

COMUNE di COLLEDIMEZZO

Alleg. alla Delibera GM n. 80 del 23.12.04

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI

INTRODUZIONE

Il presente documento è redatto sulla base delle disposizioni concernenti l'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dagli articoli 31- 33- 34-35 che di seguito si riportano e dall'allegato B del D.lgs. n. 196/2003.

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.

L'allegato B, punto 19 del D.Lgs. 196/03 prevede che il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza 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:

- 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 (solo per gli organismi sanitari e gli esercenti professioni sanitarie così come previsto dal punto 24 dell'all. B).

Quindi a tale fine devono essere predisposte contromisure di sicurezza volte ad assicurare:

- la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone;
- - l'integrità e la sicurezza dei dati.

Naturalmente la predisposizione di un tale piano richiede un'attenta analisi della situazione attuale del sistema informativo ed organizzativo dell'ente e di tutti i trattamenti di dati che vengono effettuati. Il presente documento rappresenta dunque una prima versione che definisce le misure minime da adottare e che dovrà essere successivamente affinata al fine di ottenere un completo manuale sulla sicurezza.

La presente trattazione è riferita al piano operativo annuale delle misure minime di sicurezza, elaborato dal Comune di Colledimezzo, per l'anno 2004, secondo quanto previsto dal D.Lgs. 196/03.

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

1. 1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

In questa sezione è inserito l'elenco dei trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della struttura che operativamente effettua il trattamento.

STRUTTURA PREPOSTA AL TRATTAMENTO	BANCHE DATI
UFFICIO ANAGRAFE E STATO CIVILE	Banca dati della popolazione residente
	Banca dati degli elettori.
	Cartellini carte d'identità
	Registri atti di nascita – morte – matrimonio
	Liste di leva
	Registri dei defunti
	Schede Istat
	Contratti cimiteriali
	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 (ruoli matricolari).
	Banca dati popolazione cancellata per emigrazione, decesso o irreperibilità
UFFICIO SERVIZI FINANZIARI UFFICIO LAVORI PUBBLICI E PATRIMONIO	Banca dati albo fornitori del comune
	Banche dati sinistri di terzi
UFFICIO PERSONALE	Banca dati dei dipendenti del Comune.
	Banca dati rilevazione presenze e permessi
	Personale del Comune.
	Banca dati modello 730.
	Banca dati INPDAP.

	Banca dati INPS
	Banca dati modello 770.
	Banca dati inquadramento contrattuale
	Banca dati degli incarichi professionali O stagionali del Comune.
	Banca dati degli amministratori del comune
UFFICIO TRIBUTI CONCESSIONARI RISCOSSIONE	DELLA Banca dati imposta comunale sugli immobili
	Banca dati tassa/tariffa di igiene urbana
UFFICIO RAGIONERIA UFFICIO TRIBUTI UFFICIO SEGRETERIA UFFICIO TECNICO (LAVORI PUBBLICI, MANUTENZIONI) UFFICIO URBANISTICA/EDILIZIA PRIVATA/SPORTELLO UNICO- COMMERCIO UFFICIO SERVIZI SOCIALI UFFICIO CULTURA/ISTRUZIONE UFFICIO POLIZIA LOCALE UFFICIO ANAGRAFE STATO CIVILE	Banca dati debitori Banca dati creditori
UFFICIO URBANISTICA	Banche dati pratiche edilizie concessioni edilizie
	Banche dati condono edilizio
UFFICIO SERVIZI SOCIALI	
	provvedimenti relativi a minori
	beneficiari contributi economici
	centro socio-educativo
	Banca dati amministratori piano di zona
	Tutela dei minori
	Banche dati associazioni e varie attinenti l'ambito sociale
	Inserimenti lavorativi disabili
UFFICIO CULTURA ISTRUZIONE SPORT E TEMPO LIBERO	Banche dati Refezione scolastica
	Banche dati Trasporto scolastico
	Banche dati Pre-scuola
	Banche dati Assistenza ad personam (alunni portatori di handicap)
	Banche dati biblioteca
	Banche dati associazioni culturali, sportive, d'arma e combattentistiche, associazioni socio-assistenziali
UFFICIO LAVORI PUBBLICI	Banche dati stato avanzamento lavori
	Assegnazione contributi regionali prima casa
	Banche dati contratti
	Parrocchie beneficiarie di contributi per edifici di culto
	Decreti di espropriazione
UFFICIO POLIZIA LOCALE	Banca dati dei verbali di contestazione alle violazioni del codice stradale
	Banca dati infrazioni al codice della strada
	Banca dati cessioni di fabbricato legge n. 191/1978

	Banca dati polizia giudiziaria
	Banca dati relativa a veicoli rubati e recuperati
	Banca dati relativi agli incidenti stradali
UFFICIO SEGRETERIA	Protocollo del comune e archivio generale
	Verbali delle deliberazioni di giunta comunale
	Verbali di delle deliberazioni del consiglio comunale
	Banca dati notificazioni messi comunali
UFFICIO URBANISTICA- COMMERCIO	Banca dati titolari di autorizzazione al commercio fisso
	Banche dati titolari di pubblici esercizi
	Banche dati commercio su aree pubbliche
	Banche dati utenti soggetti a controllo pesi e misure

2. 2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DI DATI.

Nella sezione 1 del presente documento sono state individuate le strutture preposte al trattamento dei dati nonché l'elenco dei dati gestiti da ciascuna struttura. Al vertice di ciascuna struttura c'è il responsabile del trattamento dei dati che coincide con il responsabile di servizio o nel segretario di area in via residuale. I responsabili del trattamento dei dati personali gestiti dalla struttura assegnata sono nominati con apposito provvedimento del sindaco.

Il Comune di Colledimezzo, come Titolare, e le figure individuate come Responsabili, assicureranno che il programma di sicurezza sia adeguatamente sviluppato, realizzato e mantenuto aggiornato e conforme alla legge sulla privacy e alle prescrizioni del presente documento.

Essi, nell'ambito della propria organizzazione, opereranno in modo da:

- minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati personali,
- minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali,
- minimizzare la probabilità che i trattamenti dei dati personali siano modificati senza autorizzazione.

Titolare del trattamento

Tra i compiti che la Legge assegna al Titolare e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Responsabile del trattamento di dati personali

Il Responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le seguenti responsabilità:

- promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento Programmatico sulla Sicurezza dei Dati Personali;
- informare il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti;
- promuovere lo svolgimento di un continuo programma di addestramento degli Incaricati del Trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza;

Incaricati del trattamento

Gli Incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive del Responsabile;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Responsabile in caso di incidente di sicurezza che coinvolga dati personali.

3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

Questa sezione 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.

Qui di seguito si riporta l'elenco dei rischi presenti nel comune, distinto per tipo di risorsa.

Tipo di risorse	Componenti sistema informativo	Minacce
Struttura	Tutte	<ul style="list-style-type: none"> - Accessi non autorizzati - Effrazioni - Furti - Atti vandalici
Hardware	Server di rete	<ul style="list-style-type: none"> - Malfunzionamenti dovuti a guasti o sabotaggi - Malfunzionamenti dovuti ad eventi naturali (allagamenti, incendi...) - Furti - Intercettazione
Hardware	Personal Computer	<ul style="list-style-type: none"> - Malfunzionamenti dovuti a guasti o sabotaggi - Malfunzionamenti dovuti ad eventi naturali (allagamenti, incendi...) - Furti - Intercettazione
Hardware	Linee di comunicazione	<ul style="list-style-type: none"> - Malfunzionamenti dovuti a guasti o sabotaggi - Malfunzionamenti dovuti ad eventi naturali (allagamenti, incendi...) - Furti - Intercettazione

Software	Sistemi operativi	<ul style="list-style-type: none"> - 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
Software	Applicazioni	<ul style="list-style-type: none"> - 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
Software	Gestori di basi di dati	<ul style="list-style-type: none"> - 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
Software	Codice e sorgente di applicazioni	<ul style="list-style-type: none"> - Furto - Modifica per l'inserimento di codice malizioso
Dati	Cartaceo	<ul style="list-style-type: none"> - Accesso non autorizzato - Modifiche deliberate o accidentali - Sottrazione - Distrusione
Dati	Contenuto degli archivi	<ul style="list-style-type: none"> - Accesso non autorizzato - Modifiche deliberate o accidentali
Dati	Basi di dati	<ul style="list-style-type: none"> - Accesso non autorizzato - Modifiche deliberate o accidentali
Professionali	Amministratori di sistemi	<ul style="list-style-type: none"> - Maturazione di motivi di rivalsa nei confronti dell'amministrazione - Scarsa consapevolezza del problema sicurezza
Professionali	Operatori	<ul style="list-style-type: none"> - Maturazione di motivi di rivalsa nei confronti dell'amministrazione - Scarsa consapevolezza del problema sicurezza
Professionali	Manutenzioni hardware e software	<ul style="list-style-type: none"> - Attacchi di social engineering - Maturazione di motivi di rivalsa nei confronti dell'amministrazione - Scarsa consapevolezza del problema sicurezza
Professionali	Consulenti esterni	<ul style="list-style-type: none"> - Maturazione di motivi di rivalsa nei confronti dell'amministrazione - Scarsa consapevolezza del problema sicurezza

Documentazione cartacea	Programmi	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali
Documentazione cartacea	Hardware	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali
Documentazione cartacea	Sistemi	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali
Documentazione cartacea	Procedure di gestione	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali
Documentazione cartacea	Pratiche correnti e di archivio	– Distruzione, sottrazione ed alterazione ad opera di eventi naturali, azioni accidentali e comportamenti intenzionali
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
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

4. MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI, NONCHE' LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITA'

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.

I sistemi di sicurezza adottati dal comune devono basarsi sui seguenti punti fondamentali:

- - sicurezza fisica;
- - sicurezza logica;
- - sicurezza organizzativa;
- - gestione delle crisi.

La sicurezza fisica si realizza attraverso le opportune disposizioni per :

- - controllo degli accessi
- - gestione delle chiavi
- - gruppo di continuità

La sicurezza logica si realizza attraverso le opportune disposizioni per:

- - sistemi di identificazione;
- - sistemi di autenticazione;
- - controlli antivirus;

La sicurezza organizzativa si realizza attraverso opportune disposizioni per:

- - la gestione del personale;
- - codici etici di comportamento;
- - suddivisione incarichi;
- - formazione e sensibilizzazione del personale;

La gestione dell'emergenza e delle crisi deve prevedere:

- - procedure di backup;
- - procedure di recupero dei dati;
- - procedure di ripristino.

Qui di seguito vengono indicate le misure di sicurezza che sono in parte già state adottate o che dovranno essere messe in atto nel futuro.

Verranno esposti nell'ordine:

- A) 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;
- B) i criteri e le procedure per assicurare l'integrità e la sicurezza dei dati;
- C) i criteri per l'individuazione dei rischi e la prevenzione dei danni.

<p>A. 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</p>
--

Protezione delle aree e dei locali interessati dalle misure di sicurezza (sala server e uffici comunali)

I locali e i contenitori nei quali sono archiviati o dai quali è possibile l'accesso ai dati devono essere sempre presidiati da personale autorizzato. In caso di assenza, anche temporanea, di idoneo presidio i locali e i contenitori dei dati devono essere debitamente resi inaccessibili attivando i sistemi di chiusura disponibili. Qualora le chiusure siano deteriorate o mancanti è compito del responsabile dell'ufficio dare immediata comunicazione all'ufficio preposto alla manutenzione degli immobili. La gestione delle chiavi di accesso ai contenitori dei dati o all'ufficio, qualora detti contenitori ne fossero sprovvisti, deve essere effettuata a cura del responsabile dell'ufficio che provvederà a gestire un elenco di tutti i detentori delle chiavi e a mantenerlo aggiornato entro 48 ore da ogni modifica.

Il "responsabile dell'area" ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità.

- Le persone autorizzate ad accedere sono esclusivamente gli incaricati o i responsabili del trattamento dei dati.
- I visitatori occasionali devono essere accompagnati.
- Gli ingressi fuori orario devono essere controllati.

La sala server è dotata di:

- - impianto elettrico a norma;
- - Porta chiudibile a chiave;
- - gruppo di continuità che permette il salvataggio in caso di black out.

L'accesso alla sala server è limitato ai soli addetti al sistema informativo o alle persone espressamente autorizzate dagli stessi, per il tempo strettamente necessario allo svolgimento dei compiti eventualmente assegnati (esempio: manutenzione software e/o Hardware di un server).

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

I supporti di back up vengono conservati in cassaforte.

I locali nei quali sono archiviati dati personali devono essere sempre presidiati da personale autorizzato. In caso di assenza, anche temporanea (es. durante la pausa pranzo), del personale incaricato dei trattamenti dei dati i locali e i contenitori dei dati devono essere resi inaccessibili attivando i sistemi di chiusura disponibili. Qualora le chiusure siano deteriorate o mancanti il responsabile del trattamento dei dati e gli incaricati del trattamento dei dati dell'ufficio sono tenuti a dare immediata comunicazione all'ufficio preposto alla manutenzione degli immobili.

Gli incaricati sono tenuti a fine giornata a non lasciare sulla scrivania e a riporre negli armadi tutta la documentazione contenente dati personali. I dati sensibili devono essere riposti in armadi chiusi a chiave e conservati separatamente dagli altri dati personali.

QUADRO RIASSUNTIVO DELLE MISURE VOLTE A CONTROLLARE L'ACCESSO AI LOCALI INTERESSATI DALLE MISURE DI SICUREZZA

Tipo di misura	Misura
Fisica	Impianto elettrico a norma
Fisica	Estintori almeno in ogni piano di ogni sede del Comune
Fisica	Armadi ignifughi almeno all'interno del Servizio Informatico per l'archiviazione dei backup
Fisica	Porte chiudibili a chiave per tutti gli uffici
Fisica	Conservazione dei dati personali negli armadi, fuori dagli orari di ufficio, necessariamente chiusi a chiave per la conservazione dei dati sensibili

B. CRITERI E PROCEDURE PER ASSICURARE L'INTEGRITÀ E LA SICUREZZA DEI DATI

Gestione degli elaboratori di rete

Con apposito atto del Sindaco verrà individuato il responsabile del sistema informatico del Comune di Colledimezzo. Tale responsabile potrà essere scelto tra i dipendenti comunali o potrà essere un consulente esterno.

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.

Sono considerate apparecchiature informatiche critiche ai fini della sicurezza le seguenti apparecchiature se parte del trattamento di dati personali:

- - Computer, sia server che workstation, con la sola esclusione delle workstation ad uso esclusivamente personale.
- - Unità a dischi ottici o magnetici e unità nastri (DAT, DLT, ecc.).
- - Sistemi per la gestione delle LAN, router, hub, ecc.

Le chiavi dei sistemi e delle apparecchiature devono essere rimosse.

Le apparecchiature delle LAN (Wiring hub, MAU, ecc.) non facenti parte del backbone e non situate nelle aree ad accesso controllate, devono essere riposte almeno all'interno di armadi chiusi.

Gli strumenti elettronici destinati a contenere o consentire l'accesso ai dati devono essere protetti passivamente mediante sistemi di chiusura adeguati e/o mediante l'attivazione di sistemi anti-intrusione elettronici (quando disponibili). La segnalazione dei malfunzionamenti è delegata ad ogni singolo responsabile di ufficio. La protezione attiva delle banche dati comuni è affidata a programmi e strumenti appositamente preposti alla difesa del sistema contro intrusioni e danni informatici (ant-virus, firewall) e gestiti dal responsabile del sistema informativo.

L'accesso alle risorse disponibili sulla rete locale è protetto da username e password noti conoscibile solo dall'incaricato interessato nonché al personale del CED.

Sicurezza del software

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

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

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

Il responsabile informatico, provvede alla distribuzione e all'aggiornamento automatico di opportuno software antivirus su tutta la rete comunale.

Supporti di memorizzazione

Sono considerati supporti di memorizzazione i nastri magnetici, le cassette (cartridge), i dischi magnetici o ottici rimovibili, i CD-ROM che contengono informazioni personali.

I supporti contenenti dati sensibili devono, se possibile, essere marcati con un'opportuna etichetta recante la dicitura: "Contiene dati personali sensibili secondo il D.Lgs 196/2003. Rispettare quanto previsto dal trattamento".

I supporti devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave.

Sono definite informazioni residue quei dati personali ancora leggibili dopo la cessazione di un trattamento. (es. nastri, o dischi magnetici, dischi ottici, ecc.).

I dati personali devono essere resi illeggibili quando non sia più necessario conservarli per gli scopi per cui sono stati raccolti e trattati.

E' vietato l'utilizzo di supporti magnetici esterni, l'accesso a siti web non direttamente connessi alle attività di istituto. I responsabili degli uffici possono trasferire in locali diversi da quelli dove risiedono gli originali i supporti rimovibili contenenti dati personali, sensibili o giudiziari unicamente per fini istituzionali o per la loro sicurezza.

Stampati

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Il materiale cartaceo contenente dati personali deve essere reso illeggibile prima dello smaltimento.

Integrità dei dati (backup-salvataggi)

Il responsabile del sistema informatico mantiene un elenco, da aggiornare con cadenza almeno annuale, di tutte le attrezzature informatiche dei singoli uffici e della loro locazione fisica. E' inoltre incaricato del backup giornaliero.

Controllo degli accessi (password)

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

Gli addetti al ced custodiscono un elenco aggiornato contenente i nomi e le qualifiche degli utenti autorizzati ad accedere alla rete nonché delle relative password e provvedono inoltre a:

- - Definire per ciascun utente il nome utente e la password per il primo accesso;
- - Comunicare agli interessati il nome utente e la password assegnati.

Dove tecnicamente è possibile gli addetti al ced impostano il sistema in modo da non poter utilizzare lo stesso nome utente per accedere ai software gestionali da due postazioni di lavoro distinte.

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.

Connessione con l'esterno

In un sistema integrato la sicurezza deve essere trattata in modo uniforme, in quanto l'insicurezza di una singola parte si può ripercuotere generando insicurezza in tutto il sistema. Questo vale in particolare per gli aspetti di sicurezza della rete.

Per assicurare la sicurezza di una rete è fondamentale controllare gli accessi alla rete stessa.

E' definito Gateway per le interconnessioni esterne l'insieme di hardware, software e applicazioni (es. Firewall o Proxy) che permettono l'interconnessione o l'accesso remoto.

I Gateway devono consentire l'accesso alla rete interna solamente agli utenti autorizzati.

Nel caso si mettano in evidenza delle carenze la situazione deve essere corretta nel più breve tempo possibile.

Le connessioni via modem tra il sistema informativo comunale e reti e sistemi esterni possono rappresentare un serio rischio per il Sistema stesso. Come conseguenza di collegamenti non corretti dal punto di vista della sicurezza, è possibile che si esponga a rischio l'intero sistema informativo ed i dati in esso contenuti, ciò può avvenire senza che il dipendente se ne renda conto.

Per tale motivo ogni collegamento dall'interno verso l'esterno e viceversa deve rispettare i criteri di sicurezza qui esposti e quelli che verranno stabiliti dal Titolare e/o Responsabile.

Nel caso il collegamento sia di tipo TCP/IP tramite modem, non deve essere permesso il suo uso simultaneamente al collegamento interno.

Deve essere attivato un software tipo "Personal Firewall" sulle workstation interessate.

Di norma i modem collegati alle workstation devono restare spenti se non utilizzati.

QUADRO RIASSUNTIVO DELLE MISURE VOLTE AD ASSICURARE L'INTEGRITA' DEI DATI

Tipo di misura	Misura
Fisica	Gruppo statico di continuità per supporto ai server di rete
Fisica	Utilizzo di password su ogni stazione di lavoro
Fisica	Definizione di profili di accesso degli incaricati
Fisica/Logica	Gestione delle connessioni con l'esterno
Logica	Assegnazione di un codice identificativo personale a ciascun operatore
Logica	Registrazione degli accessi per il trattamento dei dati sensibili su supporto cartaceo
Organizzativa	Backup
Organizzativa	Conservazione in luoghi sicuri (possibilmente differenziati) delle diverse copie dei backup
Organizzativa	Gestione di codici di identificazione personale e delle password da parte del personale del Servizio

	Informatico
Organizzativa	Definizione delle regole di gestione delle password
Organizzativa	Riutilizzo di supporti di memorizzazione (cartacei e/o informatici) soltanto nel caso in cui i dati precedentemente memorizzati non siano necessari
Organizzativa	Cancellazione di supporti informatici contenenti dati sensibili o giudiziari non più necessari

C. CRITERI PER L'INDIVIDUAZIONE DEI RISCHI E LA PREVENZIONE DEI DANNI

Vengono attivati sistemi antintrusione ed antivirus che si aggiornano costantemente ed automaticamente al fine di minimizzare le possibilità di danno. Gli addetti all'informatica provvedono ad effettuare gli aggiornamenti importanti ai sistemi operativi ed ai software volti a garantire l'inviolabilità dei sistemi.

5. CRITERI E MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

In caso di danneggiamento dei dati o degli strumenti elettronici sono adottate idonee misure dirette a garantire il ripristino dell'accesso ai dati , in tempi certi e non superiori a sette giorni.

6. PREVISIONE DI INTERVENTI FORMATIVI DEL PERSONALE.

I responsabili degli uffici ai quali il presente documento e le sue successive revisioni viene trasmesso, devono rendere noto a tutti i componenti dell'ufficio i contenuti del presente documento con particolare riferimento alle responsabilità individuali

7. TRATTAMENTI AFFIDATI ALL'ESTERNO

In caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare è necessario che il soggetto esterno a cui viene affidato il trattamento si assuma alcuni impegni su base contrattuale.

Pertanto il soggetto cui le attività sono affidate deve dichiarare:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal codice per la protezione dei dati personali;
3. di impegnarsi ad avvisare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
4. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

8. CONCLUSIONI

Qualsiasi abuso dei dati gestiti o che comunque si rendono accessibili tramite le strutture dell'ente deve essere immediatamente comunicato al responsabile del trattamento dei dati.

Il presente documento dovrà essere 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.