COMUNE DI NUVOLERA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ADEGUAMENTO DELLE MISURE MINIME DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI PREVISTE DAGLI ARTT. 33-34-35 ED ALLEGATO B DEL D.LGS. 30 GIUGNO 2003, N. 196

(ANNO 2005)

Il presente documento è redatto sulla base delle "Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dagli articoli 34-35 e allegato B del D.Lgs. 196/03".

Gli obiettivi specifici possono essere così articolati e definiti:

PIANO DI REALIZZAZIONE DELLE MISURE DI SICUREZZA

pag.

Premessa

IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

PIANO DI REALIZZAZIONE DELLE MISURE DI SICUREZZA

PREMESSA

INDIVIDUAZIONE DELLE FIGURE PREVISTE DAL D.LGS. 196/03

TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Comune di Nuvolera (BS)
Piazza Gen. L. Soldo n°1
25080 Nuvolera
Partita IVA 00687810176 – Codice Fiscale 80019350177
Telefono 030- 6916771; fax 030-6897563
e-mail: nuvolera.protocollo@legalmailpa.it

AMMINISTRATORE DEL SISTEMA
Mazzone Fortunato

RESPONSABILE PER IL TRATTAMENTO DEI DATI PERSONALI

Incaricato Responsabile Area Economico Finanziaria
Dr. Gallone Giuseppe

Responsabile Area Assetto del Territorio
Mazzone Fortunato

Responsabile Polizia Locale – Commercio
Bazzoli Marco

Responsabile Area Amministrativa e Servizi alla persona
Dr. Carapezza Paolo

BANCHE DATI INFORMATIZZATE

Banca dati della popolazione residente.
Banca dati degli elettori.
Banca dati degli incarichi elettorali (presidenti - segretari - scrutatori di seggio).
Banca dati italiani residenti all'estero.
Banca dati cittadini stranieri (appartenenti alla Comunità Europea ed Extracomunitari).
Banca dati leva militare.

Protocollo del Comune e archivio generale.
Banca dati dichiarazioni ICI.
Banca dati TIA.
Banca dati debitori.
Banca dati creditori.
Banca dati dei dipendenti del Comune.
Banca dati rilevazione presenze del personale del Comune.
Banca dati inquadramento contrattuale.
Banca dati degli incarichi professionali o stagionali del Comune.
Banca dati degli amministratori del Comune
Banca dati concessioni edilizie.
Banca dati condono edilizio.

Banca dati ditte per gare d'appalto.

Banca dati utenti servizi scolastici.
Banca dati associazioni culturali-ricreative-sportive.
Banca dati servizio pasti.

Banca dati dei verbali di contestazione alle violazioni del Codice stradale.
Banca dati infrazioni al codice della strada.
Banca dati titolari di autorizzazione al commercio fisso.
Banca dati titolari pubblici esercizi.
Banca dati commercio aree pubbliche.
Banca dati cimitero.
Banca dati servizi sociali.
Banca dati servizio mensa.

BANCHE DATI CARTACEE

Banca dati della popolazione residente / pratiche immigrazione - emigrazione.
Cartellini carte d'identità.
Banca dati degli elettori.
Albi sezionali e generali degli elettori.
Banca dati degli incarichi elettorali (presidenti - segretari - scrutatori di seggio).
Registri degli atti di nascita - matrimonio - morte.
Liste di leva.
Registri dei defunti.
Contratti cimiteriali.
Banca dati italiani residenti all'estero.
Banca dati cittadini stranieri (appartenenti alla Comunità Europea ed Extracomunitari).
Banca dati dichiarazioni ICI.
Banca dati TIA.
Banca dati TOSAP.
Banca dati debitori.
Banca dati creditori.
Banca dati albo dei fornitori.
Banca dati dei dipendenti.
Banca dati rilevazione presenze del personale del Comune.
Banca dati modello 730.
Banca dati INPDAP.
Banca dati modello 770.
Banca dati modello 01/M.
Banca dati inquadramento contrattuale.
Banca dati degli incarichi professionali o stagionali del Comune.
Banca dati degli amministratori del Comune.
Banca dati servizio mensa.
Banca dati concessioni edilizie.
Banca dati iscritti alla biblioteca comunale.
Banca dati utenti servizi scolastici.
Banca dati associazioni culturali-ricreative.
Banca dati associazioni sportive.
Banca dati ditte per gare d'appalto del Comune.
Banca dati condono edilizio.
Concessioni edilizie.
Banca dati stato avanzamento lavori.
Banca dati degli insediamenti produttivi.
Banca dati dei verbali di contestazione alle violazioni del Codice stradale.
Banca dati cessioni di fabbricato legge n.191/78
Banca dati relativi agli incidenti stradali.
Banca dati titolari di autorizzazione al commercio fisso.
Banca dati titolari pubblici esercizi.
Banca dati commercio su aree pubbliche.
Banca dati infrazioni al codice della strada.
Banca dati notificazioni messi comunali.
Banca dati servizio pasti

INDIVIDUAZIONE DEGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

N° scheda	**Denominazione del trattamento**	**Incaricato del trattamento**
1	Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	Benuzzi Beatrice
2	Personale / Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attività relativa al riconoscimento di benefici connessi all'invalidità civile per il personale e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa	Benuzzi Beatrice
3	Servizi demografici / Anagrafe - gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)	Mancini Ennia Patrizia
4	Servizi demografici / Stato civile - Attività di gestione dei registri di stato civile	Mancini Ennia Patrizia
5	Servizi demografici / Elettorale - attività relativa all'elettorato attivo e passivo	Mancini Ennia Patrizia
6	Servizi demografici / Elettorale - attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio	Mancini Ennia Patrizia
7	Servizi demografici / Elettorale - attività relativa alla tenuta dell'elenco dei giudici popolari	Mancini Ennia Patrizia
8	Servizi demografici / Leva - attività relativa alla tenuta del registro degli obiettori di coscienza	Mezzana Fausta
9	Servizi demografici / Leva - attività relativa alla tenuta delle liste di leva e dei registri matricolari	Mezzana Fausta
10	Servizi sociali - Attività relativa all'assistenza domiciliare	Lombardi Annamaria
11	Servizi sociali - Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale	Lombardi Annamaria
12	Servizi sociali - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc	Lombardi Annamaria
13	Servizi sociali - Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale	Lombardi Annamaria
14	Servizi sociali - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali)	Lombardi Annamaria
15	Servizi sociali - Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	Lombardi Annamaria
16	Servizi sociali - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto	Lombardi Annamaria

17	Servizi sociali - Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione)	Lombardi Annamaria
18	Servizi sociali - Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	Lombardi Annamaria
19	Servizi sociali - Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)	Lombardi Annamaria
20	Servizi sociali - Attività relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti ed abilitazioni ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e i finanziamenti in favore di associazioni, fondazioni ed enti, e le agevolazioni ed esenzioni di carattere tributario	Laffeni Daniela
21	Istruzione e cultura - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie	Laffeni Daniela
22	Istruzione e cultura - Attività di formazione ed in favore del diritto allo studio	Laffeni Daniela
23	Istruzione e cultura - Gestione delle biblioteche e dei centri di documentazione	Zambelli Marisa
24	Polizia municipale - Attività relativa all'infortunistica stradale	Leali Michelangelo
25	Polizia municipale - Gestione delle procedure sanzionatorie	Leali Michelangelo
26	Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa	Leali Michelangelo
27	Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria	Leali Michelangelo
28	Polizia municipale - Attività relativa al rilascio di permessi per invalidi	Leali Michelangelo
29	Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza	Leali Michelangelo
30	Avvocatura - Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione	Benuzzi Beatrice
31	Politiche del lavoro - Gestione delle attività relative all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale	Laffeni Daniela
32	Gestione dei dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni	Benuzzi Beatrice
33	Attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali	Benuzzi Beatrice
34	Attività del difensore civico comunale	Benuzzi Beatrice
35	Attività riguardante gli istituti di democrazia diretta	Benuzzi Beatrice
36	Protezione civile	Bresciani Marica

38	Gestione attività ricreative, promozione della cultura e dello sport, uso di beni immobili, occupazione suolo pubblico	Laffeni Daniela/Zambelli Marisa
39	Gestione albi comunali di associazioni e organizzazioni di volontariato	Lombardi Annamaria

INDIVIDUAZIONE DELLE MISURE MINIME DI SICUREZZA DA ADOTTARE PER IL TRATTAMENTO E LA CONSERVAZIONE DEI DATI PERSONALI

A. Autenticazione informatica;
B. Adozione di procedure di gestione delle credenziali di autenticazione;
C. Utilizzazione di un sistema di autorizzazione;
D. Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
E. Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
F. Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
G. Tenuta di un aggiornato documento programmatico sulla sicurezza;
H. Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Responsabile del trattamento 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 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 apposito modulo che deve essere trasmesso in copia controllata al Titolare del trattamento.

Art. 31. ***Obblighi di sicurezza***

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

Art. 33. ***Misure minime***

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

Art. 34. ***Trattamenti con strumenti elettronici***

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

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

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

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

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

Art. 36. ***Adeguamento***

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

Con l'approvazione del D.Lgs. 196/03 - "Codice in materia di protezione dei dati personali", viene nuovamente ribadito il concetto di protezione del dato personale e non del sistema elettronico in quanto tale. Vengono altresì individuati e definiti due strumenti per rendere operativo ed effettiva l'attuazione delle misure minime di sicurezza:

I. Il Custode delle Password

II. Il documento programmatico sulla sicurezza

Il Custode delle password

Sulla base del punto 10, allegato B, quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, devono essere 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.

Il documento programmatico sulla sicurezza

Sulla base dell'articolo 34 del D.Lgs. 196/03 nel caso di trattamento dei dati sensibili o giudiziari, deve essere predisposto ed aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

– la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
– per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Quindi a tale fine devono essere predisposte contromisure di sicurezza:

– **fisiche**
– **logiche**
– **organizzative.**

L'allegato B del "Codice" in materia di trattamento dei dati personali

Trattamenti con strumenti elettronici

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

Sistema di autenticazione informatica

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

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 sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

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

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

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

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.

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

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono

impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

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

Sistema di autorizzazione

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

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

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

Altre misure di sicurezza

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

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

– l'elenco dei trattamenti di dati personali;
– la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
– l'analisi dei rischi che incombono sui dati;
– le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
– la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
– la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi danno-

si, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

– la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
– per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

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

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

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

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

Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

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

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

Trattamenti senza l'ausilio di strumenti elettronici

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

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

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

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

Il sistema di sicurezza integrato

Le pubbliche amministrazioni devono fare uso di sistemi di sicurezza che principalmente si basino sui seguenti quattro punti fondamentali:

Sicurezza fisica
Sicurezza logica

Sistema di Sicurezza

Sicurezza organizzativa
Gestione delle crisi

Queste misure devono interessare:

CED **Interno edificio** **Esterno edificio**

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'allegato B, punto 19, D.Lgs. 30 giugno 2003, n. 196)

INTRODUZIONE

L'allegato B, punto 19 del D,Lgs. 196/03 impone la predisposizione e l'aggiornamento, con cadenza annuale, di un documento programmatico sulla sicurezza dei dati, 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:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Tale documento deve essere obbligatoriamente predisposto nel caso di trattamento di dati sensibili o giudiziari.

L'articolazione progettuale del documento programmatico sulla sicurezza prevede le seguenti attività:

- Contenuto del piano operativo
- Analisi del rischio
- Rassegna delle principali misure di controllo del rischio
- Definizione di misure di sicurezza fisiche, logiche ed organizzative, inclusi i siti di archiviazione dei dati, con particolare attenzione al controllo fisico e logico degli accessi
- Definizione di misure di sicurezza fisiche, logiche ed organizzative che assicurino l'integrità dei dati
- Definizione di misure di sicurezza fisiche, logiche e organizzative che assicurino la sicurezza della trasmissione telematica dei dati

– Programma di formazione degli incaricati
– Piano di verifiche e di aggiornamento periodico del documento

Naturalmente la predisposizione di un tale piano richiede un'attenta analisi della situazione attuale del sistema informativo e di tutti i trattamenti di dati che vengono effettuati. Il presente documento rappresenta dunque una prima bozza che contiene alcune indicazioni sulla redazione del piano di sicurezza e che dovrà essere successivamente affinata al fine di ottenere un completo "manuale sulla sicurezza", anche in considerazione del fatto che è prevista una ristrutturazione della sede comunale e di conseguenza del relativo Sistema Informativo.

CONTENUTO ORGANIZZATIVO

La presenta trattazione è riferita al piano operativo annuale delle misure minime di sicurezza, elaborato dal Comune di Nuvolera nell'anno 2004 e aggiornato nell'anno 2007, secondo quanto previsto dal D.Lgs. 196/03.

In particolare il piano operativo in oggetto descrive in dettaglio le misure adottate per minimizzare i rischi di istruzione o di perdita, anche accidentale, che il trattamento dei dati personali (e sensibili e giudiziari in particolare) inevitabilmente comporta.

ANALISI DEL RISCHIO

Questo modulo costituisce la fase di partenza delle attività di progettazione di un piano di sicurezza, la sua predisposizione consente di:

– Acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo
– Avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare

CONTENUTO DEL PIANO OPERATIVO

Di seguito verranno esposti nell'ordine:

1) i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate;
2) i criteri e le procedure per assicurare l'integrità dei dati;
3) i criteri e le procedure per la sicurezza del trattamento dei dati stessi;
4) il piano di intervento per l'individuazione dei rischi e la prevenzione dei danni.

1. CRITERI TECNICI ED 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

1.1. Protezione delle aree e dei locali interessati

1.1.1. La sala server è dotata di:
- impianto elettrico a norma;
- gruppo di continuità che permette il salvataggio in caso di black out.

1.1.2. In assenza di personale autorizzato, la sala server viene mantenuta a chiave.

1.1.3. I supporti di back up vengono conservati in appositi armadi, muniti di serratura e posti in locali distanti dalla sala server.

Ad oggi questi criteri di protezione non sono stati ancora implementati ma previsti dalla futura ristrutturazione della sede del Municipio.

1.2. Gestione degli apparati di rete

Se non diversamente specificato, si farà esclusivamente riferimento ad elaboratori (Personal Computer, server o terminali) che siano accessibili da altri elaboratori o terminali tramite connessione alla rete comunale.

1.2.1. Gli armadi che contengono gli apparti di rete nelle varie sedi vengono tenuti chiusi a chiave. Le chiavi vengono custodite secondo le stesse procedure previste al punto 1.1.6.

2. CRITERI E PROCEDURE PER ASSICURARE L'INTEGRITÀ DEI DATI

2.1. Sicurezza del software

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

a. Software commerciale, dotato di licenza d'uso (esempio pacchetti di office automation)

b. Software gestionale realizzato specificatamente per l'amministrazione comunale da ditte specializzate nel settore della pubblica amministrazione

c. Software realizzato internamente per soddisfare eventuali esigenze particolari del singolo servizio.

2.1.2. L'eventuale installazione di software diversi da quelli citati al punto precedente deve essere preventivamente valutata ed autorizzata dall'ufficio CED.

2.1.3. La conformità del software di cui alle lettere B e C del punto 2.1.1. viene certificata dall'ufficio CED.

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

2.1.5. Allo stesso fine, il CED, provvede mensilmente alla verifica del corretto aggiornamento del software antivirus su tutta la rete comunale.

2.1.6. In mancanza di procedure di installazione automatiche gli incaricati del trattamento sono stati istruiti per effettuare l'aggiornamento del software antivirus sulle postazioni di lavoro di propria competenza, con cadenza settimanale.

2.1.7. Per quanto riguarda l'accesso ad internet e alla posta elettronica centralizzati, la sicurezza è garantita da un software antivirus installato sulla postazione utilizzata per la ricezione della posta elettronica.

2.2. Integrità dei dati

2.2.1. In fase di installazione e configurazione del sistema di archiviazione dei file, sono stati definiti i volumi logici o le aree di disco da sottoporre a back up sui vari server.

2.2.2. I componenti del servizio CED, in qualità di responsabili della sicurezza, sono anche i responsabili incaricati del backup.

2.2.3. Il backup dei dati memorizzati sul server viene effettuato eseguendo le seguenti operazioni:

- Esecuzione quotidiana del backup, attraverso procedure manuale ed automatiche, con verifica immediata della corretta esecuzione dei backup
- Creazione e mantenimento di un elenco dei backup effettuati
- Archiviazione dei supporti secondo le disposizioni della sezione 1 punto 1.1.5

– Effettivo ripristino dei dati in caso di necessità. I tempi massimi di ripristino del server in caso di guasto sono (una volta riparato o sostituito l'hardware) dell'ordine di tre giorni lavorativi.

2.3. Sistema di monitoraggio

2.3.1. Attraverso appositi file di log presenti sui vari server, è stato realizzato un sistema di controllo e verifica della sicurezza del sistema informatico

2.3.2. Il sistema di controllo è in grado di registrare:

– Gli accessi riusciti (Success Logon) e falliti (Failure Logon) al sistema di autenticazione

3. CRITERI E PROCEDURE PER LA SICUREZZA DEL TRATTAMENTO DEI DATI

3.1. Controllo degli accessi

3.1.1. L'accesso alla rete può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password

3.1.2. Il processo di autenticazione consente di ottenere un profilo rispetto alle risorse del sistema informatico. A ciascun profilo è associato un gruppo di utenti che condividono gli stessi privilegi di accesso e di utilizzo.

3.1.3. Il custode delle password custodisce un elenco aggiornato contenente: i nomi e le qualifiche degli utenti autorizzati, provvede inoltre a:

– Definire per ciascun utente il nome utente e la password per il primo accesso
– Definire i gruppi necessari per rispettare i privilegi di utilizzo
– Consegnare agli interessati il nome utente e la password assegnati.

3.1.4. Dove tecnicamente è possibile il custode delle password imposta il sistema in modo da forzare l'utente a:

– Cambiare la propria password al momento del primo accesso
– Cambiare la password periodicamente, con una frequenza non superiore a sei mesi
– A non poter riutilizzare la stessa password
– A non poter utilizzare lo stesso nome utente per accedere contemporaneamente al sistema da due postazioni di lavoro distinte.

3.1.5. Nome utente e password sono strettamente personali. L'utente è tenuto a:

– Non comunicare a terzi la password
– A non annotare la password su supporti posti in vicinanza della propria postazione di lavoro o comunque incustoditi.

4. PIANO DI INTERVENTO PER L'INDIVIDUAZIONE DEI RISCHI E LA PREVENZIONE DEI DANNI

4.1. Piano di intervento

4.1.1. Il Responsabile CED, provvede, anche per tramite il custode delle password a informare tempestivamente gli incaricati:

- Della presenza di virus negli elaboratori d'ufficio
- Di prassi da parte del personale non conformi alle disposizioni sulla sicurezza
- Della periodica necessità di variazione della parola chiave
- Della disponibilità di programmi di aggiornamento relativi ad antivirus

4.1.2. Il Responsabile CED, in caso di necessità, provvederà ad organizzare iniziative per illustrare e diffondere gli accorgimenti da adottare in tema di sicurezza.

Un elenco non esaustivo, delle minacce al sistema informatico, distinto per classi di risorse, è indicato nella seguente tabella:

Tipo di risorse	Componenti sistema informativo	Minacce	Rischio
Hardware	Server di rete	– Malfunzionamenti dovuti a guasti o sabotaggi – Malfunzionamenti dovuti ad eventi naturali (allagamenti, incendi…) – Furti – Intercettazione	**Medio - basso**
Hardware	Personal Computer	– Malfunzionamenti dovuti a guasti o sabotaggi – Malfunzionamenti dovuti ad eventi naturali (allagamenti, incendi…) – Furti – Intercettazione	**Medio-basso**
Hardware	Stampanti	– Malfunzionamenti dovuti a guasti o sabotaggi – Malfunzionamenti dovuti ad eventi naturali (allagamenti, incendi…) – Furti	**Basso**
Hardware	Linee di comunicazione	– Malfunzionamenti dovuti a guasti o sabotaggi – Malfunzionamenti dovuti ad eventi naturali (allagamenti, incendi…) – Furti – Intercettazione	**Medio - basso**
Hardware	Sistemi operativi	– Presenza di errori involontari commessi in fase di progettazione e/o implementazione che consentono ad utenti non autorizzati l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti – Presenza di codice malizioso inserito volontariamente al fine di poter svolgere operazioni non autorizzate al sistema o per danneggiare lo stesso (virus, trojan horse, bombe logiche backdoors) – Attacchi di tipo denial of service	**Medio - basso**
Hardware	Applicazioni	– Presenza di errori involontari commessi in fase di progettazione e/o implementazione che consentono ad utenti non autorizzati l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti – Presenza di codice malizioso inserito volontariamente al fine di poter svolgere operazioni non autorizzate al sistema o per danneggiare lo stesso (virus, trojan horse, bombe logiche backdoors)	**Medio - basso**

		– Attacchi di tipo denial of service	
Software	Gestori di basi di dati	– Presenza di errori involontari commessi in fase di progettazione e/o implementazione che consentono ad utenti non autorizzati l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti – Presenza di codice malizioso inserito volontariamente al fine di poter svolgere operazioni non autorizzate al sistema o per danneggiare lo stesso (virus, trojan horse, bombe logiche backdoors) – Attacchi di tipo denial of service	**Medio - basso**
Software	Codice e sorgente di applicazioni	– Furto – Modifica per l'inserimento di codice malizioso	**Basso**
Dati	Contenuto degli archivi informatizzati	– Accesso non autorizzato – Modifiche deliberate o accidentali	**Basso**
Dati	Basi di dati	– Accesso non autorizzato – Modifiche deliberate o accidentali	**Basso**
Dati	File di log	– Accesso non autorizzato – Modifiche deliberate o accidentali	**Basso**
Professionali	Amministratori di sistemi	– Maturazione di motivi di rivalsa nei confronti dell'amministrazione – Scarsa consapevolezza del problema sicurezza	**Basso**
Professionali	Operatori	– Maturazione di motivi di rivalsa nei confronti dell'amministrazione – Scarsa consapevolezza del problema sicurezza	**Medio - basso**
Professionali	Manutenzioni hardware e software	– Attacchi di social engineering – Maturazione di motivi di rivalsa nei confronti dell'amministrazione – Scarsa consapevolezza del problema sicurezza	**Medio - basso**
Professionali	Consulenti esterni	– Maturazione di motivi di rivalsa nei confronti dell'amministrazione – Scarsa consapevolezza del problema sicurezza	**Basso**
Documentazione cartacea	Programmi	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali	**Medio - basso**
Documentazione cartacea	Hardware	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali	**Medio**
Documentazione cartacea	Sistemi	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali	**Medio**
Documentazione cartacea	Procedure di gestione	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali	**Medio - basso**
Documentazione cartacea	Pratiche correnti e di archivio	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali	**Medio - basso**
Supporti di memorizzazione	Copie software installati	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali – Deterioramento nel tempo – Inaffidabilità del mezzo fisico – Evoluzione tecnologica e del mercato	**Basso**
Supporti di memorizzazione	Backup	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali – Deterioramento nel tempo – Inaffidabilità del mezzo fisico – Evoluzione tecnologica e del mercato	**Medio - basso**
Supporti di memorizzazione	Copia dei file di log	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali – Deterioramento nel tempo – Inaffidabilità del mezzo fisico – Evoluzione tecnologica e del mercato	**Basso**

RASSEGNA DELLE PRINCIPALI MISURE DI CONTROLLO DEL RISCHIO

Sulla base dei risultati conseguiti con l'analisi di cui sopra è possibile procedere alla predisposizione di un quadro esaustivo delle misure di controllo del rischio, indicando per ciascuna pregi e difetti riferiti al particolare contesto.

Le misure di controllo del rischio dovranno essere suddivise in 3 categorie:

- Misure di sicurezza fisica.
- Misure di sicurezza logica.
- Misure di sicurezza organizzative.

Le *misure di sicurezza fisica* sono le uniche che effettivamente impediscono o rallentano un attacco al sistema.

Le *misure di sicurezza logica* sono in grado di segnalare una intrusione in atto ed eventualmente di richiamare l'intervento di un responsabile in grado di "bloccare" l'intrusione.

Le *misure di sicurezza organizzative* hanno il compito di garantire la corretta funzionalità delle misure precedenti e di assicurare in tempi brevi l'intervento di un responsabile, se necessario.

Nei paragrafi seguenti vengono indicate alcune misure di sicurezza che sono in parte già state adottate o che dovranno essere messe in atto nel futuro, le quali verranno poi integrate a seguito della completa analisi di cui sopra.

DEFINIZIONE DI MISURE DI SICUREZZA FISICHE, LOGICHE ED ORGANIZZATIVE, INCLUSI I SITI DI ARCHIVIAZIONE DEI DATI, CON PARTICOLARE ATTENZIONE AL CONTROLLO FISICO E LOGICO DEGLI ACCESSI

Tipo di misura	Misura	Esistente o da attuare
Fisica	Sistema di allarme in ogni edificio ove sono ubicati gli uffici del Comune	**Previsto dalla futura ristrutturazione**
Fisica	Inferiate alle finestre di accesso alla sala Server	**Assenti**
Fisica	Estintori almeno in ogni piano di ogni sede del Comune	**Esistenti**
Fisica	Armadi ignifughi almeno all'interno del Servizio Informatico per l'archiviazione dei backup	**Assenti**
Organizzativa	Registrazione su supporto cartaceo dell'accesso agli uffici al di fuori degli orari di lavoro da parte di personale non impiegato presso il medesimo ufficio	**Non attuata**
Organizzativa	Assegnazione di responsabilità agli incaricati della gestione dei servizi di allarme, antincendio, custodia chiavi dei locali ad accesso controllato	**Da attuare successivamente alla conclusione del progetto di ristrutturazione del Municipio**
Organizzativa	Predisposizione di un piano di disaster recovery	**Da attuare**

DEFINIZIONE DI MISURE DI SICUREZZA FISICHE, LOGICHE ED ORGANIZZATIVE CHE ASSICURINO L'INTEGRITÀ DEI DATI

Tipo di misura	Misura	Esistente o da attuare
Fisica	Gruppo statico di continuità per supporto ai server di rete	**Esistente**
Fisica	Linea elettrica dedicata al collegamento dei client	**da attuare**
Fisica	Gruppo statico di continuità per supporto alla linea elettrica dedicata al collegamento dei client	**Esistente**
Fisica	Climatizzatore nella sala server	**da attuare**
Fisica	Porte chiudibili a chiave per tutti gli uffici e per gli archivi	**da attuare**
Fisica	Armadi e cassettiere chiudibili a chiave	**da attuare**
Fisica	Utilizzo di password su ogni stazione di lavoro	**da completare**
Fisica	Definizione di profili di accesso degli incaricati	**da completare**
Fisica	Procedure atte a verificare l'integrità e l'aggiornamento dei dati personali (utilizzo di tecniche automatizzate di verifica dell'integrità dei dati)	**Esistente**

Logica	Assegnazione di un codice identificativo personale a ciascun operatore da sostituire ogni sei mesi	**Esistente**
Logica	Installazione e gestione programmi antintrusione di cui all'art. 615/ quinquies del codice penale con aggiornamenti e verifiche dell'efficacia almeno quadrimestrale	**da attuare**
Logica	Utilizzo di sistemi di crittografia per la protezione dei dati particolari (sensibili e giudiziari)	**Esistente**
Logica	Registrazione e consultazione dei file di log	**Esistente**
Logica	Registrazione degli accessi per il trattamento dei dati sensibili su supporto cartaceo: impartite disposizioni agli incaricati	**Esistente**
Logica	Registrazione degli accessi per il trattamento dei dati sensibili su elaboratori	**Esistente**
Organizzativa	Backup	**Esistente**
Organizzativa	Conservazione in luoghi sicuri (possibilmente differenziati) delle diverse copie dei backup	**Esistente**
Organizzativa	Gestione di codici di identificazione personale e delle password da parte del personale del Servizio Informatico come indicato dall'art. 4 del D.P.R. 318/99)	**Esistente**
Organizzativa	Definizione delle regole di gestione delle password	**Esistente**
Organizzativa	Registrazione, consultazione e conservazione di ogni operazione eseguita su server di rete e personal computer (installazione, sistema operativo e software vari, aggiornamenti, sostituzione componenti per malfunzionamenti e guasti)	**da attuare**
Organizzativa	Individuazione, registrazione, consultazione e conservazione di tentativi di intrusione	**da attuare**
Organizzativa	Riutilizzo di supporti di memorizzazione (cartacei e/o informatici) soltanto nel caso in cui i dati precedentemente memorizzati non siano necessari	**Esistente**
Organizzativa	Eliminazione tramite distruggi documenti di supporti cartacei contenenti dati sensibili o giudiziari non più necessari	**Esistente**
Organizzativa	Smagnetizzazione di supporti informatici contenenti dati sensibili o giudiziari non più necessari	**Esistente**
Organizzativa	Assegnazione di autorizzazione agli incaricati per il trattamento dei dati sensibili e/o giudiziari così come prescritto dall'art. 5 del D.P.R. 318/99	**Esistente**

DEFINIZIONE DI MISURE DI SICUREZZA FISICHE, LOGICHE ED ORGANIZZATIVE CHE ASSICURINO LA SICUREZZA NELLA TRASMISSIONE DEI DATI

Tipo di misura	Misura	Esistente o da attuare
Fisica	Criptazione di file contenenti dati sensibili o comunque personali prima della trasmissione	**Non attuata**
Fisica	Predisposizione di procedure antintrusione al sistema informativo automatizzato	**Non attuata**
Fisica	Utilizzo di sistemi di crittografia e della firma digitale	**Non attuata**
Logica	Predisposizione di un manuale sulle modalità di spedizione di documenti cartacei, utilizzo di dispositivi facsimile…..	**Esistente (Manuale di gestione del Protocollo informatico)**

PIANO DI VERIFICHE E DI AGGIORNAMENTO PERIODICO DEI DOCUMENTI

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

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

In particolare, quindi, dovranno essere effettuati, almeno annualmente, test relativi a:

- Accesso fisico ai locali dove si svolgono trattamenti manuali e autorizzati.
- Gestione di codici identificativi personali e password.
- Gestione dei profili di accesso degli incaricati.
- Procedure atte a verificare l'integrità e l'aggiornamento dei dati personali.
- Sicurezza delle trasmissioni in rete.
- Modalità di conservazione dei documenti cartacei.
- Modalità di conservazione dei backup.
- Ripristino dei backup.
- Modalità di reimpiego dei supporti di memorizzazione.
- Livello di formazione e grado di apprendimento degli incaricati.

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