Comune di Montevarchi

Documento programmatico
sulla sicurezza dei dati

D.Lgs. 196/2003

INDICE

1 Introduzione

Il presente **Documento programmatico sulla sicurezza** definisce lo stato di attuazione nel comune di Montevarchi per quanto disposto dal D. Lgs. 30 giugno 2003 n° 196 Codice in materia di protezione dei dati personali agli articoli 31, 33, 34 e 35 e dal Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Codice).

Il contenuto di quanto segue si riferisce alla struttura organizzativa e funzionale del Comune di Montevarchi in riferimento a quanto stabilito dal Regolamento Comunale sull'ordinamento degli uffici e dei servizi.

Sulla stessa materia il Comune di Montevarchi aveva provveduto sulla base di quanto disposto dal DPR 318/99, "*Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali a norma dell'art. 15 comma 2, della Legge 31/12/1996, n.675*", alla redazione del Documento programmatico per la sicurezza dei dati, approvato con Delibera G.C. n° XXX del XXXXXXXXX e successivamente sottoposto a revisione con Delibera G.C. n° XXX del XXXXXXXXX.

Il Comune di Montevarchi ha approvato la Delibera G.C. N° 247 **del XX/XX/2004** "Distribuzione dei compiti e delle responsabilità secondo quanto disposto dal D.l.g.s. 196/2003 - Codice in materia di protezione dei dati personali".

Il Comune di Montevarchi ha approvato ai sensi del D.P.C.M. 31 ottobre 2000 – Regole tecniche per il protocollo informatico, con Delibera G.C. n° XXX del XXXXXXXXX il Manuale di gestione per la tenuta del protocollo informatico, dei flussi documentali e degli archivi *che riguardo alla sicurezza informatica fa riferimento anche a misure comprese nel presente documento.*

2 Elenco dei Trattamenti di Dati Personali

Questo comune effettua il trattamento di dati esclusivamente per lo svolgimento delle funzioni istituzionali che gli sono proprie attraverso la realizzazione dei diversi procedimenti amministrativi.
Nel trattamento dei dati il Comune di Montevarchi osserva i presupposti ed i limiti definiti dal Codice, dalla legge e dai regolamenti.

2.1 Dati trattati dal personale interno

I trattamenti dei dati personali effettuati in questa Amministrazione sono da ricondursi a quelli necessari per la esecuzione dei procedimenti amministrativi affidati ai servizi cosi come disposto dal Regolamento Comunale sull'ordinamento degli uffici e dei servizi approvato con Delibera XX n°XXXX del XXXX.
I trattamenti sono effettuati sia con l'ausilio di mezzi elettronici che senza l'ausilio di mezzi elettronici.

2.2 Dati il cui trattamento è affidato all'esterno

Le *banche dati su supporto cartaceo e/o informatizzato, contenenti dati personali assegnati* all'esterno per il trattamento sono:

-
- quelli relativi ai servizi di tesoreria affidati alla Banca XXXXXXXXXXXXXXXXX, con convenzione n° XXXX del XXXX.

Le convenzioni citate in precedenza regolano, per gli aspetti di cui al D.Lgs. 193/2003 le modalità di trattamento e di comunicazione dei dati personali comuni e sensibili.

3 Distribuzione dei compiti e delle responsabilità

Il Codice individua, oltre all'interessato (lettera i, comma1 art. 4 del Codice), i soggetti che sono coinvolti nel trattamento dei dati personali:

- il **titolare,** cioè la persona fisica o giuridica che ha la responsabilità finale ed assume le decisioni fondamentali riferite al trattamento dei dati personali (articolo 28 del Codice);

- il **responsabile**, è la persona, dotata di particolari caratteristiche di natura morale e di competenza tecnica, preposta dal titolare al trattamento dei dati personali "ivi compreso il profilo della sicurezza"; possono essere nominati anche più responsabili in base ad esigenze organizzative (articolo 29 del Codice);

- l'**incaricato** è la persona fisica che materialmente provvede al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile se nominato (articolo 29 del Codice);

3.1 Individuazione ed attribuzioni del responsabile

Il comma 2 dell'articolo 30 del Codice così recita *"Se designato, il responsabile, deve essere nominato fra i soggetti che per esperienza capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza".*
Il Sindaco, nella sua qualità di titolare, nella redazione del *Documento programmatico per la sicurezza dei dati* ex DPR 318/99 aveva individuato quali "responsabili del trattamento dei dati" i funzionari delle 5 aree nei quali è articolata l'organizzazione comunale:

- Servizio Amministrativo
- Servizio Economico Finanziario e Personale
- Servizio Urbanistica
- Servizio Lavori Pubblici e Tecnico-manutentivo
- Servizio Polizia Municipale.

Tale scelta discendeva principalmente dal fatto che, essendo il trattamento strettamente legato ai procedimenti amministrativi di competenza dei vari settori. non appariva opportuno individuare un unico *responsabile del trattamento dati* .

L'esperienza maturata dalla prima adozione del *Documento programmatico per la sicurezza dei dati* fino ad oggi consente di confermare la nomina dei funzionari responsabili dei cinque servizi quali *responsabili del trattamento dati* ai sensi dell'art. 30 del Codice con l'introduzione di una novità, consistente nella individuazione fra i citati responsabili di un **responsabile con funzioni di coordinamento**. e di un responsabile informatico.

Su questa materia è stata disposta la Deliberazione G.C. n° 247/2004 "Distribuzione dei compiti e delle responsabilita' secondo quanto disposto dal d.l.g.s. 196/2003 - Codice in ma Deliberazione G.C. n° 247/2004 teria di protezione dei dati personali" che si riporta integralmente di seguito

Riportare integralmente il testo della Deliberazione G.C. n° 247/2004

3.2 Gli Incaricati

Sono individuati quali "incaricati del trattamento dati" i dipendenti del Comune, addetti ai Servizi che costituiscono i vari Settori, che abbiano accesso, per la loro funzione, a dati personali.

Sono da considerarsi incaricati a tutti gli effetti anche i dipendenti temporanei, il personale a convenzione ed altri soggetti che hanno accesso per il loro incarico a dati personali.
Gli incaricati sono nominati dai responsabili del trattamento dati dei settori di competenza.
I dipendenti da soggetti esterni che operano nel Comune, per l'espletamento di servizi manutentivi od altro, saranno identificati ed incaricati con specifico atto dal datore di lavoro, previamente nominato dal titolare responsabile esterno.
Lo schema dell'atto di nomina dell'incaricato del trattamento dei dati è inserito nell'allegato A al presente Documento.

3.3 L'incaricato con funzione di amministratore di sistema

Il DPR 318/99 all'articolo 1 definiva l'amministratore di sistema, come soggetto cui è conferito il compito di "sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base di dati e di consentirne l'utilizzazione"; il *Documento programmatico per la sicurezza dei dati* ex DPR 318/99 del Comune stabiliva di individuare tale figura tra il personale dipendente in base al possesso di adeguate competenze informatiche.
Il Codice non prevede in modo esplicito tale figura che si può comunque ricondurre ad un particolare tipo di incaricato, denominato **incaricato con funzione di amministratore di sistema** che opererà con funzioni meramente tecniche alle dipendenze di un responsabile (**responsabile con funzione di coordinamento**).
Lo schema dell'atto di nomina dell'incaricato del trattamento dei dati è inserito nell'allegato A al presente Documento.

4 Analisi dei rischi che incombono sui dati

Per procedere all'analisi dei rischi che incombono sui dati è necessario descrivere ed analizzare la situazione attuale della amministrazione comunale.

4.1 Descrizione dello stato attuale

I dati che seguono sono relativi a una rilevazione effettuata nell'estate 2004.

4.1.1 Descrizione degli edifici e dei locali dove avviene il trattamento

Edifici dove avviene il trattamento dei dati:

A. Palazzo Municipale
B. Palazzo Martini
C. Palazzo Podestà
D. Ufficio ICI
E. Palazzo Servizi polizia municipale e commercio
F. Biblioteca
G. Archivio di deposito
H. Servizi sociali
I. Sede decentrata Levane

A) DESCRIZIONE GENERALE DEL PALAZZO MUNICIPALE

Si tratta di un antico edificio costituito da tre piani fuori terra collocato nel centro storico, utilizzato anche da altri soggetti per usi diversi (abitazioni e negozi) con accessi da piazza Varchi (ingresso principale) e da via Poggio Bracciolini e via Roma (ingressi secondari).

Tipologia accessi
Porta principale in legno massiccio con due serrature ordinarie e successivamente porta a vetri scorrevole che limita l'ingresso in orario di chiusure al pubblico.
Porta da via Roma in legno con serratura ordinaria.
Porta da via Poggio Bracciolini in legno di modestissima consistenza con serratura ordinaria.
E' possibile l'accesso anche dall'ufficio URP che da su piazza Varchi.

Non è presente sistema generale di allarme.

All'interno della porzione dell'edificio di pertinenza del Comune sono presenti locali utilizzati da soggetti esterni (ENEL, AMNIL).

Costituiscono il palazzo Municipale

PIANO TERRENO
- Atrio
- Locale utilizzato da ENEL spa per servizi
- Locali URP
- Ripostigli

PRIMO AMMEZZATO
- Ingresso
- Ufficio protocollo con piccolo archivio
- Ufficio messi comunali
- Centralino telefonico
- Ufficio attività produttive
- Ufficio contenzioso – archivio

- Con ingresso anche da via Roma 62
- Ingresso ufficio urbanistica (bancone)
- SUAP
- Archivio
- Ufficio edilizia privata
- Ufficio edilizia privata/urbanistica
- Ufficio assessore
- Ufficio dirigente
- Sala riunioni
- Archivio

PIANO PRIMO
- Corridoio
- Ufficio del sindaco
- Sala attesa
- Segreteria del sindaco
- Ufficio segretario generale
- Ufficio dirigente affari generali
- Altra segreteria del sindaco
- Ufficio segreteria generale
- Ufficio responsabile informatica
- Ufficio informatica
- Uffici tributi (2 locali)
- Economato
- Aff gen???

Ragioneria bilancio
Dirigente ragioneria
Uffici ragioneria (2 locali)
Locale server

SECONDO AMMEZZATO
Ufficio cultura sport e scuola
Ufficio funzionario P.I.
Ufficio cultura
ufficio sport

PIANO SECONDO
Ufficio personale + archivio
Ufficio personale paghe
Dirigente personale
Ufficio statistica

Servizio elettorale (3 vani)
Stato civile
Uffici anagrafe (2 locali collegati fra loro)
Funzionario anagrafe

PIANO TERRENO

Da piazza Varchi attraverso il portone principale ed una porta a vetri scorrevole, chiusa quando gli uffici non sono aperti al pubblico, si accede all'atrio.
Il locale che ospita il servizio accoglienza è costantemente presidiato da personale in orario di apertura.
Nell'atrio sono presenti l'ascensore e la scala per i piani superiori, l'accesso ai locali dell'URP, ad un locale utilizzato dall'ENEL e ad altri locali usati come ripostigli che conducono all'accesso secondario di via P. Bracciolini.

SERVIZIO UFFICIO RELAZIONI CON IL PUBBLICO

Si tratta di due locali, fra loro collegati, uno ha due accessi da piazza Varchi, l'altro è accessibile dall'atrio del palazzo municipale.
Metallo e vetro con serratura ordinaria.
Le porte di accesso da Piazza Varchi sono protette da vetri antisfondamento e dotate di efficienti. La porta di accesso dall'atrio è legno con serratura ordinaria.
Sono presenti N° 4 posti di lavoro e N° 6 P.C. in rete.
Gli arredi sono costituiti da scrivanie, armadi in legno e metallo che contengono documentazione amministrativa.

PRIMO AMMEZZATO

Dalla scala proveniente dall'atrio attraverso una porta in legno con serratura ordinaria si entra in un ingresso cui si affacciano i locali del piano; nell'ingresso sono presenti armadi metallici contenenti documentazione amministrativa (contratti, tributi).
Dall'ingresso si accede a: Ufficio messi comunali, Centralino telefonico, Ufficio controllo di gestione, Ufficio contenzioso – archivio ufficio attività produttive i caratteri generali sono i seguenti:
porte di accesso in legno e vetro con serrature ordinarie;
finestre difficilmente accessibili;
arredi in gran parte non dotati di adeguate protezioni.
assenza del sistema di allarme
Ufficio messi comunali: N° 1 posto di lavoro N° 1 PC in rete; custodia di dati sensibili e giudiziari:
Ufficio controllo di gestione: N° 1 posto di lavoro N° 1 PC in rete; custodia di dati sensibili e giudiziari.

Ufficio contenzioso e archivio di gestione: N° 2 posti di lavoro N° 2 PC in rete; custodia di dati sensibili e giudiziari.
Centralino: N° 1 posto di lavoro.

Ufficio attività produttive

Vi si accede dalla scala proveniente dall'atrio attraverso una porta in legno dotata di apriporta con combinazione. L'ufficio è costituito da n.3 stanze più un atrio di ingresso con funzione di sala di attesa.
Le finestre non sono accessibili per posizione.
Gli arredi, armadi in legno e scrivanie, non dotati di particolari caratteri di sicurezza, contengono documentazione amministrativa.
Gli uffici sono dotati di n.4 pc in rete.

Ufficio protocollo

Vi si accede dalla scala proveniente dall'atrio attraverso una porta in legno con serratura ordinaria è costituito da due stanza fra loro collegate; le finestre non sono accessibili.
Gli arredi, armadi in legno e scrivanie, non dotati di particolari caratteri di sicurezza contengono la corrispondenza in arrivo e partenza.
Sono presenti N° 4 postazioni di lavoro e N° 3 PC in rete.

Ufficio urbanistica e edilizia privata

Da via Roma attraverso una porta in legno con serratura ordinaria si accede ad una scala che dividendosi in due rampe contrapposte i locali che ospitano il settore urbanistica con accessi agli uffici: SUAP, archivio; edilizia privata; edilizia privata/urbanistica; assessore; sala riunioni e archivio, oltre al corridoio del palazzo comunale attraverso una porta in legno alla quale è stato collegato un apriporta e un citofono.
Gli uffici hanno i seguenti caratteri:
porte in legno con serratura ordinaria;
finestre non accessibili per posizione;
arredi, armadi in legno e scrivanie, non dotati di particolari caratteri di sicurezza che contengono documentazione amministrativa.
Sono presenti N° 11 PC in rete con le relative postazioni di lavoro.

PIANO PRIMO

Al primo piano del palazzo si arriva dall'atrio attraverso la scala principale e l'ascensore e da una scala secondaria dal primo ammezzato.
Dalle scale attraverso una porta a vetri si entra in un corridoio sul quale si affacciano la sala giunta, l'ufficio del sindaco; la segreteria del sindaco, l'ufficio del segretario generale, l'ufficio del dirigente degli affari generali, altra segreteria del sindaco; l'ufficio della segreteria generale; da un piccolo disimpegno si accede a due uffici del servizio informatica e a due uffici del servizio tributi.
Al termine del corridoio, sul quale si affacciano anche le porte dei servizi igienici, di ripostigli e dell'ufficio del messo di conciliazione, attraverso una scala si giunge ad un ballatoio sul quale si affaccia la porta dell'ufficio economato (parete a vetri)ed una porta che da accesso ad un'area comprendente cinque uffici del servizio economico e finanziario ed il locale che ospita i server.
Gli uffici hanno i seguenti caratteri:

- porte dei locali che si affacciano sul corridoio principale in legno di modesta consistenza con serrature di tipo ordinario (yale);
- porte degli altri locali in legno e vetro di modesta consistenza con serrature di tipo ordinario (yale);
- ufficio economato con parete a vetri verso il corridoio
- finestre dei locali non accessibili per posizione;
- gli arredi , armadi in legno, in metallo ed in metallo e vetro, scaffalature e scrivanie, non dotati di particolari caratteri di sicurezza contengono documentazione amministrativa comprendente secondo la tipologia degli uffici anche dati sensibili e giudiziari;
- sistema di allarme assente.

Sono presenti N° 24 PC in rete con le relative postazioni di lavoro.

SECONDO AMMEZZATO

Dalla scala proveniente dall'atrio attraverso una porta in legno con serratura ordinaria si entra nell'ufficio scuola sul quale si affacciano le porte degli uffici cultura, sport e scuola e del dirigente di settore e una scala secondaria che conduce al piano superiore.
L'ufficio scuola è di passaggio per gli altri locali ha una finestra non accessibile per posizione, comprende un posto di lavoro con N° 1 PC in rete ed armadi in legno, senza serrature efficienti, contenenti documentazione amministrativa comprendente anche dati sensibili.
Gli altri uffici dell'area hanno i seguenti caratteri:

- porte in legno di modesta consistenza con serrature di tipo passepartout;
- finestre dei locali non accessibili per posizione;
- gli arredi , armadi in legno, in metallo ed in metallo e vetro, scaffalature e scrivanie, non dotati di particolari caratteri di sicurezza contengono documentazione amministrativa comprendente secondo la tipologia degli uffici anche dati sensibili e giudiziari;
- non presente sistema di allarme.

Sono presenti N° 6 posto di lavoro e N° 6 PC in rete.

PIANO SECONDO

Al secondo piano del palazzo si arriva dall'atrio attraverso la scala principale e l'ascensore; sul ballatoio sono presenti due porte da una si accede all'area del servizio elettorale dall'altra all'area comprendente i servizi demografici e personale.
L'area dei servizi elettorali comprende tre locali fra loro collegati; la porta che da accesso all'area è in legno di modesta consistenza con serratura ordinaria; le finestre sono inaccessibili per posizione; gli arredi consistono in scrivanie armadi in metalli e legno, classificatori e schedari metallici con serrature efficienti: sono presenti N° 2 posti di lavoro e N° 2 PC in rete.
Dal ballatoio attraverso una porta a vetri con serratura si entra in un corridoio sul quale si affaccia la porta, dell'ascensore ed una porta a vetri con accesso a codice e campanello elettrico verso l'ufficio stato civile e gli uffici dell'anagrafe e del personale.
L'ufficio stato civile è dotato di una porta con serratura ordinaria e di finestra non accessibile per posizione; sono presenti N° 2 PC in rete con relative postazioni di lavoro; armadi metallici con serrature efficienti contengono i registri dello stato civile e documentazione connessa; non è presente sistema di allarme.
L'area dell'anagrafe comprende un corridoio, di passaggio per gli uffici personale, sul quale è presente una parete a vetri comprendente gli sportelli per il pubblico, e gli accessi per i due uffici anagrafe e del dirigente della stessa.
L'area dell'anagrafe è dotata di sistema di allarme, di porte di accesso ordinarie con serratura efficiente, di finestre non accessibili per posizione; gli arredi consistenti in schedari, armadi in metallo e legno sono dotati in parte di serrature efficienti..

Dal corridoio dell'anagrafe si accede all'area degli uffici del personale e della statistica; si tratta di quattro locali con i seguenti caratteri:

- porte dei locali che si affacciano sul corridoio in legno di modesta consistenza con serrature di tipo ordinario (yale);
- finestre dei locali non accessibili per posizione;
- gli arredi , armadi in legno, in metallo, scaffalature e scrivanie, non dotati di particolari caratteri di sicurezza contengono documentazione amministrativa comprendente secondo la tipologia degli uffici anche dati sensibili;
- Nell'area è presente un sistema di allarme.

Sono presenti N° 6 posti di lavoro e N° 6 PC in rete

B) DESCRIZIONE GENERALE DI PALAZZO MARTINI

Si tratta di un grande edificio di tre piani, collocato nel centro storico e comprendente corti interne fra loro collegate sulle quali si affacciano gli ingressi a vari locali.
Gli accessi all'edificio sono da Piazza Varchi e dalla retrostante via.
La maggior parte dei locali presenti nell'edificio sono utilizzati da diversi soggetti pubblici e privati.
La maggior parte dei locali presenti nell'edificio sono utilizzati da diversi soggetti pubblici e privati.
Il palazzo ospita l'Ufficio Tecnico e l'Ufficio Cimitero Catasto e Gas.

Locali interessati al trattamento

Piano terreno
- Ufficio Cimitero Catasto e Gas
- Ufficio Casa

Piano primo
- Ufficio casa
- Ufficio gare e appalti
- Servizio ambiente e qualità
- Assessore

Piano secondo
- cinque aree fra loro collegate che ospitano i servizi lavori pubblici, espropri e patrimonio.

Descrizione Ufficio Cimitero Catasto e Gas

L'ufficio è costituito da un unico locale isolato al piano terreno, con accesso esclusivo da una corte interna.
L'unica finestra non ha protezioni ed è accessibile, se pur con qualche difficoltà, dalla pubblica via.
La porta di accesso è in metallo e vetro con serratura ordinaria protetta da vetri *antisfondamento. legno con serratura di sicurezza.*
Sono presenti N° 3 postazioni di lavoro e N° 4 3 P.C. un due dipendente comunale che si occupa della gestione dei servizi cimiteriali e del catasto, sono presenti dipendenti della società (esterna) del gas e del catasto.
Gli arredi costituiti da scrivanie, armadi in legno e metallo e scaffali non possiedono particolari caratteri di sicurezza e contengono documentazione amministrativa (contratti etc), vecchi registri cimiteriali e documentazione varia.
Non è presente sistema di allarme.

Descrizione Ufficio Casa

L'ufficio è costituito da un unico locale al piano terreno, con accesso esclusivo da una corte interna. Dalla corte interna di accede ad un disimpegno dove si trovano un bagno per portatori di handicap, l'ascensore per i piani superiori e lo stesso ufficio casa protetto da porta in legno con serratura ordinaria
L'unica finestra non ha protezioni ed è accessibile, se pur con qualche difficoltà, dalla pubblica via.
La porta di accesso è in metallo e vetro con serratura ordinaria protetta da vetri antisfondamento.
Sono presenti N° 1 postazioni di lavoro e N° 1 dipendente comunale che si occupa dell'ufficio casa
Nell'ufficio casa sono trattati anche documenti contenenti dati sensibili e giudiziari

Descrizione Ufficio Casa, gare e appalti, servizio ambiente e qualità urbana, ufficio dell'assessore, lavori pubblici e patrimonio.

Da una corte interna attraverso una scala si giunge ad un ingresso protetto da un cancello con serratura efficiente (accesso a codice) ; oltre il cancello si trova una porta a vetri con serratura ordinaria dalla quale si entra nell'area che ospita gli uffici collocata su due piani.

Non è presente sistema di allarme.

Piano primo

Al piano primo da un corridoio si accede all'ingresso sul quale si affacciano quattro locali: ufficio casa;ufficio assicurazione, ufficio gare e appalti, servizio ambiente e qualità, assessore ufficio, del dirigente.
Nell'ingresso in un'area delimitata da un bancone sono poste tre postazioni di lavoro con N° 3 PC in rete; tale area ospita oltre ad altri servizi l'ufficio casa; gli arredi costituiti da armadi in legno e vetro, scrivanie e scaffali non possiedono particolari caratteri di sicurezza.
Nell'ufficio casa sono trattati anche documenti contenenti dati sensibili e giudiziari.
Le finestre non sono accessibili per posizione,
L'area è di passaggio per accedere agli altri locali e per svolgere attività di servizio è accessibile agli utenti dell'ufficio casa gare ed appalti e ufficio dell'assessore
Gli altri quatto locali, dotati di porte in legno con serratura ordinaria contengono arredi (armadi in legno e vetro, scrivanie e scaffali) non dotati di particolari caratteri di sicurezza; le finestre non sono accessibili per posizione. La documentazione custodita presso gli uffici è costituita in gran parte da atti amministrativi e comprende anche dati sensibili e giudiziari).

Piano secondo

Al piano secondo, cui si accede dal primo attraverso una scala è presente un unico locale diviso da pannelli in cinque aree fra loro collegate che ospitano i servizi lavori pubblici, espropri e patrimonio.
Sono presenti varie postazioni di lavoro dotate di PC in rete.
Le finestre non sono accessibili per posizione
Gli arredi costituiti da armadi in legno e vetro, scrivanie e scaffali non possiedono particolari caratteri di sicurezza.
La documentazione custodita è rappresentata per la quasi totalità da atti amministrativi.

Descrizione immobile posto in Piazza Umberto I n.3 piano primo

Da Piazza Umberto attraverso una porta in legno, con serratura ordinaria, si accede ad una scala che porta al piano primo e con una porta in legno, sempre dotata di serratura ordinaria, si accede ai locali che ospitano l'ufficio di piano (servizio governo del territorio) ed una appendice dell'ufficio toponomastica. L'immobile è costituito da un disimpegno che distribuisce 3 stanze.
Gli uffici hanno le seguenti caratteristiche:
porte in legno con serratura ordinaria;
finestre non accessibili per posizione;
arredi, e scrivanie, non dotati di particolari caratteri di sicurezza e che contengono documentazione amministrativa.
Sono presenti N° 8 PC in rete con le relative postazioni di lavoro oltre ad un portatile.

Descrizione immobile posto Via Roma 109 piano primo (archivio edilizia e urbanistica)

Da Via Roma, attraverso una porta in legno, con serratura ordinaria, si accede ad una scala che porta al piano primo e con una porta antincendio dotata di serratura ordinaria, con maniglia antipanico posta all'interno dei locali, si accede all'archivio. L'ingresso costituisce sala di attesa e ufficio di accettazione richieste e distribuzione pratiche. Da questo vano si accede ad un ampio locale dotato di scaffalature in ferro oltre ad una ulteriore stanza sempre dotata di scaffalature metalliche dalla quale è possibile accedere mediante porta in legno con serratura ordinaria ai locali archivio del Settore Gestione del Territorio.
Gli uffici hanno le seguenti caratteristiche:
porta in legno con serratura ordinaria di collegamento all'archivio del Settore Gestione del Territorio;
finestre e portafinestra con balcone non accessibili per posizione;
arredi, e scrivanie, non dotati di particolari caratteri di sicurezza e che contengono documentazione amministrativa.

Sono presenti N° 2 PC in rete con le relative postazioni di lavoro.

C) DESCRIZIONE GENERALE DEL PALAZZO DEL PODESTA'

Si tratta di un antico palazzo di due, collocato nel centro storico con accesso da Piazza Varchi.
Il portone principale è in legno massiccio con serratura ordinaria.
Non è presente sistema generale di allarme.
Il palazzo oltre ad alcuni uffici ospita la sala utilizzata per le riunioni del consiglio comunale che viene concessa a soggetti pubblici e privati per iniziative di vario genere. Gli uffici non attivi in modo continuo ma con orari diversi a seconda delle iniziative.

Costituiscono il palazzo

PIANO TERRENO
- Atrio
- Ufficio difensore civico e segretario presidente consiglio comunale
- Centro ascolto cittadini stranieri

PIANO PRIMO
- Sala consiliare
- Locale capigruppo
- Locale presidente consiglio comunale

Dal portone di accesso si entra nell'atrio sul quale si affacciano le porte di due uffici e la scala per il piano superiore.
L'atrio non è presidiato con continuità da personale, il portone di accesso viene aperto solo in orario di apertura degli uffici e quando vengono tenute iniziative di vario genere.

Gli uffici hanno porte in legno massiccio, dotate di serrature ordinarie; sono presenti arredi senza particolari dotazioni di sicurezza e PC in rete.
Le finestre non sono facilmente accessibili dall'esterno.

D) UFFICIO ICI

Si tratta di due locali, fra loro collegati, precedentemente utilizzati come negozio. Il locale principale, cui si accede direttamente dalla pubblica via, è utilizzato come ufficio il secondo come archivio
I locali sono collocati al piano stradale dotati di due accessi attigui da via Poggio Bracciolini
Le porta di accesso è in metallo e vetro con serratura ordinaria protetta da serrande metalliche con serrature efficienti; non ci sono finestre.
E' assente sistema di allarme.
Sono presenti, ordinariamente, tre postazioni di lavoro e N° 6 P.C. in rete
Gli arredi consistono in scrivanie, armadi in legno e metallo senza particolari dotazioni di sicurezza e scaffali.
La documentazione conservata riguarda atti riferiti alla gestione dell'ICI.

E) DESCRIZIONE GENERALE DELL'EDIFICIO CHE OSPITA I SERVIZI POLIZIA MUNICIPALE E ATTIVITA' PRODUTTIVE

Il palazzo, ad un solo piano, utilizzato in modo esclusivo da uffici comunali è collocato in piazza Umberto I° con accesso anche da via dei Mille.

Tipologia accessi
Da piazza Umberto I° porta in metallo e legno con serratura ordinaria
Da via dei Mille porta in metallo e vetro serratura ordinaria protetta da serranda metallica.
Non è presente sistema di allarme

SERVIZIO POLIZIA MUNICIPALE
Dalla piazza Umberto I° attraverso una porta si accede ad un vasto locale che ospita la parte dei servizi della Polizia municipale rivolti al pubblico; il locale è diviso in due parti da un bancone; nella parte riservata al pubblico si affaccia una porta che conduce verso gli altri uffici.
Nella parte del locale riservata al personale sono presenti N° 4 posti di lavoro e N° 4 PC in rete, telefax e fotocopiatrici , non tutti dotati di serrature efficienti. Dall'area descritta si accede ad un secondo ufficio con N° 4 posti di lavoro e N° 4 PC in rete, dal locale si accede allo spogliatoio ai servizi igienici e attraverso una porta ad un corridoio che conduce agli altri uffici. Gli arredi, nei due locali descritti, consistono in schedari metallici, armadi in legno e metallo, scaffali e scrivanie; i documenti conservati comprendono, dati i compiti della Polizia Municipale, anche dati personali sensibili e giudiziari.
Dall'ingresso attraverso una porta, in legno con serratura ordinaria, normalmente chiusa si accede a corridoio sui quali si affacciano gli uffici dell'assessore e del comandante della Polizia Municipale. Gli uffici citati hanno un posto di lavoro ognuno, senza dotazioni informatiche, le porte sono in legno con serratura ordinaria e finestre non accessibili; gli arredi consistenti in scrivanie, armadi in legno e scaffali contengono documentazione amministrativa ordinaria.
Il corridoio descritto in precedenza si può accedere attraverso un disimpegno e due porte all'area del servizio attività produttive e commercio.

SERVIZIO ATTIVITÀ PRODUTTIVE E COMMERCIO
Dalla via dei Mille attraverso una porta in metallo e vetro con serratura ordinaria, protetta da grata metallica, si accede ad un corridoio-ingresso sul quale si affacciano le due porte dell'ufficio attività produttive e commercio e dell'ufficio agricoltura e caccia. Il corridoio-ingresso non è presidiato da personale e ospita un armadio in legno con serrature efficienti nel quale sono custoditi atti amministrativi del settore commercio.
L'ufficio attività produttive ha porte in legno con serrature ordinarie, finestre inaccessibili (protette da grate) N° 3 posti di lavoro e N° 3 PC in rete; gli arredi scrivanie, armadi in legno e metallo sono dotati di serrature efficienti.
La porta dell'ufficio agricoltura e caccia è in legno con serratura ordinaria; danno su una corte interna; è presente N° posto di lavoro e N° 1 PC in rete negli arredi, scrivani, armadi in legno e metallo, sono contenuti atti amministrativi del servizio.

F) DESCRIZIONE GENERALE DELL'EDIFICIO CHE OSPITA LA BIBLIOTECA

Il palazzo, ad un solo piano, utilizzato in modo esclusivo da uffici comunali è collocato in via dei Mille.

L'edificio è dotato di n° 4 porte di ingresso, ordinarie senza particolari dotazioni di sicurezza.
Sono presenti vie di accesso (finestre) non protette; non è presente sistema di allarme
La struttura comprende:

- aree dedicate alla lettura;
- *un ufficio del responsabile (n° 1 PC in rete, n° 1 posto di lavoro, arredi ordinari* contenenti documentazione amministrativa)
- zona prestito (n° 2 PC, n° 2 posti di lavoro, arredi ordinari); un bancone delimita l'area di accesso per il pubblico
- area dove vengono conservati i libri e riviste;
- area dove viene custodito l'archivio storico;
- area di consultazione banche dati per il pubblico, dotata di 3 PC.

Sono presenti inoltre locali di servizio: magazzino, servizi igienici, centrale termica (accessibile *solo dall'esterno del fabbricato).*

I dati personali trattati, relativi ad atti amministrativi e all'attività istituzionale, sono di natura non sensibile.

G) DESCRIZIONE GENERALE DELL'EDIFICIO CHE OSPITA L' ARCHIVIO DI DEPOSITO

La struttura di cui si tratta è ospitata in una porzione di fabbricato situato in Piazza C. Battisti al piano terreno

Tipologia accessi
Due accessi da piazza C. Battisti, protetti da serrande metalliche e dotati di porta ordinaria; serrande e porte hanno serrature ordinarie.
Non è presente sistema di allarme

Scaffali metallici ospitano materiale archivistico afferente la sezione storica e la sezione di deposito.

Non sono presenti posti di lavoro e dotazioni informatiche.

H) DESCRIZIONE GENERALE DELL'EDIFICIO CHE OSPITA I SERVIZI SOCIALI

L'edificio, di due piani, sede degli uffici USL è all'interno di un'area recintata cui si accede attraverso un cancello metallico che da sulla via Podgora. E' presente illuminazione esterna efficiente
Sono presenti più accessi; alla zona che occupa gli uffici di cui si tratta si accede attraverso una porta in metallo e vetro (antisfondamento??) con serratura ordinaria.
Presente di tipo volumetrico nell'atrio (di uso comune con Azienda USL) al momento non ancora attivato
La maggior parte dei locali presenti nell'edificio sono utilizzati direttamente dall'USL per lo svolgimento delle proprie attività istituzionali.
Sono presenti numerose vie di accesso non protette al piano terreno.

Descrizione dei locali interessati al trattamento
Si tratta di n° 8 locali, utilizzati come uffici, collocati al piano primo dell'edificio e di un garage, utilizzato come archivio, al quale si accede dal cortile.
Agli uffici si giunge dall'atrio attraverso una scala; al piano sono presenti altri locali utilizzati dall'USL; la compartimentazione rispetto al resto dell'edificio non appare adeguata.
I locali hanno caratteristiche simili:

- unico accesso dal corridoio/ballatoio (salvo per due uffici fra loro comunicanti);
- porte di modesta consistenza dotate di serrature passepartout;
- finestre difficilmente accessibili per posizione;
- ospitano ognuno N° 1 posto di lavoro dotato di PC in rete;
- arredi di varie tipologie e consistenza: schedari metallici; armadi in metallo, armadi in legno; solo una piccola parte degli arredi è dotata di serrature efficienti;
- negli arredi è custodita documentazione costituita in gran parte da dati personali sensibili (cartelle personali degli assistiti, corrispondenza, referti medici etc.).

Il sistema informatico è costituito da 8 PC in rete VPN collegata con router CISCO criptati alla rete dell'Amministrazione.

I) DESCRIZIONE DELLA SEDE DECENTRATA DI LEVANE

La .struttura di cui si tratta, attualmente in via di ristrutturazione è ospitata in locali posti al piano terreno in via XXXXX.
Gli accessi non sono dotati di adeguate protezioni, i locali sono utilizzati anche da altri soggetti.pubblici (AUSL); non presente sistema di allarme.
Sono presenti due posti di lavoro e due PC in rete; gli arredi non presentano particolari caratteri di sicurezza e contengono documentazione amministrativa, compresi dati personali

4.1.2 Gestione delle chiavi

Chiavi di accesso agli edifici
Data la distribuzione degli uffici dell'Amministrazione in più edifici; e la utilizzazione di aree e locali in comune con altri soggetti la gestione delle chiavi di accesso ai diversi edifici e aree interessate appare oggettivamente complessa.
Attualmente nell'Ente non è definita formalmente una modalità unica per la gestione delle chiavi; per cui la situazione, in ordine alla sicurezza, appare differenziata a seconda degli edifici e degli uffici; in alcuni casi sono state adottate, da parte dei dirigenti, procedure di gestione (verbali di affidamento, procedure per la custodia delle copie di sicurezza), più spesso le chiavi sono affidate senza formalità al personale di ufficio, agli amministratori, a soggetti esterni autorizzati.

Chiavi di accesso agli uffici
Le chiavi degli uffici dove vengono trattati dati sono gestite dai dirigenti e dai responsabili dei diversi servizi ed affidate, salvo eccezioni, senza formalità agli incaricati; in alcuni casi le chiavi sono conservate in luoghi facilmente accessibili e visibili, anche al pubblico, senza alcuna misura di protezione o di controllo.

Chiavi degli archivi
Le chiavi degli archivi che contengono dati personali sono gestite dai responsabili e da questi affidate agli incaricati in generale senza formalità; non sempre sono disponibili copie di sicurezza.

4.1.3 Rilevazione struttura sistema informatico

Comune di Montevarchi

RILEVAZIONE STRUTTURA SISTEMA INFORMATIVO

1-Tipologia della rete/i

Unica LAN in fibra ottica in tutte le sedi
Sede Levane
Uffici presso la sede USL

2- Tipologia delle risorse hardware

- *N° 7 Server*
- *N° 130 Clients*
- *N° 8 Portatili*

3- Collocazione server

- *N° 1 Server (Uff. Anagrafe)*
- *N° 6 Servers (Sala Server palazzo municipale)*

4- Accesso alle risorse Internet

- *VAL.it*

5- Posta elettronica

-

TIPOLOGIA DELLE RISORSE SOFTWARE

6- Sistema operativo usato sul server

- *Windows 2000 Server*

7-Sistemi operativi usati sui client

Licenze di Office Automation Microsoft

- *Windows 2000 (70%)*
- *Windows XP (25%)*
- *Windows 95 e 98 (5% a esaurimento)*

Licenze antivirus

- *McAfee*

Elenco procedure

- *DELTA DATOR (Anagrafe, Stato civile, Elettorale)*
- *CEDAF (Finanziari)*
- *CCT (Tributi)*
- *SITER (Urbanistica)*
- *PERSONAL Zucchetti*

8- Supervisore di rete

- *Servizio informativo (Uff.*

9- Progetto e certificazione della rete

- *SMAN (certificazione in classe 5)*

10- Planimetria della rete

- Si

11- Uso della rete

- *Condivisione documenti e dati*

12- Interventi di formazione del personale

- *Corsi di alfabetizzazione per tutti i dipendenti I° e II°*
- *Corsi avanzati per i tecnici informatici*

13- Assegnazione di nomi logici per le periferiche di rete

- *Si*

14- Assegnazione delle password di accesso alle singole macchine

- *Parziale*

15- Assegnazione dei codici identificativi personali

- *In corso di assegnazione*

16- Collaboratori esterni o temporanei che hanno accesso alla rete

- Manutentori software e hardware

PREVENZIONE DELLA PERDITA DEI DATI

17- Software antivirus

- Sul server
  McAfee
- Modalità aggiornamento
  Dalla rete

18- Incarico formale dell'esecuzione dei backup

- *In corso di assegnazione*

19- Supporto sul quale viene effettuato il backup (copie di sicurezza)

- Dati residenti sul/sui Server/s
  DAT
- Dati residenti sui Clients
  Cartella condivisa salvata su server
- Dati residenti su PC Stand Alone
  Cartella condivisa salvata su server
- Dati residenti su PC Portatili (Palmari, Notebooks ecc)
  Vedi: LISTA DI CONTROLLO SULLA SICUREZZA DEI MICROCOMPUTER

20- Libro mastro della programmazione dei backup

- *No*

21 – Contenitore e locale dove vengono custodite le copie di backup

- *Cassaforte (in luogo sicuro)*

22- Strumenti di difesa antiintrusione

ROUTER
CISCO 825
FIREWALL
HW e SW e Proxy

23- Gruppo/gruppi di continuità

- *Sui servers e in alcuni clients*

24- Manutenzione delle risorse hardware e software

software:
Società fornitrici

hardware:
Sui servers ???

Microcomputer, portatili e stand-alone

E' presente, presso il servizio informatico, un registro aggiornato che contiene l'elenco di tutti i microcomputers, portatili e stand alone presenti.
Le macchine di cui si tratta sono assegnate ad personam, ancora non è presente una lista aggiornata degli utenti affidatari.
La formazione e l'addestramento dei consegnatari sulle modalità di uso sicuro e sulle prescrizioni minime di sicurezza è stata realizzata solo in parte.
I sistemi di autenticazione e autorizzazione sono entrambi presenti e coerenti con il profilo dei consegnatari.
Non tutte le macchine sono dotate di antivirus aggiornato.
La documentazione di utente del software viene mantenuta aggiornata e custodita.
Quando vengono introdotte modifiche (nuove applicazioni, rotazione personale, dispositivi telecomunicazione) non viene sempre effettuata una analisi aggiornata dei rischi, e su questi ultimi non viene eseguita una valutazione periodica della loro entità.
Su tali macchine non vengono, in via generale, trattati dati sensibili e/o giudiziari, tuttavia non sono presenti dispositivi di sicurezza per limitare il rischio di furto e di accesso non autorizzato all'uso di tali PC, come pure non sono stati individuati supporti di memoria rimovibili dove vengono registrati dati personali, anche perché i salvataggi vengono effettuati, sporadicamente, dal personale affidatario degli stessi su supporti di diversa natura.

4.2 Analisi dei rischi

4.2.1 Rischi riguardanti le basi di dati trattate senza strumenti informatici

I rischi sotto elencati afferiscono alle attività di trattamento dei dati effettuato con mezzi manuali:

A) **Palazzo Municipale**

Dalla situazione del Palazzo come descritta in precedenza emergono numerose situazioni problematiche in ordine alla sicurezza nel trattamento dei dati personali.
Occorre considerare, infatti, che le strutture che compongono il palazzo sono solo in minima parte adatte, da più punti di vista, alla utilizzazione come uffici ed in più date le loro caratteristiche difficilmente trasformabili ed adattabili senza un intervento radicale, per più ragioni impraticabile.
Alcuni punti critici dal punto di vista della sicurezza sono i seguenti:

- disposizione dei locali tale da rendere difficile in generale la compartimentazione di aree e la delimitazione dell'accesso per il pubblico;
- contenitori (armadi, schedari ecc) solo in parte dotati di caratteri di sicurezza chiusure efficienti;
- carenza di spazi nei quali conservare adeguatamente la documentazione; per cui parte della stessa è collocata in aree accessibili al pubblico;
- modesta consistenza delle porte interne ed affidabilità delle serrature
- presenza del sistema di allarme solo in una area.

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento per cause naturali appare pressoché nullo, data la collocazione, per la quasi totalità dei locali;
il rischio di allagamento a causa di guasti alle condotte idriche e termiche è presente, benché limitato, ai locali posti al piano terreno;
i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo le aree e secondo gli orari;

durante l'orario di chiusura i rischi sono presenti e di livello diverso secondo le aree: basso per quella con sistema di allarme (anagrafe); presente e rilevante per le altre aree data la citata mancanza di compartimentazione, assenza di un sistema generale di allarme, modesta consistenza delle porte interne degli uffici, mancanza di misure di sicurezza antintrusione nelle porte di accesso esterne;

durante l'orario di apertura i rischi, anche se ridotti dalla presenza di personale che opera nei rispettivi uffici, sono comunque presenti e riferibili alle seguenti cause: presenza nei corridoi di armadi, contenenti documentazione di varia natura, senza particolari garanzie di sicurezza; mancata adozione e diffusione, fatti salvi i casi di auto-responsabilizzazione del personale amministrativo, di regole di comportamento idonee che scongiurino la sottrazione di documenti nel momento in cui il funzionario si assenti dal proprio ufficio (chiusura degli armadi che si trovano all'interno dell'ufficio, chiusura della porta di accesso allo stesso); vasta ampiezza e dispersività del municipio che rende estremamente difficile un controllo "a vista".

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**

la situazione appare differenziata: in alcune aree (ad esempio per la zona dell'anagrafe e dello stato civile) sono adottate misure tecniche in grado di abbattere notevolmente il rischio, mentre in altre, anche per cause strutturali dovute alla disposizione degli uffici e degli arredi, il rischio è di livello medio.

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, non appaiono in gran parte adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso presente e rilevante; in particolare segnaliamo la presenza di archivi (armadi, scaffali, schedari contenenti dati personali, in parte sensibili, in locali accessibili al pubblico e sprovvisti di garanzie di sicurezza).

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al Palazzo municipale, sia per la mancanza di una procedura formale di affidamento delle chiavi, e di un elenco degli affidatari delle stesse, che per la insufficiente qualità delle serrature.

B) **Palazzo Martini**

Dalla situazione come descritta in precedenza emergono numerose situazioni problematiche in ordine alla sicurezza nel trattamento dei dati personali che occorre riferire in modo specifico alle diverse aree occupate dagli uffici comunali.

Ufficio cimitero, catasto e gas
- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento per cause naturali appare pressoché nullo, data la collocazione, per la quasi totalità dei locali;
il rischio di allagamento a causa di guasti alle condotte idriche e termiche è presente ma non di particolare rilevanza;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono secondo gli orari;

durante l'orario di chiusura i rischi sono presenti, data la mancanza di sistema di allarme, se pur limitati dalla consistenza della porta e dalla difficoltà di accesso alla finestra che da sulla pubblica via;

durante l'orario di apertura i rischi sono pressoché inesistenti data la presenza continua di personale

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
il rischio è presente e rilevante dato che nell'ufficio operano anche dipendenti da un soggetto esterno;

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, non appaiono in gran parte adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso presente e rilevante

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al all'ufficio, sia per la mancanza di una procedura formale di affidamento delle chiavi, e di un elenco degli affidatari delle stesse.

Ufficio casa, gare ed appalti, servizio ambiente e qualità urbana, lavori pubblici e patrimonio

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento per cause naturali o a causa di guasti alle condotte idriche e termiche appare nullo, data la collocazione, per la totalità dei locali;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo gli orari;
durante l'orario di chiusura i rischi sono presenti, data la mancanza di sistema di allarme, se pur limitati dal cancello metallico a protezione della porta e dalla difficile accessibilità delle finestre;

durante l'orario di apertura i rischi sono molto bassi data la presenza continua di personale ed il controllo degli accessi

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
il rischio è presente e rilevante dato che per cause strutturali in particolare al primo piano, nonostante la presenza di un bancone, non è possibile delimitare l'area cui può accedere il pubblico,

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, non appaiono in gran parte adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso presente e

rilevante; in particolare segnaliamo la presenza di archivi (armadi, scaffali, schedari contenenti dati personali, in parte sensibili, in locali accessibili al pubblico e sprovvisti di garanzie di sicurezza).

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al all'ufficio, sia per la mancanza di una procedura formale di affidamento delle chiavi, e di un elenco degli affidatari delle stesse.

C) **Palazzo del Podestà**

Il palazzo non è aperto al pubblico con continuità e non dispone di personale impiegato nel controllo dell'accesso.

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento per cause naturali o a causa di guasti alle condotte idriche e termiche appare nullo, data la collocazione, per la totalità dei locali;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono secondo gli orari;

durante l'orario di chiusura i rischi sono presenti, data la mancanza di sistema di allarme, se pur limitati dalla consistenza della porta e dalla difficoltà di accesso alle finestre che da sulla pubblica via;

durante l'orario di apertura i rischi sono presenti e rilevanti data la mancanza di presidio degli accessi, e visti gli orari diversi degli uffici, dalla modesta consistenza dei controllo all'interno del palazzo;

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
il rischio è di livello medio dato che gli uffici in orario di apertura sono costantemente presidiati e non sono presenti archivi di dati personali in aree accessibili al pubblico (corridoi); ,

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, non appaiono in gran parte adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso presente e rilevante

- ***connessi con la gestione delle chiavi di accesso:***
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al all'ufficio, sia per la mancanza di una procedura formale di affidamento delle chiavi e di un elenco degli affidatari delle stesse, ed anche in considerazione dell'uso della struttura.

D) **Ufficio ICI**

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento a causa di guasti alle condotte idriche e termiche appare presente e di media entità, data la collocazione, per la totalità dei locali;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo gli orari;
durante l'orario di chiusura i rischi di furto sono presenti, data la mancanza di sistema di allarme, se pur limitati dalle grate a protezione degli accessi; i rischi di danneggiamento per atti vandalici appare presente e rilevante data la tipologia delle porta (metallo e vetro) e la documentazione disposta nelle vetrine;

durante l'orario di apertura i rischi sono limitati dato il presidio continuo dell'ufficio da parte del personale;

- **_connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
l rischio è presente e rilevante dato che per cause strutturali non è possibile delimitare l'area cui può accedere il pubblico;

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, non appaiono in gran parte adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso presente e rilevante

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al all'ufficio, sia per la mancanza di una procedura formale di affidamento delle chiavi e di un elenco degli affidatari delle stesse.

E) **Palazzo Servizi polizia municipale e Attività produttive**

Dalla situazione del Palazzo come descritta in precedenza emergono numerose situazioni problematiche in ordine alla sicurezza nel trattamento dei dati personali.

Servizio Polizia Municipale
- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento per cause naturali appare pressoché nullo, data la collocazione, per la quasi totalità dei locali;

il rischio di allagamento a causa di guasti alle condotte idriche e termiche è presente ma non di particolare rilevanza;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo gli orari;

durante l'orario di chiusura i rischi sono presenti, data la mancanza di sistema di allarme, se pur limitati dalla consistenza della porta e dalle protezioni alle finestre;

durante l'orario di apertura i rischi sono pressochè inesistenti data la presenza continua di personale nell'ingresso ed il controllo dell'accesso agli uffici;

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
il rischio è molto limitato data la delimitazione dell'area cui ha accesso il pubblico (presenza di un bancone nell'ingresso) ed il controllo dell'ingresso negli uffici;

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, appaiono in gran parte adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso modesto

- ***connessi con la gestione delle chiavi di accesso:***
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al all'ufficio, sia per la mancanza di una procedura formale di affidamento delle chiavi, e di un elenco degli affidatari delle stesse.

Servizio Attività produttive
- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento per cause naturali appare pressoché nullo, data la collocazione, per la quasi totalità dei locali;
il rischio di allagamento a causa di guasti alle condotte idriche e termiche è presente ma non di particolare rilevanza;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo gli orari;

durante l'orario di chiusura i rischi sono presenti, data la mancanza di sistema di allarme, se pur limitati dalle protezioni della porta e delle finestre (grate);

durante l'orario di apertura i rischi sono presenti data la mancanza di un presidio continuo dell'accesso alla struttura e la presenza di archivi di dati personali in aree accessibili al pubblico;

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
il rischio è presente dato che non è delimitata l'area degli uffici cui può avere accesso il pubblico;

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, appaiono in gran parte non adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso presente e di media entità

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al all'ufficio, sia per la mancanza di una procedura formale di affidamento delle chiavi, e di un elenco degli affidatari delle stesse.

F) **Biblioteca**

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento a causa di guasti alle condotte idriche e termiche appare presente e di modesta entità, data la collocazione, per la totalità dei locali;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo gli orari;
durante l'orario di chiusura i rischi di furto sono presenti, data la mancanza di sistema di allarme, e di protezioni alle vie di accesso;
durante l'orario di apertura i rischi sono limitati dato il presidio continuo dell'ufficio da parte del personale;

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
il rischio è molto basso dato che è delimitata l'area cui può accedere il pubblico;

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, non appaiono in gran parte adeguati, per struttura , alle norme, il rischio appare nel complesso presente

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al all'ufficio, sia per la mancanza di una procedura formale di affidamento delle chiavi e di un elenco degli affidatari delle stesse.

G) **Archivio di deposito**

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento a causa di guasti alle condotte idriche e termiche appare presente , data la collocazione ;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo gli orari;
durante l'orario di chiusura i rischi di furto sono presenti, data la mancanza di sistema di allarme, e di protezioni alle vie di accesso;
durante l'orario di apertura i rischi sono nulli visto che il pubblico non ha accesso ed il presidio continuo del locale da parte del personale;

- ***connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento* non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di *personale interno*:**
il rischio è molto basso dato che ai locali hanno accesso solo dipendenti autorizzati;

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
rischio non presente

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso al all'ufficio, sia per la mancanza di una procedura formale di affidamento delle chiavi e di un elenco degli affidatari delle stesse.

H) **Servizi sociali**

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento a causa di guasti alle condotte idriche e termiche o per cause naturali appare presente , data la collocazione; solo per il garage utilizzato come archivio posto al pino terreno;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo gli orari;
durante l'orario di chiusura i rischi di furto sono presenti, data la mancanza di sistema di allarme, di protezioni alle numerose vie di accesso all'edificio; la modesta consistenza delle porte degli uffici;
durante l'orario di apertura i rischi sono bassi visto il presidio continuo degli uffici da parte del personale;

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**
tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
il rischio è presente dato che per cause strutturali non è possibile delimitare l'area cui può accedere il pubblico,

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, non appaiono in gran parte adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso presente e rilevante; in particolare segnaliamo la presenza di archivi (armadi, scaffali, schedari contenenti dati personali, in parte sensibili, in locali accessibili al pubblico e sprovvisti di garanzie di sicurezza).

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso agli uffici, sia per la mancanza di una procedura formale di affidamento delle chiavi e di un elenco degli affidatari delle stesse.

I) **<u>Sede decentrata di Levane</u>**

- **distruzione o perdita accidentale dei dati a causa di eventi naturali, allagamenti, furto, danneggiamento, etc.:**

il rischio di allagamento a causa di guasti alle condotte idriche e termiche o per cause naturali appare, data la collocazione, presente e di media entità;

i rischi di furto e/o danneggiamento per atti vandalici e simili appaiono differenziati secondo gli orari;
durante l'orario di chiusura i rischi di furto sono presenti, data la mancanza di sistema di allarme, di protezioni alle vie di accesso all'edificio; la modesta consistenza della porta di accesso;
durante l'orario di apertura i rischi sono bassi visto il presidio continuo della sede da parte del personale;

- **connessi alla integrità dei dati per utilizzo di supporti o modalità di trattamento non stabili:**

tale tipo di rischio è da considerarsi, nel complesso, basso anche se si ritengono opportune verifiche periodiche dei supporti cartacei.

- **accesso non autorizzato ai dati, da parte di soggetti esterni o da parte di personale interno:**
il rischio è presente dato che per cause strutturali non è possibile delimitare l'area cui può accedere il pubblico,

- **trattamento non consentito o non conforme alle finalità di raccolta - diffusione, comunicazione, manomissione:**
il rischio attualmente appare presente dato che non sono state definite procedure formali per il trattamento dei dati ed il personale, pur essendo in generale esperto e consapevole delle problematiche relative al trattamento dei dati personali, non è stato ad oggi sottoposto a specifica formazione.

- **connessi all'utilizzo di archivi e contenitori con serrature:**
gli archivi ed i contenitori delle banche di dati personali, non appaiono in gran parte adeguati, sia per struttura che per collocazione, alle norme, il rischio appare nel complesso presente e rilevante; in particolare segnaliamo la presenza di archivi (armadi, scaffali, schedari contenenti dati personali, in parte sensibili, in locali accessibili al pubblico e sprovvisti di garanzie di sicurezza).

- **connessi con la gestione delle chiavi di accesso:**
presenti e rilevanti appaiono i rischi derivanti dalla attuale gestione delle chiavi di accesso agli uffici, sia per la mancanza di una procedura formale di affidamento delle chiavi e di un elenco degli affidatari delle stesse.

4.2.2 Rischi per il sistema informativo automatizzato

L'analisi dei rischi consiste nella individuazione degli elementi del sistema informativo automatizzato che necessitano di protezione e delle minacce cui gli stessi possono essere sottoposti, tenendo conto del fattore tecnologico e del fattore umano.

Le principali fonti di rischio per un sistema informatico sono aggregabili, ai fini della analisi oggetto del presente paragrafo, nel modo che segue:

FR1 - maltempo, inondazioni, fulmini, terremoti, fuoco, attentati, furti etc.

FR2 - guasti hardware, caduta di corrente, omissioni hardware, errori e difetti software, sabotaggi, haking, programmi software maligni (malware,virus, worm)

FR3 - comportamenti errati, cattiva organizzazione, errata logistica

Sistema informatico ed elaboratori in rete

Il sistema informatico dell'Amministrazione, come descritto al precedente punto 4.1.3, è distribuito nei vari uffici; per cui per quanto riguarda i rischi compresi nel gruppo FR1 si fa riferimento a quanto detto al precedente punto 4.2.1.

Riguardo alle fonti di rischio comprese nel gruppo FR2, fino ad oggi anche da una analisi della serie storiche riguardanti il sistema informatico emerge quanto segue:

- non si sono registrati consistenti guasti hardware, anche per la continua manutenzione dello stesso e l'uso di macchine affidabili;
- nella zona in cui insistono i locali che ospitano il sistema informatico *non si verificano frequentemente cadute di corrente; il rischio è comunque contenuto dato che il sistema è dotato di gruppi continuità sui servers e alcuni clients;*
- il sistema consente il salvataggio dei dati per gli archivi delle procedure gestionali e per i dati residenti nei singoli clients;
- il sistema è dotato di antivirus *McAfee* che viene aggiornato via Internet anche giornalmente;
- riguardo il rischio di accesso abusivo, con i rischi connessi quali conoscenza dati a persone non autorizzate, distruzione o perdita totale, danneggiamento dei dati etc, fino ad oggi non si sono registrati eventi dannosi. In ogni modo il sistema appare vulnerabile dato che non sono state completamente assegnate passwords e codici identificativi personali;
- gli strumenti di difesa da intrusioni esterne appaiono adeguati.

Per le fonti di rischio comprese nel gruppo FR3 dall'analisi della rilevazione effettuata risulta quanto segue.
Le credenziali di autenticazione, consistenti in un codice per l'autenticazione associato ad una parola chiave non sono ancora gestite in modo corretto.
Nonostante le misure adottate il rischio di perdita di dati è presente, data la mancanza di una procedura formale per il salvataggio (individuazione formale dell'incaricato per l'esecuzione dei backups, definizione della periodicità, creazione di un registro dove vengono annotati i salvataggi).

Elaboratori non in rete

Per i PC stand-alone collocati, come descritto al punto 4.1.1, nei locali dove si esegue il trattamento dati senza l'ausilio di strumenti informatici per cui per quanto riguarda i rischi compresi nel gruppo FR1 si fa riferimento a quanto detto al precedente punto 4.2.1.
Per gli strumenti compresi nella categoria dei portatili (notebooks, laptops, palmari ecc.) la valutazione dei rischi citati appare più complessa anche perché ad oggi non sono state definite le norme di comportamento in ordine alla sicurezza per gli affidatari delle macchine.

Anche se non sono stati registrati, fino ad oggi, eventi dannosi riferiti alle categorie di rischio considerate riteniamo il rischio presente e rilevante in particolare riguardo al furto ed al danneggiamento.

Riguardo alle fonti di rischio comprese nel gruppo FR2, fino ad oggi anche da una analisi della serie storiche riguardanti il sistema informatico emerge quanto segue:

- *non si sono registrati consistenti guasti hardware, anche per la continua manutenzione dello stesso e l'uso di macchine affidabili;*
- nella zona in cui insistono i locali che ospitano i PC stand alone *non si verificano frequentemente cadute di corrente; il rischio è comunque presente dato che non vi sono gruppi di continuità;*
- i portatili e gli stand alone hanno dispositivi che consentono il salvataggio dei dati;
- solo una parte dei PC di cui si tratta è dotata di antivirus aggiornato;
- riguardo il rischio di accesso abusivo, con i rischi connessi quali conoscenza dati a persone non autorizzate, distruzione o perdita totale, danneggiamento dei dati ecc, *fino ad oggi non si sono registrati eventi dannosi. In ogni modo il sistema appare vulnerabile dato che nonostante siano state assegnate le passwords ai singoli PC* non sono stati attribuiti, in modo generalizzato, i codici identificativi personali. Gli strumenti di difesa da intrusioni esterne non sempre appaiono adeguati (mancano firewall software aggiornati).

Per le fonti di rischio comprese nel gruppo FR3 dall'analisi della rilevazione effettuata risulta quanto segue.
Le credenziali di autenticazione, consistenti in un codice per l'autenticazione associato ad una parola chiave non sono ancora gestite in modo corretto.
Circa il salvataggio dei dati il rischio è presente e rilevante dato che ad oggi non è stata adottata una procedura formale per il salvataggio.

5 Misure da adottare per garantire l'integrità e la disponibilità dei dati

5.1 Misure fisiche

I requisiti di sicurezza fisica sono tesi a:

- proteggere le persone che operano sui sistemi,
- proteggere le aree
- proteggere gli archivi.

5.1.1 Sicurezza di area

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza degli archivi e delle attrezzature informatiche rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

Come si evince da quanto riportato in precedenza (Descrizione stato attuale e Analisi dei rischi) i locali, e le strutture del Comune di Montevarchi presentano numerose e complesse problematiche di sicurezza, di seguito si individuano sia le contromisure da adottare rispetto ai rischi individuati che i soggetti cui spetta l'attuazione delle stesse

Adeguamento 1
Dotare le porte di accesso agli edifici dove avviene il trattamento di dati personali da parte del Comune di serrature efficienti e sicure.

Adeguamento 2
Provvedere in modo adeguato alla gestione delle chiavi di accesso agli edifici attraverso:

- misure che identifichino e responsabilizzino i soggetti interni o esterni cui vengono affidate;
- la custodia di copie di sicurezza.

Adeguamento 3
Provvedere a mettere in sicurezza le finestre accessibili attraverso la installazione di idonee protezioni, o in alternativa dotando i locali di sistema di allarme

Adeguamento 4
Mettere in sicurezza, ove necessario, le porte di accesso agli uffici ove sono trattati dati personali, anche attraverso l'installazione di serrature efficienti e sicure.

Adeguamento 5
Provvedere in modo adeguato alla gestione delle chiavi di accesso agli uffici attraverso:

- misure che identifichino e responsabilizzino i soggetti interni o esterni cui vengono affidate;
- la custodia di copie di sicurezza.

5.1.2 Sicurezza degli archivi

Adeguamento 6
Dotare ogni posto di lavoro ove opera un incaricato del trattamento dati sensibili e giudiziari di almeno un contenitore (cassetto, armadio) con serratura efficiente e sicura. Provvedere in modo corretto alla gestione delle chiavi (affidamento formale, custodia della copia da parte del responsabile del servizio).

Adeguamento 7
Le banche di dati personali (sensibili e non) devono essere contenute in contenitori adeguati (schedari, armadi) dotati di serratura efficiente e sicura. Provvedere in modo corretto alla gestione delle chiavi (affidamento formale, custodia della copia da parte del responsabile del servizio).

Adeguamento 8

a) Devono essere indicati con adeguata segnaletica i locali interdetti al pubblico.
b) Nei locali accessibili al pubblico deve essere delimitata l'area di accesso.
c) Nei locali accessibili al pubblico per i quali non è possibile, per ragioni strutturali delimitare l'area di accesso, gli utenti sono ammessi uno alla volta adottando opportune misure organizzative (comunicazioni scritte, segnaletica o altro)

Adeguamento 9

Per i locali dell'archivio come prescrive anche il DPR 445/2000, il responsabile con funzioni di coordinamento autorizzerà per scritto l'accesso ed i trattamenti consentiti.

5.1.3 Attuazione degli adeguamenti riferiti alle misure fisiche

- L'attuazione degli adeguamenti 1,2,3, 4 sarà effettuata a cura del Servizio Lavori Pubblici e *Tecnico-manutentivo entro i termini di legge.*

- L'attuazione degli adeguamenti 5, 6, 7 e 8 sarà curata dai responsabili competenti.

5.2 Misure informatiche

Il campo di applicazione della Sicurezza Logica riguarda la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento e utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.
Il Disciplinare tecnico in materia di misure minime di sicurezza, allegato B al Codice, prescrive l'adozione di alcune modalità tecniche che nel comune di Montevarchi si sintetizzano come segue.

5.2.1 Sistema di autenticazione

Adeguamento 10

Devono essere rese operative per gli incaricati di trattamento le credenziali di autenticazione.
Le credenziali per l'autenticazione consistono, nel sistema informatico attualmente in uso, in coerenza con quanto prescritto dal Disciplinare tecnico – allegato B al Codice punto 2, da un codice per l'identificazione dell'incaricato associato a una parola chiave.
La gestione del sistema di autenticazione informatica, per gli incaricati, sarà disposto dal responsabile informatico, come segue:

a) la parola chiave viene assegnata dal responsabile all'incaricato all'avvio dell'applicazione delle norme definite dal presente Documento o all'atto del primo conferimento dell'incarico.
b) la parola chiave deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi;
c) in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;
d) la parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato;
e) le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle autorizzate per scopi di gestione tecnica;
f) ad ogni modifica della parola chiave, la parola chiave scelta dall'incaricato è inserita in una busta sigillata con all'esterno dati identificativi dell'interessato e la data di consegna; la busta sarà consegnata al responsabile (di settore o informatico) che la custodirà garantendo la segretezza del contenuto;
g) in caso di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il responsabile potrà accedere alla credenziale; provvedendo ad avvertire tempestivamente l'incaricato.

Adeguamento 11

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della credenziale per l'autenticazione (punto 10 del Disciplinare

Tecnico in materia di misure minime di sicurezza), il responsabile informatico definisce la procedura con la quale il titolare può assicurarsi la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento del responsabile informatico stesso.

5.2.2 Sistema di autorizzazione

Adeguamento 12
La gestione del sistema di autorizzazione, previsto per le procedure informatiche centralizzate viene disposto dal responsabile, per il servizio di competenza.
I profili di autorizzazione sono individuati e configurati all'avvio dell'applicazione delle norme definite dal presente Documento, su indicazione del responsabile, attraverso il responsabile informatico.

5.2.3 Altre misure

Adeguamento 13
I responsabili redigono entro XXXXXXXXXXX, per la propria area di competenza, la lista degli incaricati di trattamento specificando l'ambito di trattamento consentito ed i relativi profili di autorizzazione.
Almeno annualmente sarà verificata da parte dei responsabili, per la propria area di competenza, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Si allega al presente documento lo schema di lista per l'individuazione degli incaricati di trattamento con strumenti informatici con i relativi profili di accesso.
La lista viene conservata dal responsabile e copia della stessa inserita nel "fascicolo della privacy" a cura del responsabile con funzioni di coordinamento.

Adeguamento14
Il responsabile informatico,
a) dispone che i dati personali siano protetti contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
b) impartisce istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale e provvede all'istituzione di un registro per il backup;
c) provvede alla custodia in un luogo sicuro delle copie di backup;
d) dispone la custodia dei supporti rimovibili contenenti dati personali individuando contenitori con idonee caratteristiche di sicurezza;
e) dispone la distruzione di supporti rimovibili contenenti dati sensibili e giudiziari non più utilizzati;
f) dispone e verifica la cancellazione di tutti i dati personali dagli strumenti informatici non più utilizzati o utilizzati in attività diverse da quelle amministrative.

Adeguamento 15
Il responsabile informatico quando l'Amministrazione si avvarrà di soggetti esterni per la fornitura di prodotti o servizi finalizzati alla realizzazione di misure minime di sicurezza, si farà consegnare dal soggetto medesimo una descrizione scritta dell'intervento che ne attesti la conformità a quanto disposto dal disciplinare tecnico allegato B del Codice.

Adeguamento 16
Per gli elaboratori non in rete (stand alone) è necessario, in aggiunta agli adeguamenti precedenti, che il responsabile informatico provveda a:
- definire puntualmente e attraverso la redazione un apposito registro degli utenti;
- le modalità per l'esecuzione del backup (procedura, incaricato, supporto, custodia delle copie);
- dotare i PC di un gruppo di continuità;
- dotare i PC di un software antivirus aggiornato
- se il PC ha la possibilità di accedere alla rete Internet in modo autonomo è necessario dotarlo di un Firewall software

Adeguamento 17
Per gli elaboratori portatili è necessario, in aggiunta agli adeguamenti precedenti, che il responsabile informatico provveda a:

- creare un registro con la lista aggiornata degli affidatari e degli utenti;
- impartire istruzioni per la realizzazione del salvataggio;
- provvedere all'addestramento degli utenti autorizzati all'utilizzo sicuro degli apparati con riferimento specifico alle misure minime di sicurezza in materia di trattamento dei dati personali;
- curare l'installazione di dispositivi aggiuntivi di sicurezza, con procedure di utilizzo, per diminuire il rischio di furto;

Adeguamento 18
Provvedere alla istituzione e all'aggiornamento, da parte del responsabile informatico, di un registro nel quale vengano annotati guasti o malfunzionamenti hardware e software.

Adeguamento 19
Provvedere a dotare di apposita segnaletica (conforme con quella indicata dal Garante) le aree sottoposte a videosorveglianza.

5.2.4 Attuazione degli adeguamenti riferiti alle misure informatiche

Per quanto attiene agli adeguamenti del sistema informatico descritti ai punti precedenti l'Amministrazione può provvedere nei tempi previsti dato che:

a) il software di gestione appare in linea con le norme e si tratta quindi solo di attivare le previste procedure di autenticazione;

b) l'attivazione di idonei strumenti elettronici per prevenire il rischio di intrusione nel sistema informatico ha aspetti tecnici, organizzativi e economici sostenibili;

c) l'attivazione di idonei strumenti per prevenire la perdita dei dati è del pari realizzabile mediante misure organizzative e con modesti impegni economici.

5.3 Misure organizzative

Accanto all'adozione di misure tecnologiche già illustrate, è necessario, come richiamato, vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo di sicurezza.

Gli aspetti organizzativi riguardano principalmente:

- la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo Sicurezza;
- l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

Un ulteriore aspetto inerente la Sicurezza Organizzativa è quello concernente i controlli sulla consistenza e sulla affidabilità degli apparati.

In ordine alla norme di comportamento, si rimanda a quanto è definito nei documenti di nomina per l'assegnazione di responsabilità ed incarichi ed a quanto specificato nell'allegato A.

I responsabili relativamente ai propri ambiti di competenza, aggiornano almeno annualmente la lista degli incaricati (redatta anche per classi omogenee di incarico) con i relativi profili di autorizzazione utilizzando gli allegati B e C.

6 Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di affidamento del trattamento a soggetti esterni

Nel caso di affidamento da parte dell'Amministrazione a soggetti esterni di attività che comportino trattamento dei dati conviene distinguere fra:

a) affidamento a persone fisiche;
b) affidamento a persone giuridiche.

6.1 Affidamento a persone fisiche.

Nel caso che il soggetto sia una persona fisica lo stesso sarà nominato, dal titolare o dal responsabile competente, incaricato di trattamento dati attraverso un atto di nomina che specifichi puntualmente le norme di comportamento da seguire.
Sarà cura del titolare e dei responsabili, per i settori di competenza, individuare i soggetti esterni che per l'espletamento di incarichi conferiti dall'Amministrazione devono avere accesso a dati personali.
Ove necessario il titolare o il responsabile competente provvederanno a informare l'incaricato sui contenuti fondamentali delle norme che disciplinano il trattamento dei dati personali.
Il titolare o il responsabile verificheranno periodicamente, nelle forme ritenute più opportune, sulla correttezza del trattamento, con particolare riferimento all'adozione delle misure minime di sicurezza, da parte degli incaricati

6.2 Affidamento a persone giuridiche.

Nel caso che il soggetto cui viene affidato un incarico sia una persona giuridica la stessa sarà nominata dal titolare **responsabile esterno di trattamento dati,** attraverso un atto di nomina che specifichi puntualmente le norme di comportamento da seguire con specifico riferimento alle misure minime di sicurezza da adottare.
Il titolare vigilerà sulle attività relative al trattamento dipendenti dal responsabile esterno e si farà rilasciare dallo stesso una dichiarazione di conformità a quanto stabilito dalle norme di legge e dal presente documento.

7 Modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Il responsabile con funzioni di coordinamento nel caso del verificarsi di eventi che provochino la distruzione od il danneggiamento dei dati personali contenuti nelle banche dati del sistema informatico, provvederà senza ritardo a ripristinare la funzionalità delle banche dati.

Il ripristino della disponibilità dei dati andati perduti a causa di eventi di diversa natura consiste di norma

- nella installazione del software di base, dei programmi, di tutti i file di dati,
- nella sostituzione di componenti hardware che hanno provocato la interruzione dei trattamenti.

La re-installazione del software di base, dei programmi di office automation e dei file di dati residenti nei PC sarà effettuata dall'incaricato con funzioni di amministratore di sistema.
La re-istallazione del software di rete, dei programmi gestionali e dei file di dati residenti nel server sarà effettuato dal soggetto titolare del contratto di manutenzione software.
La sostituzione di componenti hardware non funzionanti sarà effettuato dal soggetto titolare del contratto di manutenzione hardware.
Nei contratti di manutenzione stipulati con i fornitori di software e hardware dovrà essere inserita una specifica clausola che consenta il ripristino della funzionalità del sistema informatico e della disponibilità dei dati entro il tempo stabilito dalla legge.

8 Interventi formativi

Il personale del Servizio informatico ha partecipato a specifiche attività formative organizzate da soggetti esterni.
Nell'estate 2004 alcuni dirigenti e funzionari hanno partecipato ad una attività formativa organizzata dall'amministrazione, nella quale sono stati illustrati i principali contenuti del D.Lgs. 196/2003 e gli adempimenti connessi

8.2 Interventi formativi iniziali

In coerenza con quanto previsto dalle norme è necessario, insieme alla realizzazione degli adempimenti riguardanti la sicurezza del trattamento dei dati personali, provvedere alla formazione iniziale di tutto il personale in servizio.

8.3 Interventi formativi al momento dell'ingresso in servizio

Il personale che prende per la prima volta servizio nel Comune verrà (in)formato sui contenuti del Codice, anche attraverso la fornitura di materiale di sintesi, dal responsabile competente.
In sede di verifica dell'efficacia delle misure di sicurezza il responsabile con funzioni di coordinamento in accordo con il responsabile informatico, qualora necessario, programmerà attività formative per il personale che ha preso servizio nella istituzione e che non è stato in precedenza sottoposto a formazione sui temi di cui si tratta.
Il personale a convenzione al momento dell'ingresso in servizio verrà (in)formato sui contenuti del Codice e sui doveri da esso derivanti, anche attraverso la fornitura di materiale informativo, di sintesi dal responsabile competente.

8.4 Interventi formativi di aggiornamento

In sede di verifica dell'efficacia delle misure di sicurezza, anche in relazione a novità che si dovessero presentare nelle norme di legge e/o in relazione all'evoluzione tecnica del settore, il responsabile con funzioni di coordinamento, in accordo con il responsabile informatico, programmerà le necessarie attività formative.

9 Misure specifiche per i dati personali idonei a rivelare lo stato di salute

Questa istituzione tratta dati idonei a rivelare lo stato di salute esclusivamente per finalità previste dalla legge.
Secondo quanto prescritto dall'articolo 22 comma 7 del D. lgs 196/2003 i dati idonei a rivelare lo stato di salute *"sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo"*; inoltre il comma 7 dello stesso articolo dispone che i dati idonei a rivelare lo stato di salute, qualora contenuti in banche dati informatiche vengano trattati *"con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altre soluzioni, che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità"*.

Il trattamento dei dati di cui si tratta al momento è realizzato senza l'ausilio di strumenti elettronici,

a) Dati riguardanti il personale
I dati consistono essenzialmente in certificati medici, necessari per lo svolgimento di specifici procedimenti, consegnati o fatti pervenire all'ufficio personale
Dopo la ricezione, durante il trattamento (protocollazione etc) saranno inseriti in una contenitore chiuso riferito all'interessato e successivamente inseriti nel fascicolo personale, dove saranno conservati all'interno di una busta chiusa recante l'indicazione del contenuto separatamente dagli altri documenti.

b) Dati riguardanti interessati non dipendenti
I dati consistono essenzialmente in certificati medici, necessari per lo svolgimento di specifici procedimenti riferiti ai servizi sociali e ai servizi scolastici.
Dopo la ricezione e protocollazione i dati saranno inseriti in un contenitore chiuso riferito all'interessato e successivamente trattati da personale incaricato e custoditi in appositi contenitori chiusi.

Allegati

A – documenti di nomina per l'assegnazione di responsabilità ed incarichi
B – lista degli incaricati di trattamento con strumenti elettronici
C – lista degli incaricati di trattamento senza l'ausilio di strumenti elettronici