MANUALE per la SICUREZZA

e il corretto Trattamento dei Dati Personali

Decreto Legislativo 196/03

Ad uso degli Incaricati

30 marzo 2007

Indice

" Decreto Legislativo 196/03

Art. 1 - ***Diritto alla protezione dei dati personali***

1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano. "

1. Premessa

Dal 1° gennaio 2004 è entrato in vigore il Decreto Legislativo 30 giugno 2003 n. 196, noto come Codice in materia di protezione dei dati personali (d'ora in poi il Codice).

Il nuovo Codice riunisce in sé la grande varietà di provvedimenti in materia, stratificatisi nel tempo a livello nazionale e comunitario, provvedendo alla loro razionalizzazione, favorendone la conoscenza ed il conseguente rispetto.
Il Codice rappresenta una significativa evoluzione dei precedenti regolamenti, per quanto riguarda l'aderenza alle attuali realtà operative e tecnologiche del Trattamento dei dati, facendo sì che la circolazione dei dati personali possa avvenire

nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, alla identità personale e al diritto alla protezione dei dati personali

(come da art. 2 - Finalità - comma 1 del Codice).

E' necessario pertanto che ogni *operatore* sviluppi sempre più una consapevole cultura circa la "preziosità" e "delicatezza" delle informazioni che quotidianamente è chiamato a trattare e conservare, e che si adoperi, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, affinché vengano compiutamente rispettate, nel suo settore di attività, tutte le misure di sicurezza previste a protezione dei dati stessi, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, anche per evitare di incorrere nelle pesanti sanzioni amministrative, a volte anche di carattere penale, previste dal legislatore a tutela degli interessati.

Il principio guida dell'azione organizzativa e operativa è rappresentato dal "principio di necessità del trattamento" (art. 3 del Codice), il quale, assieme ai correlati principi di "pertinenza e non eccedenza", rappresenta un presupposto di liceità del trattamento medesimo.

Nell'ottica di una efficace tutela delle informazioni e dei dati personali gestiti dalla nostra Associazione, il presente *Manuale per la Sicurezza* ha lo scopo di fornire le regole cui attenersi e le indicazioni e istruzioni di massima circa il complesso delle misure organizzative, logistiche, tecniche, ed informatiche da adottare in tutta la struttura, affinché siano rispettati gli obblighi previsti dal Codice.
In questo documento sono riportati alcuni articoli del codice, scritti *in corsivo*, quanto qui non riportato è comunque consultabile sul sito web del Garante (www.garanteprivacy.it).

L'ambito di validità e di osservanza delle regole contenute nel presente documento è l'Associazione Croce Verde Torino, per i trattamenti di dati personali sensibili gestiti dall'Associazione stessa.

2. Definizioni

Ai sensi di quanto previsto dal Codice all' art. 4 si intende per:

*"**trattamento",** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;*

***"dato personale",** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;*

***"dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;*

***"dati sensibili",** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*

***"dati giudiziari",** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;*

***"titolare",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;*

***"responsabile",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;*

***"incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;*

***"interessato",** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;*

***"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*

***"diffusione",** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;*

***"dato anonimo",** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;*

***"blocco",** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;*

"banca di dati", *qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti*

"Garante", *l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.*

Ai sensi di quanto previsto dal Codice all'art. 7 si definisce che:

Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorchè pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

3. Regole generali per il Trattamento dei Dati

Ai sensi di quanto previsto dal Codice all'art. 11 si definisce che:

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

In relazione alla Informativa da rendere all'Interessato, all'art.13 del Codice si definisce che:

Art. 13. Informativa

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) 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;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:

a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

In relazione al Consenso dell'Interessato, ai sensi di quanto previsto dal Codice agli artt. 23 e 24 si definisce che:

Art. 23. Consenso

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge,da un regolamento o dalla normativa comunitaria;

b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un

diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

In relazione alla Sicurezza dei Dati e dei Sistemi di seguito riportiamo il testo integrale, estratto dal Codice attualmente in vigore,

del TITOLO V - Capitoli I e II e

dell'Allegato B - Disciplinare Tecnico in Materia di Misure Minime di Sicurezza.

Questi articoli e il Disciplinare Tecnico completano le regole e le indicazioni cui attenersi per una corretta gestione dei dati personali.

CAPO I - MISURE DI SICUREZZA

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 32. Particolari titolari

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è

tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

CAPO II - MISURE MINIME DI SICUREZZA

Art. 33. Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari
del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi
dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi
previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono
adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36. Adeguamento

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Come si evince dall'art. 36 suddetto, il Disciplinare Tecnico che segue è soggetto ad aggiornamento periodico. Quello qui riportato è quello in vigore al 15 Giugno 2005. Per il testo aggiornato si faccia riferimento a quello reso disponibile e aggiornato sul sito del Garante (www.garanteprivacy.it).

ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa

segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in

occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. 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.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi

all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Per la Sicurezza dei Dati e dei beni l'Associazione, nel corso del 2006, si è dotata di impianto di Videosorveglianza.

In relazione alla normativa che regola la videosorveglianza, riportiamo il testo integrale, estratto dal Codice attualmente in vigore,

della Parte II, TITOLO X

Capo III - Videosorveglianza

Art. 134. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11.

L'impianto di videosorveglianza a circuito chiuso, costituito da telecamere, videoregistratori e monitor, la cui composizione è descritta in dettaglio nel documento di Installazione dell'impianto di Videosorveglianza, è stato installato rispettando il principio di propozionalità tra i mezzi impiegati ed i fini perseguiti, e a seguito di regolare delibera secondo l'accordo ex.art. 4 comma 2 con le parti sociali. In relazione a tale Accordo si faccia riferimento al Verbale di Accordo ex.art. 4 L. 300/70 (Statuto dei Lavoratori) presente in Associazione.

La presenza delle telecamere è segnalata mediante il modello semplificato dell'informativa, qui riportato, contenuto nel "Provvedimento generale sulla videosorveglianza" del Garante per la Protezione di Dati Personali, pubblicato il 29 aprile 2004.

Le immagini riprese potranno essere visualizzate soltanto dai Responsabili del trattamento, per le finalità riportate nell'Accordo suddetto.

4. Soggetti che effettuano il Trattamento

Ai sensi di quanto previsto dal Codice al Titolo IV si definisce che:

Art. 28. Titolare del trattamento

1. 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.

Il Titolare del Trattamento nella nostra struttura è il suo Presidente pro tempore, indicato nel documento "**Elenco degli Incaricati al Trattamento dei dati - Titolare e Responsabili**".

Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti 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.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Nella nostra struttura sono nominati due Responsabili del Trattamento, uno per i Dipendenti che è anche Responsabile della Sicurezza dei Dati, e uno per i Volontari, indicati nel documento "**Elenco degli Incaricati al Trattamento dei dati - Titolare e Responsabili**".

La nomina a Responsabili è effettuata, in sede di prima applicazione della normativa di riferimento.

L'ambito di responsabilità si estende al trattamento dei dati effettuati, sia con l'ausilio di strumenti elettronici che in maniera cartacea, nell'ambito della unità organizzativa cui il soggetto fa riferimento, e si riferisce alle tipologie di dati e di trattamenti indicati dal responsabile medesimo nell'apposita Lettera di Incarico.

L'Associazione si riserva di effettuare, comunque, ulteriori nomine di Responsabili, laddove si rendesse necessario delegare, per lo svolgimento dell'attività istituzionale, a soggetti terzi esterni alla Associazione il trattamento di alcuni dati.

Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare e contenute nel presente Manuale.

Sono compiti del Responsabile del trattamento per i Dipendenti e del Responsabile della Sicurezza dei Dati:

- nominare e incaricare per iscritto i dipendenti incaricati al trattamento e impartire loro le istruzioni e l'ambito del trattamento consentito.
- predisporre un piano di formazione in caso di cambio di mansione degli incaricati al trattamento
- vigilare - secondo le prassi istituite ed in accordo con gli altri collaboratori del titolare - che gli incaricati al trattamento dei dati si attengano alle procedure di volta in volta indicate specificamente, sia oralmente che per iscritto, anche in relazione all'applicazione delle misure organizzative, fisiche e logiche sulla sicurezza nel trattamento
- vigilare sulle modalità e procedure di trattamento e conservazione dei dati effettuate su supporto cartaceo o comunque in modo diverso da quello effettuato con strumenti elettronici o automatizzati. Dovrà inoltre procedere ad attuare tutti gli adempimenti relativi all'affidamento ed alla conservazione - fuori dall'archivio - dei dati medesimi nei prescritti contenitori muniti di serratura nonché alla restituzione degli stessi da parte degli incaricati; sempre nel caso in cui si proceda al trattamento di dati sensibili, al nominato responsabile è altresì affidato il controllo, l'identificazione e la registrazione dei soggetti che hanno accesso agli archivi cartacei dopo l'orario di chiusura degli uffici.

In codesta Associazione il "Responsabile del trattamento per la sicurezza dei dati" si occupa altresì di operare in qualità di Amministratore di Sistema, di Responsabile della gestione e manutenzione degli strumenti informatici e di Incaricato alle copie di sicurezza delle banche dati, ed ha quindi anche il compito di:

- valutare i rischi sulla sicurezza delle banche dati e stabilire i metodi e la frequenza di salvataggio delle stesse al fine di consentire il ripristino degli archivi in caso di distruzione o danneggiamento
- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up (salvataggio) secondo i criteri stabiliti
- assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro
- stabilire e applicare i metodi di accesso agli archivi (base dati)
- redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete
- su indicazione del Responsabile del trattamento, assegnare ad ogni incaricato un "Codice identificativo personale" (USER–ID) per l'utilizzazione dell'elaboratore, che deve essere

individuabile e non riutilizzabile, e attivare le relative credenziali di autenticazione e di autorizzazione alla base dati di competenza

- fare in modo che sia prevista la disattivazione dei "codici identificativi personali" (User-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore e/o alla base dati, oppure nel caso di mancato utilizzo dei "codici identificativi personali" (User-ID) per oltre 6 mesi
- revocare, ove necessario, le autorizzazioni assegnate
- vigilare che l'accesso ai dati da trattare, da parte degli incaricati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette autorizzazioni il nominato responsabile avrà anche il compito di verificare la sussistenza delle condizioni che hanno determinato la loro emissione ed in difetto procedere alla loro revoca
- definire e attuare politiche per la protezione dei sistemi (pc, server, fw, altro hw) dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus informatici, mediante idonei programmi, verificandone l'efficacia con cadenza periodica almeno mensile
- definire e far applicare le modalità di accesso ai locali
- garantire che tutte le misure di sicurezza riguardanti i dati detenuti dall'Associazione siano applicate all'interno della stessa ed eventualmente al di fuori, qualora siano cedute a terzi quali "Responsabili del Trattamento", tutte o parte delle attività di trattamento
- redigere, entro i termini stabiliti, il documento programmatico sulla sicurezza
- frequentare corsi di formazione e di aggiornamento sulle procedure e sui sistemi di sicurezza organizzativi, logici, fisici e su base informatica, atti a tutelare il trattamento, la conservazione e l'integrità dei dati personali affidatigli per il trattamento
- intrattenere stretti rapporti di informazione e comunicazione con il Titolare del Trattamento e con gli altri collaboratori dello stesso
- informare il Titolare del Trattamento nella eventualità che si siano rilevati dei rischi (di qualsiasi natura) rischi relativamente alle misure di sicurezza riguardanti la salvaguardia dei dati personali sensibili.

Sono compiti del Responsabile del trattamento per i Volontari:

- nominare e incaricare per iscritto i volontari incaricati al trattamento e impartire loro le istruzioni e l'ambito del trattamento consentito.
- predisporre un piano di formazione in caso di cambio di mansione degli incaricati al trattamento
- vigilare - secondo le prassi istituite ed in accordo con gli altri collaboratori del Titolare del Trattamento - che gli incaricati al trattamento dei dati si attengano alle procedure di volta in

volta indicate specificamente, sia oralmente che per iscritto, anche in relazione all'applicazione delle misure organizzative, fisiche e logiche sulla sicurezza nel trattamento

- vigilare sulle modalità e procedure di trattamento e conservazione dei dati effettuate su supporto cartaceo o comunque in modo diverso da quello effettuato con strumenti elettronici o automatizzati. Dovrà inoltre procedere ad attuare tutti gli adempimenti relativi all'affidamento ed alla conservazione - fuori dall'archivio - dei dati medesimi nei prescritti contenitori muniti di serratura nonché alla restituzione degli stessi da parte degli incaricati; sempre nel caso in cui si proceda al trattamento di dati sensibili, al nominato responsabile è altresì affidato il controllo, l'identificazione e la registrazione dei soggetti che hanno accesso agli archivi cartacei dopo l'orario di chiusura degli uffici
- intrattenere stretti rapporti di informazione e comunicazione con il Titolare del Trattamento e con gli altri collaboratori dello stesso
- informare il Titolare del Trattamento nella eventualità che si siano rilevati dei rischi (di qualsiasi natura) rischi relativamente alle misure di sicurezza riguardanti la salvaguardia dei dati personali sensibili.

Art. 30. Incaricati del trattamento

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. 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.

Ai sensi di quanto disposto dalla normativa, gli incaricati del trattamento dei dati personali sono le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile. Nella nostra struttura gli incaricati nominati sono indicati nei documenti "**Elenco degli Incaricati al Trattamento dei dati - Dipendenti**" e "**Elenco degli Incaricati al Trattamento dei dati - Volontari - Squadra numero**" (per i Volontari un Elenco per ogni squadra).
La nomina a Incaricato è effettuata per iscritto e individua l'ambito del trattamento consentito.
Qualora il Responsabile, nello svolgimento delle sue funzioni istituzionali, ritenga necessario autorizzare soggetti diversi dai precedenti al trattamento dei dati personali inerenti la sua struttura, dovrà provvedere a designare per iscritto i medesimi.
Oltre che alle prescrizioni ed istruzioni di carattere generale contenute nel presente Manuale ogni Incaricato deve attenersi alle istruzioni impartite dal Responsabile dell'unità organizzativa cui afferisce od è assegnato relativamente alla specificità del trattamento dei dati personali effettuato nell'unità organizzativa medesima.

L'ambito di responsabilità si estende al trattamento dei dati effettuati, sia con l'ausilio di strumenti elettronici che in maniera cartacea, nell'ambito della unità organizzativa cui il soggetto fa riferimento, e si riferisce alle tipologie di dati e di trattamenti indicati dal responsabile medesimo nell'apposita Lettera di Incarico.

5. Regole e indicazioni specifiche interne

5.1 La Sicurezza

Questo documento fornisce agli incaricati del trattamento una panoramica sulle responsabilità loro spettanti, rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione. Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;

Integrità: Le informazioni non devono essere alterabili da incidenti o abusi;

Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche di opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti ne sufficienti se non usate propriamente.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

Le misure di sicurezza da adottare vengono distinte in:

- misure idonee e preventive volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- misure minime, indicate negli articoli 34 e 35 e analiticamente specificate nel Disciplinare Tecnico e diversificate a seconda che il trattamento sia effettuato o meno con strumenti elettronici.

I Titolari di trattamento di dati sono tenuti ad adottare, quanto meno, le "misure minime di sicurezza", ossia quegli accorgimenti tesi ad assicurare un livello minimo di protezione dei dati personali.

La mancata osservanza di quanto stabilito in materia di misure minime di sicurezza è sanzionata penalmente.

L'adozione delle misure minime di sicurezza non esonera tuttavia da responsabilità civile (si veda quanto specificato al capitolo 16.1 della Relazione annuale 2004 del Garante) qualora l'eventuale

danneggiato dimostri che, in base all'evoluzione tecnologica raggiunta, era possibile e raccomandabile l'utilizzo di misure di sicurezza ulteriori (le misure "idonee").

5.2 Istruzioni operative per gli incaricati

5.2.1 Trattamenti SENZA l'ausilio di strumenti elettronici

1. UTILIZZATE LE CHIAVI

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania;

pertanto, chiudete a chiave il vostro ufficio quando l'ultima unità di personale lascia il locale e, comunque, alla fine della giornata e chiudete i documenti a chiave nei cassetti o negli armadi ogni volta che potete.

2. NON COMUNICATE DATI PERSONALI A SOGGETTI NON LEGITTIMATI

L'utilizzo dei dati personali deve avvenire in base al "principio di necessità", è cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative.

I dati non devono essere comunicati all'esterno dell'Associazione e comunque a soggetti terzi, se non previa autorizzazione del Responsabile del trattamento nelle ipotesi consentite dalla normativa vigente.

3. FATE ATTENZIONE A COME DISTRUGGETE I DOCUMENTI

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

4. RADDOPPIATE LE ATTENZIONI SE I DOCUMENTI CONTENGONO DATI SENSIBILI O GIUDIZIARI

I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi molto attentamente in modo che non vi accedano persone prive di autorizzazione.

Ad esempio, la consultazione di documenti o certificati per l'inserimento in procedure informatiche di gestione/amministrazione dei servizi di assistenza prestati o di

gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattia, ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati.

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando possibilmente armadi o contenitori chiusi a chiave

Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

Riponete i documenti contenenti dati sensibili o giudiziari negli appositi contenitori o scaffali al termine delle operazioni affidate e comunque a fine giornata.

In ogni caso di allontanamento dal proprio posto di lavoro, i documenti devono essere riposti negli armadi o nei cassetti, possibilmente chiusi a chiave.

5.2.2 Trattamenti CON strumenti elettronici

1. CONSERVATE I SUPPORTI MAGNETICI RIMOVIBILI (FLOPPY DISK, CD, DVD, ...) IN UN LUOGO SICURO

Per i supporti magnetici si applicano gli stessi criteri che per i documenti cartacei,. con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. Pertanto, riponeteli sotto chiave non appena avete finito di usarli.

2. UTILIZZATE LE PASSWORD

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.

La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.

La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.

La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro, i vostri dati.

Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinte quelle degli applicativi da quella di accesso alla postazione o rete, considerando che queste

ultime due, per comodità di gestione, nella vostra struttura come nella più parte delle realtà aziendali coincidono.

Scegliete le password secondo le indicazioni della sezione "**COME SCEGLIERE UNA PASSWORD**" successiva in questo documento.

3. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

4. NON LASCIATE TRACCIA DEI DATI RISERVATI

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo.

5. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i furti. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

6. NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD

Anche se la maggioranza dei programmi non ripete in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state premendo, anche se siete veloci nella dattiloscrittura.

7. CUSTODITE LE PASSWORD IN UN LUOGO SICURO

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

8. NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ

Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

9. NON UTILIZZATE APPARECCHI NON AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete aziendale, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con il vostro Responsabile del trattamento dei dati.

10. NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il vostro Responsabile del trattamento dei dati.

11. APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

12. INFORMATEVI SULLA POLITICA LOCALE RELATIVA AI BACKUP

I vostri dati potrebbero essere gestiti da un file server, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Verificate con il personale locale la situazione.

5.2.3 Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, alcuni distruggono parte dei dati di file presenti in locale o sul server di rete o su altra postazione accessibile sulla rete, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

1. COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi prodotti o provenienti da fonti non ufficiali o sconosciute (tra cui salvaschermo);
2. Attraverso le macro dei programmi di automazione d'ufficio;
3. Attraverso allegati a mail, se aperti o eseguiti.

2. COME NON SI TRASMETTE UN VIRUS:

1. Attraverso file di dati non in grado di contenere macro (che oggi sono a titolo di esempio file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

3. QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da supporti magnetici removibili;
3. Quando si salvano file allegati a messaggi mail ricevuti;
4. Quando si scaricano dati o programmi da Internet.

4. QUALI EFFETTI HA UN VIRUS?

1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inspiegabilmente;
4. Funzioni di programma cambiano inspiegabilmente modo di operare.

5. COSA FARE PER PREVENIRE I VIRUS:

a) USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai salvaschermo e ai videogiochi, che sono spesso utilizzati per veicolare virus.

b) ***ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA FLOPPY DISK O CD O DVD***

Infatti se il dischetto o Cd o DVD fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.

c) ***PROTEGGETE I VOSTRI FLOPPY DISK DA SCRITTURA QUANDO POSSIBILE***

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

d) ***ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA AGGIORNATO***

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus disponga degli ultimi aggiornamenti (firme virali) dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informatevi con il responsabile del trattamento dati per maggiori dettagli.

e) ***APRITE GLI ALLEGATI SOLO SE ATTESI***

In questo modo eviterete di mandare in esecuzione un virus presente nell'allegato che il vostro interlocutore vi ha inviato a sua insaputa, perché la sua postazione era infettata da virus.

6. COSA NON FARE PER PREVENIRE I VIRUS:

a) ***NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA***

Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: le mail di questo tipo sono dette hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da vostra sorella o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).

b) ***NON PARTECIPATE A "CATENE DI S. ANTONIO" E SIMILI***

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

5.2.4 Importanza delle password

Nella sicurezza di un sistema il punto più debole è la password di accesso.

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo.

In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

1. COSA NON FARE

1. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.

2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.

3. Quando immettete la password NON fate sbirciare a nessuno quello che state digitando sulla tastiera.

4. NON scegliete password che si possano trovare in un dizionario o libro. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.

5. NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue. Tra queste la lingua più debole è l'inglese.

6. NON usate il Vostro nome utente. È la password più semplice da indovinare

7. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello della Vostra amata/o, dei figli, del cane o del gatto, date di nascita, numeri di telefono, codice fiscale, una delle suddette parole scritta al contrario, etc.

8. NON usate la parola "password" stessa.

2. COSA FARE

1. Cambiare la password a intervalli regolari. Poiché si trattano dati sensibili la password deve essere cambiata almeno ogni tre mesi (come specificato nell' *ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA* comma 5) .

2. Usare password lunghe almeno otto caratteri con un misto di lettere minuscole, lettere maiuscole, numeri e caratteri speciali (*,?,!,….).

3. Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi le password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarle spesso, è opportuno che siano diverse per ogni sistema o applicativo distinto.

3. COME SCEGLIERE UNA PASSWORD

Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare.

I momenti in cui la sicurezza della password può venire compromessa sono molteplici, ma la prima perdita di sicurezza della password avviene al momento della sua creazione.

In questo istante l'utente si trova davanti alla necessità di inventare qualcosa che dovrà memorizzare e digitare molto spesso.

La tentazione più forte e di scegliere un nome facile e breve.

Gli errori che solitamente si commettono nella scelta della password sono quelli indicati nel precedente capitolo **COSA NON FARE**.

Per inventare password che possano garantire un buon livello di sicurezza occorre seguire le indicazione del precedente capitolo **COSA FARE**.

Il problema è quindi come ricordare senza errori una sequenza di lettere maiuscole e minuscole, numeri e caratteri speciali.

Esempi di password:

Ta0rmina si legga Taormina, nome della località che si è visitata e gradita di più nell'ultimo periodo di tempo, o di quella che si prevede di visitare prossimamente, nel cui nome è stata inserita una lettera maiuscola, in questo caso la 'T' iniziale, e sostituita la 'O' con un numero visivamente di pari forma.

sei+ottofa14 si legga 'sei più otto fa quattordici', si scrivono in forma letterale i primi numeri ed in forma numerica l'ultimo, o viceversa, scrivendo il segno di operazione come carattere speciale. Ovviamente per ricordare la password l'operazione deve essere effettuata con numeri semplici da ricordare, numeri a noi familiari, e da calcolare.

Una parola che esprime il nostro stato d'animo desiderato, scritta in forma dialettale, nel dialetto che, probabilmente, ognuno conosce di più, magari perché è il dialetto del paese di origine, o quello parlato in famiglia. Nella parola in dialetto si potranno sostituire alcune lettere con numeri visivamente di pari forma.