CODICE DELLA PRIVACY

(D.L.vo N. 196/2003)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ANNO 2011

I redattori del documento

dott. Paolo Brambati
(Responsabile Sistemi Informativi)

Massimo Mozzi
(Ufficio CED)

Data : 31/03/2011

Comune di Lodi

p.zza Broletto 1
26900 Lodi LO

SOMMARIO

1 Sezione generale

1.1 Presentazione

Il Codice in materia di protezione dei dati personali (*Decreto Legislativo n. 196 del 2003*, di seguito Codice Privacy) entrato in vigore il primo gennaio 2004 raccoglie e riordina le numerose norme che si sono succedute in materia a partire dal 1996 (legge 675) ed innova l'intera disciplina introducendo misure di sicurezza, disposizioni e codici di deontologia per alcuni settori specifici.

Il Codice Privacy ribadisce il principio fondamentale dalla legge 675/96 relativo alla garanzia "*che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*" e, in particolare, detta una serie di principi e di regole, validi per tutti i trattamenti di dati personali:

a. **principio di trasparenza** – Il Titolare deve manifestare all'esterno gli elementi caratterizzanti la propria attività di trattamento: provvedere, se previsto, alla notifica al Garante e informare l'interessato;
b. **principio di necessità** – I sistemi informativi e i programmi informatici devono essere predisposti in modo da assicurare che i dati personali o identificativi siano utilizzati solo se indispensabili per il raggiungimento delle finalità consentite.
c. **assicurazione di qualità** – Il trattare i dati in modo lecito e secondo correttezza, predeterminando gli scopi e valutando la pertinenza, la completezza e la non eccedenza dei dati rispetto alle finalità dei trattamenti;
d. **controlli sull'attività svolta** – Le forme di controllo esercitabili da parte del Garante e dello stesso interessato;
e. **adozione di misure di sicurezza** – I mezzi e gli strumenti di protezione adottati, al fine di garantire l'integrità dei dati ed escludere accessi non autorizzati.

1.2 Oggetto e finalità

Questo elaborato costituisce il "Documento Programmatico sulla Sicurezza" (di seguito DPS), la cui adozione è imposta dall'art. 34 del Codice Privacy, nei modi previsti dal punto 19 dell'Allegato B.

Riferimenti al DPS ed alle finalità in esso enunciate compaiono nel "Codice dell'amministrazione digitale (D.Lgs. n.82/2005)", capi III, IV e V; il DPS costituisce inoltre un allegato del "Manuale per la gestione del protocollo informatico, dei flussi documentali e degli archivi del Comune di Lodi".

Il DPS deve essere redatto, per tutti i trattamenti di dati personali effettuati con strumenti elettronici (*gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento*), entro il 31 marzo di ogni anno; comunque, in virtù dell'art. 34 del Codice Privacy, tale documento va aggiornato in caso di cambiamenti relativi alle informazioni in esso contenute. La finalità di questo documento è fornire un quadro delle misure di sicurezza adottate e da adottare, nell'ottica di un miglioramento continuo per proteggere il patrimonio informativo dell'Ente da attività che possono comportare il maltrattamento dei dati personali (*distruzione o perdita, anche accidentale, dei dati stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta*).

Un sistema informativo automatizzato viene definito sicuro se soddisfa le seguenti proprietà:

a. **disponibilità** – le informazioni che il sistema eroga devono essere a disposizione degli utenti, compatibilmente con i livelli di servizio;
b. **integrità e autenticità** – le informazioni possono essere create, modificate o cancellate solo dalle persone autorizzate a svolgere tali operazioni e vi deve essere certezza della loro provenienza;
c. **riservatezza o confidenzialità** – le informazioni possono essere fruite solo dalle persone autorizzate a compiere tali operazioni.

Il DPS partendo dall'esame dei trattamenti, dalla distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati e dall'analisi dei rischi, descrive:

a. le misure adottate per garantire l'integrità, la disponibilità, la confidenzialità dei dati;
b. le misure di protezione delle aree e dei locali, rilevanti ai fini della custodia ed accessibilità dei dati;
c. i criteri e le modalità per il ripristino dei dati in seguito a distruzione o danneggiamento;
d. il programma degli interventi formativi per gli incaricati del trattamento.

1.3 Applicabilità

Il presente documento si applica a tutte le attività svolte dal Comune di Lodi che abbiano riflesso sul trattamento dei dati personali.

1.4 Definizioni

AMMINISTRATORE DI SISTEMA: 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. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali; ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

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

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

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA: il soggetto preposto dal titolare alla gestione della sicurezza informatica e non. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è il Sindaco del Comune di Lodi e la titolarità è esercitata dal rappresentante legale, tra i compiti che la legge gli assegna 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. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

1.5 Responsabilità

La legislazione vigente individua una serie di figure preposte all'adozione di misure di sicurezza e alla gestione delle stesse; in particolare nel Comune di Lodi si hanno:

a. il **titolare del trattamento** – la persona giuridica cui competono le decisioni in ordine alle finalità e alle modalità del trattamento di dati personali e agli strumenti utilizzati: nomina i responsabili del trattamento e, nella persona del legale rappresentante, è responsabile anche penalmente dell'adozione delle misure di sicurezza;
b. i **responsabili del trattamento** – sono corresponsabili del titolare, nell'ambito dei trattamenti loro assegnati. Il responsabile del trattamento, designabile facoltativamente, può essere sia una persona fisica che giuridica preposta dal titolare al trattamento dei dati: in ogni caso assicura esperienza, capacità ed affidabilità tali da garantire il pieno rispetto delle "vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza";
c. gli **incaricati del trattamento** – le persone fisiche che, incaricate, effettuano le operazioni di trattamento sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni loro impartite;

d. il **custode delle credenziali** – è il soggetto preposto per iscritto alla custodia delle copie delle credenziali o che ha accesso alle informazioni che concernono le stesse. La normativa impone di individuare preventivamente per iscritto i soggetti incaricati della custodia delle password. L'individuazione e la nomina del custode delle credenziali è una misura minima di sicurezza;

e. l'**amministratore di sistema** - è una figura essenziale per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. È un esperto chiamato a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici.

   Su quest'ultima figura il garante nel gennaio 2009 ha segnalato una criticità emanando le misure e le cautele che seguono:

   - adozione di sistemi di controllo che consentano la registrazione degli accessi effettuati dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici; le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
   - verifica almeno annuale da parte del titolare del trattamento sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali; a tal fine l'amministratore di sistema, invierà al titolare del trattamento entro il 30 Giugno di ogni anno una relazione esplicativa sul proprio operato;
   - inserimento nel documento programmatico della sicurezza degli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite.

1.6 Organigramma della Sicurezza

Si riporta nel seguito l'organigramma relativo alla sicurezza del Comune di Lodi:

- **titolare del trattamento:** Comune di Lodi, nella persona del Sindaco;
- **responsabile del trattamento**: Il Comune di Lodi, titolare del trattamento, ha individuato i responsabili del trattamento, facendoli coincidere con i responsabili dei settori/unità organizzative in cui è articolato l'ente:

Settore/Unità Organizzativa	Resp. trattamento
1 – Amministrazione Generale, Organizzazione e Metodo	Luna Loris
2 – Servizi al Cittadino	Salvarani Giorgio
3 – Economico Finanziario	Depaoli Milena
4 – Affari Culturali	Demuro Giuseppe
5 – Politiche Sociali	Massazza Sabrina
6 - Qualità dell'Ambiente e Sviluppo Sostenibile, Opere Pubbliche	Trabattoni Luigi
7 – Urbanistica, Edilizia e Manutenzione Patrimonio	Ligi Giovanni
8 - Istruzione	De Mattè Marcella
Unità Organizzativa Polizia Municipale, Mobilità	Micciché Salvatore

- **amministratore di sistema:** è il responsabile dell'Ufficio CED, Brambati Paolo, cui vengono affidati i seguenti compiti specifici:
  - creare, sostituire, gestire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dati per l'accesso alla rete informatica comunale, nel rispetto delle massime misure di sicurezza;
  - adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal Dlgs.196/2003 ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware;
  - controllare periodicamente l'efficienza dei sistemi tecnici adottati;
  - prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di backup;
  - assicurarsi della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
  - fare in modo che sia prevista la disattivazione dei codici identificativi personali, 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 per oltre 6 mesi;
  - indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego;
  - provvedere alla nomina e coordinare le attività di uno o più incaricati dell'assistenza e della manutenzione degli strumenti elettronici, a cui conferire i compiti successivamente dettagliati.

- **custode delle credenziali**: Brambati Paolo;

- **incaricati dell'assistenza e della manutenzione degli strumenti elettronici**: Deluca Federica, Mozzi Massimo, ai quali vengono affidati i seguenti compiti specifici:
  - accedere direttamente o da remoto alle postazioni "server" e "client" per eseguire operazioni di installazione e manutenzione degli stessi; tale accesso potrà avvenire tramite credenziali specifiche di tipo "amministrativo", anch'esse a cura del custode delle credenziali;
  - accedere direttamente o da remoto alle banche dati (database), con l'obiettivo di controllarne funzionalità e prestazioni, ma non di consultazione dei contenuti;
  - accedere direttamente o da remoto alle apparecchiature di rete, firewall, stampanti e qualsiasi altra apparecchiatura presente nella rete comunale, per eseguire operazioni di installazione e manutenzione degli stessi.

- **incaricati del trattamento**: ciascun Dirigente, tramite proprio Decreto dirigenziale ed eventuali successive integrazioni, ha nominato gli incaricati, secondo quanto previsto dall'art. 30 DLGS 196/2003). Copia dei suddetti decreti è disponibile presso l'Ufficio del Personale.

1.7 Aggiornamento del piano

Il presente piano è soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo di ogni anno, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 Num. 196.

Inoltre il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo del Comune ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo del Comune tali da dover correggere ed aggiornare i livelli minimi di sicurezza, previa analisi dell'evento e del rischio.

2 Analisi dei rischi

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

- descrizione dell'organizzazione e delle strutture, individuando sinteticamente compiti e responsabilità;
- individuazione di tutte le risorse del patrimonio informativo;
- identificazione dei rischi a cui tali risorse sono sottoposte, con un indicazione della probabilità del verificarsi dell'evento e della gravità delle conseguenze;
- definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
  - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio;
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
  - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

2.1 Descrizione della struttura organizzativa

Struttura	Descrizione dei compiti e delle responsabilità della struttura	Trattamenti effettuati dalla struttura
Settore 1 – Amministrazione Generale, Organizzazione e Metodo		
Uff. Affari Legali	Il servizio si occupa di garantire all'Ente l'assistenza giudiziale e stragiudiziale, nonché di fornire consulenza giuridica ai diversi servizi ed organi del Comune.	Provvede alla tenuta e aggiornamento dell'archivio dei fascicoli contenziosi; cura l'istruttoria dei sinistri e relative richieste di risarcimento danni intrattenendo rapporti con le compagnie assicurative anche per il tramite del broker; provvede alla gestione dei sinistri/pratiche attive in favore dell'Ente; provvede ad affidare incarichi legali e peritali ed al controllo e liquidazione delle parcelle; svolge/affida gli incarichi stragiudiziali per la composizione delle controversie; fornisce consulenza per la prevenzione di contenziosi; gestisce l'aspetto amministrativo delle procedure espropriative

Uff. CED/Sistemi Informativi	L'ufficio CED gestisce tutte le problematiche relative alla manutenzione informatica dell'ente (hardware, software e rete di trasmissione dati) e si occupa anche di risolvere le problematiche relative alla telefonia fissa.	
Uff. Personale	Gestione normativa del personale comunale, gestione della dotazione organica, gestione delle relazioni sindacali, rilevazione presenze ed assenze del personale.	Tenuta fascicolo personale dei dipendenti contenente dati personali e dati sensibili (certificati medici – infortuni, accertamenti sanitari del medico del lavoro – iscrizione organizzazioni sindacali)
Uff. Presidenza del Consiglio Comunale/ Delibere e Determine	Assistenza alle attività del Consiglio comunale e della Giunta comunale e gestione degli atti dirigenziali (pubblicazione delibere/determine).	Supporto ai lavori del Consiglio comunale e dell'ufficio di presidenza (presidente del consiglio comunale e capigruppo), nonché alle funzioni dei consiglieri comunali, gestione atti deliberativi, di Consiglio e di Giunta e atti dirigenziali, organizzazione e gestione attività ed iniziative decise dall'ufficio di presidenza, gestione delle risorse assegnate all'ufficio di presidenza e ai gruppi consiliari, nomine in enti aziende e istituzioni.
Uff.Staff del Sindaco	Coordina tutte le attività del Sindaco della città di Lodi.	Gestione segreteria particolare del sindaco, cerimoniale e celebrazioni, attività della dirigenza di area, dei collegamenti con gli organi di informazione
Uff. Ceprido / Uff. Centro Grafico	Si occupano della produzione e riproduzione di documenti ed atti redatti dai vari uffici del Comune.	
Uff. U.R.P. e comunicazione	Cura il rapporto tra i cittadini, singoli ed associati, e l'Amministrazione comunale, promuovendo ed agevolando la loro partecipazione, ed erogando informazioni al pubblico (via telefono, via mail, direttamente in ufficio); cura la comunicazione pubblica dell'Ente, assicurando la corretta informazione all'opinione pubblica di temi di natura politica e di servizi offerti.	Ricezione di istanze, reclami, segnalazioni riguardanti il territorio comunale ed i servizi; valutazione con gli uffici e risposta alle richieste dei cittadini; direzione del periodico comunale LODICittà; attività editoriali: DVD, CD, volumi, flyers, volantini, manifesti…; collaborazione con l'ufficio stampa nei rapporti con i media (foto, notizie brevi, servizi); cura ed aggiornamento del sito web dell'Ente e dei tre attuali canali del social network (Facebook, Youtube, Twitter) ideati per la comunicazione pubblica; cura ed implementazione dell'archivio fotografico digitale dell'Ente; cura la presenza dell'Ente su riviste e/o elenchi di pubblica utilità (cartacei ed on line)

Uff. Tempi	L'Ufficio tempi gestisce i progetti del Piano Territoriale degli orari (L. 53/2000 e L.R. 28/2004), approvato dal Consiglio comunale.	L'Ufficio tempi ha compiti di: progettazione, gestione operativa e monitoraggio dei progetti decisi dalla Giunta comunale; offrire competenze tecniche sia per gli aspetti orari e temporali, sia per gli aspetti di gestione di reti di attori; partecipare alla definizione e attuazione del Piano Urbano della Mobilità e del Piano di Governo del Territorio; sviluppare un metodo di lavoro trasversale tra gli uffici e i settori del Comune.
Uff. Statistica	L'Ufficio statistica si occupa di elaborare i dati statistici relativi ai servizi demografici: nati, morti, matrimoni, immigrati ed emigrati. Si occupa inoltre di condurre la rilevazione dei consumi delle famiglie italiane, la rilevazione dei prezzi al consumo e delle indagini statistiche curate dall'Istituto Nazionale di Statistica (ISTAT) ed assegnate al Comune per l'esecuzione.	Statistiche sulla popolazione cittadina; indice dei prezzi al consumo; rilevazione prezzi al consumo; ufficio regionale ISTAT
Uff. Stipendi	Gestione delle retribuzioni e degli oneri previdenziali e fiscali del personale comunale dipendente ed ex-dipendente.	Trattamento dati personali e dati sensibili per iscrizioni sindacali e pratiche infortunio.
Settore 2 – Servizi al Cittadino		
Uff. Anagrafe	L'Ufficio anagrafe ha la funzione di registrare nominativamente, secondo determinati caratteri naturali e sociali, gli abitanti residenti nel Comune sia come singoli sia come componenti di una famiglia o componenti di una convivenza, nonché le successive variazioni che si verificano nella popolazione stessa.	Si occupa dei seguenti documenti: statistiche sulla popolazione cittadina, pratiche migratorie, cambi di abitazione, A.I.R.E. (Anagrafe Italiani Residenti all'Estero), carta d'identità, documento di riconoscimento per i minori di 15 anni, autocertificazione, toponomastica.
Uff. Cimiteri	L'Ufficio servizi cimiteriali oltre a dare informazioni sui servizi cimiteriali in generale, svolge tutte le pratiche amministrative relative alle procedure cimiteriali.	Si occupa in particolare di contratti per concessioni cimiteriali, pratiche relative alle cremazioni di residenti, deceduti in Lodi e di deceduti provenienti da altri comuni, programmazione e relative pratiche delle operazioni di esumazione ed estumulazione, verifica contratti tombe di famiglia, collaborazione con il servizio tecnico cimiteriale, ricezione delle imprese di onoranze funebri e loro assistenza, comunicazione ai custodi dei cimiteri civici degli eventuali servizi funebri e operazioni cimiteriali, informazioni relative all'orario di apertura dei cimiteri.

Uff. Elettorale	L'Ufficio elettorale ha la funzione di gestire l'archivio elettorale, ovvero provvede a tenere costantemente aggiornate le liste elettorali provvedendo alla cancellazione degli elettori che hanno perso il diritto di voto, i deceduti e gli emigrati ed iscrivendo gli immigrati, i diciottenni e coloro che hanno riacquistato il diritto di voto. Si occupa inoltre della tenuta degli Albi dei Presidenti di seggio, degli scrutatori, dei Giudici Popolari.	Risultati elettorali, revisione delle liste elettorali, albo dei presidenti di seggio, albo degli scrutatori, compensi ai componenti ai seggi, albo dei giudici popolari.
Uff. Protocollo e Messi	Riceve, protocolla e smista agli uffici interessati gli atti indirizzati all'Amministrazione comunale. Si occupa inoltre della tenuta di Archivio e Albo Pretorio. Provvede alla notificazione degli atti e alla spedizione della posta.	Vigila sulla tenuta dell'Albo Pretorio on line e pubblica solo i documenti pervenuti dall'esterno, gestisce in entrata e smista la documentazione pervenuta su casella di posta elettronica certificata istituzionale dell'ente (PEC), archivia copia di ordinanze e decreti sindacali, vigila sulla formazione e tenuta dell'archivio corrente e di deposito, vigila sulla fascicolazione documentale dei vari uffici, provvede alla consegna delle convocazioni del Consiglio comunale e delle varie commissioni consigliari, riceve il deposito in casa comunale degli atti con destinatari irreperibili da parte di altri enti
Uff. Stato Civile	L'ufficio di Stato Civile ha la funzione di formare gli atti nei quali vanno a confluire i fatti che incidono sullo status dell'individuo. L'Ufficiale di stato civile riceve le dichiarazioni verbali ovvero documenti essenziali relativi all'evento e li riproduce in atti critti o annotati ad altri atti già registrati, che andranno a costituire i Registri di stato civile.	Redazione dei seguenti atti: certificati, estratti e copie integrali, pluralità di nomi, divorzio, matrimonio civile, pubblicazioni di matrimonio, riconoscimento di figlio naturale, matrimoni, cittadinanza, dichiarazioni di morte, dichiarazioni di nascita
Settore 3 – Economico Finanziario		
Uff. Contratti	L'Ufficio offre supporto all'attività contrattuale dei vari servizi, ivi compreso lo svolgimento delle procedure di gara d'appalto.	
Uff. Economato	Il servizio si occupa di programmazione e gestione delle procedure di acquisto ben mobili e di acquisto e distribuzione materiali per uffici.	Gestione magazzino, gestione delle spese economali, gestione della cassa economale, riscossione diritti di segreteria, gestione oggetti e valori ritrovati.

Uff. Ragioneria	Gestione dei pagamenti e delle entrate delle casse del Comune di Lodi.	Il servizio si occupa di programmazione e gestione economico-finanziaria, redazione del bilancio di previsione e della parte contabile del Piano Esecutivo di Gestione (PEG), redazione del conto consuntivo, contabilità finanziaria, contabilità economica, assunzione, gestione ed ammortamento mutui, gestione fiscale, emissione di mandati di pagamento, gestione reversali di incasso, riaccertamento dei residui, controllo degli equilibri finanziari, controllo flussi finanziari per rispetto patto di stabilità, controllo di gestione, finanziamento deliberazioni e determinazioni, controllo finanziario trimestrale, supporto per redazione atti di impegno e liquidazione.
Uff. Tributi	Si occupa di gestione e riscossione dell'ICI e della TARSU	Ricezione di denunce per il conseguente aggiornamento della banca dati in materia di ICI, attività di accertamento e liquidazione e conseguente predisposizione dei relativi provvedimenti, attività di rimborso agli utenti, attività di controllo in merito alla concessione di riduzione e/o agevolazioni, ricezione delle denunce di occupazione e/o detenzione locali ai fini della predisposizione degli avvisi di pagamento in materia di tassa rifiuti, contenzioso tributario.
Settore 4 – Affari Culturali		
Archivio Storico	L'Archivio storico conserva gli atti del Comune di Lodi fino al 1951, suddivisi in: archivio storico municipale, XVI-XIX secolo (581 buste), archivio comunale 1859-1900 (76 buste), archivio storico municipale 1901-1951 (252 buste), registri dell'archivio storico municipale, fondo soccorsi lodigiani alla insurrezione in Sicilia 1860 e avvisi del governo provvisorio di Milano dal 18 marzo al 9 aprile 1848 (una busta), archivio diplomatico di Lodi.	Conservazione documentazione archivistica e redazione degli inventari; servizio agli utenti: consultazione di materiali in sede, supporto alla ricerca per singoli studiosi e gruppi; organizzazione di attività di promozione: incontri, presentazione di libri, mostre; collegamenti e collaborazione con GIONA per digitalizzazione mappe e altro materiale archivistico; formazione e studio; produzione di ricerche su materiale archivistico; organizzazione di convegni di storia e archivistica; incontri con le scuole secondo il progetto "L'Archivio va a scuola"; collaborazione con la Società Storica Lodigiana e l'Istituto lodigiano per la storia della Resistenza e dell'età contemporanea; rapporti con la Regione Lombardia, la Provincia di Lodi e l'Ufficio provinciale scolastico. L'Archivio è sede della Società storica lodigiana, dell'Istituto lodigiano per la storia della Resistenza e dell'età contemporanea.

Biblioteca	E' suddivisa in Biblioteca storica, biblioteca degli adulti (biblioteca di pubblica lettura), nel cui catalogo è conservata una rilevante sezione ottocentesca, e biblioteca dei ragazzi. Il patrimonio della biblioteca è attualmente composto da circa 95.000 volumi facenti parte del fondo moderno, circa 11.000 volumi appartenenti al fondo antico e 350 periodici tra correnti e cessati. Sono ammessi al prestito tutti i volumi del fondo moderno salvo alcune eccezioni (anno di pubblicazione, opere di consultazione, particolari condizioni dei volumi).	Acquisizione e ingressatura volumi, iscrizione, consultazione, prestito, prestito interbibliotecario provinciale e nazionale/internazionale, document delivery, quick reference, community information, emeroteca, servizio riproduzioni, sezione storia locale, deposito legale stampati, attività culturali correlate con il mondo dei libri e delle biblioteche, statistiche, sezioni materiali antichi/microfilmati, bibliografie/book/elenchi novità e spazio novità, gestione spazi web, cooperazione in ambito sistema bibliotecario provinciale.
Centro Donna	Il Centro Donna favorisce l'aggregazione e la partecipazione attiva delle donne. Promuove e organizza attraverso un gruppo di coordinamento, che opera in collaborazione con l'assessorato alle Pari Opportunità, iniziative nell'ambito dei diritti, della cultura, dell'arte, della salute e della creatività. Prevede un tesseramento gratuito che da diritto ad accedere ad agevolazioni e sconti con negozi e ditte convenzionate.	Gestisce tutte le iniziative legate alle donne del Comune di Lodi.
Uff. Cultura	Gestione amministrativa dell'ufficio cultura, del servizio turismo, gestione amministrativa del teatro alle Vigne e delle sue stagioni teatrale, musicale e per ragazzi, organizzazione degli eventi: lodi al sole, rassegna estiva di spettacoli, musica ed iniziative culturali, e i concerti di fine anno; organizzazione delle mostre. Gestione delle sale: sala San Paolo, aula magna del liceo classico Pietro Verri, chiesa dell'Angelo, chiesa di San Cristoforo, aula magna della scuola Spezzaferri; gestione del materiale comunale: palchi, sedie, attrezzature per mostre.	Prenotazione sale, prenotazione del materiale comunale per iniziative culturali, servizio di segreteria.
Centro Informagiovani	L'Informagiovani offre informazione orientativa sui 9 settori di interesse giovanile: scuola e formazione, professioni, lavoro, educazione permanente, vita sociale, cultura e tempo libero, vacanze e turismo, estero, sport.le informazioni sono facilmente autoconsultabili e disponibili in archivi cartacei, bacheche, banche dati, pubblicazioni e guide. Gli operatori sono a disposizione per approfondimenti e per consulenze specifiche	Informazioni per i giovani, Internet Point. Promuove inoltre l e collabora con iniziative promosse dai giovani e per i giovani.

Museo Civico	Il museo civico di Lodi fu costituito nel 1868 con lo scopo di raccogliere e conservare i reperti archeologici rinvenuti nel territorio di Lodivecchio e i dipinti di scuola lodigiana provenienti dalle chiese o dalle raccolte cittadine; consta di tre principali collezioni relative ai materiali archeologici, alla collezione delle maioliche, alla quadreria.	Gestione, cura e valorizzazione delle collezioni del museo civico nell'ambito delle quali vengono svolte le seguenti operazioni: programmazione degli interventi di conservazione e restauro, valutazione e indicazione sulle modalità di incremento e inalienabilità dei beni, predisporre gli atti relativi alla registrazione e alla documentazione, definire periodicamente i criteri in merito all'esposizione permanente e ad eventuali esposizioni temporanee, assicurare la corretta gestione dei prestiti in entrata e in uscita, sviluppare la ricerca scientifica per garantire una migliore comprensione delle collezioni e per migliorare e aggiornare lo stato della loro conoscenza, stabilire, anche in forma temporanea, rapporti con le scuole, le università, con esperti e studiosi avvalendosi delle loro competenze e risorse per conseguire risultati di comune interesse a fini pubblici, garantire il servizio di custodia nell'ambito della sorveglianza degli ambienti, delle collezioni, del primo contatto con l'utenza e il controllo dell'efficienza delle apparecchiature tecniche e degli impianti del museo.
Uff. Sport	Il servizio Sport ha lo scopo di incentivare la pratica sportiva a tutti i livelli, a tutte le età, nelle varie forme possibili. L'Ufficio coopera di fatto quotidianamente con le associazioni sportive del territorio al fine di potenziare le opportunità di accesso alle diverse discipline sportive.	Apertura piscine estive, lodi al sole, sport: corsi gratuiti, contributi ordinari e straordinari, tariffe, assegnazione impianti e gestione calendari impianti e piscine.
Settore 5 – Politiche Sociali		
Uff. Servizi Sociali	Informazione e orientamento sui servizi socio-assistenziali del territorio. Opera principalmente in 3 aree: anziani, adulti in difficoltà, minori.	Servizio civile nazionale, il progetto condominio solidale, informativa sul buono sociale, segretariato sociale, contributi abbattimento barriere architettoniche, sportello affitto, teleassistenza, telesoccorso, telesicurezza, prontobus, trasporti individuali agevolati, assistenza domiciliare, pasti a domicilio, contributi economici, comunità alloggio, inserimenti presso strutture residenziali, sportello stranieri, assegno maternità, asili nido. Il personale addetto mantiene e gestisce dati personali e sensibili per l'istruttoria delle pratiche di propria competenza.

Settore 6 – Qualità dell'ambiente e sviluppo sostenibile – Opere pubbliche		
Uff. Ambiente ed Ecologia	Il servizio tratta problematiche ambientali dal punto di vista amministrativo, con particolare riguardo all'inquinamento atmosferico, acustico, elettromagnetico, del suolo e sottosuolo; coordina il servizio delle Guardie Ecologiche Volontarie; coordina il progetto di attivazione di Agenda 21 Locale.	Comunicazione per taglio piante, richiesta contributi per interventi sugli impianti termici, bonifica di piccoli quantitativi di amianto, lotta agli insetti, piano di zonizzazione acustica, incentivi per l'uso di carburanti gassosi (metano e gpl), autorizzazioni scarichi idrici su suolo e sottosuolo, autorizzazioni ai piani utilizzo agronomico ex l.r. 37/93, autorizzazioni ai piani di bonifica ex d.m. 471/99.
Settore 7 – Urbanistica edilizia e manutenzione patrimonio		
Sportello Unico Attività Produttive e Commercio	Il servizio è competente nelle seguenti materie: commercio su area privata (negozi) e su area pubblica (mercati e fiere); pubblici esercizi (bar, ristoranti); spettacoli, trattenimenti pubblici e giochi (compresi i videogiochi); parrucchieri ed estetisti; taxi e noleggio con e senza conducente; strutture ricettive (alberghi, affittacamere, bed and breakfast); progetti in variante allo strumento urbanistico, con procedura ex. art. 5 del DPR 447/98 e s.m.i.; permessi di costruire, DIA, SCIA per attività economiche, terziario e produttive; impianti di distribuzione carburante; mercati	L'Ufficio gestisce i procedimenti amministrativi necessari per l'esercizio e la cessazione di tali attività (a seconda dei casi, denunce in luogo di autorizzazione o autorizzazioni). In base al d.Lgs. 267/00, inoltre, il dirigente dell'Ufficio emana i provvedimenti sanzionatori contro gli illeciti amministrativi in materia. Rilascio di provvedimenti edilizi in materia commerciale, artigianale, terziario e produttivo.
Uff. Lavori Pubblici	Il settore si occupa di lavori inerenti al patrimonio comunale, il settore acquisisce poi tutti pareri preventivi per la realizzazione delle opere, rilasciati da enti come Asl, comando Vigili del Fuoco, soprintendenza,… , cura anche la manutenzione straordinaria per la cura delle strade e degli edifici pubblici.	Rifacimento di manti stradali, costruzione di nuove strade, piste ciclabili e parcheggi, costruzione di edifici di interesse pubblico come scuole e biblioteche, oltre alla loro messa a norma sia in campo impiantistico che di sicurezza.
Uff. Patrimonio	Gestione e manutenzione di tutto il patrimonio del Comune di Lodi.	Assegnazione e gestione degli alloggi di Edilizia Residenziale Pubblica (ERP), locazione e concessione di beni immobili non residenziali (negozi, box, sedi associazioni, magazzini), acquisizione e vendita di beni immobili, permute di immobili, concessione in uso di suolo pubblico, di aree di proprietà comunale, gestione polizze assicurative servizi comunali, comunalizzazione delle vie, strade e piazze cittadine, locazione di immobili da terzi per eventuali esigenze dell'amministrazione comunale.

Uff. Urbanistica ed Edilizia Privata	Il servizio attua la pianificazione urbana del territorio comunale fissando le direttive generali per l'assetto e l'ordinato sviluppo urbanistico della città, detta le prescrizioni ed i vincoli per l'attività urbanistica ed edilizia, cura l'istruttoria delle pratiche edilizie.	In attuazione del P.G.T., l'ufficio cura la gestione e stesura dei piani attuativi dei Piani integrati di iniziativa privata e pubblica, di nuova edificazione, di recupero e riqualificazione urbana ed ambientale. Istruisce e rilascia i provvedimenti edilizi: permessi di costruire, DIA, SCIA etc. Redige certificati di destinazione urbanistica e provvedimenti in materia edilizia e di pianificazione territoriale.
Uff. Viabilità	L'Ufficio viabilità si occupa della stesura ed adozione dei provvedimenti viabilistici provvisori e permanenti, del rilascio delle autorizzazioni per l'occupazione di suolo pubblico nonché del rilascio dei pareri viabilistici in ordine alla collocazione di: mezzi pubblicitari, arredo urbano, dissuasori di sosta, dissuasori di velocità, cantieri edili, tagli stradali.	Si occupa del rilascio dei contrassegni disabili, della regolarizzazione dei passi carrabili e delle autorizzazioni per il transito di trasporti eccezionali. Attraverso il servizio segnaletica provvede alla realizzazione/manutenzione della segnaletica stradale (verticale ed orizzontale) ed alla gestione della rete semaforica cittadina. L'ufficio viabilità si occupa inoltre del rilascio delle autorizzazioni inerenti la posa da parte dei pubblici esercizi di tavolini, sedie, ombrelloni, ecc.
Settore 8 – Istruzione		
Uff. Istruzione	Il servizio istruzione fornisce servizi di supporto della frequenza scolastica e di sostegno della qualità dell'offerta formativa nelle scuole dell'infanzia, primarie e secondarie di primo grado.	Refezione scolastica, pre/post scuola, assistenza scuolabus, integrazione scolastica alunni diversamente abili, attività e progetti da svolgersi in orario scolastico, contributi a sostegno di iniziative proposte dalle scuole stesse, contributi alle scuole dell'infanzia e primarie private ai fini del trattamento paritario.
Unità Organizzativa Polizia Municipale - Mobilità		
Uff. Polizia Locale	Il servizio ha la finalità di assicurare ai cittadini ed alla città un'attività di prevenzione, controllo e vigilanza sull'osservanza delle norme, delle regole e dei comportamenti, tale da garantire la legittimità e la correttezza della convivenza civile.	Svolge numerose attività, tra cui, interventi inerenti al controllo ed alla disciplina della circolazione stradale, rilevazione degli incidenti stradali e redazione degli atti conseguenti, esercizio delle funzioni ausiliarie di pubblica sicurezza, gestione delle procedure sanzionatorie, pronto intervento in casi di privati e pubblici infortuni, vigilanza in materia di Polizia Giudiziaria, polizia commerciale ed amministrativa, polizia edilizia, iniziative di educazione stradale e corsi per il conseguimento del patentino per il ciclomotore, supporto agli interventi di protezione civile, compiti di rappresentanza dell'ente in occasione di ricorrenze pubbliche e manifestazioni.

2.2 Individuazione delle risorse da proteggere

Le risorse da proteggere sono: banche dati/informazioni; documenti cartacei; hardware; software. Nei paragrafi che seguono vengono elencate e dettagliate tali risorse.

2.2.1 Elenco trattamenti

Finalità perseguita o attività svolta	Categorie di interessati	Natura dei dati trattati	Struttura di riferimento	Altre strutture che concorrono al trattamento[1]
Attività di pubblica sicurezza	Privati, imprese ed enti	Dati personali sensibili/giudiziari	Polizia Locale	
Gestione ambiente	Privati, imprese ed enti	Dati personali sensibili/giudiziari	Uff. Ambiente ed Ecologia	Polizia Locale, Polizia Provinciale
Gestione attività ed iniziative culturali	Privati, imprese ed enti	Dati personali semplici	Uff. Cultura, Museo Civico, Archivio Storico, Informagiovani, Centro donna	
Gestione attività sportive	Privati/ Associazioni sportive	Dati personali sensibili/giudiziari	Uff. Sport	
Gestione certificati anagrafici/stato civile/elettorale	Privati, imprese ed enti	Dati personali sensibili/giudiziari e sanitari	Uff. Anagrafe, Uff. Stato Civile, Uff. Elettorale	Uff. Cimiteri
Gestione clienti e fornitori	Privati, imprese ed enti, associazioni	Dati personali sensibili/giudiziari	Uff. Ragioneria	Uff. Economato, Uff. Contratti
Gestione mense scolastiche/servizi parascolastici	Privati	Dati personali sensibili/giudiziari e sanitari	Uff. Istruzione	Uff. Servizi Sociali, Uff. Dietista
Gestione attività produttive	Privati, imprese ed enti	Dati personali semplici e sensibili/giudiziari	Sportello Unico Attività Produttive e Commercio	Uff. Viabilità, Uff. Tributi, Polizia Locale
Gestione permessi viabilistici	Privati, imprese ed enti	Dati personali semplici e sanitari	Uff. Viabilità	Polizia Locale
Gestione personale	Privati (anche personale dip.), imprese ed enti	Dati personali sensibili/giudiziari	Uff. Personale, Uff. Stipendi	
Gestione pratiche edilizie	Privati, imprese, enti e professionisti	Dati personali semplici e sanitari	Uff. Urbanistica ed edilizia privata, Sportello Unico Attività Produttive e Commercio	Uff. Lavori Pubblici
Gestione pratiche legali/contratti	Privati imprese ed enti	Dati personali sensibili/giudiziari e sanitari	Uff. Affari Legali, Uff. Contratti	Professionisti esterni
Gestione rapporti con il cittadino	Privati	Dati personali semplici	Uff. U.R.P. e comunicazioni	Uffici interessati al problema
Gestione spese ed anticipi economali	Privati, (anche personale dip.)	Dati personali semplici	Uff. Economato	Uff. Ragioneria, Uff. Servizi Sociali
Gestione tematiche sociali	Privati	Dati personali sensibili/giudiziari e sanitari	Uff. Servizi Sociali	Uff. Anagrafe
Gestione tributi	Privati, imprese ed enti	Dati personali semplici	Uff. Tributi	
Manutenzione stabili comunali	Privati, imprese ed enti	Dati personali semplici	Uff. Lavori Pubblici	Uff. Patrimonio, Uff. Contratti
Gestione comunicazioni in ingresso all'Ente	Tutte le categorie	Dati anonimi, dati personali semplici, sensibili/giudiziari	Uff. Protocollo e Messi	

[1] Con "Altre strutture che concorrono al trattamento" si intendono uffici dell'Ente.

Relativamente alla categoria di dati personali sensibili/giudiziari e sanitari, per un miglior dettaglio delle modalità di trattamento, si faccia riferimento alle delibere di Consiglio comunale N. 164 del 19/12/2005 e N. 29 del 20/3/2007.

2.2.2 Trattamenti affidati all'esterno

In conformità al codice, il Comune di Lodi ha affidato/concesso a terzi i seguenti trattamenti di dati personali:

Soggetto esterno	Attività affidata	Banche dati interessate	Natura dei dati trattati
Engineering Tributi Spa	Gestione tributi - Accertamento tributi	ICI e TARSU	Dati personali semplici
Serist S.p.A.	Gestione mense scolastiche	Gestione diete	Dati personali sanitari
G.I.S. Srl (partecipata dal Comune)	Gestione attività sportive	Gestione impianti sportivi	Dati personali semplici
GIONA Srl (partecipata dal Comune)	Gestione attività ed iniziative culturali	Gestione eventi culturali	Dati anonimi
ISAC Spa	Gestione personale - Sorveglianza sanitaria	Dipendenti e collaboratori	Dati personali sanitari
Ufficio del piano di zona (Ente strumentale a supporto dei comuni del piano di zona della provincia di Lodi)	Gestione tematiche sociali	Pratiche Servizi Sociali	Dati personali sensibili/giudiziari

Il Comune di Lodi, in virtù di specifiche autorizzazioni rilasciate dall'ufficiale d'Anagrafe (Settore 2 – Servizi al cittadino), ha inoltre concesso, in conformità al codice, l'accesso remoto alla base dati dell'Anagrafe, per la sola finalità di visualizzazione di dati personali semplici; segue elenco:

- Engineering Tributi Spa;
- ASL di Lodi;
- ATM di Milano;
- Comando dei Carabinieri di Lodi;
- Comando della Guardia di Finanza di Lodi;
- Inail di Lodi;
- INPS di Lodi;
- Questura di Lodi;
- Tribunale di Lodi;
- Motorizzazione Civile di Lodi;
- Prefettura di Lodi;
- Consorzio lodigiano servizi alla persona.

2.2.3 Architettura del Sistema Informatico**2**

Collegati alla rete, sussistono n° 288 personal Computer, suddivisi come segue:

- N 14 server dotati di sistema operativo Microsoft Windows Server 2000/2003/2008 e Redhat Enterprise Linux Server 5.2;
- N° 257 PC desktop dotati di sistema operativo Microsoft Windows XP Professional;
- N° 17 PC portatili dotati di sistema operativo Microsoft Windows XP Professional.

2.2.3.1 Connettività Internet[3]

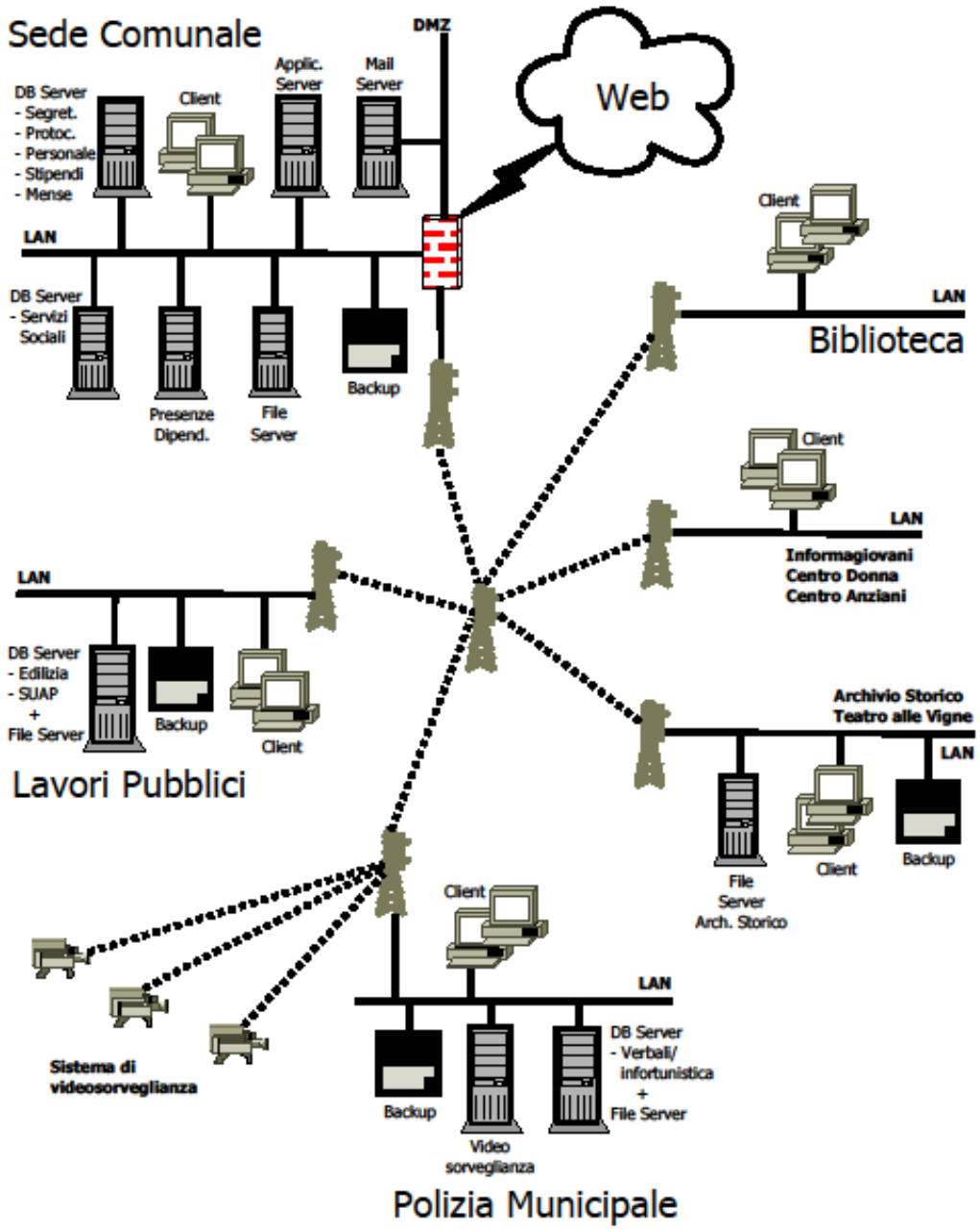
Sede	Connettività	Apparecchiature di comunicazione	Provider
Sede Comunale	HDSL (8Mb bmg 4Mb)	Router Cisco	Telecom
	HDSL (2Mb bmg 1Mb)	Router Cisco	Telecom
Polizia Locale	ADSL (20Mb/96F)	Router Thomson	Telecom
Asilo Salvemini, Asilo Volturno	ADSL (1,2Mb/256F)	Router Thomson	Telecom
Cimitero Maggiore, Cimitero Riolo	ADSL (1,2Mb/256F)	Router Thomson	Telecom
Biblioteca (sede provvisoria)	ADSL (1,2Mb/256F)	Router Thomson	Telecom
Informagiovani (Internet point)	ADSL (1,2Mb/256F)	Router Thomson	Telecom

2.2.3.2 Rete di trasmissione dati

La rete di trasmissione dati del Comune di Lodi utilizza un sistema HyperLan con un centro stella, attraverso il quale vengono messe in comunicazione le seguenti sedi:

- Sede comunale – piazza Broletto 1;
- Lavori Pubblici – piazzale Forni, 1;
- Polizia Municipale – via Cadamosto, 13
- Biblioteca Comunale[4] – corso Umberto I, 63
- Archivio Storico – via Fissiraga, 17
- Teatro alle Vigne – via Cavour, 66
- Centro Informagiovani – via Gorini, 21
- Centro donna – via delle Orfane, 12
- Centro anziani – via Volturno, 4

[2] Per ragioni di sicurezza non vengono riportate informazioni specifiche riguardanti le singole apparecchiature informatiche.
[3] Le apparecchiature di comunicazione sono in comodato d'uso ed il provider detiene le password per la configurazione e la manutenzione delle stesse.
[4] La Biblioteca, attualmente nella sede provvisoria di via S. Francesco n. 13, verrà reinserita nella rete al termine dei lavori di ristrutturazione della sede ufficiale (corso Umberto I, 63), previsto per dicembre 2011.



2.2.3.3 Soggetti esterni manutentori dei sistemi

La manutenzione ordinaria delle apparecchiature informatiche del Comune di Lodi è a carico dell'Ufficio CED; in occasione di eventi di carattere straordinario, ad esempio un guasto hardware o un problema segnalato dall'utente relativo ad un software applicativo, ad alcuni fornitori è contrattualmente concesso l'accesso remoto alle risorse (Server ed apparecchiature di rete). In conformità alla regola N° 25 del "Disciplinare tecnico in materia di misure minime di sicurezza" (vedi par. 3.1 del presente documento), terminato l'intervento il fornitore è tenuto ad inviare, all'Ufficio CED del Comune, una comunicazione riportante:

- una breve sintesi dell'intervento effettuato;
- il modulo software e/o l'apparecchiatura oggetto dell'intervento;
- il nominativo del tecnico manutentore.

Segue l'elenco dei soggetti autorizzati e delle risorse alle quali hanno facoltà di accedere:

Azienda	Ambito della manutenzione	Tipo connessione	Login dedicata
ADS Spa	Software Segreteria, Protocollo, Anagrafe, Stato Civile, Mense, Contabilità, Pianificazione Strategica	RDP	SI
Artech Srl	Software rilevazione/gestione presenze	TeamViewer	SI
Gruppo Marche	Software cimiteriali	Teamviewer	SI
Italsoft Srl	Software Lavori Pubblici	Teamviewer	SI
Koinè Sistemi Srl	Manutenzione sala Consiglio	Teamviewer	SI
Maggioli Spa	Software gestione multe e verbali	Client dedicato	SI
Starch Srl	Software edilizia privata	Client dedicato	SI
Tecnosys Srl	Software gestione patrimonio	Teamviewer	SI
Telecom Italia	Manutenzione router linee di comunicazione	Telnet sui router	SI
Gemma	Manutenzione centralino Polizia Locale	Client dedicato	SI
Antelma	Manutenzione centralino Sede Municipale	Client dedicato	SI
Telcom	Manutenzione centralino Lavori Pubblici	Client dedicato	SI

2.3 Individuazione ed identificazione dei rischi

I rischi ipotizzabili sono elencati qui di seguito (come suggerito dalla "Guida operativa per redigere il DPS" prodotta dal Garante):

1 Comportamenti degli operatori

1.1 Sottrazione di credenziali di autenticazione;

1.2 carenza di consapevolezza, disattenzione o incuria;

1.3 comportamenti sleali o fraudolenti quali l'alterazione dolosa della correttezza e della esattezza o modifica intenzionale dei dati trattati;

1.4 errore materiale consistente nell'alterazione della correttezza e della esattezza o modifica non volontaria né controllata dei dati trattati, dovuta a carenza di consapevolezza, disattenzione, incuria o, anche, a carenze nella documentazione operativa (manuali per l'utilizzo dei programmi informatici, procedure, ecc.);

1.5 altro evento quali ad esempio il trattamento non autorizzato, cioè un trattamento effettuato in mancanza del consenso dell'interessato e/o non elencato nell'informativa.

2 Eventi relativi agli strumenti

2.1 Azione di virus informatici o di programmi suscettibili di recare danno ed in particolare di software programmato al fine di poter svolgere operazioni non autorizzate sul sistema informatico o per danneggiare lo stesso; sono compresi in questa categoria anche gli attacchi di tipo denial of service, che saturano la capacità di risposta di un servizio con l'obiettivo di renderlo inutilizzabile agli altri utenti del sistema;

2.2 spamming o tecniche di sabotaggio;

2.3 malfunzionamento, indisponibilità o degrado degli strumenti dovuti a malfunzionamento dell'hardware che impedisce l'accesso agli archivi che contengono dati personali o provoca la perdita degli stessi; cattivo funzionamento o blocco totale di servizi con conseguenti danni al sistema informatico;

2.4 accessi esterni non autorizzati con l'introduzione nel sistema informatico da parte di persone non autorizzate (interne e/o esterne) tramite superamento delle procedure di autenticazione e meccanismi di sicurezza;

2.5 intercettazione di informazioni in rete attraverso l'introduzione nel sistema informatico da parte di persone non autorizzate tramite rete di telecomunicazione;

2.6 altro evento quale ad esempio l'impossibilità di ripristinare i dati personali a fronte di una loro alterazione o perdita.

3 <u>Eventi relativi al contesto</u>

3.1 Accessi non autorizzati a locali ad accesso ristretto;

3.2 sottrazione di strumenti contenenti dati come ad esempio il furto di hardware e supporti di memorizzazione contenenti archivi di dati personali o di documentazione cartacea;

3.3 eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.) nonché dolosi, accidentali o dovuti ad incuria;

3.4 guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.);

3.5 errori umani nella gestione della sicurezza fisica (porte dimenticate aperte, armadi non chiusi, PC lasciato incustodito, ecc..).

L'entità dei rischi è stata valutata utilizzando il seguente criterio:

indicando con:
P = la *probabilità* del verificarsi dell'evento pericoloso;
G = la *gravità* delle conseguenze che l'evento pericoloso determinerebbe;

l'**entità del rischio** sarà uguale a:
R = **P x G** (prodotto della *probabilità* per *la gravità)*

In questa formula al parametro **P** sono stati assegnati i valori numerici da 1 a 4 secondo la probabilità di accadimento valutata con riferimento all'attuale organizzazione delle attività:

1 = Improbabile **2** = Poco probabile **3** = Probabile **4** = Altamente probabile

L'indice di probabilità, nonostante l'obiettivo sia fornire un'espressione quantitativa dell'entità del rischio, si fonda sull'identificazione soggettiva diretta della probabilità di accadimento, in quanto le variabili in gioco non sono trattabili ricorrendo a modelli matematici o probabilistici e si riferiscono ad eventi non stimabili statisticamente sulla base di dati appositamente acquisiti.

Nella seguente tabella ad ogni valore di probabilità viene associato un livello e più definizioni o criteri di giudizio.

SCALA DELLE PROBABILITÀ "**P**"

Valore	Livello	Definizioni / criteri
4	Altamente probabile	• Esiste correlazione diretta fra l'organizzazione dell'Ente ed il verificarsi dell'evento; • si sono già verificati spesso eventi dello stesso tipo nell'Ente o in Enti simili.
3	Probabile	• Data l'organizzazione dell'Ente l'evento ipotizzato può verificarsi, anche se non in modo automatico o diretto; • è noto qualche episodio in cui l'evento ipotizzato si è verificato.
2	Poco probabile	• Data l'organizzazione dell'Ente l'evento ipotizzato può verificarsi solo in circostanze sfortunate; • sono noti solo rarissimi episodi in cui l'evento ipotizzato si è già verificato.
1	Improbabile	• Data l'organizzazione dell'Ente l'evento ipotizzato può verificarsi solo per la concomitanza di fattori poco probabili e indipendenti; • non sono noti episodi in cui l'evento ipotizzato si è già verificato.

Al parametro **G**, che nel nostro caso non è esprimibile in termini di mero danno economico, sono stati dati valori numerici da 1 a 4 tenendo conto sia degli effetti del trattamento indebito del dato personale sia delle conseguenze che ne potrebbero derivare all'Ente, quali, a puro titolo esemplificativo:

- sanzioni penali irrogate al titolare del trattamento;
- sanzioni amministrative comminate all'Ente;
- richieste di risarcimento di danni patrimoniali e non patrimoniali;
- blocco del trattamento ad opera dell'Autorità giudiziaria o del Garante per la protezione dei dati personali;
- lesione dell'immagine pubblica dell'Ente a seguito della pubblicità negativa sui media conseguente al verificarsi di tali fatti (per effetto di denunce, condanne, citazioni in giudizio, ecc.): per esempio per l'omessa o inidonea informativa è applicabile (ex art. 165 del Codice privacy) anche la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione sulla stampa.

SCALA DELLA GRAVITÀ DEL DANNO "**G**"

Valore	Livello
4	**Gravissimo**
3	**Grave**
2	**Medio**
1	**Lieve**

I risultati dell'analisi sono riepilogati nella tabella che segue:

Rischio		P	G	R
Comportamenti degli operatori	1.1 Sottrazione di credenziali di autenticazione	1	4	**4**
	1.2 Carenza di consapevolezza, disattenzione o incuria	3	3	**9**
	1.3 Comportamenti sleali o fraudolenti	1	4	**4**
	1.4 Errore materiale	2	2	**4**
	1.5 Trattamento non autorizzato	2	1	**2**
Eventi relativi agli strumenti	2.1 Azione di *virus* informatici	1	3	**3**
	2.2 *Spamming* o tecniche di sabotaggio	2	2	**4**
	2.3 Malfunzionamento, indisponibilità o degrado degli strumenti	2	2	**4**
	2.4 Accessi esterni non autorizzati	1	3	**3**
	2.5 Intercettazione di informazioni in rete	1	2	**2**
	2.6 Impossibilità di ripristinare i dati personali	2	4	**8**
Eventi relativi al contesto	3.1 Accessi non autorizzati a locali ad accesso ristretto	1	3	**3**
	3.2 Sottrazione di strumenti contenenti dati	1	3	**3**
	3.3 Eventi distruttivi	1	4	**4**
	3.4 Guasto ai sistemi complementari	1	3	**3**
	3.5 Errori umani nella gestione della sicurezza fisica	2	2	**4**

Sono state infine individuate tre fasce dell'entità del rischio che comportano necessità di interventi correttivi o migliorativi con diversa caratteristica di urgenza, delle quali si terrà conto in sede di definizione delle contromisure da adottare:

rischio **basso**: $1 \leq R \leq 4$ $\Rightarrow$ azioni migliorative e/o di mantenimento da valutare in fase di programmazione

rischio **medio**: $5 \leq R \leq 8$ $\Rightarrow$ azioni correttive o migliorative da programmare a medio termine

rischio **alto**: $9 \leq R \leq 16$ $\Rightarrow$ azioni correttive da programmare a breve termine

3 Misure di prevenzione e protezione adottate

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce.

Si riporta nel seguito l'elenco delle misure minime, definite sulla base di quanto riportato nel "Disciplinare tecnico in materia di misure minime di sicurezza" (Allegato "B" al D.lgs 196/2003); per ogni voce presente in tabella viene indicato se già "in essere" o se è una misura da adottare in futuro (in quest'ultimo caso, per avere un'indicazione temporale in merito, si faccia riferimento al paragrafo denominato "piano operativo").

3.1 Trattamenti con l'ausilio di strumenti elettronici

Misura		Rischi contrastati	misura già in essere	misura da adottare
Sistema di autenticazione informatica				
Reg. 1	Credenziali e procedura di autenticazione	1.1 - 1.3 - 1.5	X	
Reg. 2	Codice di identificazione personale e parola chiave riservata		X	
Reg. 3	Credenziali individuali		X	
Reg. 4	Istruzioni di diligente custodia			X
Reg. 5	Lunghezza della password pari a 8 caratteri o pari al massimo consentito dal sistema			X
	Controllo sulla complessità delle password			X
	Modifica password al primo accesso			X
	Possibilità di sostituzione autonoma della password		X	
	Scadenza della password per dati sensibili e giudiziari entro 3 mesi			X
Reg. 6	Il codice identificativo deve essere univoco		X	
Reg. 7	Scadenza delle credenziali non utilizzate da 6 mesi			X
Reg. 8	Disattivazione delle credenziali in caso di perdita della qualità per l'accesso		X	
Reg. 9	Istruzioni per l'incaricato a non lasciare incustodito lo strumento elettronico in caso di prolungata assenza dal posto di lavoro	1.2 – 3.5 - 3.2	X	
Reg. 10	Gestione delle credenziali in caso di prolungata assenza o impedimento dell'incaricato per la disponibilità dei dati o degli strumenti elettronici	1.3 – 1.5	X	
Reg. 11	Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione	--	X	
Sistema di autorizzazione				
Reg. 12	Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione	1.4	X	
Reg. 13	Assegnazione dei profili per utente o classi omogenee di utenti anteriormente all'inizio del trattamento		X	
Reg. 14	Verifica della sussistenza delle condizioni per la conservazione dei profili (almeno annualmente)		X	

Altre misure di sicurezza				
Reg. 15	Individuazione con cadenza almeno annuale della lista degli incaricati anche organizzata per classi omogenee di incarico e relativi profili di autorizzazione	1.5		X
Reg. 16	Protezione dei dati dal rischio di intrusione e dall'azione di programmi pericolosi – Antivirus (aggiornamento almeno semestrale)	2.1 – 2.2 – 2.4 – 2.5	X	
Reg 17	Programmi per elaboratore atti a prevenire vulnerabilità degli strumenti elettronici aggiornati almeno annualmente, o semestralmente per i dati sensibili o giudiziari	2.3	X	
Reg. 18	Istruzioni organizzative e tecniche che prevedono il salvataggio dei dati almeno settimanalmente (backup dei database, documenti in formato elettronico, …)	2.3 – 2.6 – 3.3 - 3.4	X	
Reg. 19	Redazione annuale del Documento Programmatico sulla Sicurezza	--	X	
Ulteriori misure in caso di trattamento di dati sensibili e giudiziari				
Reg. 20	Protezione dei dati sensibili e giudiziari contro l'accesso abusivo di cui all'art. 615-ter, mediante utilizzo di strumenti elettronici	--	X	
Reg. 21	Controllo sull'utilizzo dei supporti rimovibili di memorizzazione (es. chiavette USB) ad evitare l'accesso non autorizzato o il trattamento non consentito	3.2		X
Reg. 22	Distruzione dei supporti rimovibili non più utilizzati contenenti dati sensibili / giudiziari o riutilizzo solo se le informazioni precedentemente contenute non possono essere tecnicamente ricostruibili	1.2 - 3.2	X	
Reg. 23	Misure di ripristino per l'accesso ai dati in caso di danneggiamento degli stessi e degli strumenti in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni	2.3 – 2.6 – 3.3 - 3.4		X
Reg. 24	Cifratura, codici identificativi o separazione dei dati su sistemi distinti per il trattamento dei dati sensibili e giudiziari atti a prevenire l'accesso a persone prive di autorizzazione.	1.3 – 1.5	X	
	Locali attrezzati di opportune misure di sicurezza per il trattamento di dati idonei a rilevare l'identità genetica degli interessati.	N/A	N/A	N/A
	Il trasporto all'esterno dei dati genetici deve avvenire solo con contenitori muniti di serratura.	N/A	N/A	N/A
	Il trasferimento dei dati in formato elettronico dei dati genetici è cifrato.	N/A	N/A	N/A
Misure di tutela e garanzia				
Reg. 25	I soggetti esterni che effettuano attività di installazione/manutenzione dei sistemi da remoto inviano comunicazione scritta relativa all'intervento, attestandone la conformità alla presente regola	2.4		X
Reg. 26	Attestazione di Avvenuta redazione del DPS e citazione nella relazione accompagnatoria del bilancio d'esercizio (se dovuta).	--	X	

3.2 Trattamenti senza l'ausilio di strumenti elettronici

Misura		Rischi contrastati	misura già in essere	misura da adottare
Reg. 27	Istruzioni per l'incaricato atte al controllo e custodia degli atti e documenti. Mantenimento di un aggiornato elenco degli incaricati e del loro profilo di autorizzazione con cadenza annuale	1.2	X	

Reg. 28	Istruzioni per la custodia e il controllo di atti e documenti contenenti dati sensibili o giudiziari	1.2	X	
Reg. 29	Controllo di accesso agli archivi contenenti dati sensibili o giudiziari	3.1	X	
	Le persone autorizzate all'accesso fuori dall'orario di ufficio sono individuate e registrate	3.1	X	
	In mancanza di strumenti elettronici per il controllo degli accessi nei locali o di personale di vigilanza, le persone abilitate all'accesso sono preventivamente autorizzate.	3.5	X	

3.3 Contromisure specifiche

Il Comune di Lodi, per raggiungere un livello di protezione adeguato ai trattamenti che svolge, ha inoltre stabilito quanto segue:

- le apparecchiature informatiche critiche utilizzate per il trattamento dei dati personali/sensibili/giudiziari (Database Server, Server di rete…) e le apparecchiature di telecomunicazione verso il mondo esterno (modem, router…) sono situati in un locale apposito ad accesso controllato e chiuso a chiave, denominato "locale CED"; le chiavi del locale CED sono custodite a cura del personale dell'ufficio; è inoltre prevista l'installazione nel locale CED di un sistema di allarme antincendio, di pareti e porta tagliafuoco/anti-intrusione e di un sistema di apertura porta/rilevazione degli accessi automatizzato;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal responsabile del trattamento o da un suo delegato;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati cartacei sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'incaricato del trattamento di tali dati;
- utilizzo di server con configurazioni di ridondanza (dischi, scheda di rete, alimentatori);
- presenza di un gruppo di continuità elettrica da 16 KW per l'intera sala server;
- attivazione di un sistema di backup centralizzato ed automatizzato su dischi rigidi di rete per i dati dei server con periodicità settimanale e storico quindicinale; non appena possibile, tali supporti verranno posizionati in un locale ad accesso controllato differente dalla sala server e con caratteristiche di sicurezza non inferiori a quest'ultima;
- presenza di un firewall di tipo hardware dedicato (FORTINET A200a) per proteggere la rete dagli accessi indesiderati attraverso internet;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, gestito e configurato centralmente, per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza giornaliera e la scansione sia periodica che in tempo reale dei supporti di memoria.

3.4 Piano operativo

In relazione all'analisi dei rischi e alle misure di prevenzione riportate nel presente capitolo, è stato predisposto il programma operativo, illustrato nel seguito.

Anomalia da risolvere	Tempo di risoluzione		
	Immediato	Entro tre mesi	Entro sei mesi
Istruzioni di diligente custodia delle password - regole 4 delle misure minime di sicurezza	X		
Adozione nuova politica per la gestione delle password personali – regole 5 e 7 delle misure minime di sicurezza			X
Definizione della lista degli incaricati ai trattamenti, organizzata per classi omogenee di incarico e relativi profili di autorizzazione – regola 15 delle misure minime di sicurezza	X		
Controllo sull'utilizzo dei supporti rimovibili di memorizzazione – regola 21 delle misure minime di sicurezza			X
Misure di ripristino per l'accesso ai dati in caso di danneggiamento degli stessi e degli strumenti in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni - regola 23 delle misure minime di sicurezza			X
Ricezione comunicazione descrittiva dell'intervento sistemistico effettuato da soggetti esterni - regola 25 delle misure minime di sicurezza			X
Allarme antincendio, pareti e porta tagliafuoco anti-intrusione e rilevazione accessi per la protezione del locale CED			X

4 Gestione degli incidenti e modalità di ripristino dei dati

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile del trattamento dei dati o l'amministratore di sistema nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti).

Contemporaneamente, l'amministratore di sistema e gli incaricati dell'assistenza e della manutenzione degli strumenti elettronici devono monitorare costantemente i sistemi, al fine di individuare le seguenti:

- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

Prendendo atto del fatto che sussiste una violazione della legge o il mancato rispetto di norme comportamentali del personale, l'amministratore di sistema o i dirigenti competenti, sulla base delle evidenze in loro possesso, hanno la facoltà di aprire formalmente un "incidente", al quale farà seguito una procedura atta al ripristino della normale operatività.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone[5];
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente; una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;
4. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, l'eventuale ripristino dei dati può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali, a partire dalle ultime copie di backup ritenute valide. Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti; la successiva fase di indagine e di ripristino del sistema sarà condotta da personale autorizzato, tenendo presente quanto sotto indicato:

- eseguire una copia "bit a bit" degli hard disk del sistema compromesso;
- se l'incidente riguarda i dati, il recupero degli stessi può avvenire a partire dalle ultime copie di backup ritenute valide;
- se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software malevolo (malware, spyware, troian…) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

[5] Nel caso in cui l'incidente sia conseguente ad un evento che possa mettere a rischio l'incolumità delle persone (ad esempio un incendio o un'alluvione).

Si ricorda inoltre che l'amministratore di sistema, per poter effettuare le attività di verifica sopra riportate, ha a disposizione strumenti di tracciamento delle connessioni ai sistemi informatici e delle operazioni effettuate (registro elettronico delle attività o file di log), i cui output possono essere soggetti ad indagini, nel rispetto sia di quanto sancito dal D.L.vo 30 giugno 2003, n. 196, sia dell'art. 4 dello Statuto dei Lavoratori, ovvero il "... divieto di utilizzo da parte del datore di lavoro di apparecchiature atte al controllo a distanza dell'attività del lavoratore, salvo che esigenze organizzative, produttive o di sicurezza non abbiano determinato, previo accordo con le rappresentanze sindacali, la lecita introduzione in azienda".

5 Norme per il personale

Tutti i dipendenti concorrono alla realizzazione della sicurezza e pertanto sono tenuti a proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa.

A tale scopo, il Comune di Lodi ha formalizzato una serie di regole di comportamento per il corretto utilizzo delle apparecchiature informatiche, nel seguito riportate.

Tali regole riguardano inoltre le figure informatiche (amministratore di sistema e incaricati dell'assistenza e della manutenzione delle apparecchiature elettroniche), nel corso dello svolgimento delle attività di manutenzione ordinaria e straordinaria.

Sono state classificate nei seguenti tre gruppi:

- Regole per la gestione di strumenti elettronico/informatici.
- Regole di comportamento per minimizzare i rischi da virus.
- Regole per la gestione delle password.

5.1 Regole per la gestione di strumenti elettronico/informatici

Per l'accesso a server (anche tramite la rete telematica) o archivi con dati personali, devono essere rispettate le seguenti misure:

- le condivisioni totali o parziali dei dischi delle postazioni di lavoro sono vietate; l'eventuale condivisione delle risorse dovrà avvenire utilizzando opportune cartelle di rete (sul file server) suddivise per attività/ufficio; tale modalità di lavoro permette la possibilità di effettuare copie di salvataggio dei dati e riduce la possibilità di diffusione dei virus informatici;
- gli hard disk non devono essere condivisi in rete; per operazioni temporanee di copia verranno predisposte opportune aree di "scambio";
- tutte le operazioni effettuate on-site o da remoto dalla ditta che sostiene la manutenzione dei sistemi devono avvenire previa autorizzazione dell'amministratore di sistema o da un suo incaricato, secondo quanto previsto dall'organigramma della sicurezza;
- le copie di backup realizzate su dischi esterni vanno conservate in luoghi chiusi a chiave ed accessibili solo al personale del CED;
- divieto di utilizzare floppy disk o chiavette USB come mezzo per il backup;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito ed accessibile lo strumento elettronico stesso. l'utente che abbandona la postazione è invitato a bloccarla tramite opportuna combinazione di tasti (ctrl+alt+canc) in modo che al suo ritorno vengano richieste le credenziali di accesso alla rete;
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro, non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di consultazione di siti web o di utilizzo di posta elettronica durante il normale orario di lavoro, quando tale attività non sia pertinente con le mansioni affidate, come l'art. 1024 del codice civile prevede nel principio generale di diligenza del lavoratore;

- il controllo dei documenti stampati è responsabilità degli incaricati al trattamento;
- la stampa di documenti contenenti dati personali o sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato; prossimamente il controllo verrà integrato con codici di autorizzazione per le stampe riservate;
- la manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che i supporti di memorizzazione interni (hard disk) vengano preventivamente svuotati degli eventuali dati personali o sensibili; nel caso in cui ciò non fosse possibile, per esempio causa guasto del supporto, quest'ultimo deve essere comunque rimosso;
- lo smaltimento di apparecchiature obsolete deve essere effettuato in modo che non sussista il rischio di rilasciare all'esterno informazioni riservate o addirittura dati personali o sensibili; pertanto si raccomanda la rimozione o quantomeno la cancellazione fisica dei dati presenti sugli hard disk dei personal computer in smaltimento e la deconfigurazione (reset) delle apparecchiature di rete in smaltimento (tipicamente router che vengono sostituiti a fronte di modifiche dell'infrastruttura di rete).

5.2 Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei personal computer devono adottare le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, dvd, chiavette usb);
- controllare (scansionando con il software antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti; a tal scopo deve essere mantenuta attiva la funzionalità di "auto-protect" sia per il file system sia per la posta elettronica;
- evitare l'uso di programmi di pubblico dominio (freeware, shareware…), ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non;
- attivare la protezione massima per gli utenti del programma di posta elettronica, al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con il software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto e l'antivirus non sia riuscito ad effettuarne la disattivazione/rimozione.

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore di sistema, o gli incaricati dell'assistenza e della manutenzione degli strumenti elettronici, procedono a reinstallare il sistema operativo, i programmi applicativi ed a recuperare i dati dai backup, seguendo la procedura indicata:

- formattare l'Hard Disk, definire le partizioni e reinstallate il sistema operativo, utilizzando i CD di ripristino del produttore; a tale scopo i CD di ripristino devono essere custoditi presso l'Ufficio CED, in modo che siano immediatamente disponibili per questo tipo di attività;
- installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il ripristino dei soli dati a partire da una copia di backup recente; nessun programma eseguibile deve essere ripristinato dalla copia di backup;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti alla ripresa del lavoro.

Al fine di velocizzare la procedura di ripristino sopra riportata, tutte le componenti devono essere immediatamente disponibili al personale dell'Ufficio CED che si farà carico di custodire, in appositi raccoglitori:

- i dischi di ripristino del sistema operativo di tutti i computer del Comune;
- le copie originali di tutti i programmi applicativi utilizzati e l'eventuale copia di backup consentita per legge;
- le copie originali di tutti i programmi applicativi licenziati ed utilizzati dal personale del Comune;
- le copie di tutti i driver delle periferiche, quali stampanti, schede di rete, monitor, ecc…

5.3 Regole per la gestione delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.

- User-id e password iniziali sono assegnati dal custode delle password, sono strettamente personali e non possono essere riassegnate ad altri utenti;
- la User-id è costituita dall'iniziale del nome e dal cognome completo, con un punto di separazione tra essi. In caso di omonimia si procede con le successive lettere del nome, sino alla risoluzione dell'omonimia;
- il custode delle password comunica la password iniziale all'incaricato; detta password, composta da 8 caratteri alfanumerici, non contiene elementi facilmente ricollegabili all'organizzazione o almeno alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema;
- le password di amministratore di tutti i Server e PC che lo prevedono sono assegnate dall'Amministratore di sistema e sono conservate in busta chiusa in apposito armadio ignifugo;
- in caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.

Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili.

Per la definizione/gestione della password devono essere rispettate le seguenti regole:

- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;

- deve contenere almeno un carattere alfabetico ed uno numerico;
- deve essere diversa dalla User-id;
- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- la nuova password non deve essere uguale ad una delle due precedenti;
- la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina dopo sei mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia, comunicando all'amministratore di sistema l'anomalia.

5.4 Sanzioni

Il mancato rispetto delle norme può comportare responsabilità civili e penali per i danni cagionati in relazione al trattamento dei dati personali; a titolo di esempio si possono elencare:

- la responsabilità civile disciplinata dall'art. 2050 del Codice Civile e art. 15 D.Lgs. 196/03, ovvero "chi cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo";
- la sanzione penale che colpisce chi, essendovi tenuto, omette di adottare le misure di sicurezza (art. 169 del D.Lgs. 196/03), pari all'arresto fino a due anni o ad ammenda da 10mila a 50mila euro, ma con estinzione del reato in caso di regolarizzazione entro 6 mesi dall'accertamento del reato e pagamento di somma determinata dal Garante.

6 Piano di formazione degli incaricati

La formazione degli incaricati deve essere effettuata all'ingresso in servizio o in conseguenza della nomina o successivamente all'installazione di nuovi strumenti per il trattamento dei dati.

Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali/sensibili/giudiziari;
- proporre buone pratiche di utilizzo sicuro della delle apparecchiature informatiche e della rete (vedi capitolo “Norme per il personale”);
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

Il corso di formazione prevede un programma minimo, comprendente i seguenti argomenti:

- Introduzione alla normativa sulla privacy.
- Principi generali:
  - diritto alla protezione dei dati personali;
  - definizioni;
  - modalità del trattamento e requisiti dei dati.
- Diritti dell’Interessato:
  - diritto di accesso ai dati personali ed altri diritti;
  - modalità di esercizio dei diritti;
  - riscontro all’interessato.
- Ruoli soggettivi:
  - Titolare, responsabile e incaricati del trattamento;
- Sicurezza dei dati e dei sistemi:
  - obblighi di sicurezza: misure idonee;
  - misure minime di sicurezza (allegato B: Disciplinare tecnico in materia di misure minime di sicurezza):
    - trattamenti con strumenti elettronici;
    - trattamenti senza l’ausilio di strumenti elettronici.
- Norme per il corretto utilizzo delle apparecchiature informatiche.
- Sanzioni penali, amministrative e conseguenze civili.

7 Videosorveglianza

Nell'esercitare attività di videosorveglianza, viene rispettato il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti, in particolare si precisa che:

- il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
- l'attività è svolta per la prevenzione di un pericolo concreto o di specifici reati e solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

- sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- è scrupolosamente rispettato il divieto di controllo a distanza dei lavoratori;
- sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
- il periodo di conservazione dei dati è limitato allo stretto necessario e non eccede mai i 7 giorni.

La conservazione dei dati oltre il termine dei 7 giorni è possibile solo in relazioni al verificarsi di illeciti o quando siano in corso indagini giudiziarie.

I dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.

Ogni ulteriore precisazione sull'attività di videosorveglianza è regolata dagli appositi regolamenti emessi dal comando di polizia locale, competente in materia (si faccia a tal proposito riferimento al "Regolamento per l'utilizzo di impianti di videosorveglianza del territorio", approvato con delibera del Consiglio Comunale n. 76 del 16/7/2007 e successive integrazioni).