COMUNE DI LAVAGNA
Provincia di Genova

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Seduta del 28/03/2013

N. 42

OGGETTO : AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (D.P.S.S.) - ANNO 2013.

L'anno Duemilatredici, addì ventotto del mese di Marzo, alle ore 15:30 convocata nei modi e nei termini di legge, si è riunita nella solita sala delle adunanze la Giunta Comunale composta dai Signori:

			PRESENTE	ASSENTE
1.	VACCAREZZA GIULIANO	- Sindaco	X	
2.	CAVERI MAURO	- Vice Sindaco	X	
3.	ARMANINO MAURO	- Assessore	X	
4.	BACCHELLA LAURA	- Assessore	X	
5.	DASSO LORENZO	- Assessore	X	
6.	MANCA RAFFAELE	- Assessore	X	
7.	STEFANI GUIDO	- Assessore		X
		TOTALE	6	1

Partecipa il Segretario Generale Dott. ORLANDO CONCETTA

Il Sig. Giuliano Vaccarezza, nella Sua qualità di Sindaco, assunta la Presidenza, constatata la legalità dell'adunanza e dichiarata aperta la seduta, invita la Giunta a trattare le pratiche elencate nell'ordine del giorno.

LA GIUNTA COMUNALE

Su relazione dell'Assessore all' Innovazione, **Mauro Caveri** ed in conformità della proposta di deliberazione allegata all'originale;

Premesso:

che il Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali" (di seguito Codice) disciplina - al titolo V (Articoli 31 e seguenti) - la sicurezza dei dati e dei sistemi, prevedendo l'obbligo di adottare le misure di sicurezza volte ad assicurare un livello minimo di protezione dei dati personali in caso di trattamenti effettuati sia con strumenti elettronici sia senza di essi;

che, in particolare, il disciplinare tecnico allegato al predetto Codice (Allegato B) detta specifiche disposizioni da seguire per garantire tali misure minime;

Dato atto che, in ottemperanza alla suesposta normativa, il Comune di Lavagna ha sempre provveduto, nei termini e con le modalità previste dalla legge, alla stesura ed all'aggiornamento annuale del Documento programmatico sulla Sicurezza, previsto dalla lettera g) dell'articolo 34 del D. Lgs. n. 196/2003;

Considerato che la normativa in materia di protezione dei dati personali ha subito alcune rilevanti modifiche con riferimento agli adempimenti previsti in materia di misure minime; infatti, l'articolo 45 del Decreto legge n. 5 del 9.2.2012 "Disposizioni urgenti in materia di semplificazione e sviluppo", modificando l'articolo 34 del Codice sulla Privacy, ha soppresso l'obbligo di redigere annualmente il DPSS (previsto dall'articolo 34, comma 1, lett. g) nonché i paragrafi 19 (punti da 19.1 a 19.8) e 26 del relativo disciplinare tecnico sulle misure minime di sicurezza;

Tuttavia, pur essendo stati semplificati gli adempimenti previsti non risulta essere in alcun modo venuto meno l'obbligo di garantire la sussistenza delle misure minime di sicurezza per il trattamento dei dati, né le sanzioni relative ad eventuali omissioni in tal senso (articolo 169 del Codice);

Richiamata la deliberazione di Giunta Comunale n. 34 del 23.02.2012, avente ad oggetto " Adozione di misure organizzative in materia di protezione dei dati personali di cui al Decreto Legislativo n. 196/2003 e successive modifiche ed integrazioni", con la quale - tra l'altro - è stato disposto che pur essendo venuto meno l'obbligo di redigere il Documento Programmatico sulla Sicurezza, si provveda, comunque, all'elaborazione ed all'aggiornamento annuale di un documento

che non costituisca mero adempimento burocratico ma risponda all'esigenza, sempre presente, di verificare periodicamente le dotazioni informatiche e di sicurezza nonché l'adeguatezza delle misure organizzative, fisiche ed informatiche adottate;

Verificato che, con la suesposta deliberazione, si è già provveduto all'approvazione di un disciplinare tecnico in materia di trattamento dei dati personali affidati ai lavoratori, adeguatamente divulgato tra tutto il personale, che viene espressamente richiamato nel Documento sulla sicurezza;

Dato atto che per quanto sopra la Giunta Comunale, con deliberazione n. 51 del 29.03.2012, ha ritenuto necessario approvare il Documento programmatico sulla Sicurezza per l'anno 2012 ritenendo che lo stesso, seppur superato dal punto di vista del mero adempimento normativo, continui a costituire uno strumento indispensabile di verifica per l'adeguatezza delle misure si sicurezza adottate all'interno dell'ente;

che con la predetta deliberazione è stato disposto l'aggiornamento annuale del documento a cura di un gruppo di professionalità esistenti all'interno dell'ente, ciascuna coinvolta per la parte di competenza e così costituito:

Anna E. Ferri - Responsabile URP Servizi Demografici
Elisabetta Canepa - Ufficio Risorse Umane
Giuseppe Benini - Ufficio CED
Enrico Agosti - Responsabili UO Lavori Pubblici e Ambiente
Giampiero Donati - Responsabile Ufficio impianti Tecnologici

Il predetto gruppo di lavoro ha l'incarico di aggiornare annualmente il Documento sulla Sicurezza in stretta collaborazione con il Comitato di Direzione dell'Ente.
L'aggiornamento del documento per l'anno 2013 è quindi avvenuto da parte del gruppo come sopra incaricato, integrato dal Dott. Ing. Simone Menini, assunto presso questo ente in data 31.12.2012 in qualità di Istruttore Direttivo Servizi Informatici - assegnato all'Ufficio CED e nominato Amministratore di Sistema con atto del Sindaco n. 953 del 09.01.2013;

Dato atto che la bozza di Documento sulla sicurezza predisposto dal gruppo incaricato, contenente gli aggiornamenti per l'anno 2013 è stata trasmesso ai Dirigenti dell'Ente per eventuali modifiche o integrazioni;

Dato atto che l'adozione del presente provvedimento non comporta alcun onere a carico dell'Amministrazione Comunale e che pertanto non è necessario il parere contabile di cui all'articolo 49 del Decreto Legislativo n. 267/2000;

Dato atto, relativamente alla proposta di deliberazione in argomento, del parere, ai sensi dell'art. 49, comma 1 e 147 bis del D.Lgs. 18.08.2000, n. 267 e ss.mm.ii., seguente ed agli atti:
- parere favorevole del Dirigente del Settore Servizi Finanziari di Staff e Tributi Dott. ssa Enrica Olivieri in ordine alla regolarità tecnica attestante la regolarità e la correttezza dell'azione amministrativa in data 28/03/2013;

Rilevato che l'istruttoria del presente atto è stata svolta dal Responsabile dell'UO Relazioni con il Pubblico - Servizi Demografici - Dott.ssa Anna Elisabetta Ferri;

Con voti favorevoli n° 6, (assente l'Assessore Guido Stefani), palesemente espressi.

DELIBERA

1. Di approvare l'aggiornamento per l'anno 2013 del Documento Programmatico sulla Sicurezza ed i suoi Allegati (Allegato "A" - Elenco dei trattamenti, distribuzione dei compiti e delle responsabilità - ed Allegato "B" Misure di sicurezza adottate o da adottare), allegato alla presente quale parte integrante;

2. Di dare atto che predetto Documento dovrà essere soggetto a revisione ed aggiornamento annuale a cura del gruppo di lavoro così costituito:

   Centro Elaborazione Dati - Simone Menini e Giuseppe Benini
   Lavori Pubblici e Impianti Tecnologici - Enrico Agosti e Pietro Donati
   Risorse Umane - Elisabetta Canepa
   Relazioni con il Pubblico - Anna E. Ferri

3. Di incaricare l'Ufficio Segreteria della trasmissione del presente provvedimento ai Dirigenti, ai titolari di Posizione Organizzativa, al Sindaco ed alla Giunta;

4. Di dare atto che il responsabile del procedimento è la Dott.ssa Anna Elisabetta Ferri, che ha curato l'istruttoria.

Comune di Lavagna
Provincia di Genova

COMUNE DI LAVAGNA

Documento sulla Sicurezza (Ex DPSS)
(D.L.gs.196/2003 e ss.mm.ii.)

AGGIORNAMENTO ANNO 2013
A cura del Gruppo di Lavoro così costituito:
Ufficio CED (Simone Menini – Giuseppe Benini)
Ufficio Impianti Tecnologici (Pietro Donati)
Ufficio Risorse Umane (Elisabetta Canepa)
Ufficio Relazioni con il Pubblico (Anna E. Ferri)

Redatto ai sensi del Decreto Legislativo 30.06.2003 n. 196 "Codice in materia di Protezione dei Dati Personali" e delle successive modifiche e integrazioni ed aggiornato alla luce delle seguenti disposizioni legislative:
(Decreto Legge 6 dicembre 2011 n.201 "Salva Italia" – Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici - convertito, con modificazioni, dalla Legge 22 dicembre 2011 n. 214 e D.L. n. 5 del 9 febbraio 2012 "Decreto Semplificazione" – Disposizioni urgenti in materia di semplificazioni e sviluppo).

INDICE

Allegati:

Introduzione

Il Codice in materia di protezione dei dati personali, emanato con il Decreto Legislativo 30 giugno 2003 n. 196, il cui testo è stato consolidato con la legge 26 febbraio 2004, n. 45, di conversione con modificazioni del DL 24 dicembre 2003 n. 354, riunisce in un unico corpo, omogeneizzandole, tutte le precedenti norme in materia di tutela dei dati personali.
Il comma 1 dell'articolo 5 del Codice in materia di protezione dei dati personali (di seguito Codice) stabilisce che lo tesso *"disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato"*.
L'articolo 31 del Codice enuncia che *" i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione e perdita, anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"*.
Il Codice è stato oggetto di alcune importanti modifiche che hanno, da un lato, profondamente modificato la definizione di "dato personale" e, dall'altro, hanno ridotto gli adempimenti in materia di misure minime di sicurezza. Di seguito si analizzano, nel dettaglio, i seguenti interventi legislativi:

Il cd. Decreto "Salva Italia" – Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici - (Decreto legge 6 dicembre 2011 n. 201, convertito, con modificazioni dalla Legge 22 dicembre 2011 n. 214), all'articolo 40, comma 2 , dispone che:

Per la riduzione degli oneri in materia di privacy, sono apportate le seguenti modifiche al decreto legislativo 20 giugno 2003 n. 196:

a) All'articolo 4, comma 1, alla lettera b) le parole "persona giuridica, ente od associazione" sono soppresse e le parole "identificati o identificabili" sono sostituite dalle parole "identificata o identificabile".[1]
b) All'articolo 4, comma 1, alla lettera i) le parole "la persona giuridica, l'ente o l'associazione" sono soppresse.[2]
c) Il comma 3-bis dell'articolo 5 è abrogato.[3]

---

[1] b) Art. 4, comma 1 lett. b) "dato personale, qualsiasi informazione relativa a persona fisica, **persona giuridica, ente od associazione, identificati o identificabili**, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale";

[2] Art. 4, comma 1 lett. i): "interessato" la persona fisica, **giuridica, l'ente o l'associazione** cui si riferiscono i dati personali;

[3] **Art. 5 comma 3-bis: "il trattamento dei dati personali, relativi a persone giuridiche, imprese enti o associazioni effettuato nell'ambito di rapporti intercorrenti esclusivamente tra i medesimi soggetti per le finalità amministrativo – contabili, come definite dall'articolo 34 comma 1-ter, non è soggetto all'applicazione del presente codice;**

d) Al comma 4 dell'articolo 9, l'ultimo periodo è soppresso.[4]
e) La lettera h) del comma 1 dell'articolo 43 è soppressa.[5]

Da quanto sopra si evince, quindi che è considerato "**dato personale**" "qualunque informazione relativa alla persona fisica e, quindi, non più i dati relativi a società, enti o associazioni; stessa cosa dicasi per la definizione di **interessato,** identificato armai solo con la persona fisica a cui si riferiscono i dati personali. Tuttavia, da queste modifiche, emerge un dato non trascurabile: tra le disposizioni modificate resta immutato il concetto di "**titolare del trattamento**", che è sempre "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo a cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*".
Le suesposte modifiche non devono indurre a pensare che vi siano stati alleggerimenti in materia di privacy o che siano stati abrogati gli obblighi previsti dalla normativa.

---

[4] Articolo 9 comma 4 :" l'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. **Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti".**

[5] Art. 43 : "Trasferimenti consentiti in paesi terzi"
1. Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione Europea è consentito quando:
   a) L'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili", in forma scritta;
   b) E' necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o l'esecuzione di un contratto stipulato a favore dell'interessato;
   c) È necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato i individuato ai sensi degli articolo 20 e 21;
   d) E' necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato o quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82 comma 2.
   e) E' necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n. 397 o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale.
   f) E' effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia.
   g) E' necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi provati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999 n, 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;
   h) Il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

Infatti, con l'abrogazione del comma b bis dell'articolo 5, che prevedeva l'esclusione dall'applicazione del Codice qualora il trattamento dei dati personali fosse effettuato da persone giuridiche, imprese, enti e associazioni, nell'ambito di rapporti intercorrenti tra i medesimi soggetti esclusivamente per finalità amministrativo – contabili, è chiaro che la privacy e tutti i suoi adempimenti continuano ad applicarsi per tutti i titolari del trattamento (siano essi persone fisiche, giuridiche, enti o associazioni).
Inoltre, basti pensare al riformato "Codice dell'Amministrazione Digitale" che ha introdotto notevoli misure di sicurezza tecnologiche ed organizzative (si pensi all'articolo 50 bis sulla "continuità operativa"), che non avrebbero più senso se si intendesse l'attuale riforma del Codice Privacy come semplice alleggerimento degli adempimenti per persone giuridiche ed enti.

Un'altra tornata di modifiche al Codice è stata introdotta dal "Decreto semplificazione" – Disposizioni urgenti in materia di semplificazioni e sviluppo (D.L. n. 5 del 9/2/2012). In particolare dall'articolo 45 (Semplificazioni in materia di dati personali) che testualmente recita:

1. Al decreto legislativo 30 giugno 2003, n, 196, sono apportate le seguenti modificazioni:
    a) All'articolo 21 dopo il comma 1 è inserito il seguente: "1 bis - il trattamento dei dati giudiziari è altresì consentito quando è effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'Interno o con i suoi uffici periferici di cui all'art. 15, comma 2 del decreto legislativo 30 luglio 1999 n. 300, che specificano la tipologia dei dati trattati e delle operazioni eseguibili";
    b) All'articolo 27 comma 1 è aggiunto, infine, il seguente periodo "Si applica quanto previsto dall'articolo 21, comma 1 bis";
    c) All'articolo 34 è soppressa la lettera g) del comma 1 ed è abrogato il comma 1 bis.[6]

---

[6] Art. 34 – Trattamenti con strumenti elettronici.
Comma 1 – il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

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

1-bis: Per i soggetti che trattano soltanto dati personali non sensibili o che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa da titolare del trattamento ai sensi dell'art. 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle misure minime di sicurezza previste dal presente codice e dal disciplinate tecnico contenuto nell'allegato B). in

d) Nel disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B sono soppressi i paragrafi da 19 a 19.8 e 26. [7]

A seguito delle modifiche introdotte dal Decreto Semplificazione, si evince che è stato eliminato uno degli adempimenti in materia di tutela della riservatezza dei dati che fin qui si era tenuti ad osservare: la predisposizione e l'aggiornamento annuale del Documento Programmatico sulla Sicurezza (di seguito DPSS). Ciò non significa, però, che siano venuti meno gli altri obblighi previsti dal Codice in materia di misure minime di sicurezza, né le relative sanzioni in caso di inadempienza. Così come, a parte l'abrogazione dei paragrafi da 19 a 19.8 del Disciplinare Tecnico allegato B) del Codice – disciplinanti appunto le modalità di relazione del DPSS – e del paragrafo 26 (obbligo di dare atto nella relazione accompagnatoria al bilancio della stesura e dell'aggiornamento del DPSS), non sembrano aver perso valore impositivo le modalità tecniche da adottare in caso di trattamento dei dati con strumenti elettronici.
E' del tutto evidente che l'eliminazione del DPSS non equivale in alcun modo all'eliminazione delle misure minime; pertanto, pur non sussistendo più l'obbligo di legge,

---

relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrativo – contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentiti il Ministro per la semplificazione normativa e il Ministro per la pubblica amministrazione e l'innovazione, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico contenuto nel citato allegato B) in ordine all'adozione delle misure minime di cui al comma 1.
1 – ter : ai fini dell' applicazione delle disposizioni in materia di protezione dei dati personali, i trattamenti effettuati per finalità amministrativo – contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale – assistenziale, di salute, igiene e sicurezza sul lavoro.

[7] **Paragrafo 19 dell'Allegato B) :Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o dati giudiziari redige, anche attraverso, il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:**

19.1 l'elenco dei trattamenti di dati personali;
19.2 la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3 l'analisi dei rischi che incombono sui dati;
19.4 le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5 la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6 la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7 la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8 per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato;

Paragrafo 26 dell'allegato B) il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

di formulare il DPSS nelle rigide modalità tecniche originariamente previste, si è ritenuto comunque indispensabile – nell'anno 2012 - formulare un documento nel quale, partendo dalle analisi –annualmente aggiornate - del DPSS, le stesse continuino ad essere elencate, riassunte e pianificate in base ai rischi.

E' altresì evidente che il Comune di Lavagna, in quanto pubblica amministrazione, svolge una serie di attività nei confronti di cittadini ed imprese e, quindi, gestendo una notevole quantità di dati personali (di cui una parte può definirsi come "dati sensibili" ed una parte come "dati giudiziari"), continui ad elaborare un **documento** relativo alle misure minime di sicurezza nel trattamento di tali dati.

Infatti, con deliberazione di Giunta Comunale n. 51 del 29.03.2012 è stato approvato il **Documento sulla Sicurezza per l'anno 2012,** al quale sono stati allegati l'elenco dei trattamenti, distribuzione dei compiti e responsabilità e la descrizione, a seguito dell'analisi dei rischi, delle misure di sicurezza specificandone l'adozione, la parziale adozione o la mancata adozione. Nella predetta deliberazione si è altresì stabilito che il documento in questione venga aggiornato annualmente da parte di un gruppo di persone operanti all'interno degli Uffici comunali (CED, Risorse Umane, URP, Settore Lavori Pubblici e Impianti Tecnologici) in stretta collaborazione con il Comitato di Direzione dell'ente.

Il predetto gruppo, riunitosi durante il mese di marzo 2013, ha provveduto all'aggiornamento del documento per l'anno 2013.

Termini e definizioni

Di seguito vengono riportate alcune definizioni, riprese dal decreto legislativo n. 196/2003, aggiornate con le modifiche apportate dai più recenti provvedimenti legislativi (testo consolidato vigente).

Codice: si intende il Codice in materia di protezione dei dati personali emanato con il decreto legislativo 30 giugno 2003, n. 196, il cui testo è stato consolidato con la legge 26 febbraio 2004 n. 45, di conversione con modificazioni del d.l. 24 dicembre 2003, n. 354 – e sue successive modificazioni ed integrazioni.

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

Dato personale: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso il numero di identificazione personale.

Dati identificativi: i dati personali che consentono l'identificazione diretta dell'interessato.

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

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u) del DPR 4 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dai relativi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo, cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazioni od organismo preposti dal titolare al trattamento di dati personali.
Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.
Interessato: la persona fisica cui si riferiscono i dati personali;
Banca dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti.

Verranno utilizzati inoltre i seguenti termini:

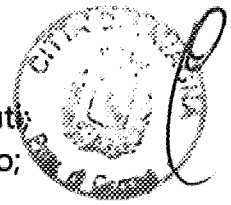
Sicurezza fisica: proteggere le persone che operano sui sistemi, le aree e le componenti del sistema informativo; può essere ricondotta alla sicurezza di area e sicurezza delle apparecchiature.
Sicurezza logica: protezione dell'informazione e, di conseguenza, di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. Sono da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa.

Organigramma della Sicurezza

Con deliberazione della Giunta Comunale n. 34 del 23.02.2012, esecutiva ai sensi di legge, è stato individuato come titolare del trattamento dei dati il Comune di Lavagna rappresentato dal Sindaco *pro tempore*, il quale esercita le prerogative ed adempie agli obblighi che la Legge attribuisce al titolare del trattamento.

Con atti del Sindaco sono stati individuati come responsabili del trattamento, ciascuno per il proprio settore i seguenti dirigenti/incaricati di posizione organizzativa:

- Avv. Dott.ssa Concetta Orlando – Segretario Direttore Generale;
- Dott.ssa Lorella Cella - Vice Segretario – Dirigente Settore Servizi alla Persona, amministrativi di staff;



- ❖ Dott.ssa Enrica Olivieri – Dirigente Settore Servizi Finanziari di staff e tributi;
- ❖ Ing. Renato Cogorno – Dirigente Settore Servizi alle Imprese e al Territorio;
- ❖ Dott. Fabio Terrile – Comandante del Corpo Polizia Municipale.
- ❖ Dott.ssa Anna Elisabetta Ferri – Responsabile Unità Organizzativa Ufficio Relazioni con il Pubblico – Servizi Demografici.

I Responsabili, come sopra indicati, hanno provveduto, con proprio atto scritto, ad individuare il personale incaricato del trattamento al quale sono state fornite le opportune istruzioni.

Con atto del Sindaco prot. n. 5804 del 02.03.2012 è stato nominato Amministratore di Sistema il dipendente addetto all'Ufficio CED, Sig. Giuseppe Benini.
A seguito del potenziamento dell'Ufficio CED con l'assunzione a fine 2012 di un'unità lavorativa nel profilo di "Istruttore Direttivo Servizi Informatici", con atto del Sindaco n. 953 del 09.01.2013 è stato nominato Amministratore di Sistema anche il dott. Ing. Simone Menini.

Elenco dei trattamenti e distribuzione dei compiti e delle responsabilità

La rilevazione dei trattamenti effettuati nei diversi servizi comunali per l'anno 2013 è stata eseguita dal personale incaricato della preparazione del documento e quindi integrata e corretta dai Dirigenti.
L'elenco finale, elaborato sulla base dell'organigramma vigente e indicante, oltre ai trattamenti anche i soggetti individuati quali responsabili ed incaricati del trattamento è allegato al presente documento (**Allegato "A" – Elenco dei trattamenti, distribuzione dei compiti e delle responsabilità**) e ne costituisce parte integrante e sostanziale.
Si precisa che con riferimento alle banche dati:

- I profili di utilizzazione degli applicativi IRIDE MAGGIOLI e LIBRA MAGGIOLI sono differenziati in base alle necessità dei singoli servizi e alle funzioni istituzionali svolte;
- Con riferimento all'applicativo E-DEMOS MAGGIOLI è stata effettuata nel corso del 2013 una ricognizione degli accessi esistenti e sono stati consentiti gli accessi, in modalità visualizzazione, e previa autorizzazione rilasciata dal Responsabile del trattamento (Responsabile URP – Servizi Demografici) a personale dei comune non operante nei servizi demografici sulla base delle richieste motivate dei Dirigenti in relazione alle mansioni svolte ed alle funzioni istituzionali;
- Per quanto riguarda l'accesso alla banca dati SIATEL si rimanda alle determinazioni ed alle disposizioni fornite dall'amministratore di sistema dell'Anagrafe Tributaria dott.ssa Enrica Olivieri.

Analisi dei rischi

Con riferimento all'analisi dei rischi, si ritiene opportuno ribadire alcune note di inquadramento del contesto di riferimento, nonché dare dei chiarimenti rispetto alle

terminologie usate che potrebbero non essere di immediata comprensione per i non addetti ai lavori.

L'infrastruttura informatica

Il palazzo comunale è dotato di una rete locale di tipo Ethernet 10/100 cablata secondo una tipologia a stella, con la dorsale realizzata in fibra ottica. Il centro della stella è costituito da Switch, posto nell'armadio installato al secondo piano, Sala Server, al quale sono collegati, sempre con cavi in fibra ottica, gli altri switch posizionati, negli armadi posti ad ogni piano del palazzo.La distribuzione orizzontale dagli armadi di piano ai terminali è realizzata con cavi in rame UTP di tipologia 6. Il sistema informatico del Comune di Lavagna ha adottato una soluzione di Server Consolidation con l'attivazione di un dispositivo hardware ad elevate prestazioni, in configurazione ridondata e con servizio di manutenzione professionale, su cui è attiva un'infrastruttura di virtualizzazione basata su S.O. VMware ESXi per l'ospitalità dei 5 server di rete su piattaforma Microsoft Windows su cui sono installati gli applicativi dell'ente. Tale soluzione ha permesso l'ottimizzazione delle risorse e delle prestazioni dei dispositivi hardware, la minimizzazione dei costi hardware e di gestione e vista la possibilità di effettuare il Backup dell'intero sistema e quindi di diminuire i tempi di ripristino in caso di compromissione del server virtuale. Attraverso questa soluzione è stato possibile suddividere su più server virtuali i servizi gestiti con un miglioramento dell'efficienza e delle prestazioni senza che questo comporti l'acquisto di hardware aggiuntivo.
Rimane in servizio, ma con programma di dismissione il server IBM AS/400 mod. 800ESERVER, al cui interno è collocata una base dati in sola consultazione dotata di unità nastro per il back-up giornaliero su nastro automatizzato dei dati contenuti. L'impossibilità della virtualizzazione di tale server è conseguenza della non compatibilità del S.O. IBM con la piattaforma VMware ESXi.

Dispositivi della struttura di rete del Comune di Lavagna:

- Server Firewall per la gestione dei seguenti servizi di rete: gestione permessi di accesso alla rete dati, regole di firewalling, protezione della rete
- Gestione della posta elettronica (no PEC) per il dominio: @comune.lavagna.ge.it
- Servizio di Proxy Server per filtraggio della navigazione internet da parte delle postazioni client della rete.
- Servizio di Deposito per lo scambio di file di grosse dimensioni
- Server QNap Storage, sistema NAS Linux per la gestione dei servizi di rete utenti.
- Server QNap Backup , sistema analogo di mirroring d Backup dell'apparato QNap Storage

Si prevede, per l'anno 2013, di creare un sistema di backup fisico dei server in modo tale da permettere un recupero ancora più veloce dei dati in caso di guasto dell'attuale sistema. La virtualizzazione permette, infatti, l'esportazione rapida dei sistemi operativi da un dispositivo fisico all'altro, in quanto il sistema di virtualizzazione astrae la parte fisica variabile del server per creare calcolatori virtuali uniformi e, quindi, altamente sostituibili.

Questa necessità è partita dalla considerazione che la virtualizzazione permette di integrare tutti i server virtuali su un unico server fisico, creando grandi vantaggi per la riduzione dei costi di manutenzione del sistema ma ponendo potenziali problemi per la sicurezza, in quanto concentrare tutte le informazioni in un unico sistema, qualora si dovessero creare problemi a tale dispositivo che non ne consentissero l'uso per periodo di tempo prolungati, impedirebbero l'uso non solo delle basi di dati, ma anche della posta elettronica e della connessione verso l'esterno in generale.

Sistemi di ridondanza

Sono attive delle procedure automatiche per il backup di due tipologie:

- Backup di dati e delle configurazioni degli applicativi più basi dati e utenti.
- Backup dei sistemi virtuali.

Il dispositivo principale di Backup dati è l'apparato "QNap Backup", mentre il dispositivo secondario è l'apparato "QNap Storage". I due apparati sono posizionati presso locali distinti in modo da garantire l'affidabilità in caso di eventi ambientali localizzati.

Backup dati, configurazioni e basi dati

La procedura è automatica con cadenza giornaliera sull'apparato QNap Backup e le retention dei dati archiviati segue lo schema:

- Storico giornaliero lunedì (retention 4: vengono mantenuti i dati a 4 lunedì precedenti)
- Storico giornaliero (retention 1)
- Storico mensile, ogni primo del mese (retention 12)

Backup dei sistemi virtuali

La procedura viene avviata in modo automatico con cadenza mensile e procede al backup di tutti i sistemi virtuali presenti sulla piattaforma VMware.

Di seguito viene riportato - in forma tabellare – uno schema dei possibili guasti/situazioni di anomalie e le relative operazioni che potranno essere intraprese per la riconduzione ad una situazione di operatività stabile

TIPOLOGIA DI GUASTO	AZIONI	TEMPI STIMATI DI RISOLUZIONE
Anomalia applicativi/perdita dati	Ripristino macchina virtuale	Ripristino one-click
	Ripristino dati da back up	Dipendente da tempi fornitore/assistenza su applicativo e dal volume/tempi di copiatura dati
Anomalia sistemistica su server	Ripristino macchina virtuale	Dipendente dai tempi di copiatura da apparato di back-up riattivazione one-click
	Ripristino dati da back up	Dipendente da tempi fornitore/assistenza su applicativo e dal volume/tempi di copiatura dati
Anomalia hardware bloccante su server piattaforma virtuale	Ripristino hardware	Dipendente da tempistiche di assistenza HW

	Ripristino macchina virtuale	Dipendente dai tempi di copiatura da apparato di back-up riattivazione one-click
	Ripristino dati da back up	Dipendente da tempi fornitore/assistenza su applicativo e dal volume/tempi di copiatura dati
Anomala hardware bloccante su server firewall	Attivazione sistema virtuale copia	Attivazione one-click
	Allineamento dati da back-up	Dipendente dal volume dati e dal tempo di copia

I locali

Per quanto riguarda la sala macchine essa è posta nel locale del CED - denominato "Sala Server" - il quale, a sua volta, è collegato al corridoio tramite una porta che, quando il locale non è presidiato, viene mantenuta chiusa a chiave.
Le pareti peraltro offrono molta resistenza ma nel caso di voluto scasso i vetri superiori, lato corridoio, sono facilmente smontabili.
Tutte le altre stanze del palazzo offrono un grado di protezione minimo in quanto chiusi da porte dotati di serratura a chiave ma facilmente apribili non è quindi difficile introdursi negli uffici ed asportare il materiale.
Un discorso a parte meritano gli uffici Anagrafe e Stato Civile, nonché l'URP dotati di impianto di allarme anti intrusione. L'URP inoltre è dotato anche di allarme antincendio e porte dotate di sistemi anti intrusione. Occorre sottolineare inoltre che nell'anno 2012 sono è in corso una ristrutturazione ed adeguamento normativo di alcuni locali situati al piano terra, in particolare Anagrafe e Stato Civile e successivamente i locali attualmente dedicati al Corpo di Polizia Municipale.
A livello di protezione generale dell'edificio bisogna ricordare che è in funzione un sistema di videosorveglianza che permette il monitoraggio delle persone che entrano ed escono dall'accesso principale del Palazzo Comunale. Tale sistema consente la registrazione che può essere quindi utilizzata in caso di furto o altri eventi delittuosi. Tale sistema di videosorveglianza non permette di monitorare gli accessi ai locali URP.
In relazione alla protezione da eventi naturali (acqua, fuoco, ecc.) la sala macchine pur trovandosi al secondo piano e quindi riparata in caso di alluvioni non ha protezioni e allarmi anti incendio ed è quindi in una situazione simile a quella delle di altre stanze del palazzo comunale per le quali sono attivi solo quegli strumenti di protezione a carattere generale previsti dalle normative vigenti ma nelle quali non esistono rilevatori di fumo, impianto e dispositivi anti incendio, le porte di accesso si aprono verso l'interno anziché verso l'esterno, ecc. La stanza, non essendo climatizzata, in particolari periodi dell'anno, corre rischi potenzialmente più alti di danni e malfunzionamenti, dovuti all'inevitabile surriscaldamento delle macchine.
Per mancanza di spazi, attualmente la stanza è adibita anche ad altri usi rispetto al semplice contenimento dei server (magazzino vecchi e nuovi apparati), aumentando pertanto i rischi in caso di incendio. In futuro dovrà porsi particolare attenzione al tentativo di minimizzare lo spazio occupato nella sala server da parte di altro materiale.
Per quanto riguarda le attrezzature informatiche queste sono state il più possibile posizionate distanti dalle finestre per evitare, soprattutto nei mesi estivi, di essere esposte a raggi termici che ne possono compromettere il funzionamento e ridurre l'esposizione a

schizzi indiretti di acqua sulle apparecchiature che potrebbero verificarsi in caso di violenti i temporali.

La protezione elettrica

Nel corso del mese di marzo 2013 sono stati eseguiti lavori di rifacimento completo del quadro generale di comando del palazzo comunale e successiva installazione di nuove dorsali principali. Quindi, l'alimentazione elettrica della sala macchine è dotata di una linea elettrica dedicata e sezionata da un apposito interruttore separato da quelli degli altri uffici, dall'armadio di piano.
Le attrezzature principali sono poi collegate alla rete elettrica tramite un gruppo di continuità (con funzioni anche di stabilizzatore) che garantisce il corretto mantenimento delle macchine in caso di interruzione momentanea di alimentazione. Gli armadi di piano sono dotati di una linea elettrica dedicata facente capo all'unità ups (gruppo di continuità) presente nella sala server. Il nuovo impianto elettrico a servizio del palazzo comunale è dotato di impianto di protezione contro le scariche atmosferiche.

Protezione da altri tipi di eventi

Per altri eventi quali incendio, allagamento, ecc. si rinvia l'analisi alla sezione dedicata specificatamente al dettaglio dei rischi.

L'accesso ai dati

Tutte le stazioni di lavoro per connettersi alla rete interna richiedono obbligatoriamente (ed il vincolo non è tecnicamente aggirabile dagli utenti) una fase di riconoscimento tramite un profilo di dominio pubblico ed una parola chiave che deve essere conosciuta solamente dal singolo operatore (e questo garantisce non solo da accessi indesiderati ma anche che ogni utente abbia a disposizione esclusivamente i dati e le funzioni che gli sono stati assegnati).
Le procedure gestionali poi a loro volta richiedono un ulteriore riconoscimento dell'utente, sempre tramite nome utente e password. Le credenziali di accesso al computer rispettano i criteri di sicurezza con policy di dominio (lunghezza minima della password di 8 caratteri, di cui uno numerico, uno maiuscolo, un carattere speciale) con scadenza ogni sei mesi. A sua volta gli applicativi di accesso alle banche dati dispongono di credenziali di accesso dedicate rispondenti ai criteri minimi di sicurezza.
Le chiavi di accesso e le parole riservate relative ai profili tecnici di gestione dei server (che quindi hanno autorizzazioni diverse e superiori a quelle dei normali utenti) sono conosciute dall'Amministratore di Sistema e dallo stesso adeguatamente conservate.
Allo scopo di aumentare le possibilità di recupero dei dati in caso di problemi da parte delle postazioni e, al contempo, aumentare la sicurezza, si sta attualmente cercando di spostare completamente l'attività dell'utenza dalle singole postazioni ai server, tramite la creazione di cartelle di rete che contengano i documenti di tutte le utenze e fisicamente ubicate sui server, che dispongono di un sistema (RAID 5) che garantisce una maggiore sicurezza rispetto ai normali personal computer in dotazione all'utenza. Su tali cartelle

vengono applicati criteri di sicurezza tali da permettere il salvataggio, la cancellazione e la visualizzazione dei dati unicamente al proprietario della cartella. Parallelamente a questa attività, si sta cercando di incentivare l'utilizzo di "gruppi di lavoro", con la creazione di appositi gruppi e relative cartelle di lavoro in cui sia possibile l'attività collaborativa tra gli appartenenti al medesimo gruppo.

La sicurezza logica

Anche il termine "sicurezza logica" è di non facile definizione e comprende una moltitudine di attività che hanno come obiettivo quello di garantire la congruità dei dati, la loro riservatezza, il loro costante aggiornamento e la disponibilità esclusivamente per quegli utenti che ne hanno l'autorizzazione.
In effetti quando si parla di "accesso ai dati" viene coinvolta sia la "sicurezza fisica", cioè la possibilità materiale di poter disporre di una stazione di lavoro connessa alla banca dati voluta, sia la "sicurezza logica", cioè il controllo che, una volta attivata la stazione di lavoro e collegata alle banche dati necessarie, vengano resi disponibili esclusivamente i dati previsti e che questi siano esatti e congruenti.

La congruità dei dati

Intendiamo con questo termine l'esigenza che le informazioni logicamente collegate siano coerenti tra di loro anche se fisicamente registrate su archivi diversi (evitare, per fare un esempio, che un utente risulti residente ad un determinato indirizzo per un servizio e ad un indirizzo diverso per un altro).
E' una operazione difficile da realizzare totalmente perché nessun programma può evitare errori di immissione dei dati da parte dell'operatore se questi non appaiono evidentemente assurdi; nessun programma, per quanto sofisticato, sarà mai in grado di correggere l'errore di digitazione "GRASSO" invece di "GROSSO" dato che in ogni caso il codice fiscale riporterà le lettere "GRS".
Quello che può essere chiesto invece ai programmi è di intercettare i dati evidentemente scorretti (date inesistenti, sesso diverso da "maschio" o "femmina", condizioni di stato civile non codificate, ecc.) e di effettuare tutti i controlli logici con gli altri dati già disponibili per verificarne la correttezza.
Bisogna però rilevare che la maggior parte dei programmi attualmente installati sono stati realizzati all'esterno da società di software che non sempre hanno ben tenuto presente queste esigenze e per le quali un intervento di modifica complessiva dei propri programmi spesso comporta investimenti finanziari non sostenibili.
Quello che può essere (e viene) fatto è di sollecitare continuamente le società perché in occasione delle nuove versioni dei programmi provvedano ad inserire almeno alcuni di questi controlli. Un altro tipo di problema è relativo alla "integrità referenziale" dei dati cioè al fatto che se una informazione fa riferimento ad un dato registrato su un altro archivio questo deve esistere e non è possibile eliminare un dato se prima non si sono eliminati tutti quelli da lui dipendenti (ad esempio non deve essere possibile cancellare le informazioni relative al nome di una persona se vengono mantenute le informazioni

relative al suo matrimonio).
Oggigiorno tutti i programmi di gestione dei data base di un certo livello offrono questa funzionalità ma la sua attivazione pratica richiede un sensibile sforzo di analisi e di implementazione, soprattutto per quegli archivi ormai esistenti da molto tempo. Una ulteriore problematica nasce dall'esigenza di mantenere allineate le informazioni su banche dati diverse (per fare un esempio banale sarebbe auspicabile che il nome di una persona fosse registrato sempre uguale su qualsiasi archivio contenga questa informazione). Anche in questo caso l'applicazione pratica di questa teoria apparentemente evidente e banale si scontra con il fatto che non vi è un'unica banca dati centralizzata ed omogenea ma una moltitudine sempre crescente di archivi progettati e gestiti da utenti diversi magari su sistemi informatici diversi. Pur nell'ipotesi ottimale che almeno all'inizio i dati vengano direttamente derivati da un archivio affidabile non è pensabile ipotizzare che questi rimangano aggiornati nel tempo (se un utente estrae ad esempio dai dati anagrafici della popolazione alcune informazioni e le trasferisce sul suo personal computer per farne delle elaborazioni particolari siamo certi che questi saranno esattamente "allineati" al momento del trasferimento ma siamo altrettanto sicuri che non lo saranno più nel momento stesso che l'ufficio anagrafe registrerà una qualsiasi variazione sui propri archivi).
Altro elemento da tenere in considerazione è il passaggio dei dati da un database all'altro. Nel tentativo di uniformare sempre maggiormente le basi di dati e trarre vantaggio dalla comunicazione tra i vari applicativi, accade infatti spesso di dover far comunicare tra loro database di tipo differente e di diversi fornitori o di dover fare un import dei dati da una banca dati ad un'altra. Queste operazioni sono spesso automatizzate, basandosi su procedure standard che vengono ripetute per tutti i record dei database. Durante questi passaggi è possibile che si verifichino errori, con conseguente perdita o modifica dei dati. Spesso, questi tipi di errore sono anche di difficile individuazione considerata l'elevata quantità di dati.

Il controllo degli accessi

Con riferimento al controllo degli accessi, si rimanda al **"disciplinare tecnico in materia di trattamento dei dati personali affidati ai lavoratori",** approvato con deliberazione di Giunta Comunale n. 34 del 23.02.2012 ("Adozione di misure organizzative in materia di protezione dei dati personali di cui al Decreto Legislativo n. 196/2003 e successive modifiche ed integrazioni").

Disposizioni sull'accesso ai locali ed ai dati personali

Poiché il rischio da eliminare riguarda il potenziale trattamento o la conoscenza di dati personali da parte di soggetti non autorizzati, si evidenziano le disposizioni sull'accesso ai locali del Comune da parte di altri soggetti (utenti, tecnici e manutentori, ecc.), che riguardano le misure di sicurezza minime che la struttura attualmente applica.

- **Misure di sicurezza fisiche**

Richiamando, per una parte delle informazioni necessarie, le indicazioni fornite nella parte iniziale del presente documento, si dettagliano altre misure specifiche relative ai locali ed agli uffici in cui la conservazione ed il trattamento dei dati personali assumono importanza rilevante.

- **Accesso ai locali**

Gli accessi alle parti comuni dell'edificio devono essere chiusi (a chiave nel caso delle porte) e negli orari in cui l'ente è chiuso al pubblico. Negli orari di apertura al pubblico, nessun dato personale deve essere posto in vista o deve risultare facilmente accessibile o riconoscibile da chiunque.
L'accesso agli uffici amministrativi è strettamente controllato da parte degli Incaricati che effettuano trattamenti di dati personali. Durante il normale orario di apertura degli uffici, l'accesso ai dati è controllato dai rispettivi incaricati e, qualora, per motivi diversi, un ufficio rimanga temporaneamente vuoto, l'incaricato deve chiudere a chiave la porta d'accesso dello stesso e custodire la copia di chiavi che ne permettono l'apertura (ovvero consegnarla al collega o ad altro soggetto che comunque abbia diritto ad espletare la propria attività nel medesimo ufficio).
In ogni caso, ciascun incaricato deve rendere i dati personali specificatamente trattati non consultabili o visibili da parte di eventuali terzi che abbiano diritto ad accedere all'ufficio né al collega che stia svolgendo il proprio lavoro nel medesimo locale. I terzi che possono accedere agli uffici negli orari di apertura e/o di chiusura sono espressamente determinati in apposite autorizzazioni loro conferite, nelle quali sono indicate le responsabilità loro riferite, quale ad esempio il personale di pulizia.
Tutti gli incaricati devono provvedere a non lasciare mai, in loro assenza, porte e finestre dei rispettivi uffici aperte. Gli accessi specifici (cassetti, armadi ecc.) vanno chiusi a chiave sempre, le porte solo in assenza degli addetti dei rispettivi uffici. Tutti i dati sensibili contenuti su documenti cartacei devono sempre essere conservati dentro armadi o contenitori chiusi a chiave.

I virus e i codici malefici

scherzi: producono effetti non desiderati ed a volte decisamente fastidiosi (un noto esempio storico è costituito da una pallina che improvvisamente compare sul video e comincia a rimbalzare cancellando tutto quello che trova sulla sua strada). Di solito basta spegnere il personal e poi riaccenderlo per eliminare (temporaneamente) il problema;

virus non distruttivi: possono impedire di lavorare ma non danneggiano i dati presenti sul computer (ad esempio i virus che ogni volta che viene eseguito un programma aumentano l'indicazione dello spazio occupato sul disco; dopo un po' di tempo si può avere il blocco totale delle operazioni per disco completamente pieno anche se in effetti i dati realmente presenti sono relativamente pochi);

virus distruttivi: modificano e/o distruggono le informazioni registrate, soprattutto i

programmi eseguibili ma anche i dati, con danni normalmente non ricuperabili, fino ad arrivare a rendere totalmente inutilizzabile l'intero sistema. Possono anche attaccare il settore di "boot" del disco, quella parte cioè di disco che i sistemi operativi leggono non appena iniziano ad operare e nella quale sono registrate in modo non utilizzabile dalle normali applicazioni le informazioni basilari necessarie al sistema operativo stesso. In questi casi il virus assume totalmente il controllo del computer ed in genere opera delle modifiche tali a tutta la struttura per cui il sistema operativo può continuare a funzionare (apparentemente in modo del tutto regolare) solo con l'intermediazione del virus stesso e la sua eliminazione provoca l'impossibilità per il sistema operativo di riconoscere le componenti corrette e quindi di funzionare (per fare un esempio è come se un virus criptasse e nascondesse alcune tabelle con dati fondamentali per il sistema operativo, tipo come si chiamano e dove si trovano i diversi archivi, e iniziasse a fare da traduttore e reindirizzatore di tutte le richieste di accesso; al momento dell'eliminazione del virus il sistema non sarebbe più in grado né di trovare né di interpretare il contenuto delle tabelle).

E' evidente che in una situazione nella quale vengono prodotti alcune centinaia di nuovi virus ogni mese il problema è diventato assolutamente prioritario ed obbliga a predisporre contromisure indubbiamente onerose sia dal punto di vista finanziario che da quello gestionale.

Innanzi tutto è bene chiarire che nessun anti-virus può essere totalmente efficace in quanto esiste una specie di sfida tecnica tra chi produce virus e chi li combatte ed i primi sono sempre, ovviamente, un po' più avanti nell'inventare nuove strategie di attacco.

Inoltre la grande diffusione dei collegamenti di rete se da un lato ha messo a disposizione di tutti una quantità di informazioni inimmaginabile anche solo poco tempo fa (non per niente si parla di "navigazione" in INTERNET), dall'altro ha creato una via facile e difficilmente controllabile per la diffusione dei virus; la stessa cosa si può dire per la posta elettronica.

La soluzione adottata è stata quella di installare un anti-virus centralizzato, che aggiornato continuamente, filtra tutto quello che passa, in entrata o in uscita, sia sui canali Internet che sulla posta elettronica; le singole stazioni, al momento del collegamento alla rete, in maniera automatica vengono aggiornate tramite un agente presente sul server e appositamente programmato.

Questo sistema, in uso da alcuni anni, è attualmente Kaspersky EnterpriseSpace Security.

I PC in funzione presso il Comune operano per la maggior parte con Sistema operativo Windows Xp Pro SP 3, Windows Vista e Windows 7. tenendo in considerazione che, a partire da Aprile 2014, la casa produttrice smetterà di rilasciare patch per i sistemi basati su Sistema Operativo Windows XP, a partire da tale data eventuali problemi di sicurezza non verranno più corretti e, quindi, diventerà necessario il passaggio a sistemi oprativi più recenti.

IL SISTEMA DI VIDEOSORVEGLIANZA

Gli impianti di videosorveglianza cittadina risultano costituiti da n° 55 telecamere dislocate sul territorio comunale, delle quali n° 49 consultabili direttamente in sincronismo dal Responsabile del Trattamento dei Dati, mediante collegamenti "ad isola" agli apparati periferici, in numero di 14, denominati "GAMS_PRIMO", con collegamenti in fibra ottica e/o rete criptata del gestore del gestore "Pat-Net".
I principali aspetti che riguardano le innovazioni introdotte con provvedimento emanato dal Garante della Privacy nel provvedimento dell'8 aprile 2010 sono i seguenti:

- Protezione dati/accessi abusivi di rete
- Log attivita'
- Permessi di accesso
- Cancellazione automatica delle registrazioni
- Crittografia delle trasmissioni

La conformità del sistema adottato dal Comune di Lavagna (sistema ad isola) è garantita attraverso lo sviluppo aggiornato dei sistemi periferici di videoregistrazione e dei software di centralizzazione, nel modo seguente:

Ubicazione sicura degli apparati "ad isola"

I DVR sono ubicati sul territorio comunale nelle immediate adiacenze dei singoli impianti, alloggiati all'interno di quadristica opportunamente protetta agli accessi da persone esterne non autorizzate, mediante carpenterie metalliche, in muratura o in materiale plastico autoestinguente, accessibile mediante l'uso di serratura a chiave codificata.

Sicurezza negli apparati gams

I DVR GAMS utilizzati nel n° di 14 unità dal Comune di Lavagna, forniscono diversi livelli di protezione dei dati gestiti, sia nell'accesso ai DVR, sia nella trasmissione delle immagini, sia in fase di esportazione delle registrazioni. Si riportano in questo documento le più importanti protezioni inserite che permettono ai DVR GAMS di essere non solo conformi al provvedimento per la privacy di Aprile 2010 ma di garantire un livello superiore di sicurezza.

Sicurezza in accesso

L'utilizzo dei DVR GAMS (e.g. configurazione, accesso locale, accesso remoto) avviene attraverso credenziali, definendo username e password differenziati.
Ad ogni utente è possibile assegnare un diverso livello di sicurezza che ne determina i privilegi d'accesso. E' ad esempio possibile definire un utente amministratore abilitato a tutte le funzioni dell'apparato, un utente con l'accesso solo al live remoto di determinate telecamere, un altro con anche l'accesso alle registrazioni o al comando delle telecamere dome, e così via.

Tutte le operazioni sensibili a livello privacy sono registrate nel log eventi (e.g. accesso al menu di configurazione, accesso alle registrazioni, movimentazione delle telecamere PTZ, ecc.).

Protezione dei dati salvati su HDD

Tutti i file registrati possono essere cifrati.

A tutti i file registrati viene assegnato un codice dipendente dal DVR (codice DVR) in modo da:

1. Impedirne la visualizzazione su un altro videoregistratore (copia del file sull'HDD di un altro DVR o spostamento dell'HDD)
2. Impedirne la visualizzazione a seguito di copia su PC

Protezione dei dati esportati

I DVR GAMS permettono di esportare i filmati sia da locale al DVR su un supporto di memoria USB sia da remoto attraverso il SW di centralizzazione H3 o i GAMS SDK. Durante l'esportazione il codice DVR viene sostituito con un codice che indica che i file provengono da una esportazione lecita.

E' possibile però associare una password all'esportazione proteggendola da accessi non autorizzati. Sia nel caso di esportazione protetta da password che di esportazione senza password (esportazione in chiaro) i file estratti sono comunque mantenuti cifrati (nell'ipotesi di cifratura attiva in configurazione). Questo permette di garantire la provenienza dei filmati da un DVR Bettini e impedirne la alterazione indebita: chiaramente la cifratura garantisce ciò in modo molto più sicuro che con la tradizionale tecnica di *digital watermarking*.

Per permettere la visualizzazione (e.g. alle forze dell'ordine), i file verranno accompagnati da apposito *player* GAMS in grado di decifrare le immagini eventualmente previo inserimento della password in caso sia stata scelta questa opzione in fase di export.

Protezione dei dati in trasmissione

Tra le prescrizioni definite dal Garante nel provvedimento dell'Aprile 2010 si ha la cifratura dei flussi video trasmessi via LAN. I DVR GAMS sono perfettamente aderenti a quanto definito in tutte le diverse tipologie di connessione:

- Live
- Play
- Esportazione da remoto

Standard di cifratura

In tutti i casi descritti in precedenza (protezione dei dati su HDD, esportati e in trasmissione) l'algoritmo utilizzato è HC128 con chiave a 128 bit.

DEFINIZIONE DEI RISCHI

Per una struttura pubblica come il Comune di Lavagna i danni che una persona, autorizzata o meno, può apportare, volutamente o inconsciamente, agli archivi comunque gestiti che contengano informazioni personali, sensibili e/o riservate si possono raggruppare in:

- accesso ad informazioni non autorizzate;
- modifica non controllata del contenuto delle banche dati con conseguente perdita delle caratteristiche di correttezza, completezza e congruità logica;
- distruzione delle banche dati;
- copia non autorizzata dei dati contenuti nelle banche dati;
- malfunzionamento del servizio;
- interruzione del servizio;
- inserimento nelle pagine del Comune di Lavagna di frasi od immagini non confacenti con la dignità dell'Ente;
- inserimento nelle pagine del Comune di Lavagna di informazioni non corrette, false e/o fuorvianti;
- utilizzo di macchine e indirizzi del Comune di Lavagna per compiere azioni illecite nei confronti di altri soggetti.

Esistono però anche altri tipi di rischio non legati alle attività umane ma derivanti da eventi naturali, incidenti, guasti meccanici, ecc. che possono comunque provocare malfunzionamenti o interruzioni dei servizi, di cui è necessario tenere conto.

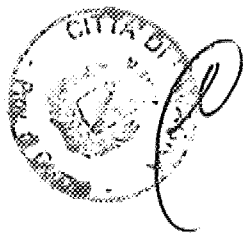
Elementi da valutare per l'esame del rischio:

- ☐ Risorse umane
- ☐ Hardware
- ☐ Software
- ☐ Dati
- ☐ Collegamenti
- ☐ Sistemi di sicurezza
- ☐ Eventi naturali
- ☐ Incidenti

Dettaglio dei rischi:

A **Risorse umane**

insufficiente conoscenza del sistema e/o dell'applicazione
insufficiente conoscenza dei rischi e delle misure di sicurezza
distrazione
negligenza
incidente
atto doloso



B **Hardware**
obsolescenza
avaria
distruzione
furto
manomissione

C **Software**
malfunzionamento
virus
distruzione
duplicazione non autorizzata
obsolescenza
modifica non controllata

D **Dati**
accesso non autorizzato
modifica non autorizzata
distruzione
mancanza di congruità
esportazione illegittima

E **Collegamenti**
malfunzionamento
interruzione
intercettazione

F **Sistemi di sicurezza**
incompletezza
mancata verifica
illeggibilità copie di backup

G **Eventi naturali**
terremoto
alluvione

H **Incidenti**
incendio
allagamento
cedimento strutturale
campi elettro-magnetici o radar

Analisi di dettaglio

A. Risorse umane

A.01 insufficiente conoscenza del sistema e/o dell'applicazione

A volte l'operatore può involontariamente compiere azioni che comportano un danno semplicemente perché non è perfettamente a conoscenza delle conseguenza del suo operato.
Il danno che può essere provocato varia da:

- blocco momentaneo della stazione di lavoro
- blocco di una o più transazioni che possono coinvolgere anche altri utenti,
- inserimento, modifica o cancellazione non volute di informazioni
- invio di dati riservati o sensibili a persone non autorizzate
- permettere la visione di dati riservati o sensibili a persone non autorizzate.

A.02 insufficiente conoscenza dei rischi e delle misure di sicurezza

Capita spesso, purtroppo, di osservare negli utenti una certa superficialità di comportamento in merito alla sicurezza dovuta, in genere, ad una non comprensione dei rischi che ne possono derivare e ad un malinteso cameratismo tra colleghi.

I casi più tipici ed evidenti sono:
diffusione nell'ambito dell'ufficio della password personale ("tanto di lui mi fido e poi comunque non ho niente da nascondere")
comunicazione a qualche collaboratore della password di chi ha autorizzazioni più elevate ("c'è da fare un lavoro particolare ma io non ho tempo, voglia, ecc.; fallo tu ed entra con la mia password")
lasciare la stazione di lavoro accesa e collegata mentre ci si assenta
lasciare in giro stampe e tabulati contenenti dati personali, sensibili o riservati
non effettuare copie di riserva dei propri documenti ed archivi.

A.03 distrazione

La distrazione può essere di tipo "fisico" o "logico".
Quella di tipo fisico (si rovescia una bibita sulla tastiera oppure, molto più grave, si rovescia una bottiglia d'acqua sul PC; si urta una attrezzatura facendola cadere e danneggiandola) in genere comporta danni alle attrezzature ed a volte, come conseguenza, danni anche ai dati.
Quella di tipo logico, invece (durante una operazione l'utente viene distratto da una telefonata e si dimentica di salvare il documento su cui stava lavorando ovvero preme inavvertitamente dei tasti che provocano l'esecuzione di operazioni non volute), in genere provoca esclusivamente danni ai dati.

A.04 negligenza

Per certi versi appare analoga alla distrazione ma presuppone un comportamento "colposo" da parte dell'utente.
A titolo di esempio potremmo ipotizzare il caso di una attrezzatura posizionata accanto ad una finestra che viene lasciata aperta durante un temporale per cui la pioggia bagna la macchina danneggiandola.

A.05 incidente

Per definizione si tratta di un avvenimento non imputabile, se non in maniera molto indiretta, all'utente ma ad una "fatalità".
Il danno può essere conseguenza di un corto circuito, di un incendio, di un allagamento dovuto alla rottura di un tubo, ecc.

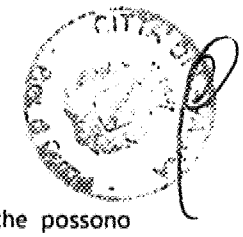
A.06 atto doloso

E' il più grave e pericoloso dei fattori di rischio legati al fattore umano in quanto presuppone una precisa volontà di manomettere o distruggere le attrezzature o i dati.

B Hardware

B.01 obsolescenza

Più che un fattore attivo di rischio l'obsolescenza delle attrezzature, che nel campo informatico è particolarmente rapida, può impedire l'attivazione di misure di sicurezza fisiche o logiche che si rendano opportune per eliminare o ridurre alcuni rischi.
A titolo di esempio può non essere tecnicamente possibile installare su un vecchio personal computer un sistema di cifratura dei dati che richiede processori di una certa potenza e sufficiente memoria.



B.02 avaria

Come tutte le macchine anche le attrezzature informatiche sono soggette a guasti che possono renderle inutilizzabili per periodi più o meno lunghi. A seconda del tipo di guasto si può avere solo un blocco dell'attività della stazione di lavoro oppure anche danneggiamento o perdita di dati (per esempio nel caso di guasto dell'hard disk).

B.03 distruzione

La distruzione, volontaria o fortuita, comporta evidentemente una totale perdita della funzionalità della stazione di lavoro e dei dati contenuti..

B.04 furto

Il furto equivale ad una distruzione totale del bene e quindi la perdita dei dati contenuti.

B.05 manomissione

Trattando di apparecchiature hardware anche la manomissione diventa rapidamente avvertibile dal momento che provoca comunque dei malfunzionamenti. Si tratta comunque quasi sempre di un intervento doloso, generalmente attuato da persona esperta, tendente ad impedire il corretto funzionamento della stazione di lavoro ad esempio mettendo fuori uso le testine di lettura/scrittura dei dischi od alterando la formattazione degli stessi per rendere non più rintracciabili le informazioni. C'è anche la possibilità che la manomissione sia la causa di una manovra sbagliata compiuta dall'operatore, magari involontariamente, per imperizia o distrazione. In molti casi la manomissione dell'hardware è conseguenza di un'infezione da virus.

C Software

C.01 malfunzionamento

Il software perfetto non esiste.
Partendo da questo assunto possiamo individuare alcune categorie di danno che il malfunzionamento del software può provocare:

- danno di immagine per l'amministrazione che utilizza o pubblica dati non corretti
- danno economico quando l'errato funzionamento di un programma provoca errori
- nell'adempimento di operazioni obbligatorie e soggette a sanzione
- danno gestionale quando questo malfunzionamento provochi un rallentamento od un blocco delle normali attività operative
- danno organizzativo (oltre che nuovamente economico) in quanto è necessario destinare risorse umane e finanziarie alla ricerca e soluzione del malfunzionamento verificatosi

C.02 virus

Oltre a danneggiare i dati (eventualità che verrà trattata nella apposita sezione) i virus possono attaccare e danneggiare più o meno profondamente anche il software installato sulle macchine ed i dati contenuti.

C.03 distruzione

Un programma, o parte di esso, può essere distrutta intenzionalmente o accidentalmente, ad esempio per una errata operazione dell'utente, per uno sbalzo elettrico, per un malfunzionamento dell'hardware, ecc.
A parte il danno derivante dal blocco temporaneo di tutta l'attività basata sul software distrutto c'è da considerare l'eventualità che non ne sia possibile la ricostruzione. Questa seconda eventualità può verificarsi, ad esempio, per:

- mancanza di copie di riserva del software
- software installato su un'unica macchina e quindi non replicabile da altre stazioni di lavoro
- software sviluppato esternamente da società che non esistono più software sviluppato internamente e non documentato o del quale si è persa la documentazione
- software particolarmente "vecchio" per il quale non c'è più manutenzione.

C.04 duplicazione non autorizzata

Il danno, in questo caso, consiste nella violazione delle norme vigenti che indicano questo evento come reato.
La diffusione non arrestabile della posta elettronica, la presenza di masterizzatori a prezzi sempre più bassi, ecc. rendono praticamente impossibile un controllo totale su questa tipologia di eventi

C.05 obsolescenza

Il rischio derivante dall'obsolescenza dei programmi consiste nell'incapacità degli stessi di rispondere correttamente alle mutate esigenze operative e/o normative.

C.06 modifica non controllata

Si tratta dell'effetto tipico di una infezione da virus; in alcuni casi però può avvenire a seguito di una modifica volontaria di un programma, realizzata in fretta o da personale che non conosce esattamente la procedura, che porta in cascata modifiche impreviste.

D Dati

D.01 accesso non autorizzato

Secondo la normativa vigente ogni operatore deve poter accedere a tutte e sole le informazioni che gli sono necessarie per svolgere correttamente il proprio lavoro.
Occorre quindi fare in modo che l'accesso ai dati personali, sensibili o riservati sia rigidamente controllato.
Le possibilità di accesso non autorizzato a dati gestiti in modalità informatica sono la conseguenza di:

- distrazione o negligenza di un utente (il quale lascia la propria stazione di lavoro collegata e si allontana)
- conoscenza della password di un altro utente
- varchi nel sistema di attribuzione del sistema di sicurezza e di assegnazione delle autorizzazioni.

Una ulteriore possibilità di accesso ai dati deriva dal non corretto utilizzo delle stampe che contengano informazioni personali, sensibili o riservate. Accade che queste stampe, prodotte come supporto al lavoro di un ufficio, vengano lasciate sulle scrivanie anche nei momenti in cui il posto di lavoro non è presidiato e, quando non servono più, vengano gettate nella carta da buttare; se invece le stampe vengono prodotte per l'invio all'esterno o ad altri servizi a volte vengono messe in contenitori non chiusi o addirittura, specie per trasmissioni interne all'amministrazione, vengono inviate senza alcun contenitore.

Altro caso significativo di accesso ai dati non autorizzato è costituito dall'utilizzo del fax; la posizione dell'apparecchiatura ricevente in un posto accessibile normalmente da tutto il personale ed anche dal pubblico e che se non presidiata, rende estremamente probabile che comunicazioni contenenti dati personali, sensibili o riservati vengano viste da persone estranee, assolutamente non autorizzate.

D.02 modifica non autorizzata

La modifica non autorizzata dei dati può essere la conseguenza di una operazione, volontaria o involontaria, dell'utente oppure la conseguenza di un virus.

Non è possibile ipotizzare di impedire agli utenti la modifica dei dati in quanto questo impedirebbe lo svolgimento del normale lavoro operativo, per cui è necessario operare sul sistema delle autorizzazioni.

Se la modifica è opera di un utente occorre distinguere tra volontarietà ed involontarietà: nel primo caso ci si trova di fronte ad un atto doloso, quindi più grave e presumibilmente più difficile da scoprire.

Nel caso di modifica involontaria questa può derivare dal cattivo funzionamento di un programma (e l'analisi di questo tipo di rischio è stata fatta nella sezione dedicata al software), oppure da un difetto delle misure di sicurezza relative all'assegnazione delle autorizzazioni.

D.03 distruzione

Oltre che come forma aggravata della modifica non autorizzata, di cui ci siamo già occupati, la distruzione dei dati può essere conseguenza di un guasto hardware (anche questo già esaminato).

D.04 mancanza di congruità

La mancanza di congruità di dati contenuti nello stesso data base o in data base diversi comporta la inattendibilità delle informazioni che ne vengono ricavate e, di conseguenza, l'inutilità complessiva della raccolta e del trattamento dei dati in questione.
La non congruità può essere "originale", ovvero esistere fin dal momento del primo caricamento dei dati, oppure può essere derivata da una operazione, volontaria o involontaria, successiva.
In particolare la non congruità originale si può manifestare nel caso di banche dati diverse, sviluppate da società diverse, che prevedono la gestione della stessa tipologia di dati (a titolo di esempio pensiamo alla procedura di gestione del personale, sviluppata da una certa società, che gestisce i dati anagrafici dei dipendenti e la procedura di gestione dei servizi demografici, sviluppata da una società diversa, che, per i dipendenti che sono anche residenti, gestisce le stesse informazioni). Al momento del caricamento iniziale delle banche dati, che derivano da archivi cartacei diversi, è molto difficile garantire la congruità fra le due applicazioni delle informazioni immesse ed è anche molto difficile garantirla durante le fasi di aggiornamento dei dati. A maggior ragione la cosa si complica se lo stesso tipo di informazione è gestita da un numero superiore di banche dati.

D.05 esportazione illegittima

L'esportazione illegittima dei dati, oltre al danno patrimoniale che può provocare ed al danno di immagine derivante dalla "fuga di notizie", si può configurare come una forma indiretta di accesso non autorizzato alle informazioni.
E' infatti evidente che questa esportazione, proprio perché illegittima, permette la conoscenza dei dati a persone fisiche o giuridiche che non ne avrebbero la possibilità.
L'esportazione può avvenire verso l'esterno (tipico esempio la fornitura di elenchi nominativi ad altri Enti Pubblici) ma anche verso l'interno (fornitura dei dati ad un altro servizio comunale per scopi non istituzionali).

E Collegamenti

E.01 malfunzionamento

I collegamenti possono essere di diverso tipo: quelli che riguardano il funzionamento delle apparecchiature (tipicamente la rete elettrica) e quelli che riguardano il flusso dei dati (rete telefonica, rete locale, ecc.).
Il malfunzionamento delle rete elettrica (ad esempio sbalzi di tensione) possono provocare momentanei blocchi delle apparecchiature oppure, nei casi più gravi, rotture di alcune componenti con possibile danneggiamento o perdita dei dati registrati.

E.02 interruzione

L'interruzione è a tutti gli effetti una forme grave di malfunzionamento che, oltre ad eventuali danni fisici alle apparecchiature e conseguenti danni ai dati, comporta inevitabilmente il fermo di tutte o parte delle attività.

E.03 intercettazione

L'intercettazione è equivalente ad un accesso non autorizzato ai dati tramite collegamento alle linee di trasmissione dati.
Può essere involontaria (malfunzionamento della linea di comunicazione o dei commutatori per cui tutti o parte dei dati "passano" anche su una linea adiacente), ma più spesso si tratta di azioni dolose effettuate da esperti.

F Sistemi di sicurezza

F.01 incompletezza

Per quanti sforzi vengano fatti per la messa a punto di un sistema di sicurezza è sempre possibile che rimangano dei varchi aperti o per una incompleta analisi o per qualche errore nell'implementazione oppure, ancora, per l'avvento di nuove tecniche di penetrazione non conosciute inizialmente.

F.02 mancata verifica

Accade che una procedura di sicurezza, perfettamente studiata a tavolino, si riveli poi inefficace per una errata o incompleta implementazione.

F.03 illeggibilità copie di backup

Tutti i supporti magnetici, per loro natura, tendono ad un degrado, con conseguente possibilità di rendere impossibile la lettura totale o parziale dei dati memorizzati. Naturalmente più un supporto è economico (floppy disk) più è soggetto a deterioramento, ma persino sui CD-ROM o sui DVD non si hanno garanzie sulla effettiva durata della registrazione. Diventa però estremamente pericoloso accorgersi che non è possibile ripristinare una copia fatta, sulla quale evidentemente si faceva affidamento. Può inoltre accadere che, per un errore materiale, la copia di riserva venga effettuata su un supporto sbagliato, già utilizzato per altre copie, con l'effetto di cancellare quelle precedenti che vengono perse.

G Eventi naturali

G.01 terremoto

La zona su cui è costruito il palazzo comunale è classificata come zona a rischio sismico di grado 3. Non si hanno però notizie di sismi che abbiano causato dati rilevanti alla struttura del palazzo che ha alcuni secoli di vita. Si ritiene pertanto di poter valutare questa tipologia di rischio come bassa.

G.02 alluvioni

Sebbene la zona su cui sorge il palazzo comunale sia considerata a rischio di esondazione (max 2 metri) in ogni caso è opportuno ricordare che il Centro Elaborazione Dati è situato al secondo piano del palazzo e quindi non è possibile che finisca sott'acqua in seguito ad alluvione.

Potrebbero invece essere danneggiate dall'acqua, se questa raggiunge altezze sensibili (dell'ordine della decina di centimetri o superiori) alcune stazioni di lavoro appoggiate a terra (PC di tipo mini tower) negli uffici posti al piano terreno, che risulta sopraelevato di alcuni centimetri rispetto alla sede stradale.

H Incidenti

H.01 incendio

All'interno della sala macchine è posizionata una scaffalatura sulla quale vengono tenuti materiali di consumo vario, generalmente contenuto in involucri di cartone, ecc. Questo materiale infiammabile costituisce un ovvio problema nel caso di incendio, allo scopo è necessaria una drastica ridistribuzione degli spazi tra i diversi servizi, al fine di per mantenere gli elaboratori centrali rigidamente separati dalle altre attrezzature in un ambiente "neutro".
In sala macchine non vi è inoltre un rilevatore di fumi; è invece presente un armadio blindato amagnetico e ignifugo per la conservazione dei nastri di backup.

Una situazione analoga, e per certi versi ancora più grave, è quella relativa alle altre stazioni di lavoro posizionate negli uffici e quindi anche più contornate da materiale infiammabile, anche se il danno sarebbe certamente inferiore in quanto le banche dati importanti sono collocate nei server ubicati in sala macchine.

H.02 allagamento

In sala CED tutte le macchine si trovano a distanza dalle finestre e i server sono posti in un apposito armadio protettivo. Il pavimento della sala però non è rialzato, tuttavia sono rialzate le macchine rispetto al pavimento. Bisogna anche notare che un ulteriore pericolo consiste nella rottura di tubi al piano immediatamente sovrastante la sala per cui questo pericolo è anch'esso abbastanza significativo. Diverso è il discorso relativamente alle stazioni di lavoro posizionate negli uffici per le quali è sempre possibile sia il danno derivante da acqua penetrata dalle finestre lasciate aperte (caso già esaminato a proposito della "negligenza" delle risorse umane), sia quello derivante da rottura dei tubi del riscaldamento che corrono lungo i muri esterni del palazzo o da infiltrazioni d'acqua dai piani superiori.

H.03 cedimento strutturale

Il palazzo comunale è una struttura antica di alcuni secoli con muri portanti di oltre un metro di spessore.
Possiamo quindi ipotizzare che non sia possibile un improvviso collasso strutturale ma che eventuali cedimenti sarebbero preceduti da segni evidenti (crepe, rigonfiamenti, ecc.) facilmente diagnosticabili dai tecnici che operano nello stesso palazzo.

H.04 campi elettro-magnetici o radar

E' noto che i campi elettro-magnetici danneggiano i supporti informatici alterando le informazioni registrate.
Se la potenza del campo è sufficiente si possono avere anche blocchi o malfunzionamenti delle apparecchiature elettro-meccaniche, elettriche ed elettroniche.
Non vi sono però nelle vicinanze del palazzo comunale fonti di emissione di potenza tale da creare problemi di questo genere; oltre a tutto la loro eventuale presenza creerebbe gravi disagi anche alle persone che lavorano nella zona per cui il rischio assumerebbe anche caratteristiche diverse e più gravi.
Molto più banalmente si possono però avere danneggiamenti ai supporti informatici ed alle apparecchiature se queste sono posizionate vicino a motori elettrici abbastanza potenti e non schermati (condizionatori, stufe elettriche, pompe, ascensori, archivi rotanti,ecc.).
Anche i fasci dei radar sono estremamente dannosi per i supporti magnetici; non risulta però che nel territorio comunale vi siano in funzione apparecchiature di questo tipo.

Una volta individuati i rischi, connessi ai beni e risorse individuati, occorre procedere alla valutazione degli stessi, attraverso una indicizzazione del tipo di danno o di lesione possibili.

In particolare, nel processo di valutazione, si tiene conto di due indici fondamentali:

- la probabilità (P): riguarda la frequenza riscontrata o riscontrabile (è importante l'anamnesi);
- la gravità (D) da valutarsi in termini sia quantitativi (ad esempio valore del bene, costi di riparazione, tempi fermo macchina), sia qualitativi (danno all'immagine, interruzione di servizio pubblico,...)

Il Rischio quindi altro non è che la risultante della probabilità di un evento o di un atto e la sua gravità: l'indice R è dato proprio dal prodotto P x D.

Secondo i criteri adottati dando a P un valore fra 1 e 5 e a D ugualmente fra 1 e 5 si otterrà il valore di R compreso fra 1 e 25.

Probabilità (P)

1. Improbabile
2. Poco probabile
3. Mediamente probabile
4. Molto probabile
5. Estremamente probabile

Danno (D)

1. Minimo
2. Lieve
3. Medio
4. Grave
5. Gravissimo

Il numero, indicato arbitrariamente con la lettera R (Rischio), dato dal prodotto dei fattori arbitrari P x D, è per l'Ente un indice della gravità dello specifico rischio residuo associato alla specifica mansione presente .

Il valore di R può quindi essere compreso, in maniera discontinua, tra 1 e 25.

Le misure di sicurezza adottate o da adottare

Gli interventi sulla sicurezza si possono raggruppare in tre tipologie:

- organizzativi (identificati sulle schede con la sigla "O")
- fisici (identificati sulle schede con la sigla "F")
- logici (identificati sulle schede con la sigla "L")

Alcuni di questi hanno una valenza assolutamente generale, non contrastano quindi uno specifico rischio ma, in senso più ampio, costituiscono il substrato indispensabile per poter parlare di applicazione dei criteri di sicurezza.
Estendendo le indicazioni fornite dal Garante per la Protezione dei Dati Personali, si è

ritenuto utile riportare nella tabella Allegata **("Allegato "B" – Misure di sicurezza adottate o da adottare),** anche l'indicazione di attuazione, non attuazione o parziale attuazione delle misure di sicurezza.

Criteri e modalità di ripristino della disponibilità dei dati

Per poter parlare di ripristino dei dati, occorre prima definire le modalità di salvataggio degli stessi.
Su questo aspetto dobbiamo distinguere tra la sala macchine e gli altri uffici: vi è infatti un preciso piano di copie giornaliere di riserve dei dati che viene regolarmente eseguito sui server per gli utenti di rete, mentre per le altre residue attività svolte in locale sui personal computer l'attività è lasciata ai singoli operatori. Anche in quest'ultimo caso gli utenti sono stati informati dei rischi e quindi invitati ad effettuare copie giornaliere o almeno settimanali sulle proprie cartelle presenti in rete. Il seguito del discorso è quindi riferito esclusivamente ai dati residenti sui server, ove risiedono i data base più importanti.
Attualmente rimane in servizio il sistema IBM/AS400, che viene utilizzato per la sola consultazione e per il quale viene effettuato il back up giornaliero su nastro. Il sistema di back up è reso possibile dalla presenza di due unità *storage* in sistema Raid (delocalizzate) che effettuano le copie giornaliere dei dati dell'ente.
In ottemperanza alle disposizioni contenute nel CAD (Codice dell'Amministrazione Digitale), i cinque server presenti nell'ente (IBM/AS400 parte Microsoft, DC 2008, ML 2008, DC 2010, Documentale) sono stati oggetto di **"virtualizzazione"**. [8] L'adozione del sistema di virtualizzazione consente una concentrazione di server su di un'unica macchina che li contiene in maniera virtuale. A tale operazione corrisponde un considerevole risparmio di risorse finanziarie relative ai costi di assistenza; altro vantaggio rilevante consiste nel ripristino dei dati in caso di *crash* di sistema, con conseguente riduzione dei tempi di interruzione dei servizi necessari al ripristino dei dati.[9]
Questo permette, in generale, di garantire il corretto ripristino dei dati in tempi accettabili anche nell' eventualità in cui il ripristino si renda necessario per operazioni errate fatte

---

[8] Con i sistemi di virtualizzazione si indica la possibilità di astrarre alcuni servizi IT dalle rispettive dipendenze (reti, sistemi di storage ed hardware), abilitando l'esecuzione di più sistemi operativi virtuali su una singola macchina fisica rimanendo però, dal punto di vista logico, distinti. Il sistema operativo "ospitante" (l'host) crea di fatto una sorta di hardware partizionato eseguendo più sistemi oprativi "ospiti" (i guest). Di fatto la parte inferiore dello stack software è occupata da una singola istanza di un sistema operativo ordinario che è installato direttamente sul server. Sopra di questo, un layer di virtualizzazione gestisce il reindirizzamento e l'emulazione che va a sua volta a comporre il computer virtuale. La combinazione di questi due layer inferiori viene quindi definita host. Quest'ultimo fornisce le varie caratteristiche del computer fino al livello del BIOS ed è in grado di generale macchine virtuali 8e indipendenti) a scelta, basandosi sulle configurazioni definite dall'utente. Come i server fisici anche quelli virtuali sono ovviamente inutili fintanto che non vi si installa un sistema operativo, ovvero i guest, i quali penseranno di avere tutta la macchina per sé, ignorando l'esistenza degli altri.

[9] I principali vantaggi che i sostenitori della tecnologia vedono in una situazione di virtualizzazione sono i seguenti:

- riduce i costi di implementazione e gestione consolidando l'hardware;
- riduce il consumo energetico dell'intero Datacenter;
- alloca le risorse dinamicamente dove e quando necessario;
- riduce in modo drastico il tempo necessario alla messa in opera di nuovi sistemi;
- isola l'architettura nel suo complesso da problemi a livello di sistema operativo e applicativo;
- abilita una gestione più semplice delle risorse eterogenee;
- facilità testing e debugging di ambienti controllati.

dagli utenti e non per casi diversi come, ad esempio, il ripristino dei dati e dell'operatività a seguito della sostituzione di più dischi fissi. La scelta di utilizzare configurazioni di dischi fissi in modalità RAID5 nasce proprio dalla possibilità , in caso di guasto, di poter sostituire uno dei dischi fissi a macchina funzionante senza perdita di dati. Il RAID5 prevede, infatti, di scarificare uno dei dischi fissi che compongono il gruppo, permettendo una memorizzazione ridondante e quindi migliorando sicurezza e praticità di ripristino in caso di guasto – il caso più comune – di un disco. Diverso è il caso di guasto contemporaneo di più dischi che comporta operazioni molto lunghe e difficoltose.
Per quanto i server, come già detto, siano tutti sotto gruppo di continuità e siano tutti dotati di dischi in modalità RAID 1 eRAID5, di cui quello principale con alimentazione e ventole ridondanti, non è al momento ipotizzabile un ripristino in tempi rapidi nel caso di guasto bloccante tipo rottura della scheda madre, guasto contemporaneo di più dischi ecc. Si tratta di eventi abbastanza rari. L'unica soluzione possibile per ridurre ulteriormente il rischio è quella di prevedere un sistema di "*disaster recovery*" da attuare con un fornitore di servizi sistemistica in sintonia con i fornitori dei software applicativi, in modo da poter ottenere il ripristino dell'operatività in tempi certi e, comunque, non superiori ad una settimana. Tale piano è attualmente allo studio di fattibilità e si dovrà, in ogni caso, obbligatoriamente approntare entro il mese di Aprile 2012, come previsto dal Codice dell'Amministrazione Digitale.
Questo, comunque, non coprirebbe da altri rischi, peraltro già definiti come estremamente improbabili, quali terremoti, grandi alluvioni, cedimenti strutturali dell'edificio, ecc, la cui prevenzione comporterebbe un ulteriore aumento e duplicazione della struttura anche in postazioni remote, con un costo allo stato attuale non sopportabile per l'ente.

Interventi formativi in materia di privacy e sicurezza informatica

Il piano per la formazione e l'aggiornamento del personale deve includere interventi riconducibili all'esigenza di fornire adeguata formazione ai responsabili ed agli incaricati del trattamento dati.

Nel corso del 2012 sono stati realizzati corsi formativi interni specifici a cura della Direzione Generale in particolare:

- un corso interno, rivolto al personale dipendente, inerente la normativa sulla Privacy e sulla sicurezza informatica.
- un corso specifico inerente la privacy e la tutela della riservatezza in materia di videosorveglianza, destinato ad un ristretto gruppo di dipendenti (Settore Impianti Tecnologici e Polizia Municipale).

In totale i dipendenti partecipanti alla formazione sono stati n. 64.

Trattamenti affidati all'esterno

Nei casi di trattamenti di dati affidati all'esterno, quali ad esempio quelli relativi a ruoli su imposte comunali, al servizio di Tesoreria, ecc., l'individuazione del Responsabile del

Trattamento o, in sub ordine, degli Incaricati, deve essere effettuata preferibilmente con la stipula degli atti convenzionali o contrattuali che regolano la prestazione del servizio.

Manutenzione softwares

MAGGIOLI Informatica SpA Via del Carpino n. 8 – 47822 - Santarcangelo di Romagna
CEDAF srl Via Meucci n.17 – 47122 – Forlì
HALLEY Informatica srl Via Circonvallazione n. 131 – 62024 - Matelica (MC)
A&B Engineering SPA Via Renata Bianchi n. 137 – 16100 – Genova
SAPIDATA srl Via Molino Vigne n. 2 – 47825 – Torriana (RN)
DEDAGROUP S.p.a. Località Palazzina 120F – 30121 Gardolo (TN)
L.S.I. – Linea Liguria Sviluppo Informatica S.r.l. – Via Zara 19 – 16100 Genova

Tali soggetti operano nei limiti dell'espletamento dell'attività di assistenza. In particolare, queste ditte si trovano nella situazione di dover periodicamente svolgere lavori di manutenzione o semplicemente di dover verificare il funzionamento di un programma o di un'attrezzatura informatica. A tal fine è praticamente obbligatorio accedere alla base di dati presenti sui server, evidenziano così una conoscenza di dati personali che, di per sé, non è collegata allo scopo per il quale la ditta effettua la propria attività. Inoltre, accade molto di frequente che, per verificare la causa di malfunzionamento di un programma, o di un temporaneo blocco dell'attività, una più o meno ampia base dati sia oggetto di invio telematico agli uffici delle ditte fornitrici.
Ai sensi del punto 25 del disciplinare tecnico allegato al D. Lgs. N. 196/2003, se l'adozione delle misure minime di sicurezza viene affidata a soggetti esterni alla propria struttura, quali appunto i fornitori di softwares dedicati, il titolare del trattamento riceve dall'installatore una descrizione dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico sopra richiamato. Pertanto, l'autorizzazione/accordo concluso con ognuno dei suddetti soggetti, indicherà i limiti e le responsabilità cui la ditta andrà incontro nel caso in cui i dati accidentalmente conosciuti vengano comunicati o diffusi in violazione della normativa sulla Privacy.
Naturalmente non sarà posta in essere alcuna violazione di legge qualora all'interno della prestazione offerta da queste ditte siano comprese anche determinate attività di elaborazione dati svolte per conto del Comune. Per le attività di elaborazione dati affidate all'esterno che si inseriscono nell'ordinario meccanismo operativo del Comune, configurando una vera e propria attività di *outsourcing*, si avrà cura di nominare il soggetto terzo Incaricato o Responsabile del trattamento, a seconda del tipo di responsabilità e di modalità operative concretamente applicate.

Conservazione digitale

Durante il mese di marzo 2013 il Comune di Lavagna ha affidato il processo di conservazione sostitutiva dei documenti firmati digitalmente alla Società ANCIDATA con sede in Roma, Via dell'Arco di Travertino 11.
Nelle condizioni generali di contratto è stato previsto:

- di nominare Ancidata Responsabile della conservazione sostitutiva delegandola a svolgere le attività di cui all'articolo 5 della Deliberazione CNIPA n. 11/2004 (Allegato C alle Condizioni Generali di contratto);
- di nominare Ancidata Responsabile esterno del trattamento dei dati personali, ai sensi dell'articolo 29 del D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" (Allegato D alle Condizioni Generali di contratto).

Gestione Sicurezza sul Lavoro (D. Lgs. N. 81/2008

L'incarico è affidato alla Società BIO – DATA Via Matteotti n.14/C – 16033 Lavagna
La predetta Ditta si occupa, con personale medico specialistico, di tutta la gestione delle visite mediche periodiche atte a rilevare l'idoneità del personale alle mansioni cui è preposto. Tale struttura fornisce al Comune tutta la relativa documentazione.
Nelle clausole contrattuali è stata espressamente prevista la nomina del Responsabile del trattamento dei dati.

Pulizia dei locali

Tali soggetti possono essere variamente organizzati ed operano su specifico incarico del Comune. Valgono le medesime precisazioni sulla circostanziata indicazione delle responsabilità e del controllo sulle prestazioni ricevute di cui al punto precedente. La Ditta incaricata della pulizia dei locali comunali può operare sotto il controllo di dipendenti dell'ente o in locali in cui il/i lavoratore/i è/sono temporaneamente solo/i e ciò potrà avvenire in qualsiasi ambiente. Nell'incarico/autorizzazione viene fatto richiamo ai locali oggetto dell'attività di pulizia disciplinando, specificatamente, all'interno di ogni struttura, eventuali locali comunque non accessibili o accessibili solamente con particolari accorgimenti o in seguito a specifiche autorizzazioni.
Tutti i soggetti come sopra elencati, in relazione a quanto specificato per ognuno di essi, sottoscrivono un accordo con il Comune che disciplina esattamente gli ambiti di responsabilità e gli obblighi che le parti sono tenute ad assumere e che si impegnano ad effettuare. Tutte le Ditte ed i soggetti che operano attraverso propri dipendenti e collaboratori, si obbligano a rendere edotti questi ultimi di tutto quanto previsto dagli accordi ed in generale dalla normativa sulla Privacy.

Aggiornamento DPSS

Il presente documento è soggetto a revisioni ed aggiornamento periodico e per tale fine è stato individuato un apposito gruppo di lavoro così costituito: Anna E. Ferri (Ufficio U.R.P.) Giampiero Donati (Impianti Tecnologici), Simone Menini e Giuseppe Benini (Ufficio C.E.D.), Elisabetta Canepa (Ufficio Risorse Umane), Enrico Agosti (Ufficio Lavori Pubblici). Il gruppo di lavoro svolgerà la sua attività in stretta collaborazione con il Comitato di Direzione dell'Ente.

ALLEGATO"A" - ELENCO DEI TRATTAMENTI, DISTRIBUZIONE DEI COMPITI E RESPONSABILITA'

Settore	Responsabile Trattamento	UO/Ufficio	Trattamento	Operazioni relative al trattamento ***	Incaricati	Banca dati informatizzata
Direzione Generale	Avv. Concetta Orlando	**Direzione Generale**	Verbalizzazione sedute organi rappresentativi, distribuzione documentazione di competenza Procedimenti disciplinari Gestione del personale Attività di collaborazione e assistenza giuridico - amministrativa agli organi dell'ente in ordine alla conformità dell'azione amministrativa, alle leggi, allo statuto, ai regolamenti	Tutte le operazioni del trattamento previste dalla Legge		IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
		Controllo di Gestione e supporto OIV	Verbalizzazioni Comitato di Direzione Programmazione budget PEG/PDO Verifica raggiungimento obiettivi definiti nella programmazione Razionalizzazione spese Piano performance	Tutte le operazioni del trattamento previste dalla Legge	Simona Sanguineti	PROMETEOWEB DEDAGROUP - IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
Servizi alla Persona	Dott.ssa Lorella Cella	**Servizi Scolastici e Sociali**	Gestione elenchi obbligati scolastici	Tutte le operazioni del trattamento previste dalla Legge	Elena Mazzino Adriana Giacomelli Stefania Pareti Rosa Maria Trimarchi Anna Crovo Anna Maria De Paoli Ornella Ghio Anna Pancsi Danila Tagliaferri Parma Maria Grazia Camezzana Carlo Comincioli Sandra Ermacora	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE) - INPS EX-INDAP
			Gestione asilo nido			
			Gestione scuole materne			
			Gestione mense e trasporti scolastici			
			Attività di formazione ed in favore del diritto allo studio			
			Attività relativa all'assistenza domiciliare			
			Attività relativa alle richieste di ricovero e inserimento in istituti, case di cura, case di riposo ecc.			
			Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale			
			Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo			
			Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludobblioteca ecc.)			
			Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto			
			Attività relativa a servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e adozione di minori			
			Attività relativa al T.S.O. e all'A.S.O.			
			Attività relativa alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario.			
		Biblioteca	Attività della Biblioteca - presito bibliotecario	Tutte le operazioni del trattamento previste dalla Legge	Ivana Avanti Sambuceti Stefano Marco Scuderi Luca Arzeno	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE) - SEBINANET (SISTEMA BIBLIOTECARIO PROVINCIALE)
		Archivio	Gestione dell'archivio storico e di deposito	Tutte le operazioni del trattamento previste dalla Legge	Marco Scuderi	IRIDE MAGGIOLI
		Servizi Culturali, promozione turistica, sportiva, comunicazione, Agricoltura	Gestione delle pratiche relative alle attività di promozione turistica e alle attività sportive	Tutte le operazioni del trattamento previste dalla Legge	Simone De Paoli Patrizia Oliveri Giuliano Fogola	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
			Gestione atti giudiziari depositati			

Servizi Amministrivi di Staff	Dott.ssa Lorella Cella	**Segreteria - Contratti**	Gestione deliberazioni di Giunta e Consiglio e altri atti relativi all'attività istituzionale	Tutte le operazioni del trattamento previste dalla Legge	Fabio Sanguineti Elisa Zolezzi	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
			Gestione documenti o accertamenti necessari per la stipula di contratti			
			Gestione dati delle imprese, associazioni ecc. partecipanti alle gare			
			Gestione elenco soggetti che hanno subito danni per causa del Comune o che hanno causato danni al Comune			
		Segreteria Sindaco	Attività di gestione indirizzario, invio materiale ed informazioni sull'attività dell'Ente	Tutte le operazioni del trattamento previste dalla Legge	Antonella Azaro	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
		Messi notificatori	Attività di notifica e gestione dell'Albo Pretorio	Tutte le operazioni del trattamento previste dalla Legge	Enrico Bertollo Valerio Ricci	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
		Risorse Umane	Selezioni, concorsi, assunzioni e contratti di lavoro	Tutte le operazioni del trattamento previste dalla Legge	Elisabetta Canepa Patrizia Cau Claudia Raso	HALLEY INFORMATICA - IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE) - INPS EX-INPDAP
			Trattamento previdenziale			
			Trattamento giuridico			
			Trattamento economico			
			Prevenzione, protezione e sicurezza sul lavoro accertamenti sanitari e verifica ido			
			Pratiche relative a concessione prestiti			
			Formazione e aggiornamento del personale			
			Contenzioso sul lavoro			
			Relazioni sindacali - contrattazione/valutazione del personale - provvedimenti di			
			Gestione sicurezza informatica D. Lgs. n. 196/2003			
Settore Servizi Finanziari di Staff e Tributi	Dott.ssa Enrica Olivieri	**Centro Elaborazione Dati**	Gestione pratiche acquisto materiali informatici e di consumo	Tutte le operazioni del trattamento previste dalla Legge	Giuseppe Benini: **AMMINISTRATORE DI SISTEMA** Simone Menini: **AMMINISTRATORE DI SISTEMA**	IRIDE MAGGIOLI - LIBRA MAGGIOLI - E-DEMOS MAGGIOLI - HALLEY INFORMATICA
			Gestione pratiche relative all'assistenza hardware e software			
			Gestione autorizzazioni accesso al sistema informativo			
			Gestione sistema informativo aziendale			
			Interventi manutentivi hardware			
			Interventi manutentivi software			
			Sviluppo applicativi software a compendio procedure esistenti			
			Assistenza agli utenti del sistema informativo aziendale			
			Rilevazioni statistiche			
			Gestione porta di accesso al CNSD e trasmissione dati			
			Gestione Sicurezza informatica D. Lgs. 196/2003			
			Attività relativa alla gestione della fatturazione delle lampade votive			
		Ragioneria - Tributi - Economato - Gestione beni patrimoniali e polizze assicurative	Gestione delle pratiche relative all'attività tributaria	Tutte le operazioni del trattamento previste dalla Legge	Leda Masucci Margherita Meldhionne Dorella Zanini Elisabetta Obertino Marco Rabaioli Milena Ferrari Ilaria Bafico Stefano Ghio Daria Gotelli Velia Ostigoni Ivo Stefanini	LIBRA MAGGIOLI ENGINEERING (EX A&B) ACCESSO LIMITATO EDIDEA IRIDE MAGGIOLI TELEMACO SISTER (Catasto)
			Gestione pratiche relative alla concessione di benefici economici, agevolazioni ed esenzioni tributarie			
			Gestione patrimonio mobiliare e polizza assicurative			
			Gestione clienti e fornitori			
			Gestione archivio lampade votive, riscossioni, preparazione fatturazione			
			Gestione dati contabili degli amministratori, personale dipendente, collaboratori			
		Protocollo - Archivio corrente	Gestione del protocollo	Tutte le operazioni del trattamento previste dalla Legge	Maria Cristina Marotti Daniela Bruni	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
			Tenuta archivio corrente			
			Gestione ricezione offerte delle imprese, associazioni ecc. partecipanti alle gare			
		U.R.P. Sportelli polifinzionali di	Passaporti, cessione fabbricati, denunce ospitalità, infortuni, permessi soggiorno		Claudia Caprini	
			Rilascio certificazioni servizi demografici			
			Rilascio carta di identità			
			Front office pratiche anagrafiche residenti ed AIRE			

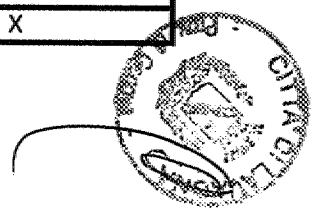
Unità Organizzativa Ufficio Relazioni con il Pubblico - Servizi Demografici	Dott.ssa Anna E. Ferri	**front office servizi demografici, sociali, pubblica istruzione,pubblica sicurezza polizia amministrativa, rilascio CDU e certificati idoneità alloggi Servizi cimiteriali**	Front office pratiche cittadinanza, immigrazione, asilo, condizione straniero, profugo, rifugiato	Tutte le operazioni del trattamento previste dalla Legge	Giuseppina Leucari Franca Cardinali Alfredo Nicora Grazia Pescio Marco Giovagnoli	E-DEMOS MAGGIOLI - IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
			Rilascio contrassegni per la sosta popolazione residente			
			Front office Servizi Sociali, Pubblica Istruzione,			
			Gestione servizio Bike Sharing			
			Rilascio CDU e certficazione idoneità alloggi			
			Rilascio certificazioni servizi demografici			
			Autenticazione firme, foto			
			Polizia Mortuaria - gestione pratiche cimiteriali			
			Raccolta firme referendum - iniziative popolari			
			Rilascio contrassegni disabili			
		Servizi Demografici Anagrafe Stato Civile Leva Elettorale Statistica	Anagrafe/ gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE).	Tutte le operazioni del trattamento previste dalla Legge	Giorgina Choino Maria Grazia Levaggi Maura Dall'Alpi Luigi Dall'orso	E DEMOS MAGGIOLI - IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
			Stato civile/ Attività di gestione dei registri di stato civile			
			Eettorale/ attività relativa all'elettorato attivo e passivo			
			Eettorale/ attività relativa alla tenuta degli albi degli scrutatori e presidenti di seggio			
			Elettorale/ attività relativa alla tenuta dell'elenco dei giudici popolari			
			Leva/ attività relativa alla tenuta del registro degli obiettori di coscienza			
			Leva/ attività relativa alla tenuta delle liste di leva e dei registri matricolari			
			Rilevazioni statistiche - trattamento per scopi statistici soggetti SISTAN			
			Gestione INA SAIA			
			Gestione rapporti con il CNSD			
Corpo Polizia Municipale	Dott. Fabio Terrile	**Comando P.M.**	Attività relativa all'infortunistica stradale	Tutte le operazioni del trattamento previste dalla Legge	Matteo Mantero Angelo Rosina Leonardo Rovatti Danilo Boccoleri Antonio Comincioli Alessandro Motto Maura Galli Giorgio Viappiani Giorgio Tosini Raffaele Barzacchi Pierluigi Orto Luca Venezia Mario Mastini Maria Teresa Peroni Daniela Raggio Mirko Mazzocco Veronica Rovatti	P.M. SAPIDATA - CONCILIA MAGGIOLI (modulo CAR CRASH) - IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE) - CONVENZIONI CON EX- MTC E PRA
			Gestione delle procedure sanzionatorie			
			Attività di polizia annonaria, commerciale ed amministrativa			
			Attività di vigilanza edilizia, in materia di ambiente e sanità			
		Struttura Unica Attività produttive, Urbanistica, Demanio.	Pratiche relative all'affidamento di incarichi a professionisti esterni	Tutte le operazioni del trattamento previste dalla Legge	Pietro Bonicelli Daniela Del Signore 50% M. Rosaria Podestà Michela Nidielli 50% Mara Barbieri 50% Valentina Massa	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE) - TELEMACO
			Pratiche legate ad attività commerciali			
			Elenco artigiani			
			Autorizzazioni sanitarie			
			Controllo presenze assenze mercati e fiere			
			Pratiche relative interventi abbattimento barriere architettoniche			
			Pratiche relative erogazione contributi ad associazioni per opere urbanizzazione			

Settore Servizi alle Imprese e Territorio	Ing. Renato Cogorno		Pratiche relative osservazioni su varianti o nuove adozioni urbanistiche			
			Procedimenti inerenti demanio			
			Sono : compiti informativi, consulenza ed istruttoria. Informazioni in senso stretto sulle istanze presentate in relazione all'iter procedimentale, informazioni in termini generali sull'applicabilità della normativa vigente. Consulenza sulla fattibilità dell'iniziativa. Istruttoria completa del procedimento e rilascio dell'atto autorizzativo finale.			
		Edilizia Privata Violazioni Edilizie Sportello Unico Edilizia Privata	Pratiche relative all'affidamento di incarichi a professionisti esterni	Tutte le operazioni del trattamento previste dalla Legge	Pietro Vabal Daniela Mazzino Marta Milone Nereo Mazzocco Elena Raggio Angela Ravera	EDIDEA - IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE)
			Pratiche relative alla gestione dei procedimenti edilizi			
			Attività di Polizia Giudiziaria e sanzionatoria in materia di abusi edilizi			
		Lavori Pubblici Manutenzione e Protezione Civile Arredo Urbano Impianti Tecnologici e Sportivi Ufficio espropriazioni Patrimonio Ambiente	Gestione elenco ditte partecipanti alle gare	Tutte le operazioni del trattamento previste dalla Legge	Enrico Agosti Michele Brizzolari Daniela Del Signore 50% Pietro Donati Sonia Cugnata Fabrizio Camarda Diego Garibaldi Ilaria Ginocchio Sandra Tedaldi Ivo Mazzino Enzo Lanata Paolo Merciari Michela Nidielli 50% Mara Barbieri 50%	IRIDE MAGGIOLI - LIBRA MAGGIOLI (IN CONSULTAZIONE) - SISTER (Catasto)
			Gestione elenco ditte esecutrici di opere			
			Pratiche relative all'affidamento di incarichi a professionisti esterni			
			Pratiche relative alla tutela ambientale			
			Attività di Protezione Civile			
			Progettazione opere e impiantistica			
			Videosorveglianza			
			Concessione passi carrabili/ attribuzione numeri civici - toponomastica			

***** Tra le operazioni effettuate sui dati personali figurano: la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.**

ALLEGATO "B" - LE MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Tipologia interventi	Cod.	Elemento di valutazione	Descrizione rischio contrastato	Adottata	Da adottare	Parzialmente adottata
	A01	RIS.UMANE	insufficiente conoscenza sistema e/o applicazione	X		
ORGANIZZATIVI ("O")	A02		insufficiente conoscenza rischi e misure di sicurezza	X		
	A03		distrazione	X		
	A04		negligenza	X		
	A05		incidente	X		
	A06		atto doloso	X		
	B02	HARDWARE	avaria	X		
	B03		distruzione	X		
	B04		furto			X
	C01	SOFTWARE	malfunzionamento	X		
	C02		virus	X		
	C03		distruzione	X		
	C04		duplicazione non autorizzata			X
	C05		obsolescenza			X
	C06		modifica non controllata			X
	D01	DATI	accesso non autorizzato	X		
	D02		modifica non autorizzata	X		
	D03		distruzione	X		
	D04		mancanza di congruità			X
	D05		esportazione illegittima			X
	E01	COLLEGAMENTI	malfunzionamento			X
	E02		interruzione	X		
	E03		intercettazione			X
	A02	RIS.UMANE	insufficiente conoscenza rischi e misure di sicurezza	X		
	A03		distrazione	X		
	A04		negligenza	X		
	A05		incidente	X		
	A06		atto doloso			X
	B01	HARDWARE	obsolescenza	X		
	B02		avaria			X
FISICI ("F")	B03		distruzione			X
	B04		furto			X



	B05		manomissione			X
	C03	SOFTWARE	distruzione	X		
	C04		duplicazione non autorizzata	X		
	C06		modifica non controllata	X		
	D02	DATI	modifica non autorizzata	X		
	D03		distruzione	X		
	E03	COLLEGAMENTI	intercettazione	X		
LOGICI ("L")	A01	RIS.UMANE	insufficiente conoscenza sistema e/o applicazione	X		
	A02		insufficiente conoscenza rischi e misure di sicurezza	X		
	A03		distrazione	X		
	A06		atto doloso	X		
	B04	HARDWARE	furto			X
	C01	SOFTWARE	malfunzionamento	X		
	C02		virus	X		
	C03		distruzione	X		
	C04		duplicazione non autorizzata			X
	C06		modifica non controllata	X		
	D01	DATI	accesso non autorizzato	X		
	D02		modifica non autorizzata	X		
	D04		mancanza di congruità			X
	D05		esportazione illegittima			X
	E01	COLLEGAMENTI	malfunzionamento	X		
	E02		interruzione	X		
	E03		intercettazione	X		

Letto, approvato e sottoscritto.

Il Sindaco
(G. Vaccarezza)

Il Segretario Generale
(C. Orlando)

==========

Pubblicata in data 02 APR. 2013 sul proprio sito informatico ai sensi dell'art. 32 della Legge n. 69/2009.

Il Messo Comunale

==========

La presente deliberazione è stata pubblicata sul sito informatico di questo Comune nei termini suindicati ed è divenuta esecutiva il_____, ai sensi dell'art. 134, comma 3, del D.Lvo 18/08/2000, n. 267.

Lavagna, _____

Il Segretario Generale
(C. Orlando)