Allegato "A" alla deliberazione della Giunta Comunale N. _30_ in data _29.03.2009____

# Documento programmatico di Sicurezza redatto ai sensi dell'allegato B del dlgs n. 196/2003

# ANNO 2010

Un argomento di primaria importanza della legge 196/2003 riguarda la salvaguardia dei dati e le opportune misure di sicurezza da adottare.

L'adeguamento della sicurezza (organizzativa e tecnologica) nel trattamento dei dati personali, interessa sia il trattamento effettuato tramite apparecchiature e procedure informatiche sia il trattamento effettuato tramite supporti cartacei e comprende quindi:

- Analisi delle vulnerabilità
- Analisi delle contromisure esistenti
- Proposte di interventi migliorativi

Molto importante è che i dati vengano custoditi in modo da ridurre al minimo i rischi derivanti da:

- distruzione
- perdita, anche accidentale
- accesso non autorizzato
- trattamento non consentito o non conforme alla finalità di raccolta.

**Il Dlgs N. 196/2003 ha individuato nel documento programmatico di sicurezza lo strumento per rendere effettiva l'attuazione delle misure minime di sicurezza:**

## A) Il documento programmatico sulla sicurezza

Il documento programmatico di sicurezza definisce le misure minime che sono adottate dal Comune di Lusigliè per garantire la tutela e l'integrità dei dati trattati sia in forma elettronica che senza ausilio di strumenti elettronici;
Per il trattamento dei dati effettuato con strumentazioni elettroniche è necessario rispettare quanto stabilito dall'allegato B:

- obbligo di autentificazione informatica, login e passward;

- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

In generale è necessario individuare
- i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali stessi,
- i criteri e le procedure per assicurare l'integrità dei dati,
- i criteri e le procedure per la sicurezza delle trasmissioni dei dati compresi quelli per le eventuali restrizioni all'accesso per via telematica,
- la formazione agli incaricati del trattamento inerente i rischi individuati e i modi per prevenire eventuali danni.

Quindi a tale fine devono essere predisposte contromisure di sicurezza

- **fisiche**

- **logiche**

- **organizzative**

## IL SISTEMA INFORMATICO DEL COMUNE DI LUSIGLIE'

## LA SITUAZIONE ATTUALE

Il Sistema Informatico di cui è dotato il Comune di Lusigliè è il seguente:

- PC1 (Area Anagrafe - Stato Civile - Elettorale ):
  - Microsoft Office Edizione 2007 Versione Office Basic OEM
    Applicativo:
  - Sintecoop Release J 02.00.01 (Anagrafe ed Elettorale)
  - " " " J 02.00.01 (Stato Civile)
  - ANAGAIRE 3.0.0
  - AIRE TXT.dll 3.0.0
  - Protocollo SINT J 02.00.03
  - Delibere
  - Segreteria
  - Collegamento internet

- PC2 (Area Contabile - Finanziaria - TRIBUTI)
  - Microsoft XP Professional Versione 2002
    Applicativo:
  - Sintecoop Rel.se J 02.00.01 (Contabilità - Finanza)
  - " " " 07.01.08 (Tarsu)
  - " " " 04.07.01 (Acquedotto)
  - Determine
  - Segreteria
  - Collegamento internet

- PC3 (Area Segreteria)
  - Microsoft XP Professional Versione 2003
  - Collegamento internet

- PC4 (Area Tecnica)
  - Microsoft Windows XP Professional Versione 2002
  - Collegamento internet

- Sistema rilevazione presenze
  - GEO Easy

- PC 5 Server FUJITSU Siemens
- Microsoft XP Professional Versione 2003
- NAS Sistema di Backup di rete: THECUS N2050

Esso rispetta le prescrizioni contenute del Dlgs 196/2003 in quanto:

- **l'autenticazione informatica è garantita, infatti:**

1. ogni Personal Computer deve essere dotato di password di accesso all'accensione conosciuta esclusivamente dall'assegnatario della stazione di lavoro(PASSWORD DI BIOS);
2. l'accesso al Sistema avviene tramite password di accesso;
3. a ciascun utente del Sistema deve essere attribuito un codice identificativo personale per l'accesso al Sistema;
4. qualora il codice non venga utilizzato da almeno sei mesi, le stesse vengono disattivate;
5. la credenziale cessa di avere valore quando il suo titolare perde la qualifica di incaricato.

**Ai sensi dell'art. 34 del dlgs n. 196/2003, il sistema di autorizzazione prevede che:**

- l'accesso ai singoli applicativi e, all'interno degli stessi, ai singoli tipi di dati e/o documenti, è determinato sulla base di autorizzazioni assegnate singolarmente o per gruppi di lavoro esclusivamente ai dipendenti che, per le mansioni che svolgono, hanno necessità di operare sui dati in essi contenuti.

* Sarebbe opportuno distinguere in:

- accesso di primo tipo lettura copia: a questi operatori non è consentita la modifica e la cancellazione dei dati;
- accesso di secondo tipo lettura copia cancellazione e modifica del documento: a questi operatori è consentito agire direttamente sul documento modificandolo o cancellandolo;

- ogni anno deve essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, ed in base ad essa operare per conseguenza;
- la validità delle richieste di accesso è verificata dal Sistema prima di consentirne l'accesso stesso, il sistema informatico di Lusigliè richiede per accedere al sistema operativo o al singolo applicativo una password di accesso conosciuta solo da chi è responsabile o incaricato del trattamento;
- tutte le informazioni contenenti dati personali e/o sensibili vengono "salvate" esclusivamente sui dispositivi di memorizzazione esterni.

**Situazione esistente allo stato attuale nel Comune di Lusigliè**

* le strutture informatiche del Comune di Lusigliè non distinguono tra accesso di primo tipo ed accesso di secondo tipo;

- bisogna procedere all'individuazione delle singole banche dati sensibili per permettere di individuare quali dati debbano essere conservati su supporti esterni;
- manca l'individuazione di un termine per la verifica dello stato di sussistenza delle autorizzazioni;

**Correttivi che l'Amministrazione intende apportare:**

* distinzione tra accesso di primo e secondo tipo, indicando quali soggetti sono legittimati ad operare nel primo e nel secondo caso, mediante apposito atto scritto. Tale distinzione dovrà già essere in atto quando il Comune di Lusigliè accederà alla rete intranet;

- individuazione delle banche dati distinte in sensibili e utilizzando l'allegato "C" oggetto di approvazione di GC n. 52/04;

- individuazione nella data del 31/12 di ogni anno del termine ultimo per verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;

**Le altre misure di sicurezza previste dall'allegato B al dlgs n. 196/2003 sono garantite in quanto:**

- ogni elaboratore è protetto contro il rischio di intrusione ad opera di programmi di cui all'articolo 615 quinques del Codice Penale mediante appositi programmi che vengono aggiornati periodicamente e la cui efficacia è verificata contestualmente all'esecuzione degli aggiornamenti;
- ogni incaricato o responsabile è dotato di una password per accedere all'elaboratore;
- le copie di Backup vengono eseguite settimanalmente di venerdì a fine sessione lavoro, salvo i dati relativi al protocollo informatico che vengono salvati quotidianamente con metodo "differenziale"
  Il metodo differenziale prevede un salvataggio dei dati relativi alla singola giornata lavorativa.
  Il Comune di Lusigliè adotta due supporti informatici formato zip distinti per giorni dispari e pari.
- Tutti i supporti magnetici formato zip utilizzati da responsabili ed incaricati sono conservati in cassaforte ignifuga ;
- **Tutte le informazioni contenenti sensibili vengono "salvate" esclusivamente sui dispositivi di memorizzazione i cui dischi sono accessibili solo dagli incaricati e dal responsabile**;
- Sono garantiti aggiornamenti periodici dei programmi volti a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti, tali aggiornamenti avvengono settimanalmente mediante programmi PC 1 McAfee 8.5.0i - PC 2 McAfee 8.5.0i - PC3 VirusScan Enterprise 8.5.0i - PC 4 McAfee 8.5.0i - PC 5 McAfee 8.5.0i

mentre la tutela da accessi indesiderati dalla rete è garantita dalla predisposizione di appositi programmi fire-wall presenti su ogni elaboratore (con accesso internet).

**Particolari misure verranno adottate per i dati sensibili conservati in una apposita cartella non condivisa ed accedibile solo da chi è stato previamente incaricato**

Per i dati sensibili che sono conservati solo su supporto cartaceo il Comune ne prevede la custodia e conservazione in appositi faldoni accedibili solo dagli incaricati o responsabili del trattamento, unici soggetti legittimati a visionare il contenuto.
Gli incaricati sono gli unici che possono permettere a soggetti esterni la visione do la copia del documento sensibile previa autorizzazione del responsabile.

## IL SISTEMA DI SICUREZZA DEL COMUNE DI LUSIGLIE'

### Criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati

Le misure di sicurezza previste sono le seguenti:

- La protezione dei locali del Municipio è garantita da un nuovo sistema di allarme, antintrusione acquistato il 31.08.2006.

- La protezione delle copie dei dati avviene utilizzando apposita cassaforte ignifuga.

- Lo Stabile Comunale si compone di due piani.

1. Al piano terra è situato il salone comunale munito di estintori.
2. Al primo piano sono presenti gli uffici e la sala del Consiglio. Su tutto il piano è in funzione un sistema di antifurto sonoro che viene inserito ogni sera dall'ultima persona che esce dallo stabile. Sono presenti estintori.

### Criteri e procedure adottate o in corso di adozione per assicurare l'integrità dei dati

Le procedure previste atte a garantire ed assicurare l'integrità ai dati sono le seguenti:

- Armadi e cassetti chiudibili a chiave
- Uffici chiudibili a chiave
- Utilizzo di Password su ogni stazione di lavoro
- Controlli anti virus aggiornati almeno ad ogni settimana. Sistema firewall.
- Copie di Badkup effettuate settimanalmente, il venerdì a fine sessione di lavoro
- Procedure di recovery
- Gruppi statici di continuità su tutti i Server
- Registrazione degli accessi per il trattamento di tutti di dati sensibili

### Criteri e procedure atte a garantire la sicurezza nella trasmissione dei dati adottati o in corso di adozione

Le procedure previste per garantire la sicurezza nella trasmissione dei dati sono le seguenti:

- Controlli di identificazione e di autenticazione all'accesso. Ogni dipendente è munito di password personale e quindi l'accesso al sistema avviene in base ad esso

- Controlli anti intrusione aggiornati almeno ogni settimana. L'aggiornamento di McAfee e del F.Secure dovrebbe garantire una adeguata sicurezza

- Accesso controllato ed indirizzato alle singole informazioni, da realizzarsi mediante un accesso graduale alle informazione. Ciò richiedera' la creazione di due accounts di livello diverso o quanto meno la protezione dei files che sono presenti sul computer e oggetto di particolare tutela di una password di accesso che ne inibisca l'utilizzo da parte di chi non è autorizzato.

- Inibizione dell'accesso a dati sensibili o da altri dati "non conoscibili" dall'esterno

- Accreditamento ed accesso graduale a tutti i dati contenuti nei pc in uso nel Comune, in base alle competenze svolte. Tali accessi ed accreditamenti sono verificati annualmente.

## Formazione del personale

La formazione degli Incaricati del trattamento avviene con:

- Istruzioni interne elencate nel paragrafo denominato "CODICE DI COMPORTAMENTO A TUTELA DELLA SICUREZZA DEI DATI".

- Corsi di aggiornamento inerenti le modalità di attuazione della legge 196/2003

- Adozione di specifiche determinazioni contenenti le linee guida sulla sicurezza.

## CODICE DI COMPORTAMENTO A TUTELA DELLA SICUREZZA DEI DATI

Tutti gli incaricati del trattamento devono attenersi scrupolosamente alle seguenti indicazioni:

- Ogni Personal Computer sarà, formalmente e per iscritto, assegnato ad un dipendente che è l'unica persona autorizzata ad utilizzarlo, salvo diversa autorizzazione del Segretario.

- E' fatto divieto al personale di consentire ad Amministratori, cittadini ed altre persone non autorizzate per iscritto dal Titolare o dal Responsabile di utilizzare gli strumenti informatici installati negli uffici.

- L'accensione del Personal Computer è protetta da password inserita dall'assegnatario stesso.

- Il dipendente deve accertarsi che nel suo computer siano sempre in funzione le password di bios, accesso al sistema e di screen saver.

- E' vietato modificare la configurazione hardware e software dei singoli Personal Computer.

- L'accesso al Sistema avviene tramite l'identificativo utente e la password ad esso abbinata. Essi sono strettamente personali e il dipendente non deve assolutamente divulgarli.

- Le operazioni di immissione delle password deve essere svolta con modalità che garantiscano la segretezza delle stesse.

- Il dipendente è responsabile di tutte le attività che sono eseguite con il suo identificativo e la sua password. Deve quindi prestare la massima attenzione nel permettere a terzi dipendenti l'uso del proprio pc.

- Tutte le password utilizzate dagli incaricati o responsabili sono conservate su supporto cartaceo custodito in cassaforte ignifuga.

- Al fine di evitare, durante le brevi assenze dell'assegnatario, l'utilizzo della stazione di lavoro da parte di persone non autorizzate, su ogni Personal Computer viene configurato apposito "Screen Saver" protetto da password

- Al termine della giornata di lavoro, il Personal Computer deve sempre e comunque essere spento.

- E' assolutamente vietato "salvare" file contenenti dati personali o sensibili sui dispositivi di memorizzazione (hard disk) delle stazioni di lavoro, diverse da cartelle o file adeguatamente protetti. Essi devono obbligatoriamente essere "salvati" sulle aree del computer cui ciascun utente ha accesso. La sicurezza in questo caso può essere garantita anche applicando una apposita password al file il cui contenuto è sensibile o giudiziario

- Qualsiasi file "scaricato" dalla Rete Internet o ricevuto tramite e-mail ovvero acquisito con qualsiasi altra modalità deve essere sottoposto immediatamente, e comunque prima del suo utilizzo, a scansione tramite il programma antivirus in dotazione.

- Il Segretario Comunale o un suo delegato hanno accesso completo a tutti i dispositivi di memorizzazione (hard disk) di singoli Personal Computer.

- E' vietato divulgare ad altri, a qualsiasi titolo, qualsivoglia informazione di natura informatica, sia essa rappresentata da procedure, programmi, archivi, dati od altro di proprietà dell'Ente. E' altresì vietata la comunicazione ad altri, siano essi privati cittadini ovvero ditte, di dati o notizie riguardanti sia singole apparecchiature sia il Sistema Informatico nel suo complesso.

- E' vietato l'accesso ai locali del CED alle persone non addette all'Ufficio. Chiunque avesse necessità di accedervi dovrà essere preventivamente autorizzato.

- I dati di natura informatica che, in virtù di leggi e regolamenti, debbano essere, con qualsiasi modalità, compresa la posta elettronica, trasferiti all'esterno devono essere preventivamente sottoposti all'autorizzazione del responsabile del trattamento.

- Gli eventuali dati sensibili registrati su supporti cartacei devono essere conservati in buste chiuse o in appositi faldoni ed in armadi chiusi. Quando vengono affidati agli incaricati del trattamento, gli stessi sono controllati e custoditi dagli incaricati fino alla restituzione al responsabile.

- La trasmissione dei dati personali, all'interno del Comune o anche verso terzi all'esterno, incaricati di trattare i dati, deve essere fatta salvaguardando la riservatezza dei dati e comunque secondo le istruzioni impartite.

Il presente codice di comportamento deve essere formalmente consegnato a ciascun incaricato.

In caso di inadempienza delle norme operative e delle istruzioni contenute nel presente documento, il dipendente resta responsabile in proprio delle conseguenze civili e penali previste dalle violazioni agli obblighi del dlgls n. 196/2003.

Modifiche avvenute nell'anno 2009