COMUNE DI MELENDUGNO

PROVINCIA DI LECCE

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi e per gli effetti dell'art. 34 comma 1 del D.Lgs. 30 giugno 2003, n. 196 e del Disciplinare Tecnico (Allegato B, punto 19)

Versione del 31.03.2009

Prima versione adottata con deliberazione della Giunta Comunale n. 55 del 28/03/2006

Seconda versione adottata con deliberazione della Giunta Comunale n. 39 del 31/03/2009

SOMMARIO

1 REVISIONI E MODIFICHE AL DOCUMENTO

Edizione	Data	Descrizione modifica
0	20.02.2006	Prima emissione
1	31.03.2009	Seconda emissione

2 AMBITO DI APPLICAZIONE E DEFINIZIONI

2.1 Introduzione

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato da:

COMUNE DI MELENDUGNO
con sede in Via San Nicola – 73026 Melendugno (Le)

Codice fiscale: 80010060756

nel seguito del documento indicato come "Titolare".

Conformemente a quanto prescrive il punto 19. del Disciplinare tecnico, allegato sub b) al Dlgs 196/2003, nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare), mediante:
   - Identificazione, inventario delle sedi fisiche nelle quali vengono effettuati i trattamenti
   - Identificazione, inventario e analisi dei dispositivi hardware (sistemi informatici)
   - Identificazione, inventario e analisi dei dispositivi software
   - Identificazione delle banche dati
   - Individuazione dei trattamenti di dati personali sensibili e/o giudiziari eseguiti
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati (punto 19.2 del disciplinare)
3. l'analisi dei rischi che incombono sui dati (punto 19.3 del disciplinare)
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati (punto 19.4 del disciplinare)
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento (punto 19.5 del disciplinare)
6. la previsione di interventi formativi degli incaricati del trattamento (punto 19.6 del disciplinare)
7. i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno (punto 19.7 del disciplinare)
8. le procedure da seguire per il controllo sullo stato della sicurezza.

2.2 Definizioni

Ai fini del D.Lgs. 196/2003 si intende per:

Termine	Definizione
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, nonché 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.
Misure minime	il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
Strumenti elettronici	gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
Autenticazione informatica	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
Credenziali di autenticazione	i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;
Parola chiave	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
Profilo di autorizzazione	l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
Sistema di autorizzazione	l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

3 ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

3.1 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Identificazione, inventario delle sedi fisiche nelle quali vengono effettuati i trattamenti

E' stato effettuato un censimento ed un sopralluogo delle sedi fisiche e dei locali nei quali vengono effettuati i trattamenti dei dati.

Il trattamento dei dati avviene nei seguenti sedi:

Sigla	Sede	Ubicazione e caratteristiche
S1	**Sede municipale e Servizi Demografici**	**Via San Nicola 6 – Melendugno**
S2	**Polizia Municipale**	**Piazza Castello 8 - Melendugno**
S3	**Frazione di Borgagne**	**Piazza S. Antonio**

Identificazione, inventario e analisi dei dispositivi hardware (sistemi informatici)

E' stato effettuato un censimento dei sistemi informatici utilizzati presso l'ente. L'elenco aggiornato è disponibile presso il responsabile del 1° Servizio Amministrazione Generale.

L'Ente manterrà l'elenco, aggiornato, di tutte le attrezzature informatiche dei singoli uffici, dello scopo cui sono destinate, della loro locazione fisica, delle misure di sicurezza su di esse adottate e delle eventuali misure di adeguamento pianificate.

Identificazione, inventario e analisi dei dispositivi software

E' stato effettuato un censimento dei dispositivi software installati presso i vari uffici dell'Ente.

L'elenco aggiornato è disponibile presso il responsabile del 1° Servizio Amministrazione Generale.

3.2 Individuazione dei trattamenti di dati personali, sensibili e/o giudiziari eseguiti dall'Ente

E' stato effettuato un censimento dei trattamenti ed un sopralluogo delle sedi fisiche e dei locali nei quali vengono effettuati i trattamenti dei dati.

L'elenco aggiornato è riportato nell'**allegato 1 – INDIVIDUAZIONE TRATTAMENTI DATI PERSONALI, SENSIBILI E/O GIUDIZIARI**

L'Ente ha approvato un "REGOLAMENTO RELATIVO ALL'IDENTIFICAZIONE DELLE ATTIVITÀ CHE PERSEGUONO RILEVANTI FINALITA' DI INTERESSE PUBBLICO, AI SENSI DEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196", in attuazione delle disposizioni di cui all'art. 20, comma 2 del citato decreto. Questo regolamento identifica i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite nei singoli casi ed espressamente elencate nella Parte II del d.lg. n. 196/2003 (artt. 59, 60, 62-73, 86, 95 e 112).

3.3 Individuazione delle banche dati

E' stato effettuato un censimento delle banche dati cartacee ed informatiche.

L'elenco aggiornato è riportato nell'**allegato 2 – INDIVIDUAZIONE BANCHE DATI INFORMATICHE E CARTACEE.**

4 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

La Giunta Comunale con **deliberazione** ha nominato responsabili del trattamento dei dati i responsabili di settore e demandando al Sindaco alla formalizzazione dei relativi incarichi nei confronti dei responsabili.

Ogni responsabile designato ha ricevuto lettera di nomina personale da parte del Sindaco con evidenziati i compiti affidati.

L'elenco aggiornato è riportato nell'**allegato 3 – ELENCO RESPONSABILI TRATTAMENTO DEI DATI** e sul sito Internet del Comune nella sezione *Privacy*.

Non è stato nominato:

- l'Amministratore di sistema, cui è conferito il compito di sovrintendere alle risorse del sistema informativo e di consentirne l'utilizzazione, coordinare le attività informatiche dell'ente e progettare, realizzare e mantenere in efficienza le misure di sicurezza relative.

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- procedure per il salvataggio dei dati
- modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (**mansionario privacy**), nell'ambito del trattamento dei dati personali.

Periodicamente, con cadenza almeno annuale, si procederà ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione verrà compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

5 ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

In questa sezione sono descritti i principali eventi potenzialmente dannosi per la sicurezza dei dati, e valutarne le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

In particolar modo sono stati individuati ed elencati gli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali.

Sono stati analizzati gli eventi raggruppandoli nelle seguenti macrocategorie:

- eventi relativi ai comportamenti degli operatori;
- eventi relativi agli strumenti;
- eventi relativi al contesto fisico-ambientale.

Nell'allegato **4 - ELENCO DELLE MINACCE** vengono descritti, dettagliatamente, i singoli eventi considerati e gli impatti relativi sulla sicurezza. Mentre nella tabella che segue vengono riportati gli elementi sintetici.

1	2		3
Evento	**Impatto sulla sicurezza dei dati**		**Rif .misure d'azione**
	Descrizione	**Gravità stimata**	
Comportamenti degli operatori			
Furto delle credenziali di autenticazione	Accesso non autorizzato al computer	bassa	Istruzioni agli Incaricati, formazione, azione del "Custode delle Parole-chiave", controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autrorizzate
Carenza di consapevolezza, disattenzione o incuria	Le credenziali perdono riservatezza o dati sono inutilmente resi visibili	bassa	Come precedente
Comportamenti sleali o fraudolenti	Accesso per fini personali ai dati (che però sono poco appetibili), che vengono conosciuti da Incaricati che non ne hanno diritto	bassa	Come precedente, inoltre: eventuale creazione di profili di autorizzazione diversificati e utilizzo cifratura per i vari files contenenti dati sensibili, giudiziari o particolari importanti.
Errore materiale	Cancellazione o perdita di dati	Bassa (esiste copia cartacea di tutto)	Formazione degli incaricati, profilo di autorizzazione che non consenta la formattazione dei dischi fissi o la cancellazione di files importanti.

Eventi relativi agli strumenti

Azione di *virus* informatici o di codici malefici	Cancellazione di dati, malfunzionamenti o blocco del sistema, trasmissione casuale di dati a indirizzi di posta elettronica memorizzati, confusione con incapacità di individuare dati utili	elevata	Regolare aggiornamento dell'antivirus e del software (patches) , con istruzioni agli incaricati e monitoraggio di controllo sull'effettiva attuazione, istruzioni a individuare e prevenire le situazioni a rischio.
Spamming (posta indesiderata e disturbante) o altre tecniche di sabotaggio	Confusione con rischio di non individuazione di messaggi utili o di loro cancellazione per errore	Medio/alta	Eventuale implementazione di un filtro antispamming, formazione degli Incaricati a riconoscere i messaggi di disturbo e a gestire le regole di assegnazione dei messaggi di posta elettronica alle varie cartelle
Malfunzionamento, indisponibilità o degrado degli strumenti	Malfunzionamenti o blocco del sistema	media	Manutenzione programmata, formazione ad individuare i sintomi di malfunzionamento per un rapido intervento, piano di backup, e continuità operativa
Accessi esterni telematici non autorizzati	Visione indebita di dati o sabotaggio	Bassa (i dati non sono appetibili e il loro valore si basa sull'originale cartaceo)	Installazione di Firewall, con regolare aggiornamento
Intercettazione di informazioni in rete	Visione indebita di dati	minima	Eventuale adozione di cifratura o firma elettronica per proteggere i dati più gravi (allo studio)

Eventi relativi al contesto fisico-ambientale

Accessi non autorizzati a locali/reparti ad accesso ristretto	Sabotaggio delle macchine, con eventuale perdita di dati; accesso abusivo se le credenziali fossero lasciate disponibili	Sabotaggio: media Altro: bassa	Solidità degli infissi dei locali, chiusura a chiave quando non presidiati (eventuale installazione di allarme antifurto), disponibilità di estintori antincendio, istruzioni a tutti gli operatori
Asportazione e furto di strumenti contenenti dati	Perdita di dati , rallentamento o blocco dell'attività per carenza di computer	Probabilità media, gravità elevata	Come punto precedente, Inoltre, regolare back-up dei dati, piano di back-up e continuità operativa
Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati , rallentamento o blocco dell'attività per carenza di computer	Probabilità minima, gravità massima	Come punto precedente, (eventuale allarme antincendio), inoltre sensibilizzazione e formazione degli Incaricati. Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti. Uso di protezioni antifulmine e contro sovratensioni elettriche. Verifica della logistica degli apparecchi e del loro corretto posizionamento. Custodia dei dischi di back-up in

			armadio ignifugo, chiusi, collocato in locale diverso dai computer.
Guasto ai sistemi complementari (impianto elettrico)	Perdita di dati e blocco del sistema	media	Gruppo di continuità
Guasto ai sistemi complementari (climatizzazione)	Surriscaldamento dei computers e in particolare della scheda madre o altre componenti, con possibilità di guasto	bassa	Allo studio una miglior ventilazione dei computers (revisione regolare delle ventole interne e loro potenziamento). Verifica della logistica degli apparecchi e del loro corretto posizionamento.
Errori umani nella gestione della sicurezza fisica	Danni agli strumenti, con possibile perdita di dati e malfunzionamenti	media	Formazione e sensibilizzazione di tutti gli Incaricati. Verifica della logistica degli apparecchi e del loro corretto posizionamento.

6 MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI

Nel presente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede alla descrizione:

- delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata, anche per adeguarsi alle novità introdotte dal Dlgs 196/2003, e dal disciplinare tecnico in materia di misure minime di sicurezza, allegato a tale decreto sub b).

Al presente Documento programmatico sulla sicurezza vengono inoltre allegate delle Schede analitiche descrittive delle misure di sicurezza, che costituiscono parte integrante del Documento programmatico sulla sicurezza stesso.

6.1 Protezione fisica di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da

- dispositivi antincendio
- gruppo di continuità dell'alimentazione elettrica (server)
- impianto di condizionamento

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da sistemi di allarme antintrusione.

6.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, dischetti, fotografie, pellicole….), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento, o direttamente al titolare.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli incaricati sono stati dotati di:

- cassetti con serratura
- armadi chiudibili a chiave

nei quali devono riporre i documenti, contenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Particolari cautele vengono previste per il trasporto di documenti, atti e supporti contenenti di relativi all'identità genetica, all'esterno dei locali riservati al loro trattamento: per questi casi, è stato prescritto che il trasporto debba avvenire in contenitori muniti di serratura, o utilizzando dispositivi equipollenti.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree (definite archivio), nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa deve avvenire in luoghi , armadi , casseforti, o dispositivi equipollenti, che possono essere chiusi.

Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione dei seguenti accorgimenti:

- ad alcune persone, aventi la scrivania prospiciente, viene dato l'incarico di vigilare gli archivi, dettando precise istruzioni in merito al fatto che una persona deve essere sempre presente, durante l'orario di apertura dell'archivio, per controllare chi vi accede
- le persone vengono autorizzate preventivamente ad accedere agli archivi, previa richiesta della chiave all'incaricato che ha il compito di custodirla

Si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, mediante l'adozione dei seguenti accorgimenti: *la chiave dell'archivio è affidata, dopo l'orario di chiusura, al titolare o ai responsabili del trattamento, o in alternativa ad uno o più soggetti incaricati per iscritto, i quali provvedono ad annotare in un apposito registro i nominativi di cloro che hanno richiesto di accedere all'archivio.*

6.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato
- realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative
- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus)
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD….), nei quali siano contenuti dati personali.

SISTEMA DI AUTENTICAZIONE INFORMATICA

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente con strumenti elettronici non contenenti dati personali, o contenenti solo dati personali destinati alla diffusione.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si utilizzano il seguente metodo: si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.
  Tale regola diverrà tassativa, allorché il Titolare avrà completato il processo di adeguamento a quanto prescritto dal Dlgs 196/2003, entro il 31 marzo 2006.
  Sino ad allora, saranno presenti alcuni casi in cui la medesima credenziale di autenticazione è attribuita a due o più persone, limitatamente alle seguenti ipotesi:
  - per l'accesso, da parte degli incaricati, ad elaboratori non in rete, le cui caratteristiche non consentono l'autonoma sostituzione delle parole chiave
  - per l'accesso, da parte degli amministratori del sistema informativo, ad elaboratori in rete, il cui sistema operativo prevede un unico livello di accesso per tale funzione

- nei casi in cui una componente della credenziale di autenticazione è costituita dal codice per l'identificazione (username), attribuito all'incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Tali regole diverranno tassative, allorché l'organizzazione avrà completato il processo di adeguamento delle applicazioni software in dotazione a quanto prescritto dal Dlgs 196/2003, entro il 31 marzo 2006.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema
  - successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia;
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata

- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

SISTEMA DI AUTORIZZAZIONE (PROFILI DI ACCESSO)

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, è stato impostato un sistema di autorizzazione con profili differenziati. Il profilo di autorizzazione è stato implementato:

- accesso in rete al server centrale;
- accesso e utilizzo delle procedure gestionali, servizi finanziari.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

PROTEZIONE DA VIRUS INFORMATICI

Per quanto riguarda la **protezione, di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

- Per garantire la sicurezza e l'integrità dei dati è stato installato su ogni postazione un prodotto antivirus;
- L'aggiornamento dell'antivirus avviene in maniera automatizzata;
- Periodicamente viene effettuata una scansione di ogni postazione.

SISTEMI DI ANTI-INTRUSIONE

Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici (firewall) che il nuovo codice privacy ha reso obbligatoria per i casi in cui si trattino dati sensibili o giudiziari.

Sui singoli PC dotati di sistema operativo Windows XP è stato attivato il firewall windows personale.

AGGIORNAMENTI SOFTWARE

Il terzo aspetto riguarda l'utilizzo di appositi programmi, la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi.

A tale riguardo la nostra organizzazione si è da tempo dotata di tali programmi, per la protezione da malfunzionamenti degli strumenti elettronici, che provvede ad aggiornare con cadenza almeno annuale, che diviene semestrale per gli strumenti con i quali si trattano dati sensibili o giudiziari attraverso interventi di manutenzione ed aggiornamento programmata da parte della società esterna di manutenzione.

Per alcuni personal computer dotati di sistema operativo Win 95/98 non sarà possibile adottare un aggiornamento automatico in quanto il fornitore ha ufficialmente dichiarato che non effettuerà aggiornamenti sui sistemi operativi suindicati. Pertanto per questi sistemi si adotteranno le seguenti misure alternative:

- Il personal computer non verrà utilizzato per memorizzare, in locale, dati personali (verrà utilizzato come postazione per collegarsi al server);
- Migrazione verso sistemi operativi attualmente in assistenza da parte del fornitore: Windows 2000 / XP Professional.
- Aggiornamento manuale semestrale da parte di un tecnico di assistenza.

CUSTODIA E USO DEI SUPPORTI RIMOVIBILI

Per quanto concerne i **supporti rimovibili** (es. floppy disk, dischi ZIP, CD….), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

SICUREZZA DEL SOFTWARE

Presso ciascun ufficio è consentita l'installazione esclusiva delle seguenti tre categorie di software:

- Software commerciale, dotato di licenza d'uso (esempio pacchetti di office automation)
- Software gestionale realizzato specificatamente per l'amministrazione comunale da ditte specializzate nel settore della pubblica amministrazione
- Software realizzato internamente per soddisfare eventuali esigenze particolari del singolo servizio.

L'eventuale installazione di software diversi da quelli citati al punto precedente deve essere preventivamente valutata ed autorizzata dal responsabile dei servizi informatici.

Al fine di prevenire ed evitare la diffusione di virus informatici, il software viene installato solo da supporti fisici originali, dei quali è nota la provenienza.

6.4 Programmazione delle misure di sicurezza da adottare

Trattamenti con l'ausilio di strumenti elettronici

Sistema di autenticazione informatica per accedere agli strumenti elettronici *(credenziali di autenticazione)*

Le procedure software installate sui Server consentono l'attivazione delle credenziali di autenticazione conformi alla normativa attuale (modificabilità della password, lunghezza obbligatoria, scadenza).

Pertanto:

- Devono essere annullate tutte le credenziali attualmente in uso e rilasciate nuove credenziali di autenticazione conformi alla normativa attraverso l'adozione di una procedura operativa e modulistica formale di rilascio.

Le postazioni di lavoro (personal computer) dotati di sistema operativo Win 95/98/ME non consentono l'adozione delle credenziali di autenticazione con i requisiti conformi alla normativa in vigore (user-id/account, password min 8 caratteri, modificabilità autonoma, scadenza ogni 6/3 mesi).

Se i suddetti PC con Windows 95/98/ME non conservano dati in locale, il problema non si pone. Se i PC con Windows 95/98/ME conservano dati in locale, si dovranno adottare le seguenti azioni alternative:

a) Spostare i dati su un server di rete e lasciare tutto il resto invariato, in modo che la protezione e l'autenticazione viene fatta dal server, e a livello di PC client si può tranquillamente continuare a utilizzare i vecchi sistemi operativi;

b) Migrare verso sistemi operativi Window XP Professional (o in alternativa Win 2000) o sostituire il personal computer con un altro più attuale;

c) Installare un software che consente di gestire in modo completo l'uso delle credenziali di autenticazione (es. psw) a prescindere del sistema operativo in uso (software aggiuntivo). Questa funzionalità permetterà di poter continuare ad usare i sistemi Windows 95/98/ME anche per il trattamento dei dati personali.

Misure logiche di autorizzazione per accedere ai dati (sistema di autorizzazione)

L'accesso alle procedure software utilizzano un sistema di autorizzazione differenziata per classi di utenti (Profili di accesso alle procedure).

Entro il 31 dicembre 2006:

- Verificare la sussistenza dei livelli autorizzativi attualmente in uso (profilo di accesso alle procedure per ogni incaricato);
- Annullare tutti i profili autorizzativi attualmente in uso e attribuire nuovi profili di autorizzazione documentando formalmente il rilascio delle autorizzazioni attraverso apposito modulo o lista (questo permette una facile revisione annuale obbligatoria annualmente).

Protezione dai virus informatici

In conformità a quanto disposto dal **punto 16 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** individuare gli idonei strumenti per la protezione degli strumenti elettronici contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento *(Software antivirus).* Anche la precedente normativa prevedeva l'uso di antivirus.

Si suggerisce:

- installare un antivirus centralizzato sul Server che permette in modo automatico l'aggiornamento a tutte le postazioni collegate in rete. In alternativa va installato un software antivirus per ogni postazione;
- Verificare scadenza licenza d'uso del software antivirus per eventuale rinnovo;
- L'antivirus e i log di scansione devono essere monitorati periodicamente da un tecnico (anche esterno).

Programmi finalizzati alla manutenzione logica degli strumenti (Aggiornamento del software)

In conformità a quanto disposto dal **punto 17 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** stabilire la frequenza con cui aggiornare i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti *(Aggiornamento periodico del software).*

Le postazioni di lavoro (personal computer) dotati di sistema operativo Win 95/98/ME non consentono di adottare la regola 17 del disciplinare B del Codice (*"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."*).

Questo perché dal 31 dicembre 2004 la Microsoft non produrrà più alcuna patch o hot-fix di sicurezza per Windows 98, quindi ovviamente non sarà più possibile applicare le patch con frequenza "almeno annualmente o semetrale", per il banale motivo che le patch non saranno più prodotte.

Se i suddetti PC con Windows 95/98/ME non hanno dati in locale, il problema non si pone. Se i PC con Windows 95/98/ME hanno dati in locale si dovranno adottare le seguenti azioni alternative:

a) Spostare i dati su un server di rete e lasciare tutto il resto invariato, in modo da utilizzare il PC esclusivamente come client per collegarsi al server;

b) Migrare verso sistemi operativi Window XP Professional (o in alternativa Win 2000) o sostituire il personal computer con un altro più attuale.

Salvataggio e ripristino dei dati

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** al fine di garantire il salvataggio dei dati periodico dei dati devono essere impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza

almeno settimanale. Inoltre devono essere previste delle procedure di ripristino dei dati entro sette giorni.

Attualmente vengono effettuate copie dei dati contenuti sul Server giornalmente su supporto esterno (nastro magnetico).

Si suggerisce di adottare le seguenti misure di sicurezza:

- Adottare una procedura di controllo dei supporti di memorizzazione;
- Custodire i supporti di salvataggio in luogo sicuro (cassaforte o armadio ignifugo) e comunque non nella stessa sede del Server centrale.

Strumenti anti – intrusione

In conformità a quanto disposto dal **punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)** individuare come proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso abusivo da parte di chiunque abusivamente si introduce nel sistema informatico o telematico *(Firewall – IDS).*

Attualmente non sono adottati dispositivi antintrusione centralizzati (firewall).

Si suggerisce di adottare le seguenti misure di sicurezza:

- La rete deve essere sbarrata all'intrusione da Internet attraverso un sistema software o un dispositivo hardware (**Firewall**) con funzioni di proxy installato su apposito Server;
- I log del traffico vengono monitorati periodicamente da un incaricato (anche soggetto esterno).

Eventuali anomalie devono essere comunicate verbalmente al responsabile dei servizi informatici (Amministratore di sistema).

Sistemi di cifratura dei dati

Per gli eventuali dati sanitari si consiglia l'utilizzo di programmi e tecniche di cifratura dei dati.

Altre misure di sicurezza

Le risorse di memorizzazione (hard disk) delle postazioni locali non devono essere condivise in rete, l'eventuale condivisione dei supporti contenenti dati personali deve essere supportata da valido sistema di autorizzazione degli accessi. E' preferibile adottare sistemi di memorizzazione centralizzati sul server dotato di sistema operativo (o software di gestione documentale) che permette la gestione degli accessi *(S.O. Win Server 2003).*

Attivare salva schermo (Screen Save) con password per non lasciare incustodito la risorsa informatica.

Nell'allegato **5 – RIEPILOGO DELLE MISURE DI SICUREZZA ADOTTATE E DA ADOTTARE** vengono descritti, dettagliatamente, le singole misure adottate e da adottare.

7 CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

La disponibilità dei dati trattati con strumenti elettronici viene garantita dalle seguenti misure:

- Periodicamente vengono effettuate **copie di backup** su supporto esterno e le stesse vengono conservate in luogo sicuro.

Il ripristino e la continuità operativa viene garantito dal "pronto intervento" da parte della struttura esterna di manutenzione dei sistemi coinvolta con apposito contratto di manutenzione preventiva. L'obiettivo di tale coinvolgimento diretto è di ripristinare i servizi informatici **entro sette giorni** e di rendere minime le perdite causate dall'interruzione dell'attività.

Periodicamente, con cadenza almeno semestrale vengono effettuate, a cura della struttura esterna addetta alla manutenzione dei sistemi, delle prove di ripristino, mediante l'esecuzione di appositi test di efficacia delle procedure di salvataggio e di ripristino dei dati adottate.

I supporti di back up vengono conservati in appositi armadi, muniti di serratura e posti in locali distanti dai sistemi elettronici.

8 PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

Sono previsti **interventi formativi degli incaricati del trattamento**, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per il trattamento dei dati o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

In ogni caso, sono previste riunioni periodiche per fare il punto sull'evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali.

Nell'allegato 6 - PIANIFICAZIONE DEGLI INTERVENTI DI FORMAZIONE si riassume un quadro sintetico dell'impegno formativo che si prevede di sostenere nell'anno 2005, in attuazione della normativa sulla privacy.

A conclusione di ogni intervento di formazione il responsabile del trattamento compilerà il modulo MD-FOR-02 Registro presenze corso di formazione riportando i partecipanti al corso, gli argomenti trattati e i docenti che sono intervenuti.

Se l'attività di formazione viene effettuata attraverso struttura esterna dell'azienda, quest'ultima rilascerà apposita relazione e/o attestazione di frequenza.

9 L'AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

1. dal Dlgs 196/2003, se il terzo destinatario è italiano
2. dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

In ogni caso, il soggetto cui le attività sono affidate dichiara:

1. di essere consapevole che i dati che tratterà, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione della normativa per la protezione dei dati personali
2. di ottemperare agli obblighi previsti dalla normativa per la protezione dei dati personali
3. di attenersi alle istruzioni specifiche, eventualmente ricevute per il trattamento dei dati personali, conformando ad esse anche le procedure eventualmente già in essere
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate, e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

Allo stato attuale risultano nominati responsabili esterni:

Trattamenti affidati all'esterno

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure

10 CONTROLLO GENERALE PERIODICO SULLO STATO DELLA SICUREZZA

Perché il piano di sicurezza possa essere realmente efficace, deve essere verificato periodicamente. Il test delle singole misure e del piano nel suo complesso è un aspetto essenziale ed è l'unico strumento che conferisce al piano una credibilità.

Pertanto tutte le aree di rischio e tutte le contromisure adottate devono essere ciclicamente verificate con tecniche e procedure che non lascino dubbi sulla completezza e credibilità del test.

All'amministratore di sistema è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

10.1 Piano di Verifiche periodiche

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile per la sicurezza (amministratore di sistema) e le persone da questo appositamente incaricate provvedono con frequenza periodica, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette
- verificare l'integrità dei dati e delle loro copie di backup
- verificare la sicurezza delle trasmissioni in rete
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

10.2 Aggiornamento periodico del documento

Il presente documento programmatico sulla sicurezza è sottoposto a revisione almeno annuale nella sua interezza, entro la scadenza del 31 marzo di ciascun anno, come previsto dal punto 19. del Disciplinare tecnico Allegato B) al D.Lgs. 196/03, in relazione al disposto dell'art. 34, lettera g) del decreto stesso.

Inoltre sarà rivisto ed aggiornato ogni qualvolta si apportino variazioni al sistema informativo, alle strutture o a qualunque altro elemento individuato dal piano o se ne dovesse ravvisare l'opportunità e/o la necessità in dipendenza di eventi non considerati dal presente programma.

11 ALLEGATI

1	Individuazione dei trattamenti dei dati personali
2	Individuazione delle banche dati
3	Elenco responsabili trattamento dei dati
4	Analisi del rischio - Elenco degli eventi e delle minacce
5	Riepilogo delle misure di sicurezza adottate e da adottare
6	Pianificazione degli interventi di formazione
7	Disposizioni per l'utilizzo degli strumenti informatici