STATUTO DEL COMUNE DI ISOLA DELLA FEMMINE
(Provincia di Palermo)

TITOLO I
PRINCIPI

Art. 1
Il Comune

1. Il Comune di Isola delle Femmine, ente autonomo locale, rappresenta la Comunità residente nel proprio territorio, promuove lo sviluppo e ne cura gli interessi secondo i principi della Costituzione e delle leggi dello Stato.
2. Il territorio del Comune comprende la parte del suolo nazionale limitato con il piano topografico, di cui all'art. 9 della legge 24 dicembre 1954, n. 1228, approvato dall'ISTAT.
3. Il Comune ha sede in Isola delle Femmine nel palazzo municipale.
4. **Il Consiglio Comunale si riunisce nella sede all'uopo specificatamente destinata. In casi particolari e per particolari esigenze, il Consiglio può autodeterminarsi di riunirsi in luoghi diversi**
5. Il Comune ha, come suo segno distintivo, lo stemma riconosciuto con decreto del Presidente della Repubblica n. 2076 del 18 aprile 1990.
6. Il Comune fa uso, nelle cerimonie ufficiali ed in altre pubbliche ricorrenze, del gonfalone descritto nel predetto D.P.R.
7. Nel palazzo, in luogo accessibile al pubblico, è indi-viduato un apposito spazio da destinare ad albo pretorio, per la pubblicazione degli atti previsti dalla legge, dallo statuto e dai regolamenti, nonché per le comunicazioni ai cittadini. Il segretario comunale, per quanto sopra, si avvale di un messo comunale e, su attestazione di questo, ne certifica l'avvenuta pubblicazione.

Art. 2
Significato dello Statuto

1. Il presente statuto è la carta fondamentale dell'autonomia locale isolana, in quanto elaborato ed adottato dal consiglio comunale interpretando la capacità di autogoverno dei cittadini residenti e la loro volontà di contribuire alla costruzione dell'Europa federata ed all'affermazione della pace tra i popoli del mondo.
2. Lo statuto costituisce la fonte normativa che, attuando i principi costituzionali e legislativi dell'autonomia locale, determina l'ordinamento generale del Comune e ne indirizza e regola i procedimenti e gli atti secondo il principio della legalità.
3. Il consiglio comunale adeguerà i contenuti dello statuto al processo di evoluzione della società civile, assicurando costante coerenza tra la normativa statutaria e le condizioni sociali, economiche e civili della comunità che rappresenta.

Art. 3
Finalità

1. 1.Il Comune promuove la piena affermazione dei diritti inviolabili della persona, consolida cd estende i valori di libertà, democrazia, solidarietà con particolare riguardo alle categorie più svantaggiate.
2. Il Comune garantisce eguaglianza di trattamento alle persone e alle formazioni sociali, senza distinzione di età, sesso, razza, lingua, religione, opinione, condizione personale o sociale.
3. Il Comune promuove pari condizioni nell'accesso ai servizi organizzati o controllati dall'amministrazione comunale e promuove azioni per favorire pari opportunità tra donne e uomini.
4. Il Comune favorisce l'organizzazione della vita urbana per meglio rispondere alle esigenze dei cittadini e dei nuclei familiari. Armonizza gli orari dei servizi con le esigenze dei cittadini. Concorre con altre istituzioni regionali, nazionali e comunitarie alla riduzione dell'inquinamento al fine di assicurare, attraverso l'utilizzazione razionale ed equa delle risorse, le necessità delle generazioni attuali e future.
5. Il Comune valorizza lo sviluppo economico e sociale della comunità e promuove la partecipazione dell'iniziativa economica privata alla realizzazione di obiettivi di interesse generale. Promuove un equilibrato assetto del territorio nel rispetto dell'ambiente. Tutela la salute dei cittadini. Favorisce la soluzione del bisogno abitativo, valorizza il patrimonio storico della città e le tradizioni culturali.
6. Il Comune rende effettivo il diritto alla partecipazione politica ed amministrativa, garantendo un'informazione completa ed effettiva sull'attività svolta. Tutela il diritto dei cittadini e delle formazioni sociali di concorrere allo svolgimento ed al controllo delle attività dell'amministrazione comunale.
7. Il Comune valorizza le risorse e le attività culturali, formative e di ricerca e promuove la più ampia collaborazione con le istituzioni culturali, educative e formative statali, regionali e locali.
8. Il Comune promuove la tutela della vita umana e della famiglia, valorizza la maternità e la paternità, assicurando sostegno ai genitori nell'educazione e nella cura dei figli.
9. Il Comune sostiene e valorizza le iniziative del volontariato e delle libere associazioni.
10. Il Comune garantisce il pieno rispetto della dignità umana e dei diritti di libertà e di autonomia della persona handicappata e promuove l'assistenza e l'integrazione sociale delle persone handicappate.
11. Il Comune promuove le attività sportive, ricreative e del tempo libero.

Art. 4
I principi dell'organizzazione dell'attività comunale

1. Il funzionamento e l'organizzazione dal Comune devono essere ispirati ai principi di trasparenza, imparzialità, efficienza, efficacia, economicità, semplificazione dei procedimenti e degli atti.
2. I regolamenti comunali dovranno tradurre le direttive emanate dalle autorità competenti in merito alla lotta contro la delinquenza di tipo mafioso.

3. Il Comune attua nella propria organizzazione il principio della separazione tra responsabilità politica e responsabilità burocratica e promuove le diverse forme di collaborazione previste dalla legge per lo svolgimento di funzioni e servizi, con soggetti pubblici e privati.

TITOLO II
ISTITUTI DI PARTECIPAZIONE

CAPO I
Partecipazione popolare

Art. 5
Titolari dei diritti di partecipazione

1. Titolari dei diritti di partecipazione di cui al presente capo, salvo espressa eccezione, sono:
a) i cittadini iscritti nelle liste elettorali del Comune h di Isola delle Femmine;
b) i cittadini residenti nel Comune, non ancora elettori, che abbiano compiuto il sedicesimo anno di età;
c) i cittadini non residenti, purché esercitino nel Comune la propria attività prevalente di lavoro;
d) gli stranieri e gli apolidi residenti nel Comune o che, comunque, svolgano la propria attività prevalente di a lavoro in Isola delle Femmine.
2. I diritti di partecipazione possono essere esercitati da persone singole o da associazioni.

Art. 6
Diritto di udienza

1. Il Comune garantisce ai cittadini, singoli o associati, il diritto di udienza, da esercitarsi nei confronti degli amministratori e dei funzionari del Comune preposti agli uffici e ai servizi comunali, nelle forme e secondo le modalità stabilite dal regolamento.
2. Il diritto di udienza si traduce nel diritto ad essere ricevuto per la prospettazione di problemi o di questioni di interesse individuale o collettivo di competenza del Comune e nel conseguente obbligo di ricevimento e di risposta da parte dei soggetti di cui al precedente comma.
3. Il regolamento stabilirà le modalità procedurali e le relative disposizioni di carattere organizzativo.

Art. 7
Libere forme associative

1. Il Comune valorizza le libere forme associative e le organizzazioni di volontariato prevedendone la partecipazione effettiva alla propria attività e assicurandone l'accesso alle strutture e ai servizi comunali nel rispetto delle norme statutarie e regolamentari a tutela della parità di trattamento.
2. Le associazioni senza scopo di lucro iscritte nel registro anagrafico di cui all'art.. 8 e le società cooperative senza scopo di lucro operanti nei settori dell'assistenza,

della protezione dell'ambiente, della cultura, della scuola e della scienza, dello sport e del tempo libero o espletanti comunque servizi di interesse collettivo, possono presentare al Comune specifici progetti, corredati di un piano tecnico e finanziario inerenti attività ed iniziative di interesse generale.
3. Qualora i progetti siano riconosciuti dall'amministrazione comunale validi e congrui sui piano tecnico e finanziario, i soggetti di cui al comma precedente possono ottenere dal Comune contributi o ausili finanziari, anche sotto forma di servizi, nei limiti e secondo le modalità stabiliti nel regolamento.
4. In ogni caso, la concessione di strutture, beni strumentali, contributi, sussidi ed ausili finanziari e servizi ad associazioni o ad altri organismi privati va disciplinata con apposite convenzioni ed è subordinata alla previa determinazione da parte del consiglio comunale e alla conseguente pubblicazione dei criteri e delle modalità cui il Comune è tenuto ad attenersi.

Le convenzioni con le organizzazioni di volontariato sono subordinate alle condizioni ed ai contenuti di cui all'ari. 8 della legge 11 agosto 1991, n. 166.
5. Ai fini del precedente comma, il consiglio comunale, in sede di approvazione del bilancio preventivo, stabilisce i settori prioritari da sostenere. Sono, in ogni caso, prioritari di diritto, gli interventi finanziari in favore delle associazioni, società cooperative e organizzazioni di volontariato per la realizzazione e il sostegno di comunità-alloggio e centri socio-riabilitativi per persone handicappate in situazioni di gravità, alle condizioni di cui all'art. 10, 3° comma della legge 5 febbraio 1992, n. 104.
6. L'elenco delle associazioni o di altri organismi privati che hanno usufruito delle concessioni di strutture, contributi o servizi, va reso annualmente pubblico dalla giunta comunale, utilizzando idonei strumenti di informazione a livello locale.

Art. 8
Anagrafe delle associazioni

1. Per potere beneficiare delle forme di sostegno di cui al precedente articolo, le associazioni senza scopo di lucro, regolarmente costituite ed operanti nel territorio del Comune da almeno un anno, debbono essere iscritte in un registro anagrafico comunale, articolato in sezioni tematiche, che viene periodicamente aggiornato a cura dell'amministrazione comunale.
2. Ai tini dell'iscrizione al registro anagrafico basta la presentazione da parte delle associazioni di una scrittura privata avente data certa, dalla quale risultino le finalità, la sede, le fonti di finanziamento e i soggetti che abbiano la rappresentanza legale dell'organismo associativo.
3. La mancata iscrizione al registro anagrafico non può, in ogni caso, costituire motivo di esclusione delle associazioni dall'esercizio dei diritti di partecipazione di cui alla legge e al presente statuto.

Art. 9
Iniziative popolari

1. Ai fini di una migliore e più efficace tutela di interessi collettivi, i cittadini, singoli o associati, possono rivolgere al Comune:

- interrogazioni per chiedere conto di comportamenti o atti o aspetti della gestione comunale non conoscibili attraverso l'esercizio del diritto di informazione di cui all'art 11;

- istanze e petizioni per l'emanazione di provvedimenti amministrativi o esporre comuni necessità;
- proposte di deliberazioni consiliari comunali, mediante la presentazione al consiglio comunale di uno schema di delibera redatto nelle forme di legge.

2. Alle interrogazioni, sottoscritte da almeno 20 cittadini, e alle istanze e petizioni, queste ultime sottoscritte da almeno 30 cittadini e depositate presso la segreteria comunale, va data risposta scritta e motivata da parte dell'organo competente, almeno entro 30 giorni dalla loro ricezione. In ogni caso, per la loro presentazione non è richiesta alcuna particolare formalità.

3. L'iniziativa popolare degli atti di competenza del consiglio comunale si esercita mediante la presentazione di un progetto di deliberazione accompagnato da una relazione illustrativa, con non meno di 100 firme autenticate raccolte nel mese precedente al deposito.

4. Il progetto di deliberazione di iniziativa popolare va esaminato dal consiglio comunale entro due mesi dal deposito del testo, sottoscritto, presso la segreteria comunale.

5. I progetti di deliberazione, di cui al precedente comma 3, sono equiparati, ai fini dei pareri previsti dall'art. 53, comma 1, della legge 8 giugno 1990, n. 142, alle proposte di deliberazione sottoposte al consiglio.

6. Per i problemi del tempo libero, della pesca, della cultura e del commercio, l'amministrazione comunale si avvarrà della consulenza di un'apposita commissione la cui composizione ed i relativi compiti saranno stabiliti da apposito regolamento che prevederà la rappresentanza, in seno a detto organo, anche delle associazioni giovanili locali, delle organizzazioni sindacali, dei commercianti e dei pescatori.

Art. 10
Consultazione popolare

1. Il consiglio comunale, su proposta della giunta o di un quinto dei componenti il consiglio stesso, può indire consultazioni popolari su problemi e questioni di interesse comune, secondo le modalità disciplinate dal regolamento, anche con la previsione dell'utilizzo di mezzi informatici e telematici.

2. Delle risultanze della consultazione va immediatamente data comunicazione da parte del sindaco al consiglio comunale, perché provveda, secondo le modalità stabilite dal regolamento, al loro tempestivo esame. Dell'esito dell'esame e dei conseguenti provvedimenti eventualmente adottati va data adeguata pubblicità a termini dell'art. 11.

3. Il Comune utilizzando questionari, indagini per campione, assemblee pubbliche e altri strumenti può acquisire, secondo le modalità disciplinate dal regolamento, su un problema specifico le valutazioni di settori particolari della popolazione come i giovani, le donne, gli anziani, il mondo del lavoro, quello della scuola e quello della famiglia.

Art. 11
Diritto di informazione

1. Al fine di assicurare la più ampia partecipazione dei cittadini alla vita sociale e politica, il Comune assicura e garantisce il diritto all'informazione, rendendo pubblici,

anche attraverso proprie pubblicazioni distribuite gratuitamente ai richiedenti, dati, criteri, indirizzi e programmi relativi alla gestione concreta delle risorse finanziarie dei Comune, agli appalti di opere pubbliche, alle forniture di beni e servizi, alla concessione di strutture, beni strumentali, contributi o servizi ad associazioni o altri organismi privati.
2. Il Comune, inoltre, provvederà ad informare, nelle stesse forme, dei criteri e delle modalità di accesso ai servizi e alle prestazioni resi dal Comune o dagli organismi da esso dipendenti o controllati, nonché termini e tempi di conclusione dei procedimenti amministrativi.
3. L'ente deve di norma avvalersi, oltre che dei sistemi tradizionali della notificazione e della pubblicazione all'albo pretorio, anche dei mezzi di comunicazione ritenuti più idonei ad assicurare il massimo della conoscenza degli atti, tipo TV locali.
4. L'informazione deve essere tempestiva e completa e, per gli atti aventi una pluralità indistinta di destinatari, deve avere carattere di generalità.
5. La giunta comunale adotta i provvedimenti organizzativi interni ritenuti idonei a dare concreta attuazione al diritto di informazione, anche con stipula di apposite convenzioni con TV locali.
6. Il regolamento sul diritto di accesso detta norme atte a garantire l'informazione ai cittadini, nel rispetto dei principi sopra enunciati.

CAPO II
REFERENDUM

Art. 12
Referendum consultivo

1. È indetto referendum consultivo quando ne facciano richiesta almeno il 15% dei cittadini; **detto quorum è calcolato sulla base dei cittadini italiani iscritti nelle liste elettorali del Comune e dei cittadini comunitari ed extracomunitari aventi residenza continuativa nel Comune da almeno 5 (cinque) anni e per i quali non sussistano cause di esclusione dall'elettorato attivo secondo i principi dell'Ordinamento vigente.**
2. **Oggetto del referendum sono proposte o questioni di rilevanza generali rientranti nella competenza dell'Ente.**
3. Il referendum consultivo può essere indetto anche dal consiglio comunale, su iniziativa della giunta comunale o di un quinto dei componenti del consiglio.
4. Nell'ipotesi di cui al primo comma del presente articolo, la richiesta di referendum va presentata da un comitato promotore composto da almeno venti cittadini **residenti**
5. Non possono sottoporsi a referendum:
   -lo statuto;
   - i regolamenti del consiglio comunale;
   - il bilancio preventivo e il conto consuntivo;
   - i provvedimenti riguardanti tributi e tariffe;
   - i provvedimenti di assunzione di mutui o relativi ad emissione di prestiti;
   - gli atti relativi al personale del Comune;
   - gli oggetti sui quali il consiglio è chiamato ad esprimersi entro termini stabiliti dalla legge;
   - gli atti riguardanti la tutela dei diritti delle minoranze etniche, religiose e degli immigrati.
6. A seguito della indizione del referendum il consiglio comunale sospende qualsiasi determinazione sull'oggetto del referendum, salvo che, con delibera adottata con la maggioranza dei due terzi dei consiglieri assegnati, non decida diversamente per ragioni particolari di necessità ed urgenza.
7. Prima della raccolta delle firme, che deve avvenire entro un arco di tempo che non può superare i due mesi, la proposta va sottoposta al giudizio di ammissibilità di un comitato dei garanti, di cui al successivo art. 15.
8. **Al voto saranno ammessi a partecipare oltre agli elettori iscritti nelle liste elettorali anche i cittadini extracomunitari in possesso del permesso di soggiorno e residenti in questo Comune da almeno sei anni nonché i cittadini comunitari residenti da almeno sei mesi.**
9. 9.Sull'oggetto del referendum è chiamato a pronunciarsi il consiglio comunale entro tre mesi dal suo svolgimento, semprecché abbiano partecipato al voto il cinquanta per cento **degli aventi diritto**.
10. Non è consentito in un anno lo svolgimento di più di una tornata referendaria e su non più di sei quesiti. Non possono essere indetti referendum nei dodici mesi precedenti la scadenza del mandato amministrativo, né possono svolgersi in concomitanza con altre operazioni di voto.

11. I criteri di formulazione del quesito referendario, che, in ogni caso, deve rispondere a requisiti di chiarezza ed omogeneità, le modalità di raccolta ed autenticazione delle firme e di svolgimento delle operazioni di voto saranno determinati dal regolamento.

Art.13
Referendum propositivo

1. E' indetto referendum propositivo quando sia stata depositata presso il consiglio comunale una proposta corredata da una relazione illustrativa, sottoscritta da almeno il 15% **degli aventi diritto come individuati al comma 1 dell'art.12.**

2. Al referendum propositivo si applicano le disposizioni contenute nel precedente art. 12.

Art. 14
Referendum di consultazione successiva

1. Alle stesse condizioni e modalità di cui all'art. 12 è indetto referendum consultivo sulle proposte di revoca di deliberazioni consiliari o, nei casi stabiliti dal regolamento, di deliberazioni della giunta, quando la proposta sia presentata entro 120 giorni dalla esecutività della deliberazione.

2. Non si procede al referendum quando l'atto oggetto della proposta sia stato annullato o revocato totalmente. Nell'ipotesi di annullamento o revoca parziale, anche se seguiti da una nuova deliberazione sul medesimo oggetto, sulla prosecuzione del referendum o sulla impraticabilità deciderà il comitato dei garanti di cui all'art. 15.

Art. 15
Comitato dei garanti

1. Il comitato dei garanti è composto da tre membri ed è eletto dal consiglio comunale con voto limitato ad uno, risultando eletti i soggetti che hanno riportato il maggior numero di voti.

Il comitato dei garanti dura in carica 4 anni.

2. I garanti sono scelti tra magistrati a riposo, professori universitari di ruolo di discipline giuridiche, funzionari pubblici in servizio o in quiescenza di grado non inferiore a dirigenti o avvocati con almeno 10 anni di esercizio nella professione.

3. Spetta al comitato dei garanti decidere sull'amrnissibilità del referendum, sulla formulazione dei quesiti e sui procedimenti conseguenti nei casi e con le modalità stabiliti dal presente statuto e dal regolamento.

4. Le decisioni del comitato sono pubbliche e vanno pubblicizzate mediante manifesto murale.

5. Al comitato dei garanti va assicurata una adeguata struttura organizzativa.

CAPO III
PARTECIPAZIONE AL PROCEDIMENTO E DIRITTO DI ACCESSO

Art. 16
Partecipazione ai procedimenti amministrativi individuali

1. in armonia con i principi di cui alla legge regionale 30 aprile 1991, n. 10 e in attuazione dei criteri ivi stabiliti di economicità, di efficacia e di pubblicità dell'azione amministrativa, il Comune garantisce la partecipazione dei destinatari, degli interessati e dei soggetti portatori di interessi pubblici o privati, nonché dei portatori di interessi diffusi costituiti in associazioni o comitati, cui possa derivare un pregiudizio dal provvedimento, ai procedimenti amministrativi, riguardanti materie di propria competenza.
2. Fermo restando il disposto del precedente comma, il regolamento avrà cura di disciplinare il diritto dei destinatari e degli interessati:
a) di essere ascoltati dal responsabile del procedimento su fatti e circostanze rilevanti ai fini dell'emanazione del provvedimento finale;
b) di assistere alle eventuali ispezioni o accertamenti rilevanti agli stessi fini;
c) di essere sostituiti da un rappresentante legale

Art. 17
Diritto di accesso ai documenti amministrativi

1. Il Comune garantisce a tutti i cittadini, singoli o associati, il diritto di accesso ai documenti amministrati, nel rispetto dei principi stabiliti nella legge regionali 30 aprile 1991, n. 10, delle disposizioni di cui all'art. 1, comma 1, lett. b) della legge regionale 11 dicembre 1991 n. 48, del presente statuto e secondo le modalità fissati dall'apposito regolamento.
2. Il regolamento, oltre a disciplinare le modalità dell'accesso e a stabilire i casi in cui lo stesso è esclusa o differito ai sensi dell'ari. 27 della legge regionale 30 aprile 1991, n. 10, provvede a dettare le misure organizzative idonee a rendere effettivo l'esercizio del diritto, anche coi la costituzione di un apposito ufficio per l'accesso.
3.I provvedimenti finali emessi dagli organi de Comune sono pubblici, anche se non ancora esecutivi a sensi di legge. I documenti in essi richiamati sono conoscibili, fatta salva la facoltà dell'amministrazione di noi con esibire quei documenti o di sopprimere quei particolari che comportino violazione del diritto alla riservatezza di persone, gruppi o imprese.

Capo IV
Difensore civico
S O P P R E S S O

TITOLO III
GLI ORGANI DI GOVERNO DEL COMUNE

Art. 18
Organi di governo

1. Sono organi di governo del Comune: il consiglio, la giunta, il sindaco.

CAPO I
IL CONSIGLIO

Art. 19
Competenze del consiglio

1. Il consiglio rappresenta l'intera comunità locale, determina l'indirizzo politico-amministrativo del Comune e ne controlla l'attuazione, adottando gli alti attribuiti dalla legge alla sua competenza.

Art. 20
Funzioni di indirizzo e di programmazione

1 La funzione di indirizzo del consiglio si esprime attraverso atti di indirizzo generale per i singoli settori omogenei che impegnano la giunta e che indicano i risultati da raggiungere, le risorse impegnate, i tempi previsti. In tal caso la giunta fornisce al consiglio rapporti periodici che consentano di verificare l'andamento della gestione rispetto agli obiettivi fissati.

2. La funzione di programmazione del consiglio si esprime in particolare attraverso l'adozione di un documento di indirizzi generali, finalizzato alla predisposizione del bilancio annuale e pluriennale, che contenga sia un'ipotesi sull'andamento complessivo delle risorse finanziarie disponibili per l'ente, che la determinazione delle priorità di intervento e l'assegnazione delle risorse per grandi aggregati.

Arl. 21
Durata in carica

1. L'elezione del consiglio, la durata in carica, il numero dei consiglieri e la loro posizione giuridica sono regolati dalla legge.

2. Il Consiglio verrà integrato da Consiglieri eletti da cittadini comunitari o extracomunitari residenti nel territorio del Comune che avranno il diritto di partecipare ad ogni sessione consiliare, con diritto di espressione sugli argomenti di rilevanza dei cittadini rappresentati. Agli stessi non spetta, in ogni caso, diritto di voto.

3. Il numero dei Consiglieri aggiunti viene fissato in 1 (uno) ogni 500 (o frazione superiore a 250) cittadini comunitari o extracomunitari residenti nel Comune.

4. L'adozione da parte dello Stato di norme più favorevoli che prevedano il diritti dei cittadini non in possesso della cittadinanza italiana all'elettorato

attivo e/o passivo comporterà l'automatica soppressione dei precedenti commi 2 e 3, con la sostituzione automatica delle previsioni normative statali.

5. Il consiglio comunale decade nei casi e con le modalità previste dalla legge.

6. I consiglieri presentano al segretario comunale, che ne fa menzione nel verbale in consiglio, le dimissioni che sono irrevocabili, immediatamente efficaci e non necessitano di presa d'atto.

7. L'eventuale rinunzia del subentrante o la presenza di cause di ineleggibilità che dovessero successivamente intervenire non alterano la completezza del consiglio stesso.

8. Il consiglio dura in carica sino all'elezione del nuovo limitandosi, dopo la pubblicazione del decreto di indizione dei comizi elettorali, ad adottare gli atti urgenti ed improrogabili.

Art. 22
I consiglieri

1. I consiglieri comunali rappresentano l'intera comunità ed esercitano la funzione senza vincolo di mandato.
2. I consiglieri sono immessi nell'esercizio delle loro funzioni con il giuramento.
3. Ciascun consigliere, secondo le procedure e le modalità stabilite dai regolamenti, ha diritto di:

a) esercitare l'iniziativa per tutti gli atti di competenza del consiglio, salvi i casi in cui l'iniziativa è riservata agli altri organi in base alla legge;

h) presentare interrogazioni e mozioni, secondo le modalità stabilite dal regolamento interno;

e) intervenire nella discussione, presentare emendamenti alle proposte di delibere poste in discussione e votare su ciascun oggetto all'ordine del giorno.

4. Le iniziative e gli emendamenti di cui al precedente comma che comportino oneri finanziari devono prevedere la copertura di bilancio. Il segretario comunale cura che le proposte siano sottoposte al consiglio corredate dai pareri previsti dalla legge.
5. I consiglieri, in numero non inferiore ad un quinto di quelli in carica, possono richiedere al presidente del consiglio la convocazione del consiglio comunale, con l'indicazione degli argomenti da trattare.

soppresso comma 6

7. Ogni consigliere è tenuto a rendere pubblica la propria situazione patrimoniale al momento dell'elezione e durante lo svolgimento del mandato, mediante deposito presso l'ente di dichiarazioni annuali concernenti i redditi, i diritti reali su beni immobili e su beni mobili, iscritti nei pubblici registri, le azioni di società e le quote di partecipazione a società, l'esercizio di funzioni di amministratore o di sindaco di società.
8. Decade il consigliere che senza giustificato motivo non intervenga a tre sedute consecutive del consiglio. La decadenza è dichiarata dal Consiglio a maggioranza dei due terzi dei suoi componenti, su iniziativa della Presidenza o di un qualsiasi Consigliere, sentito l'interessato, con preavviso di dieci giorni.

Art. 23
Accesso dei consiglieri agli atti e alle informazioni

1. I consiglieri hanno diritto di prendere visione dei provvedimenti adottati dal Comune e degli atti preparatori in essi richiamati, nonché di avere tutte le informazioni necessarie all'esercizio del mandato e di ottenere, senza spesa, copia degli atti deliberativi.
2. Le modalità di esercizio del diritto sono disciplinate dal regolamento nel rispetto dei seguenti principi:
a) il consigliere è tenuto al segreto nei casi previsti dalla legge;
b) nel caso di atti preparatori, l'accesso è ammesso nei confronti della determinazione finale dell'unità organizzativa competente ad emanarla;
c) il sindaco nega l'accesso con atto motivato nei casi previsti dalla legge.

Art. 24
Regolamento interno

1. Il consiglio comunale adotta il proprio regolamento che disciplina l'organizzazione e il funzionamento del consiglio.
2. Il regolamento è adottato con il voto favorevole della maggioranza assoluta dei consiglieri assegnati al Comune.

Art. 25
Gruppi consiliari

1. I consiglieri possono costituirsi in gruppi secondo quanto previsto nel regolamento e ne danno comunicazione al segretario comunale.
2. Qualora non si eserciti tale facoltà o nelle more della designazione, i capigruppo sono individuati nei consiglieri che abbiano riportato il maggior numero di voti per ogni lista.
3. Il regolamento dovrà prevedere l'assegnazione agli eventuali gruppi consiliari di idonee strutture per l'esercizio delle loro funzioni.

Arl. 26
Conferenza dei capigruppo

1. Il regolamento può prevedere la conferenza dei capigruppo e le relative attribuzioni.
2. La giunta mantiene rapporti con i gruppi consiliari assicurando agli stessi l'assolvimento delle loro funzioni.

Art. 27
Commissioni consiliari speciali

1 - Il consiglio può istituire commissioni speciali, formate da consiglieri in modo da rispettare proporzionalmente la consistenza numerica di ciascun gruppo consiliare, per l'esame e la risoluzione di particolari questioni, determinandone la composizione, l'organizzazione, le competenze, i poteri e la durata.
2. Alle sedute delle commissioni hanno facoltà di partecipare, anche su invito della commissione, il sindaco e gli assessori, senza diritto di voto.

3. Le commissioni possono chiedere l'intervento alle proprie riunioni dei dirigenti e dei titolari degli uffici comunali, previa autorizzazione del sindaco o dell'assessore responsabile per il settore.

Art. 28
Prima convocazione e adempimenti della prima adunanza

1- La prima convocazione del consiglio comunale è disposta dal presidente uscente entro 15 gg. dalla proclamazione degli eletti. Qualora il presidente uscente non provveda, la convocazione è disposta dal consigliere neo-eletto che ha riportato il maggior numero di preferenze e che presiede l'assemblea fino all'elezione del presidente.
2. Nella prima adunanza e, dove occorra, in quella immediatamente successiva, il consiglio procede alla convalida dei consiglieri eletti ed alle eventuali surroghe; quindi, secondo quanto previsto dalla legge, elegge nel suo seno il presidente ed il vice presidente.

Art. 29
Attribuzioni del Presidente del consiglio comunale

1. Il presidente dei consiglio comunale convoca e presiede il consiglio comunale, dirige il dibattito e cura la diramazione degli avvisi di convocazione.
2. Esso dispone l'iscrizione all'o.d.g. degli adempimenti previsti dalla legge e dallo statuto dando la precedenza, ove compatibili, alle proposte del sindaco.
3. Cura la trattazione degli atti ispettivi.
4. In collaborazione con il segretario comunale accerta che le proposte di deliberazione da iscrivere all'Od.G. siano corredate dai pareri previsti dalla legge e siano messe a disposizione dei consiglieri almeno 3 giorni prima e 24 ore prima nei casi d'urgenza.

Art. 30
Cessazione della carica di presidente

1. Il presidente del consiglio cessa dalla carica in caso di approvazione di una mozione di sfiducia costruttiva, per appello nominale, con voto della maggioranza assoluta dei consiglieri assegnati al Comune, ovvero in caso di dimissioni o per perdita della qualità di consigliere comunale, nonché per revoca consiliare.
2. La mozione motivata deve essere sottoscritta da almeno 1/3 dei consiglieri e deve contenere il nominativo del nuovo presidente del consiglio.
3. La mozione viene messa in discussione non prima di 5 e non oltre 10 giorni dalla sua presentazione, presso la segreteria comunale.
4. L'approvazione della mozione comporta la cessazione immediata dalla carica del presidente del consiglio e la proclamazione del nuovo presidente.
5. **La deliberazione di cui al comma precedente è immediatamente esecutiva.**
6. Il presidente cessa, altresì, dalla carica per dimissioni, le quali vengono presentate al consiglio mediante deposito presso la segreteria comunale ovvero a seguito di verbalizzazione nel corso di sedute di organi collegiali. Esse sono irrevocabili, immediatamente efficaci e non necessitano di presa d'atto.
7. In caso di ripetuti e persistenti violazioni di legge o di disposizioni statutarie, su proposta della giunta comunale o di 1/3 dei consigli assegnati, il consiglio può

revocare il presidente con apposito atto adottato a scrutinio palese e con la maggioranza assoluta dei consiglieri assegnati.
8. Gli istituti di cui sopra si applicano anche nei confronti del vice presidente.

Art. 31
Funzionamento del consiglio

1. Il consiglio comunale è convocato e presieduto dal presidente o, in caso di assenza o impedimento, dal vice presidente e, in mancanza del vice presidente, dal consigliere presente che ha riportato il maggior numero di preferenze individuali.
2. Nessuna proposta può essere sottoposta a deliberazione se non è stata iscritta all'ordine del giorno e se gli atti non siano stati messi a disposizione dei consiglieri almeno tre giorni utili prima o ventiquattro ore prima nei casi di urgenza.
3. Salvi i casi previsti dalla legge e dal regolamento interno, le sedute sono pubbliche e le votazioni si effettuano a scrutinio palese.

CAPO II
LA GIUNTA E IL SINDACO

Art. 32
La giunta

1. La giunta comunale è composta dal Sindaco, che la presiede, e da **un numero di assessori sino ad un massimo di un terzo del numero dei componenti il** Consiglio comunale.

2. Il Sindaco nomina tra gli assessori il vice sindaco che lo sostituisce in caso di assenza o di impedimento.

Qualora sia assente o impedito anche il vice sindaco, fa le veci del sindaco l'assessore più anziano per età.

Art. 33
Relazione sullo stato di attuazione del programma

1. Il sindaco, ogni 6 mesi, presenta al consiglio comunale una relazione scritta sullo stato di attuazione del programma e sull'attività svolta nonché su fatti particolarmente rilevanti.
2. Sulla relazione di cui al 1° comma, il consiglio Comunale, entro 10 gg., esprime le proprie valutazioni.

Art. 34
Elezione del sindaco

1. Le modalità di elezione del sindaco e le condizioni di eleggibilità sono stabilite dalla legge.
2. **Il Sindaco presta giuramento di osservare lealmente la Costituzione Italiana davanti al Consiglio nella seduta di insediamento dello stesso.**

Art. 35
Elezione e durata della giunta

1. Il sindaco nomina gli assessori secondo le modalità stabilite dalla legge.
2. La durata della giunta è fissata in anni **cinque.**
3. Il sindaco entro 10 giorni dall'insediamento comunica al consiglio la composizione della giunta.
4. Gli assessori sono immessi nell'esercizio delle loro funzioni con il giuramento.

Art. 36
Assessori

1. Le cause di ineleggibilità o incompatibilità alla carica di assessore sono stabilite dalla legge. In ogni caso la carica di componente della giunta è incompatibile con quella di consigliere comunale.

2. I componenti della giunta devono avere specifiche professionalità e/o particolari competenze in relazione all'attuazione degli obiettivi indicati nel documento programmatico.

Art. 37
Rimozione del sindaco

1. Il consiglio comunale, a seguito di deliberazione **adottata con la maggioranza dei due terzi dei suoi componenti** e secondo quanto previsto dalla legge, può promuovere, una sola volta nel **quinquennio**, la consultazione del corpo elettorale sulla rimozione del sindaco.

Art. 38
Cessazione della carica di sindaco

1. La cessazione dalla carica di sindaco, per qualsiasi motivo, comporta la cessazione dalla carica dell'intera giunta.
2. Le competenze del sindaco e della 'giunta, cessati per qualsiasi motivo, sono devolute ad un commissario nominato secondo legge.
3. Le dimissioni dalla carica del sindaco e degli assessori sono depositate nella segreteria comunale o formalizzate in giunta. Esse sono irrevocabili, definitive e non necessitano di presa d'atto.
4. La nuova elezione del sindaco ha luogo secondo quanto previsto dalla legge.
5. La decadenza del sindaco a seguito della consultazione elettorale, di cui all'art. 40 è regolata dalla legge.

Art. 39
Revoca, sostituzione e dimissioni di assessori

1. Gli assessori sono revocati dal sindaco che provvede, con atto motivato, alla nomina contemporanea dei sostituti.
2. Il sindaco comunica al consiglio comunale, entro 7 giorni, le motivazioni del provvedimento di cui al 1 comma.
3. Le dimissioni dalla carica di assessore sono presentate al sindaco.
4. Alla sostituzione dei componenti la giunta che siano dimissionari o cessati dall'ufficio per altra causa, provvede con atto motivato il sindaco mediante nomina entro 3 giorni dalla cessazione.

Art. 40
Attribuzioni della Giunta

La giunta comunale ha competenza per le materie appresso indicate:
- **schema dello statuto comunale e sue modifiche;**
- **regolamento sull'ordinamento degli uffici e dei servizi, nel rispetto dei criteri generali stabiliti dal consiglio comunale, dotazione organica del personale, costituzione dei gruppi di lavoro, assegnazione delle risorse umane agli uffici anche mediante mobilità interna ed esterna;**

- **nomina dei legali in tema di azioni e resistenze in giudizio;**
- **programma triennale dei fabbisogno di personale ed avvio delle procedure concorsuali;**
- **riassunzione di personale già dimessosi volontariamente;**
- **approvazione dei progetti preliminari e di massima;**
- **assunzione del personale, dopo l'esperimento delle procedure concorsuali, da parte dei dirigenti;**
- **atti di indirizzo relativi a: contributi, sovvenzioni, patrocini, individuazione di manifestazioni, spettacoli, attività sportive, esibizioni di artisti e simili;**
- **delega ai Comuni per la realizzazione dei servizi provinciali;**
- **piano esecutivo di gestione;**
- **autorizzazione alle transazioni;**
- **perizie di varianti che importino una maggiore spesa;**
- **indirizzi generali operativi per il riconoscimento di interessi, compensi, rimborsi ed esenzioni di competenza dei dirigenti;**
- **indennità di carica dei sindaco e degli assessori in applicazione del regolamento previsto dall'art. 19 della legge regionale n. 30/2000 in caso di modifica delle misure previste nel regolamento emanato con D.P.R.S. n. 19 del 2001;**
- **permute immobiliari;**
- **vendita suolo e sottosuolo demaniale;**
- **presa d'atto contratti di lavoro del personale e determinazione monte spesa da assegnare ai singoli settori;**
- **autorizzazione alla stipula dei contratti d'opera ai sensi dell'art. 2222 e seguenti del codice civile;**
- **modifica delle tariffe dei tributi di competenza dei Comune ed elaborazione e proposizione al consiglio dei criteri per la determinazione di quelli nuovi;**
- **assenso per la revoca del segretario generale;**
- **adotta, nei limiti e con le forme del regolamento di contabilità, il prelevamento dal fondo di riserva e lo storno di fondi tra stanziamenti appartenenti allo stesso servizio;**
- **approva e dispone le alienazioni, l'accettazione o il rifiuto di lasciti o donazioni, le servitù di ogni genere e tipo, le classificazioni dei beni patrimoniali;**
- **recepisce i contratti di lavoro e approva i contratti decentrati, per le materie non riservate ad altri organi;**
- **autorizza il sindaco a stare in giudizio come attore o come convenuto, innanzi alla magistratura ordinaria, amministrativa, agli organi amministrativi o tributari;**
- **atti di alta discrezionalità amministrativa.**

Art. 41

Competenze del sindaco *(art.* 13, legge regionale n. 7/92 arl. 41, legge regionale n. 26/93)

1. **Il Sindaco è capo dell'amministrazione comunale e la rappresenta. In particolare :**

a. **mantiene l'unità di indirizzo politico-amministrativo della giunta e ne coordina l'attività, disponendo eventualmente la costituzione di comitati interassessoriali per la trattazione di questioni determinate;**

b. trasmette al presidente del consiglio comunale le proposte di deliberazione di iniziativa della giunta;

c. verifica l'attuazione dei programmi e la conformità dell'attività degli enti, aziende ed organismi promossi dal Comune agli indirizzi deliberati dagli organi competenti e riferisce periodicamente al Consiglio;

d. adotta le ordinanze nei casi stabiliti dalla legge;

e. indice i referendum comunali;

f. promuove contatti ad incontri che garantiscano collaborazione e cooperazione con altri Comuni, la Regione, la Provincia, le amministrazioni statali e gli enti pubblici statali e regionali;

g. designa, nomina e revoca i rappresentanti presso enti, azienda ed istituzioni operanti nell'ambito del Comune o da esso controllati;

h. è tenuto a rispondere agli atti ispettivi dei consiglieri entro 30 giorni dal ricevimento;

i. nomina il responsabile degli uffici e dei servizi, attribuisce e definisce gli incarichi dirigenziali e quelli di collaborazione esterna, secondo le modalità ed i criteri dell'art. 51 della legge 8 giugno 1990, n. 142 e successive modifiche, come recepito dall'art. 1, comma 1, lett. h) della legge regionale 11 dicembre 1991, n. 48 e della legge regionale n. 3 0/2000, nonché dello statuto e dei regolamenti del Comune

j. nomina, altresì, i componenti degli organi consultivi del Comune, nel rispetto delle norme e dei criteri stabiliti dalla legge e dallo statuto comunale

2. **Il Sindaco convoca e presiede la giunta, compie tutti gli atti di amministrazione che dalla legge o dallo statuto non siano specificatamente attribuiti alla competenza di altri organi del Comune, del segretario e dei responsabili dei settori.**
3. **Il Sindaco non può nominare rappresentante del Comune presso aziende, enti, istituzioni e commissioni il proprio coniuge ed i parenti e gli affini entro il secondo grado.**
4. **Ogni sei mesi il sindaco presenta una relazione scritta al consiglio comunale sullo stato di attuazione del programma e sull'attività svolta nonché su fatti particolarmente rilevanti. Il consiglio comunale, entro dieci giorni dalla presentazione della relazione, esprime, in seduta pubblica, le proprie valutazioni (art. 17, legge regionale n. 7/92).**
5. **All'inizio del mandato, o nel caso di vacanza di sede, nomina il segretario generale, scegliendolo tra gli iscritti all'albo nazionale dei segretari comunali e provinciali.**

Art. 42
Incarichi ad esperti

1. Il sindaco può conferire incarico a tempo determinato ad un esperto in possesso del diploma di laurea purché sia estraneo all'amministrazione.
2. Sono demandate ad apposito regolamento:

- la durata dell'incarico, la quale, comunque, non potrà essere superiore alla durata in carica del sindaco che ha proceduto alla nomina;
- i criteri per la determinazione del relativo trattamento economico;
- idonee forme di valutazione analitica sull'attività degli esperti (rapporto costi/risultati).
- il Sindaco annualmente trasmette al consiglio comunale una dettagliata relazione sull'attività dell'esperto.

Art. 43
Incarichi agli assessori

1. Il sindaco affida ai singoli assessori il compito di sovrintendere ad un particolare settore di amministrazione e di dare impulso all'attività degli uffici secondo gli indirizzi stabiliti dagli organi di governo del Comune. A tal fine gli assessori possono indirizzare agli uffici apposite direttive, in attuazione dei programmi deliberati dalla giunta e nel pieno rispetto dei programmi di azione dei funzionari da questa approvati.

2. Gli incarichi conferiti agli assessori fanno riferimento agli obiettivi individuati nel documento programmatico e si estendono a tutti gli affari di ciascuno dei settori e delle unità amministrative in cui si articola l'organizzazione del Comune, affidati alla responsabilità di ciascun assessore.

3. 11 sindaco può delegare agli assessori il cornpimento degli atti rientranti nell'ambito dei settori o delle unità amministrative ai quali l'incarico si riferisce.

Art. 44
Proposte di deliberazione

Gli atti di competenza della giunta sono iscritti all'ordine del giorno su proposta dei singoli assessori o del sindaco. Quest'ultimo stabilisce, in relazione agl i obiettivi programmatici della giunta, se la proposta (di deliberazione presentata da un assessore debba essere sottoposta alla giunta ed in quale seduta.

2. La proposta di deliberazione può essere iscritta all'ordine del giorno solamente se corredata dai pareri prescritti dalla legge.

3. Il segretario comunale ed i funzionari possono, di propria iniziativa, sottoporre all'assessore responsabile del settore proposte di deliberazioni di competenza della giunta.

TITOLO IV
GLI UFFICI ED IL PERSONALE
INCARICHI E COLLABORAZIONI ESTERNE

CAPO I
Gli uffici e il personale

Art. 45
Principi e criteri

Il Comune organizza gli uffici ed il personale secondo criteri di autonomia, funzionalità, professionalità, flessibilità, coordinamento e responsabilità, in modo da assicurare che l'azione amministrativa risponda ai principi dell'efficienza, dell'efficacia, dell'imparzialità e della trasparenza.

2. Gli uffici comunali constano di unità elementari raggruppate in strutture di diversa complessità in base a criteri di omogeneità, in relazione alle funzioni dell'ente, nonché agli indirizzi ed ai programmi previsti negli atti di cui all'art. 23 del presente statuto.

Art. 46
Regolamento di organizzazione

Il regolamento di organizzazione:

a. individua gli uffici e i servizi
b. disciplina le modalità di conferimento della titolarità degli uffici;
c. stabilisce le attribuzioni e i compiti dei responsabili preposti agli uffici e servizi;
d. stabilisce le modalità di esercizio dell'attività di coordinamento tra il segretario comunale ed i capi settore;
e. stabilisce la dotazione organica del personale;
f. stabilisce l'assegnazione agli uffici del personale necessario individuato per qualifiche e posizioni;
g. ordina le qualifiche funzionali esistenti secondo i criteri di economicità, razionalità ed efficienza della gestione e in armonia con i principi del buon andamento e dell'imparzialità dell'amministrazione;
h. promuove l'aggiornamento professionale dei dipendenti e ne disciplina le progressioni di carriera.

Art. 47
Funzione dei responsabili di settore

1) La funzione dei responsabili di settore si qualifica per la capacità di:
   a) concorrere alla realizzazione degli obiettivi individuati dagli organi di governo dell'ente;
   b) partecipare alla formulazione di tali obiettivi con attività di studio e di analisi e con autonome proposte;

c) utilizzare le risorse umane e materiali disponibili, motivando e guidando i propri collaboratori;
d) promuovere l'adeguamento dell'organizzazione e delle procedure;
e) prospettare tempestivamente le esigenze alle quali il Comune è chiamato a rispondere.

2. Il comune favorisce lo sviluppo della professionalità dei responsabili di settore ed all'uopo effettua la scelta degli stessi in base alla valutazione, assoluta e comparativa, delle capacità di cui al comma 1.

Art. 48
Compiti dei responsabili dei settori

1. Ai responsabili dei settori spettano i seguenti compiti:
   a) l'organizzazione degli uffici e del personale assegnato alla struttura da essi diretta;
   b) lo svolgimento di attività di studio ed applicazione delle norme di legge e regolamentari;
   c) lo svolgimento di attività di consulenza, progettazione, programmazione;
   d) lo svolgimento di attività di carattere esecutivo di deliberazioni degli organi di governo dell'ente;
   e) l'emanazione degli atti costituenti manifestazione di giudizio e/o di conoscenza come relazioni, valutazioni, comunicazioni, diffide, verbali, attestazioni, certificazioni, autenticazioni e legalizzazioni;
   f) la predisposizione di atti e il compimento di adempimenti istruttori per provvedimenti di competenza degli organi di governo;
   g) lo svolgimento di analisi di fattibilità e la formulazione di proposte relative al complessivo utilizzo delle risorse umane e materiali.
2. In caso di mancanza dei responsabili dei settori, i compiti di cui sopra saranno , in aggiunta, espletati dai responsabili dei servizi.
3. Il regolamento può individuare ulteriori categorie di atti di gestione da attribuire alla competenza dei responsabili.
4. Le norme regolamentari possono, altresì, specificare ulteriormente la individuazione dei compiti previsti dal primo comma.
5. I responsabili dei settori o, in mancanza, i responsabili dei servizi, esprimono i pareri di cui all'art. 53 della legge 8 giugno 1990. n. 142, recepita con la legge regionale 11 dicembre 1991. n. 48.

Art. 49
Responsabilità dei capi settore

1. 1 capi settore sono responsabili dello svolgimento delle attività di competenza della struttura organizzativa alla quale sono preposti, con particolare riguardo all'attuazione dei piani di azione ed al raggiungimento degli speciali obiettivi indicati nei programmi dell'amministrazione.

Sono, altresì, responsabili della tempestività e regolarità dell'istruttoria degli atti la cui emanazione è di competenza degli organi di governo del Comune.

2. Al termine di ogni esercizio finanziario il capo settore presenta una relazione con la quale dà conto dell'attività svolta in relazione agli indirizzi, ai programmi ed agli obiettivi prefissati, illustra l'entità ed il grado di soddisfacimento dei risultati raggiunti, le ragioni delle disfunzioni e degli insuccessi eventualmente registrati e le misure adottate per porvi rimedio.

3. Nell'esercizio delle sue funzioni di soprintendenza il sindaco può richiedere al capo settore spiegazioni per specifiche disfunzioni rilevate nelle attività di competenza della struttura alla quale essi sono preposti e/o per il mancato raggiungimento degli obiettivi.

4. Le spiegazioni di cui al 3° comma del presente articolo, la capacità dimostrata dal capo settore in relazione ai criteri di cui all'art. 50, ed i risultati del controllo di gestione, costituiscono il parametro della responsabilità del capo settore.

5. Il regolamento di cui all'art. 49 stabilirà i criteri in ordine alla collaborazione e responsabilità del capo settore e di tutto il personale per il risultato dell'attività lavorativa in ragione dell'utilità pubblica, stabilendo le sanzioni sul mancato risultato.

Art. 50
Segretario comunale

1. Il segretario comunale svolge i compiti che gli sono assegnati dalla legge e dallo statuto e assiste gli organi di governo del Comune nell'azione amministrativa. In particolare, il segretario comunale coadiuva il sindaco nell'attività di soprintendenza allo svolgimento delle attività comunali.
2. Il segretario comunale sovrintende all'esecuzione delle deliberazioni del consiglio e della giunta, vigila e coordina l'attività dei responsabili di settore, partecipa con funzioni di segretario alle riunioni del consiglio e della giunta.
3. Il segretario comunale roga i contratti nell'interesse del Comune.

CAPO II
INCARICHI E COLLABORAZIONI ESTERNE

Art. 51
Incarichi e collaborazioni esterne

1. La copertura dei posti di direzione di settori di attività può aver luogo mediante contratto a tempo determinato di diritto pubblico o, in via eccezionale, e con delibera specificamente motivata, di diritto privato, fermi restando i requisiti richiesti dalla qualifica da ricoprire.
2. Gli incarichi di direzione di aree funzionali possono essere conferiti a tempo determinato per un tempo massimo di mesi 18 per il conseguimento di obiettivi e attuazione di programmi determinati dal consiglio comunale. Il loro rinnovo è disposto con provvedimento motivato che contiene la valutazione dei risultati ottenuti dal dirigente nel periodo conclusosi in relazione al conseguimento degli obiettivi e all'attuazione dei programmi, nonché al livello di efficienza e di efficacia raggiunto dai servizi dell'ente da lui diretti. L'interruzione anticipata dell'incarico può essere disposta con provvedimento motivato, quando il livello dei risultati conseguiti dal dirigente risulti inadeguato. Il conferimento degli incarichi di direzione comporta l'attribuzione di un trattamento economico aggiuntivo che cessa con la conclusione o l'interruzione dell'incarico.
3. Comunque, il rapporto non potrà in alcun modo essere convenuto o trasformato a tempo indeterminato, salva ogni contraria disposizione di legge.
4. L'esercizio della facoltà del ricorso ai contratti di cui al 1° comma è riservata alla competenza della giunta comunale.
5. Il regolamento di cui all'art. 49 prevederà collaborazioni esterne, ai sensi degli artt. 2222 e 2229 del codice civile, ad alto contenuto di professionalità, per il perseguimento di obiettivi determinati, determinandone il relativo corrispettivo economico; i rapporti conseguenti saranno regolati da apposite convenzioni la cui durata non potrà superare la durata del programma e, comunque, il raggiungimento degli obiettivi -

Si applica, in tal caso, il comma 4 del presente articolo.

TITOLO V
I SERVIZI

Art. 52
Principi

1. I servizi pubblici comunali sono organizzati in modo:
- che siano effettivamente accessibili agli utenti;
- che siano garantiti standards qualitativi delle prestazioni;
- che gli utenti risultino informati sui loro diritti e sulle condizioni e modalità di accesso al servizio;
- che il funzionamento del servizio sia controllabile e modificabile in base a criteri di efficacia, di efficienza ed economicità.

2. Alle finalità di cui al comma precedente deve essere ispirata l'organizzazione del lavoro, la disciplina dell'orario di apertura al pubblico, il rapporto con organismi di tutela dell'utente, costituiti su iniziativa di privati e di gruppi di associazioni interessate ai sensi del titolo II del presente statuto.

Art. 53
Forme di gestione dei servizi

1. I servizi pubblici comunali possono essere gestiti:
   a) in economia quando lo consentono le modeste dimensioni o le caratteristiche del servizio;
   b) in concessione a terzi, quando sussistano ragioni tecniche, economiche e di opportunità sociale;
   c) a mezzo di azienda speciale, quando lo richieda la natura economica e imprenditoriale del servizio o dei servizi interessati;
   d) a mezzo di istituzione, quando si tratta di servizi sociali senza rilevanza imprenditoriale;
   e) a mezzo di società per azioni a prevalente capitale pubblico locale quando sia opportuna, per la natura del servizio, la partecipazione di altri soggetti pubblici o privati;
   f) a mezzo di appalto o convenzione.

2. Per lo svolgimento di servizi determinati possono essere stipulate convenzioni con la Provincia regionale di Palermo e/o con i Comuni limitrofi.

3. La forma di gestione è scelta dal consiglio, previa iniziativa della giunta, sulla base della valutazione di fattibilità del progetto e della considerazione di eventuali alternative.

La scelta dovrà rispettare i principi di cui all'art. 57 ed osservare criteri di efficienza, economicità e trasparenza.

4. La scelta compiuta dal consiglio è sottoposta a verifica annuale. Sulla base dei criteri di cui al comma precedente verrà confermata la forma di organizzazione del servizio o sarà adottata una forma diversa.

Art. 54
Servizi in economia

1. Il servizio è gestito in economia quando, per la dimensione o la natura delle prestazioni, non richieda una struttura dotata di piena autonomia gestionale.
2. La proposta di gestione del servizio in economia è accompagnata da una stima analitica dei costi e delle risorse organizzative e tecniche necessarie e dall'indicazione dei mezzi per far fronte ai costi e per acquisire tali risolse.
3. La giunta riferisce annualmente al consiglio in sede di approvazione del bilancio consuntivo, sull'andamento, la qualità e i costi di ciascuno dei servizi resi in economia.

Il revisore dei conti esprime le proprie valutazioni analitiche sull'economicità dei servizi nella relazione sul consuntivo.

Art. 55
Servizi in convenzione

1. Quando il servizio debba essere organizzato col sistema della concessione, l'impresa concessionaria o il raggruppamento di imprese concessionarie sono prescelti con criteri concorsuali fra aspiranti che offrano garanzie di capacità tecnica, economica e finanziaria.
2 Il disciplinare di concessione definisce la durata del rapporto, le modalità del rinnovo, con esclusione di ogni forma di rinnovo tacito, l'eventuale diritto di prelazione del concessionario, gli obblighi di quest'ultimo, le modalità di verifica dei risultati e dei vantaggi economici conseguiti e acclarati mediante certificazione.
3 L'utente ha nei confronti del concessionario gli stessi diritti che vanta verso il Comune ai sensi dell'art. 57 e delle disposizioni contenute nel titolo II

Art. 56
Aziende speciali

1 - Per la gestione di uno o più servizi che è opportuno affidare ad una struttura dotata di piena autonomia gestionale e patrimoniale, il consiglio comunale può deliberare la costituzione di aziende speciali.
2 – Per i servizi connessi o suscettibili di essere integrati sotto il profilo tecnico ed economico va costituita unica azienda
3 - La deliberazione di costituzione dell'azienda determina gli apporti patrimoniali e finanziari del Comune ed è accompagnata da un piano di fattibilità che indica analiticamente le previsioni sulla domanda di servizi e sui costi, individua le risorse organizzative, tecniche e finanziarie necessarie, stima le entrate previste nonché le condizioni per l'equilibrio economico della gestione.
4 - L'azienda ha un proprio statuto, predisposto dal consiglio di amministrazione e approvato dal Consiglio Comunale.
5 - Lo statuto stabilisce le norme fondamentali sulla competenza degli organi e sul funzionamento dell'azienda, in modo che siano assicurate l'autonomia imprenditoriale dell'azienda stessa, l'efficienza, l'efficacia e l'economicità della gestione; individua gli atti fondamentali dell'azienda da sottoporre all'approvazione del consiglio comunale; determina le modalità di vigilanza sull'attuazione degli indirizzi impartiti dal Comune; prevede un apposito organo di revisione nonché forme autonome di verifica della gestione; disciplina i modi di partecipazione degli utenti.

6. - Gli atti fondamentali dell'azienda, ad eccezione del bilancio preventivo e del conto consuntivo si intendono approvati dal consiglio comunale, quando siano sottoposti ad approvazione, se il consiglio non si pronunci entro trenta giorni dalla comunicazione ai consiglieri.
7 – Organi dell'azienda sono il consiglio di amministrazione, il Presidente e l'amministratore.
8 - I componenti del consiglio di amministrazione, in numero di cinque, sono eletti dal consiglio comunale con voto limitato ad uno su nominativi proposti dalla giunta tra persone che risultino munite di competenza tecnica, gestionale o amministrativa comprovata da curricula che devono essere messi tempestivamente a disposizione dei consiglieri -
9.- Il presidente è eletto nel suo seno dal C.d.A.

Art. 57
Istituzioni

1. Per l'erogazione di servizi sociali senza rilevanza imprenditoriale, che richiedano tuttavia autonomia gestionale, possono essere create istituzioni ai sensi dell'art. 23 della legge n. 142/1990 come recepito dall'art. 1 della legge regionale n. 48/1991 -
2. Le istituzioni curano il coordinamento dei servizi di cui al primo comma con gli interventi di assistenza, integrazione sociale e tutela dei diritti delle persone svantaggiate, con particolare riguardo agli handicappati. A tal fine viene istituito, presso le sedi competenti, un servizio di segreteria per i rapporti con gli utenti, l'organizzazione e il funzionamento del quale è demandato al regolamento.
3. Quando lo consigli la natura delle prestazioni o risulti opportuno per ragioni di efficienza e di economicità, servizi sociali diversi possono essere gestiti da un'unica istituzione.
4. La delibera di costituzione dell'istituzione determina gli apporti finanziari del Comune ed è accompagnata da un piano di fattibilità contenente le indicazioni di cui all'art. 61, comma 3.
5. Ogni istituzione ha capacità di compiere gli atti necessari allo svolgimento dell'attività assegnatale, nei rispetto del presente statuto, dei regolamenti comunali e degli indirizzi fissati dal consiglio comunale.
6. Ogni istituzione ha un regolamento approvato dal consiglio comunale, che disciplina l'ordinamento e il funzionamento dell'istituzione stessa, le modalità di erogazione delle prestazioni, il regime contabile.
7. Le istituzioni possono disporre di entrate proprie, costituite dalle tariffe dei servizi e dai fondi offerti dai terzi al Comune perché destinati all'istituzione.
8. Il personale assegnato alle istituzioni è sottoposto alla stessa disciplina giuridica ed economica applicabile al personale comunale.
   In relazione al tipo di prestazione il regolamento dell'istituzione può differenziare singoli aspetti dell'attività lavorativa, compreso l'orario di lavoro.
9. Organi dell'istituzione sono il consiglio d'amministrazione, composto da cinque persone, il presidente e il direttore.
   I componenti del consiglio d'amministrazione sono eletti su proposta della giunta, dal consiglio comunale, con voto limitato ad uno e secondo il maggior numero di voti, tra persone che abbiano comprovata esperienza tecnica e/o amministrativa, risultante da curricula tempestivamente messi a disposizione dei consiglieri comunali.
   Il presidente è eletto dal C.d.A. nel Suo seno.

Art. 58
Revoca degli amministratori

1. Il C.d.A. dell'azienda o dell'istituzione dura in carica cinque anni e può essere revocato anticipatamente dal consiglio comunale con l'approvazione, a maggioranza assoluta dei consiglieri, di una mozione motivata che indichi i le ragioni della revoca ed enunci i nuovi obiettivi programmatici -
2. Possono essere altresì revocati, su proposta motivata del sindaco approvata a maggioranza di 3/5 dei consiglieri, singoli componenti del C.d.A.

Art. 59
Società per Azioni

1.Possono essere svolti mediante società per azioni a prevalente capitale pubblico locale servizi di carattere imprenditoriale:

a) quando ricorra l'opportunità di una gestione in regime di mercato mediante una struttura dotata di piena autonomia patrimoniale e gestionale;

b) quando risulti l'utilità dell'apporto di privati qualificati sotto il profilo imprenditoriale o finanziario o dell'esperienza acquisita nel settore, che condividano il rischio di impresa;

c) quando sia conveniente finanziare quote significative del capitale attraverso il mercato, anche con la partecipazione degli utenti e dei lavoratori alla costituzione del capitale medesimo.

2. La proposta di deliberazione della costituzione della società o della partecipazione comunale al capitale della medesima è presentata ai consiglio comunale unitamente a un piano di fattibilità che indica analiticamente revisioni sulla domanda di servizi e sui costi, stabilisce gli oneri a carico del Comune, stima le entrate previste e determina le condizioni per l'equilibrio economico della gestione.
3. I soci privati ai quali il Comune propone la sottoscrizione di quote significative di capitale o decide di associarsi, in caso di società già costituite, vanno scelti tenuto conto dell'eventuale pluralità di offerte e delle alternative esistenti, previo parere da richiedere a soggetti di elevata qualificazione professionale sugli aspetti tecnici, economici e finanziari;
4. Lo statuto della società deve prevedere:

a) la nomina diretta da parte del consiglio comunale di un numero di amministratori proporzionale all'entità della partecipazione comunale, da nominare fra persone dotate di competenza tecnica, gestionale o amnìinistrativa comprovata da curricula che debbono essere messi tempestivamente a disposizione dei consiglieri;

b) i poteri necessari all'assemblea dei soci per indirizzare l'attività sociale, garantendo al C.d.A. piena autonomia gestionale;

c) la verifica annuale, anche attraverso società di revisione, dei risultati di gestione e la comunicazione al consiglio comunale dell'esito della verifica.

Art. 60
Servizi in convenzione

1. Per singoli servizi imprenditoriali, quando non ricorrano le condizioni per l'applicazione dei precedenti 59, 60, 61 e 64, si può ricorrere all'appalto o alla convenzione nell'osservanza dei criteri concorsuali previsti disposizioni vigenti nonché dal regolamento di contabilità comunale.
2. Per singoli servizi sociali, ed in particolare per servizi di carattere assistenziale, culturale, educativo, ambientale e del tempo libero, il Comune può stipulare convenzioni con soggetti privati, assicurando agli utenti l'equipollenza al servizio pubblico, ove esista, nonché forme di controllo sull'attività. I costi non possono superare quelli che verrebbero sostenuti dal Comune in caso di gestione diretta.
3. Per l'erogazione dei servizi di cui al comma precedente, il Comune sostiene forme spontanee di autorganizzazione degli utenti e riconosce il valore sociale del volontariato, singolo e associato.

TITOLO VI

CONTABILITA' - FINANZA
CONTROLLO DI GESTIONE

Art. 61
Contabilità finanziaria

1. L'ordinamento contabile del Comune è disciplinato da apposito regolamento che il consiglio delibera nell'osservanza delle leggi sulla contabilità e finanza degli enti locali, nonché nell'osservanza delle disposizioni del presente titolo.
2. La gestione finanziaria si svolge in conformità al bilancio di previsione annuale e pluriennale che il consiglio comunale delibera annualmente in coerenza con gli obiettivi previsti dagli indirizzi e dai programmi di cui all'art.23 del presente statuto.
3. Gli emendamenti al progetto di bilancio devono indicare le modifiche da approvare ai corrispondenti atti di indirizzo e di programmazione. Diversamente sono ammissibili se accettati dalla giunta. In ogni caso, gli emendamenti che aumentino le spese o riducano le entrate devono precisare i modi per mantenere il pareggio di bilancio.
4. Il regolamento di contabilità disciplina le variazioni che possono essere apportate al bilancio con un procedimento diverso da quello previsto per la sua approvazione;; sono comunque riservate alla giunta le variazioni connesse ai prelevamenti dai fondi di riserva.

Art. 62
Controllo economico di gestione

1. Il Comune attua attraverso l'ufficio di ragioneria forme di controllo economico interno della gestione, al fine di valutare l'efficacia, l'efficienza e l'economicità dell'attività comunale.
2. Il regolamento di contabilità provvede ad individuare e disciplinare lo svolgimento del controllo economico di gestione.
3. In base alle risultanze delle verifiche svolte, l'ufficio di ragioneria predispone rapporti periodici che danno conto dell'andamento della gestione e propone alla giunta gli interventi ritenuti opportuni.

Art. 63
Revisori dei conti

1. Il consiglio comunale elegge un collegio dei revisori, secondo le disposizioni di legge.
2. Non possono essere nominati revisori dei conti:
   a) consiglieri comunali;
   b) i parenti fino al 4° grado, il coniuge, gli affini fino al 2° grado del sindaco, degli assessori, dei segretario comunale e dei dirigenti del Comune;
   c) coloro che intrattengono un rapporto di lavoro anche autonomo, con il Comune o con enti o istituzioni dipendenti dal Comune o da esso controllati;
   d) coloro che detengono partecipazioni in società appaltatrici, concessionarie di opere e/o servizi comunali;

e) coloro che hanno liti pendenti con il Comune o con enti o istituzioni dipendenti dal Comune o da esso controllati;

f) i dipendenti della Regione Siciliana, i componenti dell'organo di controllo sugli atti del Comune e i dipendenti della Provincia di Palermo.

Art. 64
Competenze del collegio dei revisori

1.- Il collegio dei revisori, collabora con il consiglio comunale ed, all'uopo, formula osservazioni e proposte volte a perseguire efficienza, economicità e produttività, vigila sulla regolarità contabile e finanziaria della gestione, e attesta l'esatta quantificazione e rappresentazione dei dati contabili.

2. - Per lo svolgimento delle proprie funzioni, il collegio dei revisori, ha diritto di accesso agli atti e documenti del Comune.

3.- Il collegio dei revisori deve partecipare alle sedute dei consiglio comunale, in particolare, in occasione della discussione del bilancio di previsione e dei conto consuntivo.

4. Il regolamento di contabilità disciplina l'esercizio delle funzioni del collegio dei revisori, gli obblighi dello stesso e le relative responsabilità, e la sua decadenza in caso di mancato o irregolare funzionamento.

TITOLO VII
ATTIVITA' NORMATIVA DEL COMUNE

Art. 65
Revisione dello Statuto

1. - Le modificazioni e l'abrogazione dello statuto sono deliberate dal consiglio comunale con la procedura prevista dalla legge regionale 11 dicembre, n. 48.
2. - La proposta della deliberazione totale dello statuto deve essere presentata in consiglio comunale congiuntamente a quello di deliberazione del nuovo statuto. L'adozione delle due deliberazioni di cui al precedente comma è contestuale: l'abrogazione totale dello statuto assume efficacia con l'approvazione del nuovo testo dello statuto.
3. - La proposta di revisione o abrogazione respinta dal consiglio comunale non può essere rinnovata se non decorso un anno dalla deliberazione di reiezione.

Art. 66
I regolamenti comunali

1. - La potestà regolamentare del Comune si esercita nell'ambito delle materie previste dalle leggi e dallo statuto.
2. I regolamenti non possono contenere disposizioni in contrasto con le fonti normative gerarchicamente superiori.
3. La loro efficacia è limitata nell'ambito comunale.
4. Non possono avere efficacia retroattiva se ledono gli interessi di alcuno.

Art. 67
Procedimenti di formazione dei regolamenti

1. - L'iniziativa per l'adozione dei regolamenti spetta alla giunta comunale, a ciascun consigliere ed alle forme associative dei cittadini.
2. I regolamenti sono soggetti a due pubblicazioni all'albo pretorio; una prima, che è contestuale alla pubblicazione della deliberazione approvativa; una seconda, da effettuarsi per ha durata di quindici giorni dopo i prescritti controlli.
3. I regolamenti entrano in vigore il giorno successivo all'ultimo giorno della seconda pubblicazione.

TITOLO VIII
DiSPOSIZIONI FINALI

Art: 68
Disposizioni finali

1. Il presente statuto approvato dal consiglio comunale entra in vigore il trentunesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale della Regione siciliana o successivo all'avvenuta affissione all'albo pretorio del Comune, se posteriore.
6. Per le modifiche statutarie si applicano le norme previste per l'approvazione dello statuto stesso, secondo il procedimento di cui all'art. 4 della legge n. 142/90, come recepita dalla legge regionale n. 48/91.
7. Lo statuto e le relative modifiche, entro 15 giorni successivi dalla loro esecutività, sono sottoposte a forme di pubblicità che ne consentano la piena ed effettiva conoscibilità.
8. – Per quanto non espressamente disciplinato dal presente Statuto; si applicano le disposizioni di legge vigenti in materia.

COMUNE DI ISOLA DELLE FEMMINE

Documento Programmatico sulla sicurezza

Documento Programmatico Sulla Sicurezza

Art. 19, Allegato B, D.l. 30 giugno 2003 n. 196

INDICE

1. PREMESSE METODOLOGICHE

1.1 MODALITA' DI COSTRUZIONE DI UN "PIANO SICUREZZA" PER IL TRATTAMENTO DEI DATI PERSONALI

Un modo pratico per procedere alla costruzione del "piano sicurezza" potrebbe essere il seguente:

- Inventario delle banche dati
- Individuazione dei responsabili e degli incaricati
- Definizione dei trattamenti
- Definizione delle misure di sicurezza
- Gestione della documentazione richiesta dalla legge.

A meno che non si tratti di una piccola azienda, in generale i sistemi informativi sono normalmente complessi e spesso collegati con i sistemi di altre strutture economiche (imprese consociate, business partner, banche, enti statali, ecc..); pertanto è sempre opportuno adottare una metodologia precisa per fare l'inventario delle banche dati che contengono informazioni soggette alla legge ed i relativi trattamenti.
Il percorso logico da seguire nell'analisi potrebbe partire:

- dalle applicazioni,

per analizzare in seguito

- le banche dati
- i dati privati
- gli archivi fisici
- i collegamenti con altre applicazioni/sistemi,
- gli archivi tecnici (copie di back-up, copie per i test),
- i log applicativi e di sistema,
- gli archivi di sicurezza per il piano di disaster recovery ed, in fine,
- gli archivi storici.

Le Applicazioni - L'inventario di tutte le applicazioni esistenti nella struttura è fondamentale per verificare se si trattano dati privati, rilevarne il trattamento e le finalità. In questo contesto è importante innanzitutto definire che cosa si intende per applicazione; per esempio sotto il titolo di applicazione del personale potrebbero ricadere tutti i programmi applicativi per la gestione delle retribuzioni, le carriere, gli skill, ecc.
Le Banche Dati - Una volta completato l'inventario delle applicazioni si può verificare il contenuto delle relative banche dati e definire se vi siano dati che abbiano le caratteristiche richieste nelle previsioni legislative.
E' in questa fase che si dovrebbe anche individuare se esistono e quali sono i cosiddetti dati *sensibili*. Infatti per questa particolare tipologia di dati viene richiesta una attenzione specifica ed un trattamento differenziato.
Si ritiene preferibile prendere in esame solo le banche dati primarie e di trattare gli altri archivi come archivi derivati, ma facenti parte di un unico trattamento.
Altri Archivi - Occorre considerare anche eventuali nastri depositati fuori dai locali della struttura nei cosiddetti archivi di sicurezza o storici o dati in elaborazione a società di servizi.
Collegamenti - Sicuramente un punto critico per molte organizzazioni; dipende dalla complessità del sistema informativo e dal suo grado di distribuzione. In un centro ben organizzato tutti i collegamenti tra applicazioni dovrebbero essere descritti nei documenti tecnici. Ciò è meno vero per gli ambienti distribuiti, soprattutto se il protocollo di rete non è di tipo gerarchico, ma paritetico. Le LAN sono reti che appartengono a questa categoria. I responsabili delle varie applicazioni dovrebbero essere la fonte delle informazioni necessarie per questo inventario.
Non bisogna inoltre escludere la ricerca ad altre categorie di archivi che sicuramente contengono dati privati, anche se non sono direttamente riconducibili alle singole applicazioni. Si fa riferimento a tutti quegli archivi che vengono creati dai sistemi operativi o fanno parte dei processi di gestione dei centri di calcolo. Ricadono sotto questa categoria per esempio i log, che contengono le informazioni delle attività fatte durante la giornata da chiunque operi sui calcolatori.
Normalmente questi log, se esistenti, contengono il codice della persona che ha operato e le indicazioni di che cosa ha fatto, ora e minuto.

1.2 CICLO DELLA SICUREZZA

Il ciclo sicurezza può essere definito nelle seguenti fasi/operazioni:

- Analisi dei rischi
- Contromisure possibili
- Definizione della politica aziendale sulla sicurezza
- Realizzazione delle misure decise
- Amministrazione
- Auditing e controlli

Analisi dei rischi: In questa fase si dovrebbe procedere all'inventario dei dati da proteggere e alla valutazione dei rischi a cui sono soggetti. Particolare attenzione va posta ai rischi dovuti alle carenze organizzative ed alla scarsa cultura sugli aspetti della sicurezza informatica. Oggi i rischi per l'integrità dei dati si sono moltiplicati. Si parla sempre più spesso di intercettazioni, di pirati informatici, di virus ecc.. Volendo classificare i rischi abbiamo i rischi secondo l'origine, le cause e le modalità.

Rischi secondo l'origine:

- **Interni** - connessi alla attività dei dipendenti della azienda. Secondo le statistiche sono i più probabili.
- **Esterni** - connessi alla attività di qualunque altra persona.
- **Ambientali** - relativi a eventi di grande portata, quali: incendi, terremoti, allagamenti, ecc..

Rischi secondo le cause:

- **Carenze organizzative** - responsabilità non correttamente assegnate, sottovalutazione dei rischi, ecc..
- **Colpa** - se causati da ignoranza, incuria o leggerezza. Statisticamente è la causa più diffusa.
- **Dolo** - In rapida crescita. Infatti con l'avvento di Internet è cresciuto enormemente il numero delle persone che possiedono le apparecchiature e le necessarie conoscenze tecniche per arrecare danno.

Rischi secondo le modalità:

- **Intercettazioni** - principalmente lungo la rete di trasmissione.
- **Ingegneria sociale** - per divertimento, si prende gioco della vittima. Sono le modalità più diffuse e pericolose
- **Backdoor** - Quando i programmatori lasciano dei punti di ingresso non noti nel software.
- **Cavalli di Troia** - lo dice lo stesso nome - software predisposto per operare in modo non noto all'utente.
- **Denial of service** - comandi che pregiudicano la efficienza delle reti e dei server.
- **Virus** - software che ha la capacità di autopropagarsi
- **Personificazione** - quando ci si presenta sotto mentite spoglie.

Ovviamente la lista potrebbe essere più lunga e completa. Si consideri che con l'avvento della informatica distribuita e di Internet, il possibile Hacker può essere chiunque e in qualunque parte del mondo ed è praticamente impossibile individuarlo.

Le Contromisure - Di fronte ad una casistica di minacce così variegata ed eterogenea e per molti versi imprevedibile, le difese parziali ed improvvisate sono destinate ad essere poco efficaci. Infatti anche per la sicurezza informatica, come per molti sistemi di sicurezza, si può dire che è l'anello più debole che determina il grado di resistenza della catena.

Definizione della politica aziendale sulla sicurezza: E' la fase più importante. E' fondamentale che il management aziendale o delle strutture economiche in genere prenda atto dei rischi e definisca una adeguata risposta in termine di politica aziendale (regole, organizzazione, responsabilità, ecc.) e relativi budget di spesa. Il bilanciamento costi benefici e l'accettazione dei rischi residui sono parte non rinunciabile di questa fase. Il risultato concreto è la pubblicazione dello **standard aziendale di sicurezza**.

Realizzazione: Occorre tradurre quanto definito nella fase precedente in atti concreti. Questa fase, in organizzazioni complesse, può richiedere tempi e molto impegno. Se i sistemi informativi nella fase di progetto non sono stati disegnati tenendo nel dovuto conto i requisiti della sicurezza, questa fase può avere costi molto elevati e talvolta non bilanciati con i benefici che si vogliono ottenere.

Amministrazione: Sicurezza vuol dire regole, vincoli, controlli, liste di accesso, permessi ecc..; ciò comporta una certa dose di inevitabile burocrazia e di lavoro amministrativo. Senza l'attività di amministrazione, dopo qualche tempo, il sistema di sicurezza si degrada e fallisce i suoi obiettivi

Auditing e controlli: Costruire un sistema di sicurezza senza, in qualche modo, verificarne l'efficacia, serve a poco. I sistemi informatici sono normalmente molto complessi (sistemi operativi, applicazioni, banche dati, reti, ecc.) e solo con test accurati si può avere una ragionevole certezza di aver costruito un sistema privo di scoperture o manchevolezze. Ovviamente non possiamo limitarci ai test iniziali, ma questi vanno ripetuti con frequenze opportune (1 o 2 volte l'anno).
Con ciò il ciclo è concluso. Ovviamente, poiché difficilmente i sistemi informativi e l'ambiente in cui operano sono statici, il ciclo della sicurezza non termina mai. E' altamente raccomandabile che almeno una volta l'anno si riparta con una revisione dei rischi e, se necessario, anche con le altre fasi.

1.3 L'ARCHITETTURA DI SICUREZZA

L'architettura di sicurezza è l'insieme di regole, funzioni, strumenti, oggetti e controlli, coerentemente disegnati e resi funzionanti, che garantiscono in ogni struttura organizzativa, ambiente informatico, sistema informativo, singolo elaboratore, ecc. il rispetto degli standard di sicurezza definiti dall'azienda.
Normalmente abbiamo architetture di sicurezza differenziate per:
- *Ambiente tradizionale* (Centro di calcolo con mainframe e rete privata)
- *Ambiente distribuito/Server* (LAN con server dipartimentali)
- *Ambiente Internet/Intranet* (Web)
- *Ambiente distribuito/Client* (Workstation, browser).

Gli elementi essenziali di una architettura sono:

- Funzioni di sicurezza
- Meccanismi di sicurezza
- Oggetti di sicurezza
- Processi di gestione

Funzioni di sicurezza : Identificazione e autenticazione degli utenti, controllo accessi ai dati ed alle applicazioni, crittografia, non rigetto, firma elettronica, ecc. sono esempi di funzioni che vanno valutate e decise. Naturalmente si focalizzerà prioritariamente l'attenzione alle funzioni previste dall'Allegato B.

Meccanismi di sicurezza : Sono i prodotti Hardware e Software che realizzano le funzioni di sicurezza previste nell'architettura.

Oggetti di sicurezza : E' importante che vengano con molta precisione individuati quegli oggetti informatici che sono funzionali ai meccanismi di sicurezza. Fanno parte di questa categoria le password, le chiavi di crittografia, le liste di accesso, ecc.. Una protezione non appropriata di questi oggetti potrebbe vanificare l'efficacia dell'intero sistema.

Processi di gestione : E' l'insieme dei processi e delle regole per la gestione delle funzioni, dei meccanismi e degli oggetti di sicurezza che fanno parte della architettura. Vi dovrebbero far parte anche processi di allarme e controllo.

Un'architettura di sicurezza così strutturata e gestita dovrebbe senz'altro rispondere a quanto previsto dall'articolo 31, D.l. 30 giugno 2003, n. 196 e soprattutto essere ***preventiva e tecnologicamente sempre aggiornata.***
In modo esplicito l'art. 31 richiede che i dati personali oggetto di trattamento siano **custoditi** ... **controllati** ... in modo da ridurre **al minimo** i rischi di **distruzione, perdita** anche accidentale, ... di **accesso non autorizzato**, ... di **trattamento non consentito**, ... di trattamento **non conforme** alla finalità della raccolta.

Funzioni di sicurezza - Di seguito verranno esaminate le *funzioni di sicurezza* che rispondono ai singoli requisiti. **Custodia** - Presuppone che siano definiti dei processi (norme e responsabilità) nell'area sia della sicurezza fisica che logica.
Sicurezza fisica - Locali dei centri di calcolo isolati e dotati di accessi controllati. E' importante che solo gli addetti ai lavori (incaricati del trattamento) vi possano accedere e che altre persone (visitatori, addetti ai lavori ausiliari, ecc.) vi accedano solo con apposita autorizzazione.
E' buona norma dotare gli ingressi di apparecchiature per la identificazione delle persone (es. lettori di badge) e tutte le aperture di allarmi per cautelarsi da intrusioni durante il periodo in cui il centro resta non presidiato.
Per i server dipartimentali o comunque distribuiti le soluzioni possono essere molte, più o meno efficaci: uso di armadietti chiusi a chiave, locali appositamente predisposti, lucchetti, ecc.. Occorre ricordare che nei Personal Computer è molto facile asportare i dischi fissi.

Poiché sono sempre possibili delle intercettazioni anche le *apparecchiature di rete* dovrebbero essere custodite opportunamente.
Un discorso a parte meritano le *nastroteche*. Nastri etichettati e gestiti con la tecnica del carico e scarico e inventari periodici di controllo (almeno una volta all'anno).
Poiché la legge parla di rischi di perdita anche accidentale, se i nastri sono unici, sarà bene dotarsi di opportuni impianti antincendio che non provochino ulteriori danni ai nastri in caso di utilizzo di dette apparecchiature.
Quanto detto per i nastri vale anche per i dischi rimovibili.
Sicurezza logica - I metodi per proteggere le informazioni dal punto di vista logico sono molti e svariati e fortemente dipendenti dalla tipologia dei sistemi operativi utilizzati (piattaforme Software).
Comunque alcune caratteristiche sono comuni a tutte le piattaforme.
Citiamo solo alcune che sono applicabili sia ai sistemi host che ai server distribuiti ed in qualche misura anche alle singole workstation.
- *Integrità del sistema operativo:* è il primo elemento chiave. Non tutti i sistemi operativi da questo punto di vista sono uguali; inoltre vanno installati e mantenuti a regola d'arte. La classificazione del TCSEC Americano aiuta a fare un primo confronto. Per avere comunque maggiori certezze è necessario far fare da personale specializzato gli opportuni test (penetration test) per individuare le scoperture ed avere le indicazioni per rimediarvi.
Deve essere sempre tenuto presente che una scopertura sul sistema operativo indebolisce tutte le altre protezioni di sicurezza.
- *Sistema chiuso o aperto:* Per stare più tranquilli ed avere minori rischi è sicuramente consigliabile disegnare il sistema di sicurezza secondo la regola che è tutto proibito meno le cose autorizzate (sistema chiuso), piuttosto che secondo lo schema opposto: è tutto permesso meno le cose proibite (sistema aperto). La prima soluzione è più costosa e richiede una accurata amministrazione.
- *Accessi discrezionali od obbligatori:* si parla di accesso discrezionale quando si demanda ad una persona (normalmente proprietario della applicazione) l'autorità di decidere a chi dare l'accesso ai dati e a chi no. Si ha l'accesso obbligatorio quando l'accesso ai dati è strutturale e controllato dal sistema di sicurezza.
Penso che per i dati sensibili sia preferibile adottare la soluzione degli accessi obbligatori.
- *Classificazione delle informazioni:* Sul piano pratico converrebbe adottare un sistema di classificazione che veda, per esempio, i dati "sensibili" classificati ad un livello più alto dei dati "personali". L'adozione di un opportuno sistema di classificazione, oltre ad accrescere la protezione dei dati, dovrebbe permettere di adottare un sistema di protezione selettivo.
Un esempio potrebbe essere:
- Informazioni "sensibili": altamente riservate
- Informazioni "private": riservate
- Altre informazioni aziendali riservate: riservate
- Altre informazioni aziendali: non classificate
un sistema di classificazione, perché sia efficace, deve comprendere anche le informazioni cartacee.
- *Metodi di accesso:* Il più usato è quello basato su parole chiave o password. Per accrescerne l'efficacia occorre che ci siano regole precise di gestione delle password. Occorre definirne la lunghezza minima, la durata, e le regole grammaticali per evitare le password facilmente indovinabili. Ogni password dovrebbe essere abbinata ad un individuo; è l'unico modo per poter risalire alle responsabilità di eventuali azioni contrarie a quanto previsto dalla legge.
- *Antivirus:* Nell'architettura di sicurezza dei Personal Computer dovrebbe essere sempre previsto non solo un Antivirus, ma anche e soprattutto un rigoroso processo di controllo dei dischetti che entrano in azienda e, se collegati ad Internet, del software che viene scaricato dalla rete.
La lista di metodologie di protezione potrebbe continuare, ma ritengo che quelle richiamate siano sufficienti per disegnare una architettura di sicurezza minima. Ovviamente se le banche dati dovessero essere inserite in un sistema particolarmente esposto, come per esempio un Web di Internet, occorrerà provvedere ad un disegno specifico e prevedere la installazione di Firewall e di protocolli di mutuo riconoscimento basati su chiavi crittografiche.
I controlli - La legge li richiede in modo esplicito; inoltre, dimostrare di averli in funzione, sarà sicuramente utile per il Responsabile, se dovesse essere necessario.
Controlli periodici - Possiamo dividere i controlli in:
- *Auditing*: personale specializzato, spesso esterno all'azienda, verifica l'aderenza dei comportamenti e delle soluzioni tecniche agli standard di sicurezza (in questo caso anche alle disposizioni di legge). L'Auditing richiede, come prerequisito, che l'azienda si sia data per iscritto le regole e abbia definito ruoli e responsabilità.
- *Revisioni interne* : differiscono dalle metodologie precedenti solo per il fatto che sono eseguite dallo stesso personale interno dell'azienda e richiedono preparazione ed impegno meno gravoso. Spesso

precedono le revisioni ufficiali vere e proprie.
- *Test* : tecnici dotati di opportuni tools e metodologie provano a violare i sistemi informativi, ad accedere ai dati ed alle applicazioni pur non avendo alcuna autorizzazione iniziale
Controlli continui - Possiamo dividere i controlli in:
- *Analisi dei log*: per prima cosa occorre che il meccanismo che registra i log (liste di attività) sia attivato sia sui sistemi operativi che sui software di sicurezza e che i log siano protetti e mantenuti per un periodo sufficiente. L'attività di analisi per la ricerca di eventi anomali e la successiva determinazione delle cause andrebbe fatta giornalmente. Accumulare log per periodi più lunghi, data la mole di dati da verificare, renderebbe vana ogni attività di verifica. L'uso di tools automatici di supporto snellisce molto questa attività e la rende meno gravosa.
Inoltre i log sono di per sé banche dati con informazioni private e pertanto da gestire opportunamente.
- *Routine di controllo*: sotto questa terminologia si intendono tutti quei software che effettuano operazioni di verifica continua sui sistemi per garantire che gli standard di sicurezza siano rispettati e che ne segnalano le deviazioni. Ritengo che si possano personalizzare queste routine facendo in modo che verifichino, laddove è possibile, che il trattamento delle banche dati personali resti conforme a quanto notificato al Garante.

1.4 L'ARCHITETTURA DI SICUREZZA E LA RIDUZIONE DEI RISCHI

In modo esplicito l'art. 31, D.l. 30 giugno 2003, n. 196, richiede che i dati personali oggetto di trattamento siano **custoditi** ... **controllati** ... in modo da ridurre **al minimo** i rischi di **distruzione, perdita** anche accidentale, ... di **accesso non autorizzato**, ... di **trattamento non consentito**, ... di trattamento **non conforme** alla finalità della raccolta.
Possiamo annoverare i rischi principalmente nella seguente casistica:

- Rischi di distruzione o perdita anche accidentale
- Rischi di accesso non autorizzato
- Rischio di trattamento non consentito o non conforme

Rischi di distruzione o perdita anche accidentale - Un dato memorizzato in un archivio elettronico può essere distrutto o perso per svariate cause:
- *comandi applicativi errati* : ciò è dovuto essenzialmente ad applicazioni non ben testate. Si riduce il rischio sia seguendo rigorose procedure di test che separando il mondo cosiddetto di sviluppo e test da quello di produzione.
- *comandi operativi errati*: Un operatore può sempre sbagliare e provocare distruzioni irreparabili. Volendo ridurre tale rischio è necessario ridurre al minimo le necessità di comandi manuali, demandando tali comandi ad applicazioni specializzate (schedulatori, sistemi di automazione).
- *software pericoloso*: metto in questa categoria, oltre ai virus, tutta quella serie di routine, per altro molto diffuse nei centri elaborazioni, che possono accedere ai dati superando le barriere dei sistemi di sicurezza e al di fuori del controllo dei programmi applicativi. L'uso di tali programmi dovrebbe essere vietato (salvo uno ristretto utilizzo in casi particolari) ed inoltre con opportuni controlli andrebbero ricercati e cancellati dalle librerie.
- *malfunzionamenti dell'Hardware*: anche l'hardware più costoso e tecnologicamente più evoluto è soggetto a malfunzionamenti. La difesa più efficace consiste nel duplicare gli archivi con frequenze prestabilite.
- *eventi disastrosi*: Mi riferisco ad incendi, allagamenti, esplosioni o atti dolosi, ecc. che distruggano i supporti magnetici su cui i dati sono registrati.
Si ritiene che la legge imponga l'adozione di misure di back-up obbligatorie (art. 34 lett. f, D.l. 30 giugno 2003, n. 196) per tutte le banche dati private. In altre parole le applicazioni che gestiscono i dati privati andrebbero inserite tra quelle vitali per l'azienda e trattate secondo le procedure di disaster/recovery.

Rischi di accesso non autorizzato - Se vogliamo tenere sotto controllo il rischio di accesso non autorizzato dobbiamo disporre di una funzione di controllo accessi che copra l'intero sistema informativo e non solo le specifiche applicazioni. Infatti dobbiamo cautelarci da ogni manomissione di dati, sia da parte del personale degli uffici che per compito deve trattare i dati privati, sia del personale tecnico del centro elaborazioni che svolge operazioni di trattamento sugli archivi interi. Particolare cura deve essere posta agli accessi da parte di applicazioni o da comandi di sistema operativo.
In altre parole i dati privati devono avere una protezione totale e le logiche con cui vengono date le autorizzazioni devono essere sotto il controllo diretto del *Responsabile del trattamento.*

Rischio di trattamento non consentito o non conforme - Per poter ridurre questa tipologia di rischio bisogna fare in modo che il trattamento definito per ogni banca dati e notificato al Garante rimanga tale

e non possa essere modificato da nessuno senza la espressa volontà del Titolare o del Responsabile a ciò delegato. Per ottenere ciò, più che sulle soluzioni tecniche, bisogna agire sulla organizzazione e l'assegnazione delle responsabilità.
Gli articoli citati, come del resto molti altri, pongono precisi limiti e divieti, a seconda dei casi, alla diffusione e comunicazione dei dati privati e/o sensibili. Ricordiamoci che è considerata comunicazione la semplice possibilità di consultazione dei dati. E' anche previsto che il Garante possa vietare la diffusione di alcuni dati e che è vietata la comunicazione e la diffusione dei dati di cui è stata ordinata la cancellazione.
Tutto questo vuol dire che l'accesso in lettura dei dati deve essere strettamente controllato e che i software di trasmissione devono essere gestiti molto accuratamente.
Una particolare comunicazione/trasmissione è il trasferimento dei dati all'estero. Sulle reti si dovranno installare dei filtri, gateway o firewall per evitare trasmissioni verso località non desiderate.

2. FINALITA' DEL PRESENTE DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente Documento Programmatico Sulla Sicurezza (DPSS) riporta i percorsi di analisi e le conseguenti misure minime di sicurezza identificate e da adottare in via preventiva, conformemente a quanto previsto dall'Allegato B del D.l. 30 giugno 2003, n. 196.
Costituisce pure un valido strumento per la adozione delle misure idonee previste dall'art.31, D.l. 30 giugno 2003, n. 196.
L'analisi e il risultato del presente Documento Programmatico sulla Sicurezza portano a pianificare e a programmare le misure necessarie per 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, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

3. CAMPO DI APPLICAZIONE

Il ***Documento Programmatico Sulla Sicurezza*** (DPSS) è il documento di programma che definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali. Dette definizioni conseguono dall'analisi dei rischi, dalla distribuzione dei compiti e delle responsabilità nell'ambito della struttura analizzata.
In particolare nel ***Documento Programmatico Sulla Sicurezza*** (DPSS) vengono definiti:

- i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
- i criteri e le procedure per assicurare l'integrità dei dati;
- i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per Via telematica;
- l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

Il ***Documento Programmatico Sulla Sicurezza*** (DPSS) riguarda tutti i dati personali:

- Sensibili
- Giudiziari
- Semisensibili
- Comuni

Il ***Documento Programmatico Sulla Sicurezza*** (DPSS) si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ad esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il ***Documento Programmatico Sulla Sicurezza*** (DPSS) deve essere conosciuto ed applicato da tutte le figure che operano nella struttura.

4. RIFERIMENTI NORMATIVI

- D.l. 30 giugno 2003, n. 196
- D.l. 30 giugno 2003, n. 196, Allegato B

5. LE FIGURE PREVISTE DALLA NORMATIVA NEL SETTORE DELLA

SICUREZZA PER LA PRIVACY

5.1 IL TITOLARE DEL TRATTAMENTO

Il D.l. 30 giugno 2003, n. 196, all'art. 28 definisce **titolare** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo *cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali*, ivi compreso il profilo della sicurezza.

5.2 IL RESPONSABILE DEL TRATTAMENTO

Il D.l. 30 giugno 2003, n. 196, all'art. 29 definisce ***Responsabile del trattamento*** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo *preposti facoltativamente dal titolare al trattamento di dati personali.*
Può quindi essere prevista, in relazione all'attività del ***Titolare del Trattamento***, la nomina di uno o più ***Responsabili del Trattamento*** con compiti diversi a seconda delle funzioni svolte, sia all'interno che all'esterno, sia da persone fisiche, sia da persone giuridiche.
L'art 29 dispone che il responsabile, se designato, deve essere nominato 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.
Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni predette e delle proprie istruzioni. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. I compiti affidati al responsabile devono essere analiticamente specificati per iscritto.

5.3 COMPITI DEL TITOLARE E DEL RESPONSABILE DEL TRATTAMENTO

Al Titolare del Trattamento quindi competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza ed il Responsabile del Trattamento è il soggetto preposti dal titolare al trattamento di dati personali.
In merito alla sicurezza dei dati l'art 33 e 31 del D.l. 30 giugno 2003, n. 196, dispongono che **il Titolare ed il Responsabile** dovranno curare che i dati personali oggetto di trattamento siano 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.
Quanto alle misure minime di sicurezza dovranno adottare quelle previste dal disciplinare tecnico dell'Allegato B.
Nel caso in cui il ***trattamento dei dati*** venisse fatto ***con strumenti elettronici o comunque automatizzati,*** in conformità all'art 28 e 29 cureranno l'adozione delle seguenti misure minime (art. 34 del D.l. 30 giugno 2003, n. 196):

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;

Qualora il trattamento effettuato da organismi sanitari abbia ad oggetto dati sensibili, cureranno l'adozione di tecniche di cifratura o di codici identificativi.

Nel caso in cui il ***trattamento dei dati personali*** viene effettuato ***con strumenti elettronici o comunque automatizzati da un fornitore di un servizio di comunicazione elettronica accessibile al pubblico***, in conformità all'art 32 del D.l. 30 giugno 2003, n. 196, il Titolare ed il Responsabile dovranno:

- adottare 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.
- nel caso in cui 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 dovrà adottare tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni.
- se sussiste un particolare rischio di violazione della sicurezza della rete, dovrà informare gli utenti e/o gli abbonati 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 dovrà essere resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

In ogni caso il Titolare del trattamento direttamente, o se delegato il responsabile, nel caso di trattamento effettuato con strumenti elettronici o automatizzati, in conformità al disposto degli artt. 1 e ss. Dell'Allegato B dovrà:

- se il trattamento di dati personali con strumenti elettronici è consentito agli incaricati, dotare gli stessi di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. 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. Ad ogni incaricato verranno assegnate o associate individualmente una o più credenziali per l'autenticazione.
- Impartire istruzioni agli incaricati in relazione all'adozione delle necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. In particolare dovranno costituire una procedura per la quale:

1. la parola chiave, quando è prevista dal sistema di autenticazione, dovrà essere 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 dovrà contenere riferimenti agevolmente riconducibili all'incaricato; dovrà essere 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 dovrà essere modificata almeno ogni tre mesi. Inoltre il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.
2. le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
3. lo strumento elettronico durante una sessione di trattamento non dovrà essere lasciato incustodito o comunque accessibile da parte di terzi non autorizzati.
4. se 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.

Perché si vuole che il contenuto del presente *"Documento Programmatico Sulla Sicurezza"* (DPSS) sia sempre attuale nel tempo e si astragga dall'organizzazione attuale e possa questo essere applicato in ogni momento anche in presenza di variazioni organizzative nel presente documento si sottintende la presenza del ***Responsabile del trattamento per la sicurezza dei dati*** e si ritiene che allo stesso siano stati affidati compiti molto vasti. Naturalmente nel caso di variazioni inerenti la nomina del ***Responsabile del Trattamento*** o dei poteri a questi delegati non vi sia o venga meno la figura del ***Responsabile del Trattamento*** o non siano più ricompresi alcuni compiti nel presente scritto previsti in capo allo stesso assegnando oneri inferiori è da intendersi che i compiti o i maggiori compiti spettino al ***Titolare del Trattamento*** che non li ha delegati, è onere del ***Titolare del Trattamento*** individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più ***Responsabili del Trattamento*** e tra questi, uno o più ***Responsabile del trattamento per la sicurezza dei dati*** (RSTD) che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi dell'art.31 del D.l. 30 giugno 2003, n. 196 . Qualora il ***Titolare del Trattamento*** ritenga di non nominare alcun ***Responsabile del Trattamento*** e alcun ***Responsabile del trattamento per la sicurezza dei dati***, o revochi o cessi la delega in precedenza conferita o pur nominando un ***"Responsabile" a questi vengano affidati compiti propri che non riguardino tutti i dati trattati sia da un punto di vista geografico sia da un punto di vista organizzativo o funzionale*** il ***Titolare del Trattamento*** ne assumerà tutte le responsabilità e funzioni.
Il ***Titolare del Trattamento*** affida al ***Responsabile del trattamento per la sicurezza dei dati*** il compito di adottare misure tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.
Il ***Titolare del Trattamento*** può affidare ai singoli ***Responsabili del Trattamento*** l'onere di individuare, nominare ed indicare per iscritto uno o più ***Incaricati del trattamento*** .
Sono compiti del ***Responsabile del trattamento per la sicurezza dei dati*** oltre a quant'altro la normativa o la delega del Titolare gli imponga quelli di:

- Individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, gli ***Amministratori di Sistema***.
- Individuare, nominare e incaricare per iscritto, un ***Custode delle password*** qualora vi siano più incaricati del trattamento che sia effettuato con mezzi informatici.
- Individuare, nominare e incaricare per iscritto, gli ***Incaricati del trattamento dei dati personali*** precisando diritti, procedure, regole e limiti in merito.
- Attribuire, con l'ausilio degli ***Amministratori di Sistema*** , ad ogni ***Utente*** (USER) o incaricato un ***Codice identificativo personale*** (USER-ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile.
- Autorizzare i singoli incaricati del trattamento e della manutenzione, e gli strumenti da utilizzare.
- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione come meglio specificato al successivo paragrafo 13, nonché l'elenco delle tipologie dei trattamenti effettuati.
- Verificare, con l'ausilio degli amministratori di sistema, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di acceso ai locali e le misure indicate al successivo paragrafo 13.
- Garantire che tutte le misure di sicurezza riguardanti i dati personali trattati siano applicate all'interno dell'azienda ed eventualmente al di fuori dell'azienda, qualora siano cedute a soggetti terzi quali ***Responsabili del Trattamento*** , tutte o parte delle attività di trattamento.
- Informare il titolare nella eventualità che si siano rilevati dei rischi.

5.4 L'AMMINISTRATORE DI SISTEMA

L'amministratore di sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione *(Art. 29* del D.l. 30 giugno 2003, n. 196*)*.
Nel caso di **trattamenti effettuati con gli elaboratori elettronici**, semprecchè non si tratti di dati personali di cui è consentita la diffusione, devono essere rispettate le seguenti misure previste dagli artt. 1 e ss. Dell'Allegato B, in materia di codice identificativo personale e di antivirus:
a) ciascun utente o incaricato del trattamento per l'utilizzazione dell'elaboratore deve avere un codice identificativo personale; uno stesso codice (fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione), non può, neppure in tempi diversi, essere assegnato a persone diverse;
b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la

disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'articolo 615 *quinquies* del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno annuale.
Per il trattamento dei dati personali l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Le autorizzazioni all'accesso sono rilasciate e revocate dal ***Titolare*** e, se designato, dal ***Responsabile***. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione. L'amministratore di sistema però dovrà verificare se l'utente o l'incaricato sia stato autorizzato all'accesso. Sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per il trattamento. Se riferita agli strumenti, l'autorizzazione deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.
La validità delle richieste di accesso ai dati personali deve essere verificata prima di consentire l'accesso stesso. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.
E' quindi compito degli ***Amministratori di Sistema*** :

- 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 secondo i criteri stabiliti dal ***Responsabile del trattamento per la sicurezza dei dati*** , conformemente a quanto più analiticamente individuato al successivo **paragrafo 12**
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro.
- Fare in modo che sia prevista l'assegnazione di ***Codici identificativi personali*** (USER-ID) per l'utilizzo dell'elaboratore, secondo i criteri in precedenza esposti e 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, oppure nel caso di mancato utilizzo dei ***Codici identificativi personali*** (USER-ID) per oltre 6 mesi.
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

5.5 CUSTODE DELLE PAROLE CHIAVE (PASSWORD) O I PREPOSTI AD ESSE

Il "***Custode delle Parole Chiave (PassWord)***" è la persona (individuata per iscritto dal ***Titolare*** o ***Responsabile***) preposta alla custodia delle parole chiave o che abbia accesso ad informazioni che concernono le medesime. Il "***Custode delle Parole Chiave (PassWord)***" deve essere nominato nel caso in cui, effettuando il trattamento dei dati personali con strumenti elettronici o comunque automatizzati, vi sia più di un incaricato del trattamento e siano in uso più parole chiave.

E' compito del ***Custode delle password*** gestire e custodire "***Password***" per l'accesso ai dati da parte degli incaricati.
Il ***Custode delle password*** deve predisporre, per ogni ***Incaricato del trattamento,*** una busta sulla quale è indicato lo "***USER-ID***" utilizzato: all'interno della busta deve essere indicata la "***Password***" usata per accedere alla "***Banca di Dati***"; ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore deve essere consentita l'autonoma sostituzione ed in questo caso occorre descrivere la procedura per detta modifica ed informare gli incaricati che nel caso di sostituzione gli stessi devono prima della sua sostituzione devono consegnare la Nuova Password al "***Custode delle Parole Chiave (PassWord)***".
Le buste con le "***Password***" debbono essere conservate in luogo chiuso e protetto.
Dette operazioni devono essere adottate, anteriormente all'inizio del trattamento da parte degli incaricati.
Nel caso in cui siano nominato un amministratore di sistema le funzioni connesse all'"*USER ID*" ed all'assegnazione iniziale della Password saranno assunte dallo stesso ed al ***Custode delle password*** competeranno le sole funzioni di custodia.
La password dovrà essere composta da almeno otto caratteri, oppure nel caso in cui lo strumento elettronico non lo consenta da un numero di caratteri pari al massimo consentito; non dovrà contenere riferimenti facilmente riconducibili all'incaricato. (art. 5, Allegato B).
La password dovrà essere sostituita almeno ogni sei mesi; nel caso di trattamento avente ad oggetto dati sensibili almeno ogni tre mesi (art. 5, Allegato B).

5.6 GLI INCARICATI DEL TRATTAMENTO

Sono Incaricati del trattamento le persone incaricate per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta autorità *(Art. 30* del D.l. 30 giugno 2003, n. 196*)*.
L'art *30* del D.l. 30 giugno 2003, n. 196, al suo primo comma dispone che gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del titolare o del responsabile.

6. NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

La nomina di ciascun ***Responsabile del trattamento per la sicurezza dei dati*** deve essere effettuata con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.
Copia della lettera di nomina accettata deve essere conservata a cura del ***Titolare del Trattamento*** in luogo sicuro.
Fra i vari ***Responsabili del Trattamento*** può esserne individuato uno o più che assicurino e garantiscano che vengano adottate le misure di sicurezza di cui all'art.31 del D.l. 30 giugno 2003, n. 196, denominati ***Responsabile del trattamento per la sicurezza dei dati.***
Il ***Titolare del Trattamento*** deve informare ciascun ***Responsabile del Trattamento*** delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dall'Allegato B.
A ciascun ***Responsabile del Trattamento*** il ***Titolare del Trattamento*** deve consegnare una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del ***Responsabile del Trattamento*** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.
La nomina del ***Responsabile del Trattamento*** può essere revocata in qualsiasi momento dal ***Titolare del Trattamento*** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

7. NOMINA DEGLI AMMINISTRATORI DI SISTEMA

L' ***"Amministratore di Sistema"*** è la persona fisica o giuridica che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di ***Banche di dati.***
Anche se non espressamente previsto dalla norma, è opportuno che il ***Responsabile del trattamento per la sicurezza dei dati*** nomini uno o più ***Amministratori di Sistema,*** specificando gli elaboratori o le banche dati che è chiamato a sovrintendere, informandolo delle responsabilità che gli sono state affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dall'Allegato B.
La lettera di incarico deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro.
Agli ***Amministratori di Sistema*** il ***Responsabile del Trattamento*** deve consegnare una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.
La figura dell' ***"Amministratore di Sistema"*** può coincidere con quella del ***Responsabile del trattamento per la sicurezza dei dati.***

8. NOMINA DEL CUSTODE DELLE PASSWORD

Il ***Responsabile del trattamento per la sicurezza dei dati*** nomina uno o più ***"Custodi delle Password"*** a cui è conferito il compito di custodire le "Parole chiave" o ***"Password"*** per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.
La nomina di ciascun ***Custode delle password*** deve essere effettuata con una lettera di incarico.
La nomina del ***Custode delle password*** deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro.
Il ***Responsabile del trattamento per la sicurezza dei dati*** deve informare ciascun ***Custode delle password*** della responsabilità che gli è stata affidata in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dall'Allegato B.
A ciascun ***Custode delle password*** il ***Responsabile del trattamento per la sicurezza dei dati*** deve consegnare una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del *Custode delle password* è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.
La nomina del *Custode delle password* può essere revocata in qualsiasi momento dal *Responsabile del trattamento per la sicurezza dei dati* dei dati senza preavviso, ed essere affidata ad altro soggetto.

9. NOMINA DEGLI INCARICATI DEL TRATTAMENTO

Ai *Responsabili del Trattamento* può essere affidato il compito di nominare, con comunicazione scritta, uno o più *Incaricati del trattamento* dei dati.
La nomina di ciascun *Incaricato del trattamento* dei dati deve essere effettuata con una lettera di incarico in cui sono specificati i compiti che gli sono affidati.
Gli *Incaricati del trattamento* devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.
Agli incaricati deve essere assegnata una parola chiave e un codice identificativo personale.
La nomina degli *Incaricati del trattamento* deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del *Responsabile del trattamento per la sicurezza dei dati* in luogo sicuro.
Agli *Incaricati del trattamento* il *Responsabile del trattamento per la sicurezza dei dati* deve consegnare una copia di tutte le norme che riguardano la Sicurezza del Trattamento dei Dati in vigore al momento della nomina.
La nomina degli *Incaricati del trattamento* è a tempo indeterminato, e decade per revoca, per sue dimissioni, o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

10. DATI AFFIDATI AD ENTI ESTERNI PER IL TRATTAMENTO IN OUT-SOURCING

10.1 TRATTAMENTO DEI DATI IN OUTSOURCING

Il *Titolare del Trattamento* può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, in Out-Sourcing, nominandoli responsabili del trattamento.
In questo caso debbono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.
Nel caso in cui questi non vengano espressamente nominati, *"Responsabili del trattamento in out-sourcing"* ai sensi dell'art.29 del Codice Unico devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.
Il *Titolare del Trattamento* o uno dei *Responsabili del Trattamento*, cui è affidato tale specifico incarico, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in qualità di *Responsabile del Trattamento*, con particolare attenzione a quei soggetti terzi in out-sourcing, ed indicare per ognuno di essi il tipo di trattamento effettuato.
Per l'inventario dei soggetti terzi, in Out-Sourcing, deve essere utilizzato il modulo D.318.e, che deve essere conservato a cura del *Responsabile del Trattamento* in luogo sicuro.

10.2 CRITERI PER LA SCELTA DEGLI ENTI TERZI A CUI AFFIDARE IL TRATTAMENTO DEI DATI IN OUT-SOURCING

Il *Titolare del Trattamento* può nominare *"Responsabile del trattamento in out-sourcing"* quei soggetti terzi che abbiano i requisiti individuati dall'art.29 del Codice Unico (esperienza, capacità ed affidabilità).
Il *"Responsabile del trattamento dei dati in out-sourcing"* deve rilasciare una dichiarazione scritta al *Titolare del Trattamento* da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dall'Allegato B.

10.3 NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI IN OUT-SOURCING

Per ogni trattamento affidato ad un soggetto esterno nominato *"Responsabile del trattamento in out-sourcing"*, il *Titolare del Trattamento* deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.
Il *Titolare del Trattamento* deve informare il *"Responsabile del trattamento dei dati in out-sourcing"* dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore, ed

in particolare di quanto stabilito dall'Allegato B.
Il "*Responsabile del trattamento dei dati in out-sourcing*" deve accettare la nomina, secondo il modello D.318.ros.
La nomina del "*Responsabile del trattamento dei dati in out-sourcing*" deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del *Titolare del Trattamento* in luogo sicuro.

11. INVENTARI E METODOLOGIE OPERATIVE DI TRATTAMENTO DEI DATI

11.1 INDIVIDUAZIONE DELLE BANCHE DI DATI OGGETTO DEL TRATTAMENTO

Al "*Responsabile del trattamento della sicurezza dei dati*" è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.
Ogni "*Banca di dati*" o archivio deve essere classificato in relazione alle informazioni in essa contenute indicando se si tratta di:

- Dati Personali Comuni
- Dati Personali Sensibili
- Dati Personali Semisensibili
- Dati Personali Giudiziari

Per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato il modulo D.318.a che deve essere conservato a cura del "*Responsabile del trattamento della sicurezza dei dati*" in luogo sicuro.

11.2 INVENTARIO DELLE SEDI IN CUI VENGONO TRATTATI I DATI

Al "*Responsabile del trattamento della sicurezza dei dati*" è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati. Per redigere l'inventario delle sedi in cui vengono trattati i dati deve essere utilizzato il modulo D.318.b che deve essere conservato a cura del "*Responsabile del trattamento della sicurezza dei dati*" in luogo sicuro.

11.3 INVENTARIO DEGLI UFFICI IN CUI VENGONO TRATTATI I DATI

Al "*Responsabile del trattamento della sicurezza dei dati*" è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati. In particolare, per ogni ufficio deve essere indicata la sede e se l'accesso è controllato. Per l'inventario degli uffici deve essere utilizzato il modulo D.318.c che deve essere conservato a cura del "*Responsabile del trattamento della sicurezza dei dati*" in luogo sicuro.

11.4 INVENTARIO DEI SISTEMI DI ELABORAZIONE

Al "*Responsabile del trattamento della sicurezza dei dati*" è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.
Per ogni sistema debbono essere descritte le caratteristiche e se si tratta di sistema di elaborazione:

- Non accessibile da altri elaboratori (stand-alone)
- In rete non accessibile al pubblico
- In rete accessibile al pubblico

Per ogni sistema deve essere specificato il nome dell'incaricato o degli incaricati che lo utilizzano nonché del *Custode delle password* .
Per l'inventario dei sistemi di elaborazione deve essere utilizzato il modulo D.318.d che deve essere conservato a cura del "*Responsabile del trattamento della sicurezza dei dati*" in luogo sicuro.

12. MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

12.1 CRITERI E PROCEDURE PER GARANTIRE L'INTEGRITÀ DEI DATI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il "*Responsabile del trattamento della sicurezza dei dati*", stabilisce, con il supporto tecnico *dell'Amministratore del sistema* la periodicità con cui debbono essere effettuate le copie di sicurezza delle *Banche di dati* trattati.
I criteri debbono essere definiti dal *Responsabile del trattamento della sicurezza dei dati* in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni ***Banca di dati*** debbono essere definite le seguenti specifiche:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta
- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- ***L'Incaricato del trattamento*** a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

Per redigere il "***Documento con le istruzioni di copia***" deve essere utilizzato per ogni "***Banca di dati***" il modulo D.318.m che deve essere conservato a cura del "***Responsabile del trattamento della sicurezza dei dati***" in luogo sicuro e deve essere trasmesso in copia controllata a:

- ***Amministratore di sistema*** di competenza
- ***Incaricati del trattamento*** di competenza

12.2 PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di Virus Informatici, il "***Responsabile del trattamento della sicurezza dei dati***", stabilisce, con il supporto tecnico dell' "***Amministratore del sistema***" quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.
Il "***Responsabile del trattamento della sicurezza dei dati***", stabilisce inoltre la periodicità, almeno ogni anno (in caso di dati sensibili o giudiziari almeno semestralmente), con cui debbono essere effettuati gli aggiornamenti dei sistemi Antivirus utilizzati per ottenere un accettabile standard di sicurezza delle ***Banche di dati*** trattate.
I criteri debbono essere definiti dal "***Responsabile del trattamento della sicurezza dei dati***" in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni sistema debbono essere definite le seguenti specifiche:

- Il tipo di programma utilizzato.
- La periodicità di aggiornamento

Per ogni sistema deve essere predisposto il modulo "Rilevazione di Virus Informatico" D.318.q sul quale debbono essere annotati eventuali virus rilevati, e se possibile la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.
I moduli compilati ed aggiornati dagli ***Incaricati del trattamento*** debbono essere conservati a cura del "***Responsabile del trattamento della sicurezza dei dati***" in luogo sicuro e debbono essere trasmessi in copia controllata all' "***Amministratore di sistema***" di competenza.

12.3 INFEZIONI E CONTAGIO DA VIRUS INFORMATICI

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da Virus Informatici ***l'Amministratore del sistema*** deve provvedere a:

- Isolare il sistema.
- Verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico.
- Identificare l'Antivirus adatto e bonificare il sistema infetto.
- Installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

L'Amministratore del sistema deve inoltre compilare il modulo di "Report dei Contagi da Virus Informatici" D.318.r.
I moduli compilati devono essere conservati a cura del "***Responsabile del trattamento della sicurezza dei dati***" in luogo sicuro.

12.4 CUSTODIA E CONSERVAZIONE DEI SUPPORTI UTILIZZATI PER IL BACK-UP DEI DATI

Il "***Responsabile del trattamento della sicurezza dei dati***", è responsabile della Custodia e della conservazione dei supporti utilizzati per il Back-Up dei dati.
Per ogni "***Banca di dati***" nel modulo D.318.m deve essere indicato il luogo di conservazione dei

supporti utilizzati per il Back-Up dei dati.
Il luogo di conservazione deve essere individuato in modo che sia protetto da:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni e atti vandalici
- Incendio
- Allagamento
- Furto

L'accesso ai supporti utilizzati per il Back-Up dei dati è limitato per ogni "***Banca di dati***" al:

- "***Responsabile del trattamento della sicurezza dei dati***" .
- Eventuale **Responsabile del Trattamento** di competenza.
- ***Incaricato del trattamento*** di competenza.
- "***Amministratore di sistema***" di competenza.

12.5 UTILIZZO E RIUTILIZZO DEI SUPPORTI MAGNETICI

Se il "***Responsabile del trattamento della sicurezza dei dati***" decide che i supporti magnetici utilizzati per le copie di Back-Up delle ***Banche di dati*** trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo illeggibili le informazioni in esso contenute.
E' compito del "***Responsabile del trattamento della sicurezza dei dati***" assicurarsi che in nessun caso vengano lasciate copie di Back-Up delle ***Banche di dati*** trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.

12.6 PIANO DI FORMAZIONE DEGLI INCARICATI

Al "***Responsabile del trattamento della sicurezza dei dati***" è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato di effettuare periodicamente le operazioni di Back-Up delle ***Banche di dati*** trattate.
Per ogni ***Incaricato del trattamento***, il "***Responsabile del trattamento della sicurezza dei dati***" definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica se è necessaria della formazione tecnica, utilizzando il modulo D.318.n che deve essere trasmesso in copia controllata al ***Titolare del Trattamento***.

13. MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO

13.1 NORME GENERALI DI PREVENZIONE

In considerazione di quanto disposto dall'Allegato B, è fatto divieto a chiunque di:
• Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal ***Responsabile del trattamento per la sicurezza dei dati*** di dati oggetto del trattamento.
• Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal ***Responsabile del trattamento per la sicurezza dei dati*** , di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
• Sottrarre, cancellare, distruggere senza l'autorizzazione del ***Responsabile del trattamento per la sicurezza dei dati***, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
• Consegnare a persone non autorizzate dal ***Responsabile del trattamento per la sicurezza dei dati***, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

13.2 PROCEDURE PER CONTROLLARE L'ACCESSO AI LOCALI IN CUI VENGONO TRATTATI I DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, nominando un apposito "***Incaricato***", con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
Il ***Responsabile del trattamento per la sicurezza dei dati*** deve definire le modalità di accesso agli

uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.
Il ***Responsabile del trattamento per la sicurezza dei dati*** deve informare con una comunicazione scritta l'***"incaricato dell'ufficio"*** dei compiti che gli sono stati affidati utilizzando il modello D.318.lcl.

13.3 PROCEDURE DI ASSEGNAZIONE DEGLI USER-ID

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve definire in accordo con gli ***Amministratori del sistema*** le modalità di assegnazione dei nomi identificativi per consentire a ciascun ***Incaricato del trattamento*** di accedere ai sistemi di trattamento delle ***Banche di dati.***
Non sono ammessi nomi identificativi di gruppo, con la sola eccezione dei codici identificativi assegnati per l'amministrazione di sistema, relativamente ad eventuali sistemi operativi che prevedono un unico livello di accesso.
In ogni caso, un codice identificativo assegnato ad un ***Incaricato del trattamento*** deve essere annullato se ***l'Incaricato del trattamento*** ha dato le dimissioni.

13.4 PROCEDURE DI ASSEGNAZIONE DELLE PASSWORD

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve definire in accordo con gli ***Amministratori del sistema*** le modalità di assegnazione delle password.
La definizione dei criteri di assegnazione delle password è descritta nel modulo D.318.s. In relazione al tipo di ***_Banca di dati"*** trattata, ***l'Amministratore del sistema*** può decidere che ogni utente ***Incaricato del trattamento*** possa modificare autonomamente la propria ***"Password"*** di accesso. In tal caso l'incaricato consegnerà una busta al _Custode della password" contenente la nuova password o se il dato viene memorizzato in particolari archivi dell'elaboratore, in questo caso la modifica equivale alla comunicazione al ***Custode delle password.***

13.5 IDENTIFICAZIONE DEGLI ELABORATORI CONNESSI IN RETE PUBBLICA

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica.
Per ogni sistema deve essere specificato ***l'Incaricato del trattamento, l'Amministratore del sistema*** e il ***Custode delle password.***
Per l'inventario dei sistemi di elaborazione deve essere utilizzato il modulo D.318.p che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata all' ***"Amministratore di sistema"*** di competenza

13.6 CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DEI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il ***Responsabile del trattamento per la sicurezza dei dati*** (RDST), stabilisce, con il supporto tecnico dell'***Amministratore del sistema*** , le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.
I criteri debbono essere definiti dal ***Responsabile del trattamento per la sicurezza dei dati*** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- le misure applicate per evitare intrusioni.
- le misure applicate per evitare contagi da "Virus Informatici".

utilizzando per ogni sistema interessato il modulo D.318.p che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata all' ***"Amministratore di sistema"*** di competenza.

14. MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

14.1 PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli ***Incaricati del trattamento*** autorizzati al trattamento dei

dati personali.
In particolare, in caso di trattamento automatizzato di dati, per ogni ***Incaricato del trattamento*** deve essere indicato lo USER-ID assegnato e la password con un numero di caratteri non inferiori a otto..
In caso di dimissioni di un ***Incaricato del trattamento*** o di revoca delle autorizzazioni al trattamento dei dati, il ***Responsabile del trattamento per la sicurezza dei dati*** , deve darne immediata comunicazione al "***Custode delle Password***" e all' "***Amministratore di sistema***" di competenza che provvederanno a disattivare la possibilità di accesso al sistema per il soggetto in questione.
Per redigere l'elenco degli ***Incaricati del trattamento*** deve essere utilizzato il modulo D.318.i che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata a:

- "***Amministratore di sistema***" di competenza
- ***Custode delle password*** di competenza

14.2 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DELLE AUTORIZZAZIONI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di verificare ogni anno, entro il 31 dicembre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando il modulo D.318.i. che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata a:

- "***Amministratore di sistema***" di competenza
- ***Custode delle password*** di competenza

14.3 DEFINIZIONE DEI CRITERI DI ASSEGNAZIONE DEI PERMESSI DI ACCESSO AI DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di redigere e di aggiornare ad ogni variazione la tabella dei "Permessi di accesso" che indica per ogni "***Banca di dati***" i tipi di permesso di accesso per ogni ***Incaricato del trattamento*** autorizzato.
In particolare per ogni ***Incaricato del trattamento*** e per ogni "***Banca di dati***" debbono essere indicati i privilegi assegnati tra i seguenti:

- Inserimento di dati
- Lettura e stampa di dati
- Variazione di dati
- Cancellazione di dati

La tabella dei "Permessi di accesso" deve essere redatta utilizzando il modulo D.318.l che deve essere conservato a cura del ***Responsabile del trattamento per la sicurezza dei dati*** in luogo sicuro e deve essere trasmesso in copia controllata a:

- "***Amministratore di sistema***" di competenza
- ***Custode delle password*** di competenza

14.4 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENERE I PERMESSI DI ACCESSO AI DATI

Al "***Responsabile del trattamento per la sicurezza dei dati*** " è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando il modulo D.318.l che deve essere in luogo sicuro e deve essere trasmesso in copia controllata a:

- "***Amministratore di sistema***" di competenza
- ***Custode delle password*** di competenza

14.5 PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale ***Incaricato del trattamento*** dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.
Per ogni utente il ***Responsabile del trattamento per la sicurezza dei dati*** definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali variazioni della normativa, le

necessità di formazione utilizzando il modulo D.318.n che deve essere trasmesso in copia controllata al *Titolare del Trattamento* .

15. MANUTENZIONE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI

15.1 MANUTENZIONE DEI SISTEMI DI ELABORAZIONE DEI DATI

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di verificare ogni anno, avvalendosi dell' "***Amministratore di Sistema***", la situazione delle apparecchiature hardware installate con cui vengono trattati i dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche.
La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

tenendo conto anche dell'evoluzione tecnologica.
Il ***Responsabile del trattamento per la sicurezza dei dati*** deve compilare il modulo di "evidenziazione dei rischi hardware" conformemente al modulo D.318.t.
Nel caso in cui esistano rischi evidenti il ***Responsabile del trattamento per la sicurezza dei dati*** deve informarne il ***Titolare del trattamento*** perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

15.2 MANUTENZIONE DEI SISTEMI OPERATIVI

Al ***Responsabile del Trattamento*** è affidato il compito di verificare ogni semestre, la situazione dei Sistemi Operativi installati sulle apparecchiature con cui vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei Sistemi Operativi utilizzati.
- Segnalazioni di Patch ,Fix o System-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Il ***Responsabile del trattamento per la sicurezza dei dati*** deve compilare il modulo di _evidenziazione dei rischi sui Sistemi Operativi" conformemente al modulo D.318.u.
Nel caso in cui esistano rischi evidenti il ***Responsabile del trattamento per la sicurezza dei dati*** deve informarne il ***Titolare del Trattamento*** perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

15.3 MANUTENZIONE DELLE APPLICAZIONI SOFTWARE

Al ***Responsabile del trattamento per la sicurezza dei dati*** è affidato il compito di verificare ogni anno (semestralmente nel caso di dati sensibili o giudiziari), la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità del software applicativo, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.
Il ***Responsabile del trattamento per la sicurezza dei dati*** deve compilare il modulo di "evidenziazione dei rischi nelle applicazioni" conformemente al modulo D.318.v.
Nel caso in cui esistano rischi evidenti il "***Responsabile del trattamento per la sicurezza dei dati"*** deve informarne il ***Titolare del Trattamento*** perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

16. MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO

CON STRUMENTI NON AUTOMATIZZATI.

16.1 NOMINA E ISTRUZIONI AGLI INCARICATI

Per ogni archivio i "***Responsabili del trattamento per la sicurezza dei dati***" debbono definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso negli archivi. Annualmente dovrà essere verificato l'ambito del trattamento consentito ai singoli incaricati.
Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli in modo che non vi possano accedere persone non autorizzate e restituirli al termine delle operazioni.
Qualora i documenti contengano dati sensibili o giudiziari gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura (questa disposizione non è più contenuta nel nuovo Codice Unico, ma è comunque consigliabile come standard operativo).
L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previo controllo o identificazione e registrazione dei soggetti

16.2 COPIE DEGLI ATTI E DEI DOCUMENTI

Quanto indicato nel punto precedente, si applica anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali.

17. ALLEGATI

D.318.a Elenco degli archivi dei dati oggetto del trattamento
D.318.a1 Finalità del trattamento
D.318.a2 Categorie di soggetti interesati
D.318.b Elenco delle sedi in cui vengono trattati i dati
D.318.c Elenco degli uffici in cui vengono trattati i dati
D.318.d Sistemi di elaborazione per il trattamento dei dati
D.318.i Elenco del personale autorizzato al trattamento dei dati

Vista la normativa in materia di trattamento dei dati personali ed in particolare:

Legge 31 dicembre 1996 n. 675
D.lgs. 28 dicembre 2001 n. 467
Legge 24 marzo 2001 n. 127
Legge 3 novembre 2000 n. 325
Legge 31 dicembre 1996 n. 676
D.lgs. 6 novembre 1998 n. 389
D.lgs. 30 luglio 1999 n. 282
D.lgs. 30 luglio 1999 n. 281
D.P.R. 28 luglio 1999 n. 318
D.lgs. 11 maggio 1999 n. 135
D.lg. 13 maggio 1998 n. 171
Legge 6 ottobre 1998 n. 344
D.lgs. 8 maggio 1998 n. 135
D.lgs. 28 luglio 1997 n. 255

Si redige il

Documento programmatico sulla sicurezza

Nel caso di trattamento dei dati sensibili, se il trattamento è effettuato con elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico, l'art. 6 impone l'obbligo di stesura del Documento programmatico sulla sicurezza. In relazione all'obbligo per le autorizzazioni all'accesso ai dati particolari potremmo schematizzare la casistica come segue:

Tipologia	**Dati "ordinari"**		**Dati "sensibili"**	
Documento programmatico sulla sicurezza	**Obbligo**	**Norma**	**Obbligo**	**Norma**
Per finalità Esclusivamente **Personali**				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*				
- con elaboratori in *rete Pubblica*				
Per finalità NON esclusivamente **personali**				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
con elaboratori in *rete Privata*				
- con elaboratori in *rete Pubblica*			si	*Art. 6*

Dispone l'art. 6 che il Documento programmatico sulla sicurezza: <<dev'essere predisposto e aggiornato, con cadenza annuale, ... per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:

a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;

b) i criteri e le procedure per assicurare l'integrità dei dati;

c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;

d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni».

Il documento è richiesto solo per i dati sensibili con accesso da rete disponibile al pubblico; tuttavia il DPSS prenderà in considerazione anche i trattamenti effettuati su supporto cartaceo o su rete non disponibile al pubblico in quanto strumento essenziale per prevenire trattamenti illeciti. Tale documento se rispecchia l'effettiva volontà del Titolare è lo strumento chiave per gestire al meglio tutti gli aspetti della sicurezza informatica, non solo per i dati che ricadono sotto la tutela della 675/1996, ma per tutti i dati aziendali che per il loro valore o interesse meritano di essere protetti.

Il documento programmatico sulla sicurezza ha lo scopo di definire programmi di adeguamento e di perfezionamento delle misure di sicurezza già in essere, da implementare e quindi sottoporre a verifica con una frequenza almeno annuale.

I profili che verranno considerati in questa programmazione saranno tre:

- protezione delle aree e dei locali interessati da misure di sicurezza relative al trattamento e perseguimento della sicurezza nella trasmissione dei dati e nel loro accesso in via telematica (tecnologie);
- protezione della integrità dei dati (procedure);
- formazione del personale incaricato del trattamento con specifico riferimento alle tematiche inerenti alla sicurezza (risorse umane).

La programmazione, a sua volta, è previsto consegua ad uno studio che consideri fattori sia oggettivi (analisi dei rischi) che soggettivi (distribuzione delle mansioni e delle responsabilità).

PROCEDURE: sono le regole di comportamento redatte al fine di prevenire trattamenti illeciti di dati personali

Le procedure per la sicurezza, previste nel regolamento, possono essere elencate nelle seguenti:

- Parola chiave per l'accesso ai dati
- Codice identificativo personale per l'utilizzazione dell' elaboratore
- Autorizzazioni all'accesso
- Reimpiego dei supporti di memorizzazione
- Accesso (ai documenti) selezionato e monitorato

Parola chiave per l'accesso ai dati (PASSWORD) - E' una misura prevista nell'art. 2 del Regolamento per il trattamento dei dati personali effettuato per fini diversi da quelli esclusivamente personali mediante elaboratori *stand alone.* Detta norma

dispone che, anteriormente all'inizio del trattamento, occorre «prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, consentirne l'autonoma sostituzione, previa comunicazione ai soggetti preposti . . . ». L'art. 4 dispone che le misure descritte dall'art. 2 debbano essere osservate anche nel caso di trattamenti effettuati con gli elaboratori accessibili in rete. Nel caso di trattamento di dati sensibili effettuato per fini esclusivamente personali mediante elaboratori accessibili in rete, l'art. 8 stabilisce che il trattamento <<è soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche dati>>.
In relazione all'obbligo di istituire la parola chiave potremmo schematizzare la casistica come segue:

Tipologia **Dati "ordinari"** **Dati "sensibili"**

Parola chiave (PASSWORD)	**Obbligo**	**Norma**	**Obbligo**	**Norma**
Per finalità Esclusivamente Personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*				
- con elaboratori in *rete Pubblica*			si	*Art. 8*
Per finalità NON esclusivamente personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*	si	*Art. 2*	si	*Art. 2*
- con elaboratori in *rete Privata*	si	*Art. 3 (A2)*	si	*Art. 3 (A2)*
- con elaboratori in *rete Pubblica*	si	*Art. 3 (A2)*	si	*Art. 3 (A2)*

Il regolamento sulla sicurezza dei dati personali prevede che le password vengano assegnate da un responsabile e stabilisce anche le precauzioni che devono essere adottate dal "custode" delle password stesse. L'art. 2 lettera b) obbliga ad individuare per iscritto:

- i custodi;

- i soggetti (non preposti alla custodia ma) che hanno accesso ad informazioni che concernano le parole chiave.

Solo poche persone devono essere autorizzate dalla procedura alla registrazione dell'utente e al rilascio della password; se generata automaticamente dal sistema, la password deve essere consegnata a mano, dal responsabile della sicurezza all'utente, e avere esclusivamente carattere temporaneo e validità sufficiente per consentire l'accesso al sistema per cambiarla. Il sistema dovrebbe automaticamente assicurare che la sostituzione avvenga entro un determinato lasso di tempo dal ricevimento della password iniziale.

Ogni utente deve essere riconosciuto per mezzo di un unico identificativo e di un'unica password personale, al fine di assicurare una contabilizzazione individuale e una univoca responsabilizzazione.

La password deve essere registrata in forma incriptata, senza possibilità di riportarla in chiaro, in modo da rendere estremamente problematica la sua individuazione. Il

sistema deve prevenire il regolare riutilizzo della password preferita registrando in un file storico le ultime utilizzate dall'utente e stabilire sia la vita utile massima che quella minima in modo da evitare che gli utenti possano cambiarla ripetutamente e tornare a impiegare la loro password preferita.

E' quindi necessario cambiare la password con una buona frequenza e regolarità normalmente entro 30-90 giorni, oppure con maggiore frequenza da parte di quegli utenti aventi particolari diritti di accesso. Il sistema deve avvisare con qualche giorno di anticipo l'utente quando la password è prossima alla scadenza e per rendere obbligatoria la sua sostituzione è indispensabile che siano sospesi i diritti di accesso attribuiti all'utente inadempiente.

La Password inizialmente deve quindi essere generata in modo protetto automaticamente dal sistema, ed abilitare esclusivamente al cambio della stessa. Una procedura in tal senso può essere:

1. l'Amministratore del sistema di sicurezza chiede la password iniziale per un nuovo utente;

2. il sistema censisce l'utente e ne genera la Password, stampandola su una stampantina apposita e su un modulo tipo quelli utilizzati per la stampa del PIN del Bancomat;

3. l'Amministratore del sistema consegna la Password all'utente, che firma per ricevuta;

4. l'utente, una volta ricevuta la password potrà modificarla e consegnare la nuova password al preposto alla custodia delle password in busta chiusa;

5. il preposto alla custodia custodirà le password così ricevute in un luogo protetto ed in un contenitore munito di serratura.

Di ognuna di queste azioni deve restare traccia, sia in formato elettronico, sia in formato cartaceo.

Istituzione dei custodi delle parole chiave - Nel caso di trattamenti per i quali si rende obbligatoria la Parola chiave l'art. 2 dispone che quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, occorre individuare per iscritto i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime. Hanno solo funzione di custodia delle parole chiave e la loro presenza si rende obbligatoria in tutti i casi d'obbligo delle parole chiave e semprechè vi sia più di una parola chiave.
I *custodi delle chiavi* attribuiscono normalmente la chiave originaria a ciascun incaricato e ne tengono memoria; così come devono trattenere memoria di ogni modifica delle chiavi, che è previsto debba essere loro comunicata. Quella del custode *delle chiavi* é comunque una nuova figura che, col DPR 318/99, fa il suo primo ingresso nella già variegata compagine di categorie soggettive coinvolte dalla disciplina del trattamento dei dati personali, dal titolare del *trattamento, al* responsabile del trattamento, all'incaricato, all'amministratore *di* sistema. E si tratta di figura tanto significativa, secondo il Regolamento, da giustificare ed imporre che la nomina dei soggetti chiamati ad impersonarla avvenga per iscritto.

L'individuazione per iscritto del custode deve avvenire quando vi è più di un incaricato del trattamento e sono in uso più parole chiave.

In caso di necessità (per esempio, se il titolare della password è assente ed è indispensabile accedere a certe informazioni o a certe funzioni, o se l'ha semplicemente dimenticata), l'amministratore di sistema disattiva la password e ne genera un'altra.

Codice identificativo personale per l'utilizzazione dell'elaboratore (ID USER) - Nel caso di trattamenti effettuati con elaboratori in rete, salvi i casi di trattamento dei dati personali di cui è consentita la diffusione, l'art. 4 comma 1 lettera a) dispone che «a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell' elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse». Alla lettera b) inoltre si dispone: «b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi».

In relazione all'obbligo di istituire l'identificativo personale potremmo schematizzare la casistica come segue:

Tipologia	**Dati "ordinari "**		**Dati "sensibili"**	
Codice identificativo personale (ID USER)	**Obbligo**	**Norma**	**Obbligo**	**Norma**
Per finalità Esclusivamente Personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*				
- con elaboratori in *rete Pubblica*				
Per finalità NON esclusivamente personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
-con elaboratori in *rete Privata*	si	Art. 4 ab	si	Art. 4 ab
con elaboratori in *rete Pubblica*	si	Art. 4 ab	si	Art. 4 ab

Nel trattamento con elaboratori in rete "non pubblica" è previsto che, per ciascun utente, alla *password, si* accompagni anche un identificativo personale; pur se il Regolamento tace sul punto, rientra comunque nelle nozioni di comune esperienza che la parola chiave costituisca strumento di validazione dell'identificativo, in occasione di ogni accesso, e che la prima debba rimanere segreta laddove il secondo possa essere anche pubblicamente conosciuto.

La gestione dei codici identificativi degli utenti deve inoltre prevedere la possibilità di disattivazione in caso di perdita da parte del titolare della qualità legittimante all'accesso nonché la disattivazione (non necessariamente automatica) in caso di mancato utilizzo dell'identificativo stesso per oltre sei mesi.

Viene richiesto, di norma, il suo non riutilizzo, anche in tempi diversi, una volta assegnato ad una persona. Non essendoci limiti temporali, in pratica, un codice una

volta assegnato ad una persona, se questa per es. lascia l'azienda non deve poter essere più riutilizzato.

La norma richiede inoltre che il codice sia disattivato nel caso la persona a cui è stato assegnato perda la necessità di accesso agli elaboratori che contengono dati personali e a cui era stato abilitato o non sia utilizzato per più di 6 mesi. Non viene precisato nessun vincolo temporale tra la perdita della necessità di accesso e la disattivazione del codice identificativo, poiché però il testo precisa che "sia prevista la disattivazione", ogni 6 mesi dovranno essere effettuate le opportune verifiche da parte dei responsabili.

Nel caso di trattamento dei dati sensibili effettuato per fini esclusivamente personali mediante elaboratori accessibili in rete, l'art. 8 stabilisce che il trattamento <<è soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una *parola chiave,* qualora i dati siano organizzati in banche di dati>>.

Trattasi non già del codice identificativo personale ma della parola chiave simile a quella regolata nell'art. 2.

Autorizzazioni all'accesso ai dati particolari - Nel caso di trattamento dei dati sensibili effettuato con gli elaboratori accessibili in rete l'art. 5 comma 1 dispone che « l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione». Le disposizioni illustrate non si applicano al trattamento dei dati personali di cui è consentita la diffusione.

Eccettuato il trattamento dei dati personali di cui è consentita la diffusione, nel caso di trattamento dei dati sensibili, se il trattamento è effettuato con elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico, l'art. 5 commi 1 e 2 dispongono che: «sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico». <<L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento>>.

In relazione all'obbligo per le autorizzazioni all'accesso ai dati particolari potremmo schematizzare la casistica come segue:

Tipologia **Dati "Oridinari"** **Dati "Sensibili"**

Autorizzazioni all'accesso	**Obbligo**	**Norma**	**Obbligo**	**Norma**
Per finalità Esclusivamente Personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*				
- con elaboratori in *rete Pubblica*				
Per finalità NON esclusivamente personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*			si	*Art. 5 c. 1*
- con elaboratori in *rete Pubblica*			si	*Art. 5 cc. 1+2*

La norma richiede una gestione precisa di questa tipologia di accessi. Vanno concessi

solo per effettiva necessità di lavoro e limitatamente ai soli dati "necessari e sufficienti" per lo svolgimento delle mansioni assegnate. Il Responsabile inoltre, deve poter dimostrare che la sua autorizzazione sia antecedente all'accesso ai dati stessi. La verifica di validità dell'accesso è comunque richiesta annualmente. Inoltre si deve tener presente che sono espressamente vietate le utenze collettive o di gruppo.

Tali autorizzazioni devono essere rilasciate dal titolare o dal responsabile del trattamento, e devono essere riviste almeno una volta all'anno. L'autorizzazione deve essere limitata ai dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento e manutenzione.
Per quanto attiene la misura autorizzativa, questa è disciplinata secondo le stesse modalità che sono proprie della autorizzazione rilasciata al personale, ivi compresa la verifica almeno annuale della permanenza dei requisiti. L'autorizzazione deve però individuare in questo caso, accanto ai soggetti, gli strumenti che possono essere utilizzati per l'interconnessione mediante reti accessibili al pubblico». Cosa sono gli strumenti per interconnettersi reciprocamente si desume attraverso il comma 2 dell'art. 5, che ci spiega che l'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento. Tale indicazione esaurisce il contenuto della autorizzazione relativa agli strumenti ed implica che si potrà accedere solo dai PC (e dai terminali) fisicamente individuati che sono contenuti in questo elenco. Non ci sono invece limiti quanto al luogo in cui gli strumenti sono posti o trasportati, o alla possibilità tutt'altro che remota che gli stessi memorizzino dati non solo in RAM, ad esempio per trattarli off line».

Criteri per il rilascio ed il controllo delle autorizzazioni di accesso - Nel caso di trattamento dei dati sensibili effettuato con gli elaboratori accessibili in rete l'art. 5 commi 3 - 6 dispongono che:

«3. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.

4. L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.

5. La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso.

6. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro».

Le disposizioni illustrate non si applicano al trattamento dei dati personali di cui è consentita la diffusione.

Il comma 5 dell'articolo in esame prevede che *la validità delle richieste di accesso é verificata prima di consentire l'accesso stesso. Il* significato di questa disposizione è che *l'amministratore del sistema* debba verificare che *l'incaricato* sia autorizzato dal *responsabile del trattamento dati* prima di dargli i diritti necessari ad accedere ai dati.

Condizioni per il reimpiego dei supporti di memorizzazione - Nel caso di trattamento dei dati sensibili, se il trattamento è effettuato con elaboratori accessibili in rete (pubblica o privata che sia), l'art. 7 impone che: «i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti».

In relazione alle cautele in merito al reimpiego dei supporti di memorizzazione potremmo schematizzare la casistica come segue:

Tipologia	Dati "Ordinari"		Dati "Sensibili"	
Reimpiego dei supporti di memorizzazione	**Obbligo**	**Norma**	**Obbligo**	**Norma**
Per finalità Esclusivamente Personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*				
- con elaboratori in *rete Pubblica*				
Per finalità NON esclusivamente personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*			si	Art. 7
- con elaboratori in *rete Pubblica*			si	Art. 7

Viceversa al trattamento dei dati sensibili mediante elaboratori connessi tra dì loro, stabilmente o meno ed a qualsiasi scopo, è indiscriminatamente applicabile la disposizione di cui all'art. 7, secondo cui i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti. Per chiarire meglio la disposizione normativa si deve rilevare che:

- i supporti sono quelli dì memorizzazione, dato che si parla di informazioni in essi contenute;
- il riutilizzo significa, al contrario del significato letterale, un utilizzo nuovo e diverso dal precedente trattamento, ed al di fuori delle cautele per esso previste;
- le informazioni precedentemente contenute si riferisce alle informazioni precedentemente contenute, e poi cancellate o corrette.

Accesso ai documenti selezionato e monitorato e conservazione degli stessi - Nel caso di trattamento dei dati personali con strumenti diversi da quelli elettronici o comunque automatizzati per fini diversi da quelli esclusivamente personali, l'art. 9 comma 1 lettera a) dispone che: « nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli artt. 8, comma 5, e 19 della legge, il titolare o, se designato, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati». L'art. 9 comma 1 lettera b) dispone che: «gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso

selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate>>.

Nel caso di trattamento di dati sensibili, oltre a quanto appena previsto, l'art. 9 comma 2 dispone che devono essere osservate le seguenti modalità:

«a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura;

b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi».

L'art. 10 dispone che «I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali sensibili, devono essere conservati e custoditi con le modalità di cui all'art. 9». E' vero che l'art. 10 fa ricadere negli obblighi previsti dall'art. 9 solo i supporti cartacei riportanti dati sensibili ma è pur vero che anche "la conservazione" è definita dall'art. 2 lett. b della Legge 675 una modalità di trattamento facendo ricadere quindi la conservazione dei supporti cartacei (contenente la riproduzione di dati personali trattati con elaboratori) negli obblighi previsti dall'art. 9.

In merito alle cautele per l'accesso ai documenti e la loro conservazione potremmo schematizzare la casistica come segue:

Tipologia	**Dati "Ordinari"**		**Dati "Sensibili"**	
Accesso e conservazione documenti	**Obbligo**	**Norma**	**Obbligo**	**Norma**
Per finalità Esclusivamente Personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*				
- con elaboratori in *rete Pubblica*				
Per finalità NON esclusivamente personali				
- senza strumenti elettronici	si	*Art. 9 c. 1*	si	*Art. 9 cc 1+2*
- con elaboratori *stand alone*	si	*Art. 9 c. 1*	si	*Art. 10 9 cc 1+2*
- con elaboratori in *rete Privata*	si	*Art. 9 c. 1*	si	*Art. 10 9 cc 1+2*
- con elaboratori in *rete Pubblica*	si	*Art. 9 c. 1*	si	*Art. 10 9 cc 1+2*

Salvo i dati trattati a fini esclusivamente personali (ad esempio i propri appunti e rubriche), i quali restano anche in questo caso in ogni modo esenti, viene previsto, sia per dati ordinari che per i dati sensibili, che le istruzioni agli *incaricati* prescrivano che l'accesso ai dati avvenga *on a need-to-know basis.*
Strumentale a questa previsione è l'altra che prescrive che i dati debbano essere conservati in archivio ad accesso selezionato e che l'incaricato del trattamento non possa disporne se non per il tempo necessario all'espletamento dell'incarico, ove gli *siano affidati*, il che implica che gli stessi siano usciti dal diretto controllo del titolare del trattamento ed affidati alla custodia del terzo incaricato.

Per quanto riguarda l'accesso agli archivi fuori orario la disposizione richiede:

- che gli atti ed i documenti siano contenuti in archivi,
- che siano contenuti in un ufficio,

- che tale ufficio abbia orari di apertura quotidiani .

Quindi negli orari di normale attività della gestione d'archivio il controllo deve investire l'intera attività di accesso, mentre al di fuori di tali orari il controllo dovrà concentrarsi sulla identificazione personale delle persone ammesse (che dovranno essere rappresentate da incaricati).

TECNOLOGIE: sono gli strumenti tecnologici che devono essere approntati al fine di prevenire trattamenti illeciti di dati personali

Misure di protezione contro il rischio di intrusione

Trattamento effettuato su supporto informatico

- Elaboratori accessibili in rete

L'art. 4 comma 1 lettera c) dispone che: « gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'articolo 615 *quinquies* del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale».
L'art. 615 quinquies del codice penale si riferisce ai programmi 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

In relazione all'obbligo per le misure di protezione contro il rischio di intrusione potremmo schematizzare la casistica come segue:

Tipologia	**Dati "ordinari"**		**Dati "sensibili"**	
Rischio di intrusione/supp. informatico	**Obbligo**	**Norma**	**Obbligo**	**Norma**
Per finalità Esclusivamente Personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*				
- con elaboratori in *rete Pubblica*				
Per finalità NON esclusivamente personali				
- senza strumenti elettronici				
- con elaboratori *stand alone*				
- con elaboratori in *rete Privata*	si	Art. 4	si	Art. 4
- con elaboratori in *rete Pubblica*	si	Art. 4	si	Art. 4

Non è prevista l'esclusione di questa misura nel caso di trattamenti dei dati personali di cui è consentita la diffusione.

Il legislatore ritiene sufficiente l'installazione e la periodica verifica della funzionalità di un antivirus.

Se gli elaboratori sono in qualche modo in rete, occorre quindi munirli di un antivirus, la cui efficacia ed aggiornamento siano verificati con cadenza almeno semestrale.

Poiché oltre l'aggiornamento periodico delle protezioni viene richiesta la verifica di efficacia dovranno essere approntati dei test di valutazione. Inoltre poiché è interesse del Responsabile dei dati personali dimostrare che verifiche ed aggiornamenti sono stati effettuati regolarmente dovranno essere documentate opportunamente le attività svolte.

Trattamento effettuato su supporto cartaceo

L'art. 9 comma 1 lett. B D.lgs. 318/1999 dispone che "gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazione affidate".
Peraltro si deve evidenziare che la norma in esame deve essere interpretata in base all'art. 15 della L. 675/1996 che dispone che i dati contenenti informazioni personali dell'interessato devono essere custoditi "in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di perdita o di distruzione, anche accidentale, dei dati stessi".

A tal proposito dovranno essere distinti gli Archivi Permanenti, individuabili in archivi in cui i dati personali vengono custoditi in modo stabile e costante, dagli Archivi correnti, individuabili in archivi dove i dati si trovano saltuariamente per esigenze lavorative degli incaricati del trattamento.

Archivi permanenti:
negli archivi permanenti dovranno essere adottate misure di sicurezza idonee a prevenire sia la distruzione anche accidentale dei dati medesimi che si sostanziano nella presenza di impianti antincendio, rilevazione fumi ed estintori, sia la relativa perdita che si sostanzia nella tenuta di un registro di carico e scarico della documentazione contenuta in archivio.

Archivi correnti:
negli archivi correnti dovranno essere adottate misure di sicurezza che potrebbero essere definite di diligenza; cioè gli incaricati al trattamento che prelevano dati personali dovranno custodirli in locali ad accesso selezionato in modo da limitare la possibile visione dei dati stessi al personale autorizzato.

Dati personali sensibili
L'art. 9 comma 2 del D.lgs. 318/1999 dispone che il trattamento deve avvenire secondo le seguenti modalità:
"se affidati agli incaricati del trattamento, gli atti ed i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura. L'accesso agli archivi deve essere controllato e devono essere identificati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi".

Archivi permanenti.
Negli archivi permanenti, oltre alle misure adottate per i dati personali, dovrà quindi essere tenuto un registro di rilevazione dei soggetti che prelevano o consultano i dati sensibili dopo l'orario di chiusura dell'archivio stesso o eventualmente la presenza di un dispositivo di controllo accessi o di rilevazione delle presenze.

Archivi correnti.

Negli archivi correnti, oltre alle misure adottate per i dati personali, i dati dovranno essere custoditi in contenitori muniti di serratura.

Tipologia	Dati "ordinari"		Dati "sensibili"	
Rischio di intrusione/supp. cartaceo	**Obbligo**	**Norma**	**Obbligo**	**Norma**
Archivio permanente				
- dispositivi di sicurezza fisica	SI	Art. 15 L.675		
- registro di carico scarico	SI	Art. 15 L.675		
- controllo accessi			SI	Art. 9 c.2 l.b
- accesso selezionato	SI	Art. 9 c.1 l.b		
- contenitori con serratura			SI	Art. 9 c. 2
Archivio corrente				
- dispositivi di sicurezza fisica				
- registro di carico scarico				
- controllo accessi				
- accesso selezionato	SI	Art. 9 c. 1 l.b		
- contenitori con serratura			Si	Art. 9 c. 2

Le misure di sicurezza previste per i dati personali dovranno essere applicate anche ai dati sensibili.

RISORSE UMANE: sono i soggetti chiamati a trattare i dati personali

I soggetti preposti all'attuazione delle misure di sicurezza sono:

- il titolare del trattamento dei dati personali;
- il responsabile (se nominato) del trattamento dei dati personali;
- gli incaricati del trattamento dei dati personali;
- gli amministratori di sistema;
- i custodi delle parole chiave.

IL TITOLARE ED IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Il titolare è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui *competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi* compreso il profilo della sicurezza *(Art. 1 Legge 675).*

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

L'art 8 della Legge 675 dispone che il responsabile, se designato, deve essere nominato 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.

Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni predette e delle proprie istruzioni. Ove necessario per esigenze

organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. L'art 9, dispone che i dati personali oggetto di trattamento devono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I compiti affidati al responsabile devono essere analiticamente specificati per iscritto.

In merito alla sicurezza dei dati l'art 15 della Legge 675 dispone che il titolare ed il responsabile dovranno curare che i dati personali oggetto di trattamento siano 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.

Quanto alle misure minime di sicurezza dovranno adottare quelle previste dal Regolamento.

Nel caso in cui il trattamento dei dati pur se effettuato per finalità esclusivamente personali venisse fatto su dati sensibili, organizzati in banche dati, con strumenti elettronici o comunque *automatizzati collegati in rete accessibile al pubblico,* in conformità all'art 8 curerà di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave.

Nel caso in cui il trattamento dei dati personali viene effettuato per finalità non esclusivamente personali e con strumenti elettronici o comunque automatizzati, in conformità all'art 2 del Regolamento il titolare ed il responsabile dovranno individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime e dovranno dare disposizione a questi ed agli incaricati affinché, anteriormente all'inizio del trattamento, sia prevista una parola chiave per l'accesso ai dati, che venga fornita agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, ne sia consentita l'autonoma sostituzione, previa comunicazione ai soggetti preposti alla custodia delle parole chiave o che hanno accesso ad informazioni che concernono le medesime.

Nel caso di **trattamenti effettuati con gli elaboratori accessibili in rete,** semprechè non si tratti di dati personali di cui è consentita la diffusione, devono essere adottate le misure previste dall'art 4 del Regolamento in materia di codice identificativo personale e di antivirus. Per gli aspetti operativi si occuperanno gli amministratori di sistema. Se il trattamento si rivolge a dati sensibili, occorre dare disposizione perché sia messa in atto la procedura prevista dall'art 5 del Regolamento. L'accesso, per effettuare le operazioni di trattamento, in questi casi, è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione. Se il trattamento è effettuato *con elaboratori in rete pubblica* devono essere oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico. L'autorizzazione, se riferita

agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento. L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione. La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

La verifica della legittimazione all'accesso (cioè se l'interessato o l'utente sia autorizzato) è effettuata in automatico o dall'amministratore di sistema.

Nel caso di trattamento dei dati sensibili effettuato con elaboratori in rete, l'art 7 del Regolamento dispone anche che i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

Nel caso di **trattamento dei dati sensibili** effettuato **mediante gli elaboratori collegati in rete pubblica,** dev'essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati.

Nel caso di **trattamento di dati personali** per fini diversi da quelli dell'uso esclusivamente personale, effettuato **con strumenti diversi da elaboratori o strumenti automatizzati,** dovranno dare disposizione per l'osservanza del contenuto dell'art. 9 del Regolamento. Devono infatti essere osservate le seguenti modalità:

a) nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli articoli 8, comma 5, e 19 della legge, il titolare o, se designato, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;

b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.

Nel caso di **trattamento di dati sensibili,** oltre a quanto appena detto, dovranno essere date disposizioni al fine di osservare le modalità previste dall'art 9 comma 2 del Regolamento, vale a dire: a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura; b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi. Ricordiamo che detti obblighi trovano applicazione anche ai documenti conservati dal titolare o responsabile anche se i relativi dati siano trattati in archivi informatizzati. In merito alla conservazione della documentazione relativa al trattamento daranno disposizione a che venga osservato il contenuto dell'art. 10 del Regolamento che dispone che i supporti non informatici (es: cartacei) contenenti la riproduzione di informazioni relative al trattamento di dati personali *sensibili:* a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura; b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi

vengono ammessi dopo l'orario di chiusura degli archivi stessi.

GLI INCARICATI DEL TRATTAMENTO

Incaricati del trattamento sono le persone incaricate per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta autorità (art. 19 *Legge* 675) . L'art. 8 della Legge 675 dispone che gli incaricati dei trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del titolare o del responsabile.

GLI AMMINISTRATORI DI SISTEMA

Gli amministratori di sistema sono i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione *(Art. 1 DPR 318).* Nel caso di **trattamenti effettuati con gli elaboratori accessibili in rete,** semprechè non si tratti di dati personali di cui è consentita la diffusione, devono essere rispettate le seguenti misure previste dall'art 4 del Regolamento in materia di codice identificativo personale e di antivirus:

a) ciascun utente o incaricato del trattamento deve avere un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice (fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione), non può, neppure in tempi diversi, essere assegnato a persone diverse;
b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'articolo 615 *quinquies* del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale. Per il trattamento dei dati sensibili con elaboratori in rete, l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.

L'amministratore di sistema dovrà verificare se l'utente o l'incaricato sia stato autorizzato all'accesso. Se il trattamento è effettuato con elaboratori in rete pubblica, sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico. Se riferita agli strumenti, l'autorizzazione deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.

La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

1 CUSTODI DELLE PAROLE CHIAVE 0 I PREPOSTI AD ESSE

Sono i soggetti preposti alla custodia delle parole chiave o che hanno accesso ad informazioni che concernono le medesime. Devono essere nominati (ed individuati per iscritto) nel caso di trattamento dei dati personali effettuato con strumenti elettronici o comunque automatizzati quando vi è più di un incaricato del trattamento e sono in uso più parole chiave.

Devono prevedere quindi una parola chiave per l'accesso ai dati, fornirla agli incaricati, ove tecnicamente possibile consentirne l'autonoma sostituzione in relazione alle caratteristiche dell'elaboratore, ricevendo dagli incaricati stessi la previa comunicazione della nuova parola chiave.

Dette operazioni devono essere adottate, anteriormente all'inizio del trattamento da parte degli incaricati. *(art 2 Regolamento DPR 318)*

Nel caso in cui sono nominati gli amministratori di sistema queste funzioni potranno essere assunte dagli stessi.

Limiti alle deleghe del Titolare del trattamento

Considerando, inoltre, le condizioni alle quali la delega può considerarsi efficace, possiamo elencare i seguenti principi generali:

1) la delega deve essere esplicita ed inequivocabile e la persona delegata (nel caso appartenga all'organico aziendale) deve ricoprire una carica superiore rispetto ai dipendenti incaricati dei trattamenti;

2) la persona delegata deve accettare la delega volontariamente ed esplicitamente;

3) il delegato deve essere persona professionalmente qualificata, in possesso delle facoltà necessarie (di natura organizzativa e tecnica);

4) il delegato deve avere a disposizione strumenti idonei per l'organizzazione delle attività relative alla funzione delegata, soprattutto di spesa. In caso contrario la responsabilità rimane in capo al vertice; infatti il delegato deve disporre di poteri e di autonomia necessari per lo svolgimento della funzione delegata: deve essere in grado di decidere autonomamente ed imporre le decisioni; deve poter decidere liberamente per quanto concerne l'impiego delle risorse finanziarie assegnategli. Per tutte le limitazioni imposte dal vertice, sarà quest'ultimo a rispondere delle conseguenze, sopportando l'applicazione delle sanzioni penali ed amministrative previste dalla Legge n. 675/96;

5) il delegato deve poter intervenire in tutte le questioni che gli competono in base all'elenco stilato nella delega. Non deve essere chiamato ad adempiere a compiti estranei o non compatibili con la delega;

6) qualora il vertice venisse a conoscenza di infrazioni alle norme, resta fermo in capo

ad esso l'obbligo di intervenire, non potendo disattendere le proprie responsabilità di carattere generale;

7) il vertice deve comunque svolgere un controllo sull'operatività del delegato.

LA FORMAZIONE DEGLI INCARICATI

L'art. 6, comma 1, lettera d) del regolamento obbliga l'operatore alla predisposizione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni» al sistema di elaborazione e gestione logica dei dati.

Il programma di formazione verterà sui temi della sicurezza in generale e sulle misure di sicurezza, adottate dall'operatore, ed alle quali l'incaricato deve conformarsi nello svolgimento delle sue attività.

I programmi sulla formazione in tema di sicurezza nel trattamento dei dati personali saranno predisposti, in accordo con gli esperti, che già svolgono attività di consulenza per l'operatore.
E' importante sottolineare come la terzietà dell'apparato formativo, nell'espletare attività didattica teorico-pratica anche *on demand,* oltre che a certificare l'evento formativo, garantirà e promuoverà sicuramente maggiori e più complete conoscenze non solo in merito alla sicurezza, ma servirà anche a comunicare eventi e situazioni che diano ai discenti-utenti una visione d'insieme delle problematiche ed in specie delle filosofie, a cui le procedure di sicurezza normalmente si ispirano, pur nella loro evoluzione.

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE
Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE **Provincia:** PA **Cap:** 90040
PartitaIva : 00801000829

Sede: BIBLIOTECA COMUNALE
Indirizzo: VIA PALERMO
Località : ISOLA DELLE FEMMINE **Provincia** PA **Cap:** 90040

Locale : BIBLIOTECA COMUNALE

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE
Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE **Provincia:** PA **Cap:** 90040
PartitaIva : 00801000829

Sede: POLIZIA MUNICIPALE
Indirizzo: VIA DEI VILLINI
Località : ISOLA DELLE FEMMINE **Provincia** PA **Cap:** 90040

Locale : **POLIZIA MUNICIPALE**

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE
Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE **Provincia:** PA **Cap:** 90040
PartitaIva : 00801000829

Sede: PUBBLICA ISTRUZIONE
Indirizzo: VIA FALCONE, 80
Località : ISOLA DELLE FEMMINE **Provincia** PA **Cap:** 90040

Locale : PUBBLICA ISTRUZIONE - TURISMO - SPORT - SPETTACOLO

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
DOCUMENTI P.I.-SPORT-TURISMO-SPETT.	Ordinari	Informatico	No	No
DOCUM.P.I.-SPORT-TURISMO-SPETT.2	Ordinari	Informatico	No	No

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE
Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE **Provincia:** PA **Cap:** 90040
PartitaIva : 00801000829

Sede: SERVIZI SOCIALI
Indirizzo: VIA FALCONE, 80
Località : ISOLA DELLE FEMMINE **Provincia** PA **Cap:** 90040

Locale : SERVIZI SOCIALI

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
DOCUMENTI SERVIZI SOCIALI	Sensibili	Informatico	No	No
DOCUMENTI SERVIZI SOCIALI 2	Sensibili	Informatico	No	No
DOCUMENTI SERVIZI SOCIALI 3	Sensibili	Informatico	No	No

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE
Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE **Provincia:** PA **Cap:** 90040
PartitaIva : 00801000829

Sede: UFFICIO TRIBUTI
Indirizzo: VIA FALCONE, 80
Località : ISOLA DELLE FEMMINE **Provincia** PA **Cap:** 90040

Locale : ICI - TARSU - ACQUEDOTTO - COMMERCIO

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
SERVIZIO ACQUEDOTTO INF.	Ordinari	Informatico	No	No
ARCHIVIO TARSU INFORMATICO	Ordinari	Informatico	No	No
ARCHIVIO ICI INFORMATICO	Ordinari	Informatico	No	No
ARCHIVIO TARSU	Ordinari	Cartaceo	Si	No
SERVIZIO ACQUEDOTTO	Ordinari	Cartaceo	No	Si
ARCHIVIO COMMERCIO	Sensibili	Cartaceo	No	Si
ARCHIVIO ICI CARTACEO	Ordinari	Cartaceo	Si	No
VARIE UFF.TRIBUTI 2	Ordinari	Informatico	No	No
VARIE UFF. TRIBUTI 3	Ordinari	Informatico	No	No
VARIE UFF.TRIBUTI 4	Ordinari	Informatico	No	No
VARIE UFF. TRIBUTI	Ordinari	Informatico	No	No

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE
Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE **Provincia:** PA **Cap:** 90040
PartitaIva : 00801000829

Sede: SERVIZI DEMOGRAFICI
Indirizzo: VIA G.FALCONE, 80
Località : ISOLA DELLE FEMMINE **Provincia** PA **Cap:** 90040

Locale : UFFICIO ANAGRAFE

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
BACKUP PROGR.ANDROMEDA	Ordinari	Informatico	No	No
DATI SIATEL	Ordinari	Informatico	No	No
GESTIONE SERVIZIO ELETTORALE	Ordinari	Informatico	No	No
Documenti vari ufficio anagrafe	Ordinari	Informatico	No	No
PROGRAMMA GESTIONE UFFICIO ANAGRAFE	Ordinari	Informatico	No	No

Locale : UFFICIO STATO CIVILE E LEVA

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
STATO CIVILE	Ordinari	Informatico	No	No
C:\ISI-ISTATEL\DATABASE	Ordinari	Informatico	No	No
GESTIONE AIRE	Ordinari	Informatico	No	No

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE
Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE **Provincia:** PA **Cap:** 90040
PartitaIva : 00801000829

Sede: PALAZZO COMUNALE
Indirizzo: LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE **Provincia** PA **Cap:** 90040

Locale : UFFICIO PROTOCOLLO

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
ARCHIVIO PROTOCOLLO	Ordinari	Informatico	No	No
ARCHIVIO PROTOCOLLO 2	Ordinari	Informatico	No	No

Locale : UFFICIO SEGRETERIA

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
ARCHIVIO DEL SEGRETARIO	Ordinari	Informatico	No	No
ARCHIVIO UFF.SEGRETERIA	Ordinari	Informatico	No	No
ARCHIVIO DELIBERAZIONI/DETERMINAZ.	Ordinari	Informatico	No	No
ARCHIVIO PROTESTI	Processuali	Informatico	No	No
ARCHIVIO UFFICIO SEGRETERIA	Ordinari	Informatico	No	No

Locale : UFFICIO ECONOMATO

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente

Locale : UFF.TECNICO - SANATORIE - URBANISTICA

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
UFFICIO TECNICO - SANATORIE	Ordinari	Informatico	No	No
UFFICIO TECNICO SANATORIE	Ordinari	Informatico	No	No
UFFICIO TECNICO URBANISTICA	Ordinari	Informatico	No	No
UFFICIO TECNICO URBANISTIC	Ordinari	Informatico	No	No

Locale : UFF. TECNICO - LL.PP.

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente

Locale : UFFICIO PERSONALE

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
ARCHIVIO UFFICIO PERSONALE	Sensibili	Informatico	No	No
ARCHIVIO UFFICIO PERSONALE 2	Sensibili	Informatico	No	No
UFFICIO PERSONALE 3	Ordinari	Informatico	No	No

Locale : UFFICIO RAGIONERIA

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
RAGIONERIA E CONTABILITA'	Ordinari	Informatico	No	No

Locale : UFF. TECNICO - CAPOSETTORE

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente

Locale : IGIENE AMBIENTALE

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
ARCHIVIO IGIENE AMBIENTALE	Ordinari	Informatico	No	No

Locale : UFFICIO RAGIONERIA CAPOSETTORE

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
PROGRAMMA CONTABILITA'	Ordinari	Informatico	No	No

Locale : UFFICIO RAGIONERIA ECONOMATO

Nome Archivio	Tipo Dati Archivio	Tipo Archivio	Archivio Corrente	Archivio Permanente
SERVIZIO ECONOMATO	Ordinari	Informatico	No	No

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE 30/06/2005

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE
Provincia : PA **Cap:** 90040
PartitaIva : 00801000829

Archivio : C:\ISI-ISTATEL\DATABASE
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Amministrazione della popolazione (gestione delle anagrafi e dei registri dello stato civile; rilascio di certificati ed estratti)

Archivio : ARCHIVIO PROTOCOLLO 2
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Altro

Archivio : VARIE UFF. TRIBUTI
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Adempimento di obblighi contabili o fiscali
di altro genere	Autorizzazioni, concessioni, permessi e licenze (rilascio e attività connesse; individuazione degli aventi diritto, controllo delle condizioni)

Archivio : DOCUM.P.I.-SPORT-TURISMO-SPETT.2
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di istruzione, cultura e tempo libero	Istruzione ed assistenza scolastica (amministrazione degli alunni, organizzazione delle attività di insegnamento e valutazione; assistenza agli alunni, anche a fini di orientamento professionale, sussidi allo studio)

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

di istruzione, cultura e tempo libero	Attività artistiche e culturali
di istruzione, cultura e tempo libero	Attività turistiche e ricreative
di istruzione, cultura e tempo libero	Attività sportive

Archivio : DOCUMENTI P.I.-SPORT-TURISMO-SPETT.
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di istruzione, cultura e tempo libero	Istruzione ed assistenza scolastica (amministrazione degli alunni, organizzazione delle attività di insegnamento e valutazione; assistenza agli alunni, anche a fini di orientamento professionale, sussidi allo studio)
di istruzione, cultura e tempo libero	Attività artistiche e culturali
di istruzione, cultura e tempo libero	Attività turistiche e ricreative
di istruzione, cultura e tempo libero	Attività sportive

Archivio : DOCUMENTI SERVIZI SOCIALI 3
Tipo di dati : Sensibili
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Finanziamenti, sussidi e sovvenzioni (concessione di finanziamenti, sussidi e sovvenzioni: individuazione degli aventi diritto, calcolo, monitoraggio)

Archivio : DOCUMENTI SERVIZI SOCIALI 2
Tipo di dati : Sensibili
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Finanziamenti, sussidi e sovvenzioni (concessione di finanziamenti, sussidi e sovvenzioni: individuazione degli aventi diritto, calcolo, monitoraggio)

Archivio : DOCUMENTI SERVIZI SOCIALI
Tipo di dati : Sensibili
Tipo di Archivio : Informatico

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Finanziamenti, sussidi e sovvenzioni (concessione di finanziamenti, sussidi e sovvenzioni: individuazione degli aventi diritto, calcolo, monitoraggio)
di altro genere	Gestione elenchi soci ed associati (persone fisiche, giuridiche, associazioni ecc.)

Archivio : VARIE UFF. TRIBUTI 3

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Riscossione tasse e imposte

Archivio : DATI SIATEL

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Gestione elenchi soci ed associati (persone fisiche, giuridiche, associazioni ecc.)

Archivio : VARIE UFF.TRIBUTI 2

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Riscossione tasse e imposte

Archivio : GESTIONE AIRE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Attività di carattere elettorale (tenuta liste elettorali; organizzazione consultazioni elettorali e referendarie)

Archivio : GESTIONE SERVIZIO ELETTORALE

Tipo di dati : Ordinari

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Attività di carattere elettorale (tenuta liste elettorali; organizzazione consultazioni elettorali e referendarie)

Archivio : PROGRAMMA GESTIONE UFFICIO ANAGRAFE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Amministrazione della popolazione (gestione delle anagrafi e dei registri dello stato civile; rilascio di certificati ed estratti)

Archivio : Documenti vari ufficio anagrafe

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Amministrazione della popolazione (gestione delle anagrafi e dei registri dello stato civile; rilascio di certificati ed estratti)

Archivio : SERVIZIO ACQUEDOTTO INF.

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Adempimento di obblighi contabili o fiscali
di altro genere	Riscossione tasse e imposte

Archivio : ARCHIVIO TARSU INFORMATICO

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Riscossione tasse e imposte

Archivio : ARCHIVIO ICI INFORMATICO

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Adempimento di obblighi contabili o fiscali
di altro genere	Riscossione tasse e imposte

Archivio : BACKUP PROGR.ANDROMEDA

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Amministrazione della popolazione (gestione delle anagrafi e dei registri dello stato civile; rilascio di certificati ed estratti)

Archivio : ARCHIVIO PROTESTI

Tipo di dati : Processuali

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
connesse al settore bancario, creditizio; assicurativo, di intermediazione e di consulenza	Altro

Archivio : ARCHIVIO PROTOCOLLO

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Altro

Archivio : ARCHIVIO IGIENE AMBIENTALE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : UFFICIO PERSONALE 3

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Altro

Archivio : ARCHIVIO UFFICIO PERSONALE 2

Tipo di dati : Sensibili

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Trattamento economico giuridico del personale (calcolo e pagamento di retribuzioni ed emolumenti vari; applicazione della legislazione sociale)
amministrativo-contabili	Gestione del personale

Archivio : ARCHIVIO UFFICIO PERSONALE

Tipo di dati : Sensibili

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Trattamento economico giuridico del personale (calcolo e pagamento di retribuzioni ed emolumenti vari; applicazione della legislazione sociale)
amministrativo-contabili	Gestione del personale
amministrativo-contabili	Reclutamento, selezione e valutazione e monitoraggio del personale
amministrativo-contabili	Reclutamento, selezione e valutazione e monitoraggio del personale
amministrativo-contabili	Adempimento di obblighi contabili o fiscali

Archivio : ARCHIVIO DEL SEGRETARIO

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

di altro genere	Altro

Archivio : STATO CIVILE
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA

Archivio : ARCHIVIO DELIBERAZIONI/DETERMINAZ.
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Altro

Archivio : VARIE UFF.TRIBUTI 4
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Riscossione tasse e imposte
di altro genere	Relazioni con il pubblico

Archivio : ARCHIVIO UFFICIO SEGRETERIA
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Altro

Archivio : SERVIZIO ECONOMATO
Tipo di dati : Ordinari
Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Gestione clientela (amministrazione della clientela; gestione contratti, ordini,

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

	spedizioni, fatture; controllo della solvibilità)
amministrativo-contabili	Gestione fornitori (amministrazione dei fornitori; gestione contratti, ordini, arrivi, fatture; selezione fornitori in rapporto alle necessità dell'impresa)

Archivio : RAGIONERIA E CONTABILITA'

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Trattamento economico giuridico del personale (calcolo e pagamento di retribuzioni ed emolumenti vari; applicazione della legislazione sociale)
di altro genere	Finanziamenti, sussidi e sovvenzioni (concessione di finanziamenti, sussidi e sovvenzioni: individuazione degli aventi diritto, calcolo, monitoraggio)
di istruzione, cultura e tempo libero	Altro

Archivio : PROGRAMMA CONTABILITA'

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Trattamento economico giuridico del personale (calcolo e pagamento di retribuzioni ed emolumenti vari; applicazione della legislazione sociale)
amministrativo-contabili	Adempimento di obblighi contabili o fiscali
di altro genere	Altro

Archivio : UFFICIO TECNICO - SANATORIE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Autorizzazioni, concessioni, permessi e licenze (rilascio e attività connesse; individuazione degli aventi diritto, controllo delle condizioni)
di altro genere	Gestione patrimoni (creazione e aggiornamento di un registro delle proprietà, mobiliari e immobiliari; rilascio di attestati)

Archivio : UFFICIO TECNICO URBANISTIC

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Autorizzazioni, concessioni, permessi e licenze (rilascio e attività connesse; individuazione degli aventi diritto, controllo delle condizioni)
di altro genere	Pianificazione urbanistica
di altro genere	Gestione elenchi soci ed associati (persone fisiche, giuridiche, associazioni ecc.)

Archivio : UFFICIO TECNICO URBANISTICA

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Autorizzazioni, concessioni, permessi e licenze (rilascio e attività connesse; individuazione degli aventi diritto, controllo delle condizioni)

Archivio : UFFICIO TECNICO SANATORIE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Gestione patrimoni (creazione e aggiornamento di un registro delle proprietà, mobiliari e immobiliari; rilascio di attestati)

Archivio : ARCHIVIO UFF.SEGRETERIA

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

FINALITA' PRIMARIA	FINALITA' SECONDARIA
di altro genere	Altro

Archivio : ARCHIVIO COMMERCIO

Tipo di dati : Sensibili

Tipo di Archivio : Cartaceo

FINALITA' PRIMARIA	FINALITA' SECONDARIA

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Finalità del trattamento

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

di altro genere	Autorizzazioni, concessioni, permessi e licenze (rilascio e attività connesse; individuazione degli aventi diritto, controllo delle condizioni)

Archivio : ARCHIVIO ICI CARTACEO

Tipo di dati : Ordinari

Tipo di Archivio : Cartaceo

FINALITA' PRIMARIA	FINALITA' SECONDARIA
amministrativo-contabili	Adempimento di obblighi contabili o fiscali

Archivio : SERVIZIO ACQUEDOTTO

Tipo di dati : Ordinari

Tipo di Archivio : Cartaceo

FINALITA' PRIMARIA	FINALITA' SECONDARIA

Archivio : ARCHIVIO TARSU

Tipo di dati : Ordinari

Tipo di Archivio : Cartaceo

FINALITA' PRIMARIA	FINALITA' SECONDARIA

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

30/06/2005

COMUNE DI ISOLA DELLE FEMMINE

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Localita : ISOLA DELLE FEMMINE
Provincia : PA **Cap:** 90040
Partita Iva: 00801000829

Archivio : GESTIONE SERVIZIO ELETTORALE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : RAGIONERIA E CONTABILITA'

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

fornitori

personale dipendente

consulenti e liberi professionisti

studi professionali e di consulenza

persone giuridiche, enti, associazioni od organismi

soggetti od organismi pubblici

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : DATI SIATEL

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : VARIE UFF. TRIBUTI

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

commercianti

artigiani

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : DOCUM.P.I.-SPORT-TURISMO-SPETT.2

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : DOCUMENTI P.I.-SPORT-TURISMO-SPETT.

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO PROTOCOLLO 2

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : UFFICIO PERSONALE 3

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : UFFICIO TECNICO - SANATORIE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

imprenditori e piccoli imprenditori

consulenti e liberi professionisti

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : C:\ISI-ISTATEL\DATABASE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO TARSU

Tipo di dati : Ordinari

Tipo di Archivio : Cartaceo

CATEGORIE SOGGETTI

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : PROGRAMMA GESTIONE UFFICIO ANAGRAFE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : Documenti vari ufficio anagrafe

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : SERVIZIO ACQUEDOTTO INF.

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO TARSU INFORMATICO

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO ICI INFORMATICO

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : BACKUP PROGR.ANDROMEDA

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO DELIBERAZIONI/DETERMINAZ.

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

personale dipendente

consulenti e liberi professionisti

studi professionali e di consulenza

persone giuridiche, enti, associazioni od organismi

soggetti od organismi pubblici

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : VARIE UFF.TRIBUTI 2

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO PROTOCOLLO

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO ICI CARTACEO

Tipo di dati : Ordinari

Tipo di Archivio : Cartaceo

CATEGORIE SOGGETTI

clienti e utenti

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : STATO CIVILE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO UFF.SEGRETERIA

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : VARIE UFF. TRIBUTI 3

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO UFFICIO SEGRETERIA

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

consulenti e liberi professionisti

studi professionali e di consulenza

persone giuridiche, enti, associazioni od organismi

soggetti od organismi pubblici

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : SERVIZIO ECONOMATO

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

fornitori

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : GESTIONE AIRE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

soci, associati ed iscritti

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : PROGRAMMA CONTABILITA'

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

fornitori

personale dipendente

consulenti e liberi professionisti

studi professionali e di consulenza

agenti e rappresentanti

soci, associati ed iscritti

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : SERVIZIO ACQUEDOTTO

Tipo di dati : Ordinari

Tipo di Archivio : Cartaceo

CATEGORIE SOGGETTI

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : UFFICIO TECNICO URBANISTIC

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

consulenti e liberi professionisti

soggetti od organismi pubblici

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : UFFICIO TECNICO URBANISTICA

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : UFFICIO TECNICO SANATORIE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : VARIE UFF.TRIBUTI 4

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO DEL SEGRETARIO

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO IGIENE AMBIENTALE

Tipo di dati : Ordinari

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : DOCUMENTI SERVIZI SOCIALI

Tipo di dati : Sensibili

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : DOCUMENTI SERVIZI SOCIALI 2

Tipo di dati : Sensibili

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : DOCUMENTI SERVIZI SOCIALI 3

Tipo di dati : Sensibili

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO UFFICIO PERSONALE

Tipo di dati : Sensibili

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

personale dipendente

altro

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO UFFICIO PERSONALE 2

Tipo di dati : Sensibili

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

personale dipendente

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO COMMERCIO

Tipo di dati : Sensibili

Tipo di Archivio : Cartaceo

CATEGORIE SOGGETTI

clienti e utenti

commercianti

artigiani

imprenditori e piccoli imprenditori

ELENCO DEGLI ARCHIVI DEI DATI OGGETTO DEL TRATTAMENTO
Categorie di soggetti interessati

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Archivio : ARCHIVIO PROTESTI

Tipo di dati : Processuali

Tipo di Archivio : Informatico

CATEGORIE SOGGETTI

clienti e utenti

ELENCO DELLE SEDI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

COMUNE DI ISOLA DELLE FEMMINE

28/06/2005

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA **Cap:** 90040
Partita Iva: 00801000829

Sede : PALAZZO COMUNALE
Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA

Sede : SERVIZI DEMOGRAFICI
Indirizzo : VIA G.FALCONE, 80
Località : ISOLA DELLE FEMMINE
Provincia : PA

Sede : UFFICIO TRIBUTI
Indirizzo : VIA FALCONE, 80
Località : ISOLA DELLE FEMMINE
Provincia : PA

Sede : SERVIZI SOCIALI
Indirizzo : VIA FALCONE, 80
Località : ISOLA DELLE FEMMINE
Provincia : PA

Sede : PUBBLICA ISTRUZIONE
Indirizzo : VIA FALCONE, 80
Località : ISOLA DELLE FEMMINE
Provincia : PA

Sede : POLIZIA MUNICIPALE
Indirizzo : VIA DEI VILLINI
Località : ISOLA DELLE FEMMINE
Provincia : PA

ELENCO DELLE SEDI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Sede : BIBLIOTECA COMUNALE

Indirizzo : VIA PALERMO

Località : ISOLA DELLE FEMMINE

Provincia : PA

COMUNE DI ISOLA DELLE FEMMINE

28/06/2005

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA Cap: 90040
Partita Iva: 00801000829

ELENCO DEI LOCALI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Sede : PALAZZO COMUNALE

Indirizzo : LARGO CRISTOFORO COLOMBO, 3

Località : ISOLA DELLE FEMMINE **Provincia**: PA

Locale : UFFICIO RAGIONERIA ECONOMATO
Tipo di accesso : Libero
Chiusura con serratura: Si

Locale : UFFICIO PROTOCOLLO
Tipo di accesso : Libero
Chiusura con serratura: Si

Locale : UFFICIO SEGRETERIA
Tipo di accesso : Libero
Chiusura con serratura: Si

Locale : UFFICIO ECONOMATO
Tipo di accesso : Libero
Chiusura con serratura: Si

Locale : UFF.TECNICO - SANATORIE - URBANISTICA
Tipo di accesso : Libero
Chiusura con serratura: Si

Locale : UFF. TECNICO - LL.PP.
Tipo di accesso : Libero
Chiusura con serratura: Si

Locale : UFFICIO PERSONALE
Tipo di accesso : Libero
Chiusura con serratura: Si

Locale : UFFICIO RAGIONERIA
Tipo di accesso : Libero
Chiusura con serratura: Si

Locale : UFF. TECNICO - CAPOSETTORE

Tipo di accesso : Libero

Chiusura con serratura: Si

Locale : IGIENE AMBIENTALE

Tipo di accesso : Libero

Chiusura con serratura: Si

Locale : UFFICIO RAGIONERIA CAPOSETTORE

Tipo di accesso : Libero

Chiusura con serratura: Si

28/06/2005

COMUNE DI ISOLA DELLE FEMMINE

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA **Cap:** 90040
Partita Iva: 00801000829

ELENCO DEI LOCALI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Sede : SERVIZI DEMOGRAFICI

Indirizzo : VIA G.FALCONE, 80

Località : ISOLA DELLE FEMMINE **Provincia:** PA

Locale : UFFICIO STATO CIVILE E LEVA

Tipo di accesso : Libero

Chiusura con serratura: Si

Locale : UFFICIO ANAGRAFE

Tipo di accesso : Libero

Chiusura con serratura: Si

COMUNE DI ISOLA DELLE FEMMINE

28/06/2005

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA Cap: 90040
Partita Iva: 00801000829

ELENCO DEI LOCALI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Sede : UFFICIO TRIBUTI

Indirizzo : VIA FALCONE, 80

Località : ISOLA DELLE FEMMINE **Provincia:** PA

Locale : ICI - TARSU - ACQUEDOTTO - COMMERCIO

Tipo di accesso : Libero

Chiusura con serratura: Si

COMUNE DI ISOLA DELLE FEMMINE

28/06/2005

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA **Cap:** 90040
Partita Iva: 00801000829

ELENCO DEI LOCALI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Sede : SERVIZI SOCIALI

Indirizzo : VIA FALCONE, 80

Località : ISOLA DELLE FEMMINE **Provincia:** PA

Locale : SERVIZI SOCIALI

Tipo di accesso : Libero

Chiusura con serratura: Si

COMUNE DI ISOLA DELLE FEMMINE

28/06/2005

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA Cap: 90040
Partita Iva: 00801000829

ELENCO DEI LOCALI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Sede : PUBBLICA ISTRUZIONE

Indirizzo : VIA FALCONE, 80

Località : ISOLA DELLE FEMMINE **Provincia:** PA

Locale : PUBBLICA ISTRUZIONE - TURISMO - SPORT - SPETTACOLO

Tipo di accesso : Libero

Chiusura con serratura: Si

COMUNE DI ISOLA DELLE FEMMINE

28/06/2005

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA Cap: 90040
Partita Iva: 00801000829

ELENCO DEI LOCALI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Sede : POLIZIA MUNICIPALE

Indirizzo : VIA DEI VILLINI

Località : ISOLA DELLE FEMMINE Provincia: PA

Locale : POLIZIA MUNICIPALE

Tipo di accesso : Libero

Chiusura con serratura: Si

COMUNE DI ISOLA DELLE FEMMINE

28/06/2005

Indirizzo : LARGO CRISTOFORO COLOMBO, 3
Località : ISOLA DELLE FEMMINE
Provincia : PA Cap: 90040
Partita Iva: 00801000829

ELENCO DEI LOCALI DOVE VENGONO TRATTATI I DATI

D.l. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";"Allegato B": "Disciplinare tecnico in materia di misure minime di sicurezza"

Sede : BIBLIOTECA COMUNALE

Indirizzo : VIA PALERMO

Località : ISOLA DELLE FEMMINE Provincia: PA

Locale : BIBLIOTECA COMUNALE

Tipo di accesso : Libero

Chiusura con serratura: Si