il complesso delle regole di sicurezza comprese nel presente documento.

2.4 Protezione dal rischio di perdita accidentale dei dati

Per ovviare al rischio di perdita accidentale dei dati sui server è presente un sistema di salvataggio automatico degli stessi mediante copia automatica su nastro (backup).

Il salvataggio automatico:
- garantisce il recupero dei dati a fronte di guasti hardware o software, limitando i disagi connessi con la discontinuità del servizio;
- consente di recuperare dati o file accidentalmente eliminati o erroneamente modificati.

3. MISURE DI SICUREZZA RELATIVE ALLE RISORSE DI RETE E DEI PC

L'operatore, tramite la procedura di accesso logico, che prevede l'utilizzo di un **identificativo utente** (user-id) e di una **password** può accedere ad una stazione di lavoro (PC) connessa alla rete della struttura. In questo modo l'operatore può:

- accedere alle risorse presenti fisicamente sulla macchina stessa (dischi fissi);
- accedere alle risorse di rete (cartelle del disco fisso del server su cui l'utente ha diritto di accesso);
- condividere con altri utenti risorse quali file, cartelle (ad es. dischi U e T) e stampanti;
- condividere con altri utenti applicazioni, quali ad es. Protocollo, Pratiche, Mouseia, ecc.;
- usufruire della centralizzazione delle operazioni di backup (nel caso in cui i dati siano salvati sul server) e di aggiornamento software.

3.1 Misure di sicurezza informatiche

In base alla configurazione appena descritta vanno adottate le seguenti misure:

- va privilegiato per la memorizzazione dei dati l'utilizzo delle risorse di rete evitando l'uso delle unità logiche presenti fisicamente sul PC (dischi fissi/locali C e D);
- in ogni caso le elaborazioni riguardanti dati personali vanno memorizzate sui dischi di rete;
- anche se alcuni programmi applicativi consentono la protezione dei singoli file mediante l'apposizione di specifiche password tale pratica va evitata.

La password sul file come misura di sicurezza non è adeguata e può essere controproducente. Infatti tali password possono essere perse o dimenticate, rendendo molto difficile il recupero dei dati, anche se esistono in commercio programmi per forzare queste password. La sola esistenza di questi programmi implica che queste password non sono da considerarsi misure di sicurezza idonee alla protezione dei dati.

3.2 Uso dei dischi fissi/locali (C:\ e altri)

L'utilizzo dei dischi fissi/locali, presenta inconvenienti sotto il profilo della sicurezza dei dati (si veda la descrizione di tali unità logiche). Pertanto se non è possibile usare le unità di rete bisogna adottare le seguenti misure di sicurezza.

I dischi fissi locali non vanno utilizzati come unico e predominante strumento di lavoro; vanno effettuati periodici backup dei dati su supporti magnetici al fine di evitarne la perdita; tali supporti vanno conservati secondo le modalità individuate nel capitolo 10 *Supporti di memorizzazione*.

4. MISURE DI SICUREZZA RELATIVE ALLE POSTAZIONI DI LAVORO

4.1 Misure di sicurezza logistiche

Una adeguata protezione dei **luoghi di lavoro** serve a garantire la sicurezza dei dati personali custoditi al loro interno, per garantire questa sicurezza vanno adottate misure logistiche idonee a garantire la protezione di documenti, supporti informatici e apparecchiature rispetto al rischio di:

- accesso fisico non autorizzato;

- distruzione o perdita dei dati dovuta ad eventi fisici.

4.2 Protezione delle postazioni da accesso fisico non autorizzato

Per accesso fisico s'intende l'accesso ai locali in cui vi sono uno o più postazioni di lavoro dotate di PC. Le misure di sicurezza devono garantire contro il rischio di accesso fisico ai locali o intrusione da parte di persone non autorizzate. L'accesso fisico alla postazione di lavoro collegata in rete da parte di estranei non identificati rappresenta comunque un potenziale rischio per la sicurezza dei dati custoditi sul server della rete, anche se la persona non può conoscere le password. Per evitare questo rischio si devono adottare le seguenti misure di sicurezza:

4.2.1 personale interno alla struttura

- le postazioni di lavoro sono accessibili solo da quanti ne hanno titolo, in qualità di responsabili o incaricati del trattamento, di amministratori del sistema, o altro, nei soli limiti in cui ciò sia funzionale allo svolgimento dei compiti della struttura o per lo svolgimento di attività di manutenzione, di pulizia e affini, nonché per altre attività comunque indispensabili;
- l'accesso fisico ai luoghi di lavoro è protetto tramite la presenza di personale di portineria ovvero tramite la chiusura delle vie di accesso;
- in ogni caso gli uffici aperti al pubblico devono essere presidiati da personale di portineria; negli orari diversi da quelle di servizio, ove non vi sia comunque un presidio, la porta di accesso all'edificio deve rimanere chiusa.

4.2.2 personale esterno alla struttura

- la persona esterna può accedere ai locali solo quando è presente qualche addetto;
- la persona esterna deve farsi riconoscere al personale di portineria e seguire le regole stabilite dal responsabile per l'accesso del pubblico alla struttura.

4.3 Protezione da accessi logici non autorizzati

L'accesso logico alle postazioni di lavoro dotate del sistema operativo Windows XP è consentito attraverso l'utilizzo combinato di una parola chiave (password) e di un identificativo utente (user-id) che autentica l'utente sul server della rete. In assenza dell'autenticazione la postazione non è immediatamente utilizzabile. A ciascun utente, all'assegnazione della dotazione informatica, viene attribuito un identificativo utente (user-id) univoco ed immutabile ed una password personale, segreta e sostituibile dall'utente stesso. La password e il codice identificativo sono personali.

Pertanto vanno osservate le seguenti misure di sicurezza:

- evitare di rendere note le password a più persone, o di condividerle; è in primo luogo interesse dell'utente evitare che altri utilizzino la sua password d'accesso: infatti, dalla registrazione dell'attività effettuata dal sistema, risulterebbe a lui attribuito il trattamento effettuato da altri, con connessa responsabilità in caso di trattamenti scorretti o non autorizzati o illeciti;
- evitare di trascrivere le password su supporti agevolmente accessibili da parte di terzi;
- evitare di utilizzare codici di accesso di personale nel frattempo cessato, assente per lungo periodo o che è stato assegnato ad altra struttura o attività.

L'utente è tenuto a:

- sostituire la password ad intervalli regolari; il sistema consente la sostituzione della password da parte dell'utente; il sistema è stato impostato per tutta la rete con un vincolo che impone a tutti gli utenti di cambiare le password entro periodi prestabiliti;
- rendere inaccessibile il sistema dalla propria postazione di lavoro ogni volta che si assenta; ciò si ottiene utilizzando la funzione di blocco *workstation* del sistema (che viene attivata premendo contemporaneamente i tasti Ctrl/Alt/Canc e cliccando sul bottone "blocca workstation");

- impostare uno *screen saver* automatico protetto da password con tempo di attivazione inferiore ai 5 minuti di inattività della macchina;
- se accede alla rete da una postazione di lavoro non assegnatagli, usare il proprio identificativo utente e la propria password e non chiedere di utilizzare la password del collega.

La scelta della password è importante per rendere difficile la sua individuazione casuale. Il sistema è stato impostato con un vincolo che obbliga l'utente a scegliere password che rispettino alcuni requisiti minimi di complessità (numero di caratteri, presenza di caratteri numerici e presenza di lettere maiuscole e minuscole).

4.4 Accesso ai dati in assenza dell'incaricato

Qualora, in caso di assenza dell'incaricato assegnatario della dotazione informatica, si renda necessario per ragioni improrogabili l'utilizzo di dati accessibili in via esclusiva con i suoi codici di accesso è necessario rispettare le seguenti regole:

- deve sussistere un'improrogabile necessità di accedere ai dati per ragioni di servizio;
- deve essere verificata l'impossibilità o la notevole difficoltà di raggiungere l'utente;
- **il dirigente**, in quanto responsabile del trattamento chiede all'amministratore di sistema di **accedere ai dati** con **i propri codici** di accesso (nome utente e password) con una procedura analoga a quella prevista per il ripristino della password;
- ad accesso effettuato il dirigente/responsabile comunica l'accesso effettuato al dipendente assente, al suo rientro.

4.5 Ripristino della password

Nel caso di perdita/dimenticanza della password da parte dell'utente, vi è una sola soluzione: l'amministratore deve impostare una nuova parola chiave e comunicarla all'utente. L'utente potrà poi provvedere alle ulteriori sostituzioni. La procedura di ripristino può essere attivata su richiesta dell'utente, in caso di perdita e dimenticanza della password

4.6 Protezione da accessi logici non autorizzati a PC non connessi alla rete

Per l'accesso logico ai PC stand-alone, cioè PC non connessi al server di rete della struttura, bisogna adottare, prima dell'inizio del trattamento dei dati personali, le seguenti misure:

- se il sistema operativo lo consente impostare password e user-id per l'accesso logico al PC, che vanno fornite a ciascun incaricato del trattamento di dati personali;
- se invece sul PC è installato un sistema operativo privo di servizi di multiutenza (Windows 95/98/ME/3.x o MS-Dos) va attivata una password a livello di BIOS del computer (poiché la procedura dipende dalla marca, modello e data di fabbricazione del personal computer, è consigliabile che tale operazione sia eseguita da un tecnico esperto); per i PC con password a livello di BIOS non è possibile impostare un identificativo utente (user-id);
- sostituzione della password ad intervalli regolari e deposito presso un custode delle password.

4.7 Protezione dai virus

I PC connessi in rete sono protetti da un prodotto antivirus installato e connesso ai sistemi server con aggiornamento periodico automatico via Internet a carico dell'amministratore di sistema.

Sui PC stand alone è invece necessario installare un prodotto antivirus ad hoc che, per risultare efficace nel tempo, dovrà essere aggiornato periodicamente secondo le modalità richieste dal prodotto stesso. L'aggiornamento è a carico dell'amministratore di sistema.

4.8 Protezione dai malintenzionati

I posti di lavoro ed i server delle strutture provinciali sono collegati alla rete Telpat; la protezione relativamente alla distruzione o perdita dati dovuta ad attacchi esterni da parte di malintenzionati, via Internet, è effettuata dal *firewall* gestito da Informatica Trentina SpA. **Si ricorda comunque che la difesa dagli attacchi di questo tipo è assicurata solo se viene data puntuale applicazione a tutto il complesso delle regole di sicurezza comprese nel presente documento.**

4.9 Protezione dal rischio di perdita accidentale dei dati

Per i dati contenuti nei dischi di rete, viene effettuato un *backup* programmato in automatico dal sistema server durante la notte su apposite, cassette da sostituire giornalmente.

Invece per i dati contenuti nei dischi installati fisicamente sul PC (C:\ e D:\) è necessario che ciascun operatore provveda a periodici backup dei dati su supporti magnetici e alla conservazione dei supporti stessi.

Si consiglia comunque di utilizzare i dischi del PC come sistema di memorizzazione dei dati solo in casi eccezionali, la memorizzazione sulle unità di rete messe a disposizione dal server **deve essere la regola**.

5. MISURE DI SICUREZZA RELATIVE AI SUPPORTI DI MEMORIZZAZIONE

5.1. Misure di sicurezza logistiche

Nell'uso e nella conservazione dei supporti di memorizzazione si devono porre in essere le misure necessarie a ridurre al minimo i rischi di:

- accesso fisico non autorizzato;
- furto e manomissione dei dati da parte di malintenzionati;
- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

Inoltre sono necessari gli ulteriori accorgimenti, di seguito riportati, derivanti dalle specifiche caratteristiche di tali supporti.

5.2 Reimpiego

Ai sensi del punto 22 del Disciplinare tecnico in materia di misure minime di sicurezza allegato al Codice i supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Si riportano di seguito indicazioni operative da seguire relative ad alcuni supporti, nel caso in cui gli stessi siano consegnati a terzi:

- floppy disk e cd-rom riscrivibili: prima di essere consegnati ai terzi, debbono essere sottoposti ad una operazione di cancellazione delle informazioni precedentemente contenute con l'apposito comando di formattazione completa del supporto;
- hard disk: prima di essere consegnato ai terzi, deve essere sottoposto ad una operazione di cancellazione delle informazioni precedentemente contenute con il comando FDISK (che rimuove la partizione) e la formattazione della partizione successivamente creata;
- nel caso in cui, a seguito di intervento tecnico, si presenti la necessità di sostituire l'hard disk, è necessario procedere al recupero dei dati contenuti nello stesso, ove possibile e opportuno; dopo aver effettuato tale verifica si potrà procedere alla cancellazione dei dati dall'hard disk sostituito; si ricorda che l'hard disk potrebbe costituire un mezzo di esportazione illegittima di dati personali qualora gli stessi fossero recuperati da personale

non autorizzato;
- nel caso in cui i supporti contenenti dati personali non siano destinati al riutilizzo essi debbono essere fisicamente distrutti mediante rottura.

6. MISURE DI SICUREZZA PER I DOCUMENTI

Nel caso di trattamento dei dati effettuato con strumenti diversi da quelli elettronici o comunque automatizzati (supporto cartaceo o altri supporti quali fotografie, fiche, slides, diapositive, ecc.) si applica quanto previsto dall'articolo 35 del Codice, che prevede alcune misure minime di sicurezza.

6.1 Misure logistiche

Il personale addetto al trattamento di dati personali deve porre in essere le misure necessarie a ridurre al minimo i rischi di:

- accesso fisico non autorizzato;
- furto o manomissione dei dati da parte di malintenzionati;
- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

6.2 Protezione dall'accesso fisico non autorizzato o dalla manomissione dei dati

Le misure idonee ad evitare l'accesso fisico non autorizzato o la manomissione dei dati da parte di malintenzionati sono le seguenti:

I documenti contenenti dati personali comuni sono conservati in archivi ad accesso selezionato: pertanto l'accesso ai dati è consentito ai soli incaricati del trattamento (ivi compreso il direttore o responsabile del settore cui il trattamento si riferisce), al dirigente/responsabile del trattamento nonché al personale che deve accedervi per l'espletamento di compiti comunque connessi con il trattamento.

I documenti possono essere estratti dall'archivio e affidati alla custodia dell'incaricato del trattamento per il tempo strettamente necessario al trattamento medesimo: egli ha cura di garantirne la riservatezza e provvede al deposito in archivio al termine delle operazioni; tale disposizione va precisata nelle istruzioni formalmente fornite all'incaricato stesso nell'atto di nomina;

La struttura che custodisce dati personali su supporto fisico deve dotarsi di arredi (cassettiere, armadi ecc.) muniti di meccanismi di serratura adatta a garantire la sicurezza, da destinare ad archivio di documenti contenenti dati personali; solo così si possono avere garanzie di sicurezza.

6.3 Protezione dei locali archivio contenenti dati personali sensibili

Poiché è obbligatorio archiviare i documenti contenenti dati personali sensibili in arredi (armadi o cassettiere) chiusi a chiave, l'accesso ai locali che contengono i documenti può non essere soggetto a particolari restrizioni. Resta fermo l'obbligo per l'incaricato e il responsabile di verificare che gli elementi di arredo siano sempre chiusi e che vengano rispettate le misure sopra riportate relative alla custodia delle chiavi e all'apertura degli archivi.

Se non c'è immediata disponibilità di arredi muniti di serratura per l'archiviazione dei documenti contenenti dati personali sensibili, gli archivi devono in ogni caso essere ubicati in appositi locali chiusi a chiave e, se appare agevole l'intrusione dall'esterno, muniti di sbarre.

Una apposita stanza-archivio chiusa a chiave può essere una soluzione adatta anche nel caso di armadi con serratura, in quanto aumenta il livello di protezione dei dati stessi.

Il personale diverso dagli incaricati del trattamento che accede a questi locali deve essere accompagnato da uno dei soggetti incaricati del trattamento o dal custode delle chiavi che deve verificare che non vi sia un accesso ai dati sensibili contenuti nei documenti (es: apertura e consultazione dei fascicoli).

6.4 Protezione dal rischio di perdita dei dati dovuta ad eventi fisici

Un archivio è sottoposto al rischio di svariati tipi di eventi che possono provocare la distruzione o il danneggiamento dei documenti. Per ridurre al minimo questo rischio le principali misure da prendere sono le seguenti:

- va tenuta presente la necessità di collocare i locali adibiti ad archivio in luoghi sicuri, evitando ad esempio scantinati e piani seminterrati che sono a rischio di allagamenti;
- nelle strutture devono essere presenti idonei dispositivi antincendio.

6.5 Misure per prevenire lo smarrimento accidentale dei documenti

Al fine di evitare lo smarrimento accidentale dei documenti l'incaricato del trattamento deve aver cura di depositare i documenti negli appositi archivi non appena cessate le operazioni di trattamento.

7. MISURE DI SICUREZZA RELATIVE A INTERNET

L'utilizzo di una connessione ad Internet (ad esempio via modem) attraverso un *provider* espone il PC utilizzato ai rischi normalmente presenti nel corso di una connessione ad Internet in assenza della protezione garantita da un *firewall*.

Inoltre:

- l'eventuale attacco alla macchina nel corso della navigazione non protetta diventa in un fattore di rischio per l'intera rete provinciale;
- sia l'accesso a siti "impropri" che lo scaricamento di file non autorizzati, in alcuni casi possono essere illegali e puniti dalla legge penale (oltre ad essere in contrasto con il codice di disciplina del dipendente provinciale).

I messaggi di posta elettronica di cui non si conosce il mittente vanno trattati con la massima circospezione; non bisogna mai cliccare sugli eventuali allegati senza riflettere; si tenga presente che i danni per virus ricevuti attraverso la posta elettronica rappresentano da soli la grande maggioranza delle cause di eventi dannosi per virus informatico all'interno delle reti aziendali.

Anche in presenza di un utente conosciuto è meglio riflettere sul contesto del messaggio per verificare se l'allegato è in qualche modo connesso con il proprio lavoro (e quindi viene effettivamente dal mittente indicato). Per fare un esempio, nel corso degli ultimi mesi del 2003 sono circolati falsi messaggi il cui mittente era apparentemente il produttore del sistema operativo Windows. Questi messaggi contenevano un virus che veniva spacciato come file di adeguamento alla sicurezza da applicare al proprio sistema.