"DOCUMENTO PROGRAMMATICO SULLA SICUREZZA"

REDATTO AI SENSI DELL'ARTICOLO 34, COMMA 1, PUNTO G) DEL D.LGS. 196/2003
E DEL DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (ALLEGATO B)

Conformemente a quanto prescritto dal punto 19 del Disciplinare Tecnico, nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare),
2. la distribuzione dei compiti e delle responsabilità (punto 19.2 del disciplinare),
3. l'analisi dei rischi che incombono sui dati (punto 19.3 del disciplinare),
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 (punto 19.4 del disciplinare);
5. la descrizione di criteri e modalità per il ripristino dei dati, in seguito a distruzione o danneggiamento (punto 19.5 del disciplinare);
6. la previsione di interventi formativi degli incaricati (punto 19.6 del disciplinare);
7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno della struttura del **Titolare** (punto 19.7 del disciplinare);
8. la dichiarazione d'impegno e la firma.

Data Revisione	Effettuata da:	Approvata da:	Firme
			…… ……

Data Revisione	Effettuata da:	Approvata da:	Firme
			…… ……

Data Revisione	Effettuata da:	Approvata da:	Firme
			…… ……

PREMESSA

Il "Codice per la protezione dei Dati Personali" richiede la garanzia che "il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali" ed impone obblighi di sicurezza per la custodia e il controllo dei dati, in modo da assicurare un elevato livello di tutela e ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamenti non consentiti dei dati personali, cioè di tutte quelle informazioni che riguardano direttamente o indirettamente le persone fisiche o le persone giuridiche.
Dette informazioni sono raccolte, trattate, divulgate e distribuite anche elettronicamente attraverso tecnologie informatiche, che vengono utilizzate da un numero crescente di soggetti con una variabilità elevata di utenti e di collegamenti.
Pertanto, il **Titolare** del presente documento, per rispondere alle esigenze di tutela prescritte dalla normativa in oggetto e fronteggiare adeguatamente i rischi connessi con il trattamento, ha provveduto, entro il **31 marzo 2009**, come prescritto dalla Regola 19 del Disciplinare Tecnico – Allegato B, ad aggiornare il Documento Programmatico sulla Sicurezza (di seguito DPS) redatto per la prima volta nel corso del 2006. Il presente documento costituisce pertanto la **quarta** versione del DPS, documento che il Titolare provvede periodicamente ad aggiornare, adeguando le procedure da osservare nel trattamento dei dati personali alle prescrizioni in materia di misure di sicurezza ed alla evoluzione delle tecnologie adottate per il trattamento stesso.
Il presente DPS è stato rielaborato nel mese di marzo 2009, dopo attenta verifica, allo scopo di descrivere le misure di sicurezza fisiche, logiche e organizzative attualmente adottate dal **Titolare**.

Campo di applicazione
Il Documento Programmatico sulla Sicurezza definisce le politiche, gli standard di sicurezza e le procedure seguite dal **Titolare** in sede di trattamento dei dati personali.
Il DPS è depositato presso gli Uffici del **Titolare**, ed è a disposizione per la consultazione da parte di Responsabili, Incaricati del trattamento e di chiunque, avendone titolo, ne faccia richiesta.
Il DPS riguarda i dati personali Sensibili e Giudiziari, nonché quelli comuni, e si applica al trattamento di tali dati con ogni strumento di elaborazione: computerizzato, telematico, elettronico, audiovisivo, cartaceo o altro.

Linee-guida
La politica di sicurezza in materia di riservatezza dei dati si fonda su alcuni principi fondamentali, qui di seguito elencati, che devono essere condivisi da tutti e devono guidare i comportamenti, l'operatività e le scelte tecnologiche:

1. I dati personali e le risorse informatiche che li raccolgono e li trattano costituiscono parte del patrimonio del **Titolare**. Essi devono essere custoditi, protetti, controllati e verificati nel tempo.
2. L'osservanza delle norme in materia di sicurezza dei dati trattati compete a tutto il personale interno alla struttura del **Titolare** ed ai fornitori, in particolare ai fornitori di servizi.
3. I dati personali, devono essere trattati esclusivamente per le finalità e con le modalità che sono state dichiarate con l'informativa data al momento della raccolta e per le quali sia stato recepito il consenso, se previsto dal Codice.
4. I dati devono essere custoditi e gestiti secondo regole precise per evitare i rischi di alterazione, sottrazione, distruzione, diffusione e intercettazione da parte di soggetti non autorizzati.
5. Le banche dati devono essere memorizzate, conservate e gestite in ambiente protetto e controllato attraverso strumenti e personale specializzati.

6. I dati personali e le risorse informatiche che li raccolgono devono essere classificati in relazione ai requisiti di sicurezza prescritti dalla normativa vigente in materia di privacy, devono essere disponibili solo alle persone autorizzate e devono essere trattati in conformità alla classificazione assegnata.
7. I sistemi informatici devono essere dotati di strumenti che impediscano accessi non autorizzati e che rilevino la presenza di eventi anomali.
8. Le risorse informatiche, ovunque siano installate, devono essere utilizzate per gestire le attività del **Titolare**, in linea con le autorizzazioni rilasciate.
9. Le risorse informatiche sono assegnate al Responsabile dell'unità organizzativa competente o all'Incaricato che le utilizza per le operazioni di trattamento; questi devono attivare ogni iniziativa utile alla loro protezione.
10. Le attività che prevedono il trattamento di dati personali anche attraverso l'utilizzo di tecnologie informatiche, devono svolgersi secondo procedure che garantiscano l'integrità e la riservatezza dei dati personali ed il rispetto degli adempimenti previsti dal legislatore in materia di privacy.
11. Le installazioni periferiche e la rete di comunicazione devono essere dotate di apparecchiature e di misure di controllo rivolte alla protezione da intrusioni negli archivi del **Titolare**. I collegamenti con risorse informatiche non rientranti sotto il governo diretto del **Titolare** devono essere gestiti con misure di controllo che impediscano accessi non autorizzati.
12. Nel caso di acquisizione di "servizi di gestione" erogati da terze parti (contratti di outsourcing, contratti di servizio, etc.), il Titolare deve attivare tutte le misure necessarie per garantire la riservatezza dei dati personali.
13. Deve essere effettuata l'informazione sui contenuti del DPS all'interno della struttura del **Titolare** poiché la necessaria riservatezza nel trattare i dati personali dipende anche dalla conoscenza e dalla condivisione delle misure concretamente adottate.
14. Devono essere attuati all'interno della struttura del **Titolare** interventi di ripasso, approfondimento e aggiornamento sulla normativa in vigore.
15. In particolare, il **Titolare** deve provvedere ad attuare, nel più breve tempo possibile, quanto previsto dalle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati"
16. Parimenti, il **Titolare** deve attenersi a quanto previsto dal provvedimento generale "linee guida in materia di posta elettronica e internet nei luoghi di lavoro".

Dati identificativi del Titolare

Lo scopo di questo documento è dunque quello di delineare il quadro delle misure di sicurezza organizzative, procedurali, logistiche, fisiche e logiche, adottate per i trattamenti dei dati personali effettuati da:

COMUNE DI PONT CANAVESE con sede in **Via Marconi n. 12 10085 Pont Canavese (TO),** Codice Fiscale 83501970012 e Partita IVA: 02413750015, (nel seguito del documento indicato come "**Titolare**").

Il Comune di Pont Canavese è un paese di **3819 abitanti (al 31/12/2008)** situato in provincia di Torino e facente parte della Comunità Montana Valli Orco e Soana.

Notificazione del trattamento

A completamento di quanto esposto, si rileva inoltre che, visto l'Art. 37 del Decreto Legislativo 196, visto anche il disposto del Garante del 31 marzo 2004, si ritiene che il **Titolare** non debba presentare notifica ai sensi dell'Art. 37 del suddetto Decreto Legislativo.

1. DATI TRATTATI E TRATTAMENTI EFFETTUATI DAL TITOLARE (Regola 19.1)

Tipologie di dati trattati

Generalità
Al fine di individuare gli strumenti più idonei per i trattamenti e le misure minime di sicurezza necessarie nei trattamenti stessi, di seguito vengono di seguito elencati, in ordine tendenzialmente crescente di "pericolosità" per la privacy, le principali tipologie di dati trattati da parte del **Titolare**:

1. Dati anagrafici, economici ed accessori di Ministeri, Enti e altri soggetti terzi, non fornitori.
2. Dati anagrafici relativi fornitori e potenziali fornitori;
3. Dati relativi al normale svolgimento delle attività economiche riguardanti i fornitori;
4. Dati anagrafici e altri dati personali comuni relativi a cittadini e fruitori di servizi;
5. Dati relativi al personale dipendente di sede (dati necessari alla gestione del rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi; dati richiesti a fini fiscali e previdenziali; dati di natura bancaria; dati curriculari), nonché i dati riguardanti candidati a nuove assunzioni;
6. Dati, in alcuni casi anche sensibili, relativi al personale dipendente di sede (conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o concernenti l'adesione ad organizzazioni sindacali, o relativi a cessioni del quinto dello stipendio, anamnesi dei dipendenti), nonché i dati riguardanti candidati a nuove assunzioni;
7. Dati sensibili e giudiziari relativi a cittadini e fruitori di servizi.

Al fine di individuare gli strumenti più idonei per i trattamenti e le misure minime di sicurezza necessarie nei trattamenti stessi, di seguito vengono dettagliati, in ordine tendenzialmente crescente di "pericolosità" per la privacy, le principali tipologie di dati trattati da parte del **Titolare**:

1) Dati riguardanti la tenuta degli atti e dei registri dell'anagrafe e dello stato civile;
2) Dati riguardanti la tenuta degli atti e dei registri relativi all'elettorato e alle attività di gestione delle consultazioni elettorali;
3) Dati riguardanti la tenuta degli atti e dei registri relativi alle liste di leva;
4) Dati in materia di popolazione straniera o nomade;
5) Dati riguardanti la gestione cimiteriale;
6) Dati riguardanti la gestione degli enti scolastici (scuola materna, scuola primaria e secondaria di primo grado) e connesse attività di istruzione complementari;
7) Dati riguardanti attività relative all'integrazione sociale (anche in ambito scolastico) di soggetti portatori di handicap o in condizioni di disagio sociale;
8) Dati riguardanti apparati per il Telesoccorso;
9) Dati relativi alla gestione di Attività ricreative per la promozione del benessere della persona e della comunità;
10) Dati relativi di trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)
11) Dati relativi alla concessione di benefici economici;
12) Dati relativi alla gestione della biblioteca civica e dell'ufficio turistico/punto informativo;
13) Dati riguardanti l'attività di Polizia municipale, di gestione di procedure sanzionatorie , di rilascio di permessi di occupazione del suolo pubblico e di gestione dell'area mercatale;
14) Dati riguardanti il normale svolgimento di attività di gestione delle pratiche edilizie pubbliche e private;

15) Dati riguardanti la gestione della riscossione dei tributi presso i contribuenti e alla concessione, liquidazione, modifica e revoca di benefici economici;
16) Dati riguardanti l'attività di rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza;
17) Dati relativi al normale svolgimento delle attività economiche e finanziarie riguardanti i fornitori;
18) Dati relativi all'attività di protocollazione e di archiviazione delle delibere e delle determine;
19) Dati comuni relativi al personale dipendente (dati necessari alla gestione del rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi; dati richiesti a fini fiscali e previdenziali; dati di natura bancaria; dati curriculari), nonché i dati riguardanti candidati a nuove assunzioni;
20) Dati relativi al personale dipendente (conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o concernenti l'adesione ad organizzazioni sindacali, o relativi a cessioni del quinto dello stipendio, anamnesi dei dipendenti), nonché i dati riguardanti candidati a nuove assunzioni;
21) dati riguardanti il rilascio delle attestazioni di soggiorno per i Cittadini dell'Unione Europea ai sensi del D.Lgs. 30/2007;
22) Dati relativi alle attività istituzionali sancite dalla legge e dai regolamenti.

Dati dei dipendenti
Il **Titolare** tratta i dati ed effettua i trattamenti necessari all'elaborazione periodica delle retribuzioni e degli oneri del personale (oneri sociali, ratei di mensilità aggiuntive e di ferie, TFR, ecc.). I curricula che arrivano via e-mail vengono stampati e poi archiviati, a cura di un incaricato, sul proprio client. La copia cartacea viene inviata al responsabile dell'unità organizzativa potenzialmente interessata.
I trattamenti effettuati presso la sede legale e amministrativa del **Titolare**, o presso il consulente del lavoro, sono quelli necessari a:
- ✓ ottemperare a obblighi di legge, regolamenti e normative comunitarie;
- ✓ disbrigare pratiche relative all'assunzione del dipendente;
- ✓ adempiere agli obblighi derivanti dal contratto di lavoro;
- ✓ ottemperare a obblighi di natura contabile e fiscale;
- ✓ elaborare retribuzioni e trattenute, eventualmente anche sindacali;
- ✓ adempiere a obblighi di natura previdenziale e assistenziale;
- ✓ comunicare a enti pubblici (Inps, Inail, ecc.), istituti di credito o associazioni sindacali quanto necessario nell'ambito del normale rapporto di lavoro;
- ✓ gestire l'organizzazione del lavoro dei dipendenti e la loro prestazione di lavoro;

Dati sensibili o giudiziari dei dipendenti
Il **Titolare** tratta dati sensibili in ambito gestione del rapporto di lavoro con il personale dipendente (dati idonei a rilevare lo stato di salute, dati idonei a rivelare l'origine razziale, adesione a sindacati o organizzazioni di categoria a carattere associativo, ecc.). Occasionalmente potrebbe dover trattare dati giudiziari. Eventuali dati di carattere giudiziario verrebbero comunque conservati all'interno dell'ufficio in armadi chiusi a chiave o in archivi riservati.

Dati dei cittadini
Il **Titolare** tratta i dati personali dei cittadini per ottemperare a obblighi istituzionali, per finalità di rilevante interesse pubblico e per attività necessarie al rapporto tra ente pubblico locale e cittadino. Tali dati sono trattati dal Servizio alla Persona, dal Servizio Amministrativo e Finanziario, dal Servizio Tecnico, dal Servizio di Polizia Municipale e dagli Amministratori. Tali dati

sono registrati, elaborati in modalità informatizzata e conservati su supporti cartacei e magnetici presso la sede del **Titolare**.
Il trattamento dei dati dei cittadini è finalizzato a gestire:

- ✓ l'anagrafe della popolazione residente e l'anagrafe della popolazione residente all'estero (AIRE);
- ✓ i registri di stato civile;
- ✓ l'elettorato attivo e passivo e l'esercizio di altri diritti politici;
- ✓ la tenuta degli albi degli scrutatori e dei presidenti di seggio;
- ✓ la tenuta dell'elenco dei giudici popolari;
- ✓ la tenuta delle liste di leva e dei registri matricolari;
- ✓ la tenuta del registro degli obiettori di coscienza;
- ✓ attività di gestione del servizio cimiteriale;
- ✓ attività relative all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale;
- ✓ 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 relative all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro anziani, ludoteca, ecc.);
- ✓ attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.);
- ✓ la scuola materna, quella primaria e quella secondaria di 1° grado;
- ✓ attività di formazione ed in favore del diritto allo studio;
- ✓ attività relative all'infortunistica stradale;
- ✓ le procedure sanzionatorie;
- ✓ attività di polizia annonaria, commerciale ed amministrativa;
- ✓ attività di vigilanza edilizia, in materia di ambiente e sanità;
- ✓ attività di tenuta dei registri di dichiarazione di ospitalità ai sensi del D.Lgs. 286/1998 e di comunicazione di cessione di fabbricato ai sensi della legge 191/1978;
- ✓ la riscossione dei tributi presso i contribuenti;
- ✓ la protocollazione e la tenuta del registro protocollo.
- ✓ pratiche edilizie pubbliche e private.

Dati dei fruitori di servizi

Il Titolare tratta i dati dei soggetti che ad esso si rivolgono per accedere a servizi di rilevante interesse pubblico o altri servizi ad essi rivolti. Tali dati sono trattati dal Servizio alla Persona, dal Servizio Amministrativo e Finanziario, dal Servizio Tecnico, dal Servizio di Polizia Municipale e dagli Amministratori. Tali dati sono registrati, elaborati in modalità informatizzata e conservati su supporti cartacei e magnetici presso la sede del **Titolare**.
Il trattamento dei dati dei fruitori che richiedono servizi è finalizzato a gestire:

- ✓ le attività relative alla richiesta di apparati per il telesoccorso;
- ✓ attività relative alla valutazione dei requisiti necessari per la concessione di riduzioni delle tariffe stabilite per l'erogazione di servizi (per soggetti audiolesi, non vedenti, pluriminorati o disabili o con disagi psico-sociali);
- ✓ le richieste di concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario;
- ✓ gli accessi alla biblioteca e il prestito libri;
- ✓ gli adempimenti previsti dalla Legge 155/2005 relativamente alla disciplina degli accessi a Internet effettuati dai punti pubblici di accesso per il contrasto del terrorismo internazionale;
- ✓ le richieste all'ufficio turistico/punto informativo;
- ✓ le richieste di assegnazione delle aree mercatali e delle fiere o mostre;
- ✓ attività di gestione del servizio cimiteriale per non residenti;

- ✓ attività di richieste di permessi per invalidi;
- ✓ il rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza;
- ✓ la concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- ✓ pratiche edilizie pubbliche e private;
- ✓ la riscossione dei tributi presso i contribuenti;
- ✓ gli adempimenti previsti dal D.Lgs. 30/2007 relativamente al rilascio delle attestazioni di soggiorno per i Cittadini dell'Unione Europea.

Dati dei fornitori

I dati personali di fornitori e potenziali fornitori sono raccolti in albi che ognuno dei quattro servizi del **Titolare,** a seconda delle proprie esigenze, mantiene**.** Essi vengono registrati, elaborati in modalità informatizzata e conservati su supporti cartacei e magnetici presso la sede del **Titolare**.
Il trattamento dei dati di fornitori e potenziali fornitori è finalizzato a:

- ✓ ottemperare a obblighi di legge, regolamenti e normative comunitarie;
- ✓ adempiere agli obblighi derivanti dalla determina/delibera di acquisto;
- ✓ ottemperare ad obblighi di natura contabile e fiscale;
- ✓ gestire il normale rapporto con il fornitore;
- ✓ elaborare analisi, valutazioni e dati statistici ad esclusivo uso interno.

Dati relativi ad attività istituzionali

Il Titolare tratta dati di fornitori, dipendenti, cittadini e soggetti terzi per ottemperare alle attività istituzionali che gli competono. Tali dati sono trattati dal Servizio alla Persona, dal Servizio Amministrativo e Finanziario, dal Servizio Tecnico, dal Servizio di Polizia Municipale e dagli Amministratori. Tali dati sono registrati, elaborati in modalità informatizzata e conservati su supporti cartacei e magnetici presso la sede del **Titolare**.
Il trattamento dei dati sopra descritti è finalizzato a gestire le seguenti attività istituzionali:

- ✓ attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione;
- ✓ attività istituzionali dell'ente, dei difensori civici, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni;
- ✓ conduzione di attività politica, di indirizzo e di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali;
- ✓ attività relative alla gestione di istituti di democrazia diretta.

Dati di Ministeri, Enti Pubblici Centrali e locali, altri soggetti terzi

In modo analogo a quanto previsto per i fornitori, il Titolare tratta dati di Ministeri, Enti Pubblici locali o centrali, altri soggetti terzi, pubblici o privati. I dati personali di questi soggetti sono raccolti di norma presso gli interessati e talvolta da pubblici elenchi. Sono poi trattati presso la sede del **Titolare**, registrati, elaborati in modalità cartacea e informatizzata e conservati su supporti cartacei e magnetici presso la sede del **Titolare**. Il trattamento è finalizzato a:

- ✓ acquisire e gestire permessi, autorizzazioni e concessioni;
- ✓ adempiere agli obblighi previsti dalla legge;
- ✓ comunicare dati e rendiconti;
- ✓ partecipare a riunioni, seminari, incontri tematici di settore.

Fonte dei dati
I dati personali non provenienti da pubblici elenchi sono stati sempre forniti direttamente dagli interessati, di norma presso le sedi del **Titolare**, o, nel caso di clienti e fornitori, presso le sedi degli interessati, dopo che essi abbiano ricevuto adeguata ed esaustiva informativa ed eventualmente sottoscritto idonea concessione di consenso. La modulistica usata per fornire l'informativa o per la richiesta di consenso al personale dipendente, ai clienti, fornitori e potenziali fornitori, è allegata al presente documento.

Informativa e consenso
Tutti i dipendenti anno ricevuto e sottoscritto l'informativa con richiesta di consenso al trattamento dei dati personali, anche sensibili.
I fornitori ricevono l'informativa attraverso apposita formula apposta nei bandi di gara o negli inviti a partecipare alle trattative private.
I cittadini e i fruitori dei servizi ricevono l'informativa o attraverso formulazione apposta sui moduli utilizzati per le diverse richieste oppure attraverso cartelli esposti in bella vista nei diversi uffici ove i cittadini e i fruitori di servizi si recano per richiedere il servizio stesso.
L'informativa è anche consultabile sul sito internet del Comune.
Se, per un qualsiasi motivo connesso con l'erogazione dei servizi, il personale del **Titolare** viene chiamato ad effettuare trattamenti di dati diversi da quelli per i quali gli interessati hanno già ricevuto l'informativa, lo stesso personale incaricato provvede a fornire, anche solo verbalmente, adeguata informativa complementare.

Dati sensibili o giudiziari
Il **Titolare** tratta dati sensibili in ambito gestione del rapporto di lavoro. Occasionalmente potrebbe dover trattare dati giudiziari.
In ogni caso, i trattamenti avvengono nei limiti e secondo le modalità indicate nella Autorizzazione n. 1/2007 al trattamento dei dati sensibili nei rapporti di lavoro - 28 giugno 2007 *(G.U. n. 196 del 24-8-2007 Suppl. Ordinario n.186.*

Destinatari della comunicazione dei dati
Nell'effettuare i trattamenti sopra elencati, il Titolare ha necessità di comunicare alcuni dati ai seguenti soggetti:

- ✓ INAIL
- ✓ INPS
- ✓ Istituti bancari
- ✓ Organizzazioni sindacali
- ✓ Ufficio di collocamento
- ✓ Ufficio Regionale del lavoro
- ✓ Ufficio Provinciale del lavoro
- ✓ Fondi di previdenza
- ✓ Fondi di assistenza
- ✓ Amministrazione finanziaria
- ✓ Agenzia delle Entrate
- ✓ Forze di Polizia
- ✓ G.D.F.
- ✓ Carabinieri
- ✓ Uffici Giudiziari
- ✓ Società per la formazione del personale
- ✓ Medico competente

- ✓ Consulenti
- ✓ Professionisti
- ✓ Vettori
- ✓ Stampatori
- ✓ Studi legali
- ✓ Società di consulenza informatica
- ✓ Poste Italiane
- ✓ Internet Services Provider
- ✓ Fornitori di beni e servizi necessari all'erogazione del servizio
- ✓ ASL
- ✓ Ministero dei Trasporti – Direzione Motorizzazione Civile
- ✓ Regione
- ✓ Provincia
- ✓ Enti e associazioni che erogano servizi socio-assistenziali

Natura dei dati trattati

Per quanto attiene la natura dei dati trattati, questa è riepilogata nella tabella che segue:

Tipo di dati	Natura dei dati
dati anagrafici dei dipendenti	Dati personali identificativi, di norma non sensibili, anche se in talvolta le generalità potrebbero indicare razza, religione, etnia
dati retributivi dei dipendenti	Dati personali riconducibili all'interessato che presentano natura sensibile se riguardano malattia o trattenute sindacali
dati accessori dei dipendenti	Dati personali e informazioni riconducibili all'interessato che possono avere natura sensibile
dati anagrafici dei cittadini	Si tratta di dati personali identificativi comuni
dati economici dei cittadini	Dati di per se stessi spesso anonimi, di norma riferiti o imposte, tasse, tributi dovuti dall'interessato. In ogni caso, non sensibili.
dati accessori dei cittadini	Dati personali e informazioni riconducibili all'interessato che possono avere natura sensibile (situazioni familiari,portatori di handicapp,ecc.)
dati anagrafici dei fruitori di servizi	Si tratta di dati personali identificativi comuni
dati economici dei fruitori di servizi	Dati di per se stessi spesso anonimi, di norma riferiti o imposte, tasse, tributi dovuti dall'interessato. In ogni caso, non sensibili.
dati accessori dei fruitori di servizi	Dati personali e informazioni riconducibili all'interessato che possono avere natura sensibile (situazioni familiari,portatori di handicapp,ecc.)
dati anagrafici dei fornitori	Di norma si tratta di dati personali identificativi comuni
dati economici dei fornitori	Dati spesso anonimi, riferiti o riferibili all'interessato, concernenti le transazioni commerciali intercorse. In ogni caso, mai sensibili.
dati accessori dei fornitori	Dati personali comuni, notizie e commenti riferibili all'interessato, mai sensibili.
dati anagrafici di Ministeri, Enti e altri	Dati personali identificativi comuni
dati economici di Ministeri, Enti e altri	Dati spesso anonimi, riferiti o riferibili all'interessato. In ogni caso, mai sensibili.
dati accessori di Ministeri, Enti e altri	Dati personali comuni, notizie e commenti riferibili all'interessato, mai sensibili.

Natura degli archivi e ubicazione dei dati trattati

La tabella che segue mette in evidenza la natura degli archivi ed il supporto sul quale sono ubicati i dati oggetto di trattamento:

Tipo di dati	Ubicazione dei dati
dati anagrafici dei dipendenti	I dati anagrafici dei dipendenti sono organizzati in archivio residente sul server; sono trattati anche sul client del responsabile del personale e su carta.
dati retributivi dei dipendenti	I dati retributivi dei dipendenti sono organizzati in archivio residente sul server; sono trattati anche sul client del responsabile del personale e su carta.
dati accessori dei dipendenti	I dati accessori dei dipendenti sono di norma trattati su carta. Alcuni particolari trattamenti (rilevazioni statistiche ad hoc) possono essere effettuati sul client del responsabile del personale e su carta.
dati anagrafici dei cittadini	I dati anagrafici dei cittadini sono organizzati in archivio residente sul server. Questi dati, rielaborati in documenti di vario genere, sono trattati anche su carta e sui client.
dati economici dei cittadini	I dati economici dei cittadini sono organizzati in archivio residente sul server. Questi dati, rielaborati in documenti di vario genere, sono trattati anche su carta e sui client.
dati accessori dei cittadini	Questi dati sono trattati su carta e sui client
dati anagrafici dei fruitori di servizi	I dati anagrafici dei fruitori di servizi sono organizzati in archivio residente sul server. Questi dati, rielaborati in documenti di vario genere, sono trattati anche su carta e sui client.
dati economici dei fruitori di servizi	I dati economici dei fruitori di servizi sono organizzati in archivio residente sul server. Questi dati, rielaborati in documenti di vario genere, sono trattati anche su carta e sui client.
dati accessori dei fruitori di servizi	Questi dati sono trattati su carta e sui client
dati anagrafici dei fornitori	I dati anagrafici dei fornitori sono organizzati in archivio residente sul server. Questi dati, rielaborati in documenti di vario genere, sono trattati anche su carta e sui client.
dati economici dei fornitori	I dati di economici dei fornitori sono organizzati in archivio residente sul server. Questi dati, rielaborati in documenti di vario genere, sono trattati anche su carta e sui client.
dati accessori dei fornitori	Questi dati sono trattati su carta e sui client
dati anagrafici di Ministero, Enti e altri	Questi dati sono trattati sul server, su carta e sui client
dati economici di Ministeri, Enti e altri	Questi dati sono trattati sul server, su carta e sui client
dati accessori di Ministero, Enti e altri	Questi dati sono trattati sul server, su carta e sui client

Correlazione tra dati e trattamenti

I trattamenti effettuati dal **Titolare** agiscono sui dati secondo lo schema riportato in tabella:

Trattamenti effettuati	Dati sui quali agiscono
Trattamento giuridico ed economico del personale	Dati anagrafici e retributivi dei dipendenti. Anche dati sensibili
Adempimenti connessi con l'esercizio dei diritti sindacali	Dati anagrafici e retributivi dei dipendenti. Anche dati sensibili
Rilevazione stato di salute e idoneità alla mansione	Dati anagrafici dei dipendenti. Anche dati sensibili
Gestione organizzativa del personale	Dati anagrafici e accessori dei dipendenti
Valutazione e selezione del personale	Dati anagrafici e curriculari
Gestione Anagrafe e stato civile	Dati anagrafici dei cittadini. In taluni casi, anche dati sensibili
Gestione Servizi elettorali	Dati anagrafici e accessori dei cittadini
Fornitura di servizi socio assistenziali	Dati anagrafici, economici e accessori di cittadini e fruitori di servizi. In taluni casi, anche dati sensibili
Fornitura di servizi TSO e ASO	Dati anagrafici, economici e accessori di cittadini e fruitori di servizi. In taluni casi, anche dati sensibili
Fornitura di servizi di trasporto	Dati anagrafici, economici e accessori di cittadini e fruitori di servizi. In taluni casi, anche dati sensibili
Fornitura di servizi di mensa	Dati anagrafici, economici e accessori di cittadini e fruitori di servizi. In taluni casi, anche dati sensibili
Fornitura di servizi sport, cultura e tempo libero	Dati anagrafici, economici e accessori di cittadini e fruitori di servizi. In taluni casi, anche dati sensibili
Concessione di licenze per attività economiche produttive	Dati anagrafici e accessori dei soggetti richiedenti
Concessione licenze per Es. Pubblici	Dati anagrafici e accessori dei soggetti richiedenti
Concessione di licenze edilizie	Dati anagrafici e accessori dei soggetti richiedenti
Riscossione sanzioni	Dati anagrafici, economici e accessori di cittadini e fruitori di servizi
Riscossione tributi	Dati anagrafici, economici e accessori di cittadini e fruitori di servizi
Altre finalità di rilevante interesse pubblico	Dati anagrafici di tutti i soggetti. In taluni casi, anche dati sensibili
Gestione del protocollo	Dati anagrafici di tutti i soggetti
Gestione delibere e determine	Dati anagrafici ed economici di tutti i soggetti. In taluni casi, anche dati sensibili
Produzione di stampati	Dati anagrafici dei fornitori Dati anagrafici ed accessori di Enti.
Elaborazione bandi, gare e capitolati	Dati anagrafici, economici e accessori dei fornitori
Valutazione di offerte, proposte e fornitori	Dati anagrafici ed economici dei fornitori
Acquisto di beni e di servizi	Dati anagrafici, economici e accessori dei fornitori
Gestione dei fornitori e dei relativi pagamenti	Dati anagrafici ed economici dei fornitori

Gestione del contenzioso	Dati anagrafici e retributivi dei dipendenti Dati anagrafici ed economici dei fornitori Dati anagrafici ed economici di cittadini e fruitori Dati anagrafici ed economici di Enti
Gestione contabile e amministrativa generale	Dati anagrafici ed economici di tutti i soggetti
Trasferimenti da e verso altri Enti della Pubblica amministrazione	Dati anagrafici ed economici di Enti.
Rendicontazione di dati e attività	Dati anagrafici ed accessori di Enti. Dati anagrafici ed economici di tutti i restanti soggetti
Acquisizione di dati da Internet e gestione servizi via Internet	Dati anagrafici ed economici di cittadini e fruitori; dati anagrafici e curriculari di candidati

Strumenti utilizzati per i trattamenti

Schedari, documenti e altri supporti cartacei

I supporti cartacei vengono ordinatamente raccolti in schedari o armadi dotati di chiusura, ovvero in apposite cartelle relative alla pratica o al particolare argomento a cui si riferiscono. Terminato il ciclo lavorativo, o chiusa la pratica, detti supporti vengono riposti nei corrispondenti archivi a ciò preposti.
L'accesso ai suddetti archivi è consentito solo ai responsabili dei trattamenti ovvero agli incaricati a ciò autorizzati, ovvero a personale espressamente autorizzato dai responsabili o dagli incaricati.
Le comunicazioni ricevute a mezzo posta, o a mezzo telefax, vengono protocollate, smistate e consegnate ai destinatari in tempi brevi e seguendo percorsi certi e definiti. Quando è impartito il comando di stampa di un documento, questo viene prontamente prelevato dall'interessato.
E' stata data specifica istruzione scritta affinché il materiale cartaceo destinato allo smaltimento sia riposto negli appositi contenitori di plastica dopo essere stato spezzettato in modo da renderlo molto difficilmente leggibile, che detti contenitori siano poi chiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detti contenitori chiusi siano giornalmente asportati per avviarli in discarica.
Il Comune dispone di un locale adibito ad archivio storico ubicato all'ultimo piano della scuola primaria, il cui edificio è di proprietà del Comune . Gli altri archivi di deposito sono ubicati presso il palazzo del Comune: due al piano interrato, uno al piano terreno e due al secondo piano; tali locali sono inaccessibili al pubblico. Inoltre ogni piano è dotato di un locale archivio "corrente" inaccessibile al pubblico.

Sistemi informatici e altre risorse ICT

Il server del Comune di Pont Canavese è posizionato in una saletta dedicata, ubicata al primo piano accessibile solo tramite l'ufficio del Responsabile del Servizio Amministrativo e Finanziario. Esso controlla e gestisce la rete interna condivisa, gestisce la posta elettronica, ospita i software di gestione dei diversi servizi e i relativi archivi, disciplina l'accesso degli incaricati ai diversi applicativi ed effettua il backup dei dati trattati.
Il server può essere così descritto:

- Server con sistema operativo Linux e partitura Windows per la gestione degli applicativi Microsoft Office, contenente i software e gli archivi per la gestione di:
  servizi demografici, contabilità finanziaria e controllo di gestione, personale e stipendi, ufficio tecnico, bollettazione acqua, il protocollo (applicativi forniti da Kibernetes che ne cura anche la manutenzione sia in locale che in modalità remota); la registrazione delle presenze (effettuata con badge magnetico tramite appositi lettori (software di Cabril Service Srl e da essa manutenuto); la posta elettronica (software di Giorgio Pozzi Srl e da essa manutenuto); la gestione cimiteriale, la gestione di Polizia Municipale e contravvenzioni, , la gestione della cessione fabbricati (legge anti terrorismo), la gestione delle delibere e delle determine, gestione tributi e ufficio tecnico (software forniti da Siscom e manutenuti da WinXPal).
  Inoltre, su questo server risiedono le copie degli archivi Tarsu e Tosap ed un vecchio archivio relativo alla gestione dei servizi sanitari.
  Tale server contiene anche i file condivisi del software Microsoft Office per la produzione di documenti e smista le email che riceve dal server esterno situato presso la ditta ePublic Srl, cui è affidata la gestione del sito internet.

Il sistema informativo del Comune dispone di un firewall hardware con software a bordo e di un antivirus centralizzato (Trend Micro), installato sul server Linux.
[ss1]

Elaboratori client fissi e portatili

Gli elaboratori utilizzati per effettuare i trattamenti dei dati personali sono 16 client fissi e 1 computer portatile. I client utilizzano i sistemi operativi Windows XP Professional e Windows 2000.[ss2]

Tutti i computer sono, o comunque possono venire, collegati alla rete comunale e attraverso un router su linea ADSL possono accedere ad Internet. Su tutti i computer è installato ed adoperato il programma Internet Explorer, mentre per la gestione della posta elettronica viene utilizzato l'applicativo Outlook.

Tutti i client, utilizzando gli applicativi Office 2000, archiviano i documenti sul server Linux.

Su due client è installata l'applicazione di gestione della vecchia bollettazione acqua (e il relativo archivio storico), mentre su altri due client è installata la gestione Tarsu e su uno di questi anche la gestione Tosap.

Su un client del servizio personale è installato l'applicativo INPS per la gestione contributiva e pensionistica dei dipendenti; su un altro client sono installati la gestione dei pubblici esercizi e del commercio in sede fissa; infine, su un altro client è conservato l'archivio storico delle pratiche edilizie.

Nei locali del Comune è inoltre custodito il computer portatile di proprietà della Comunità Montana Valli Orco e Soana, sul quale risiedono i dati relativi alle contravvenzioni redatte dai vigili urbani dei comuni aderenti al Servizio Associato di Polizia Municipale.

[ss3]

Elaboratori delle sedi distaccate

Nella sede distaccata della biblioteca vi sono 7 elaboratori in rete privata fissi. Tale rete è indipendente rispetto a quella installata nell'edificio comunale ed è dotata di router per l'accesso a internet tramite linea ADSL. Uno di questi pc è adibito alla gestione degli accessi ai locali e dei prestiti libri e funge da server verso gli altri pc, essendo in esso installato l'antivirus centralizzato.

La rete informatica della biblioteca è dotata di firewall hardware e il pc che funge da server è dotato di gruppo di continuità.

I restanti 6 pc sono dotati del programma Internet Explorer per la navigazione su internet e vengono utilizzati, nel rispetto delle vigenti norme di legge in materia di controllo degli Internet point, dagli utenti della biblioteca a tale scopo.

Tutti i pc hanno installato il sistema operativo Windows XP.

Nella sede distaccata dell'ufficio turistico c'è 1 pc portatile collegato alla rete informatica della biblioteca tramite connessione wireless. E' dotato di antivirus centralizzato (installato sul pc della biblioteca che funge da server) e di sistema operativo Windows XP Home Edition.

Esso viene utilizzato dall'addetta per ricerche su Internet di informazioni di pubblica utilità ed è quindi dotato di browser Internet Explorer.

Mappa dei trattamenti

Incrociando i tipi di dati trattati con gli strumenti usati per i trattamenti, si ottiene la "mappa dei trattamenti" effettuati dal **Titolare**. Nella tabella che segue, elaborata incrociando le due coordinate, si evidenzia con il simbolo "X" la circostanza di porre in essere il trattamento di determinati dati personali con l'utilizzo di determinati strumenti:

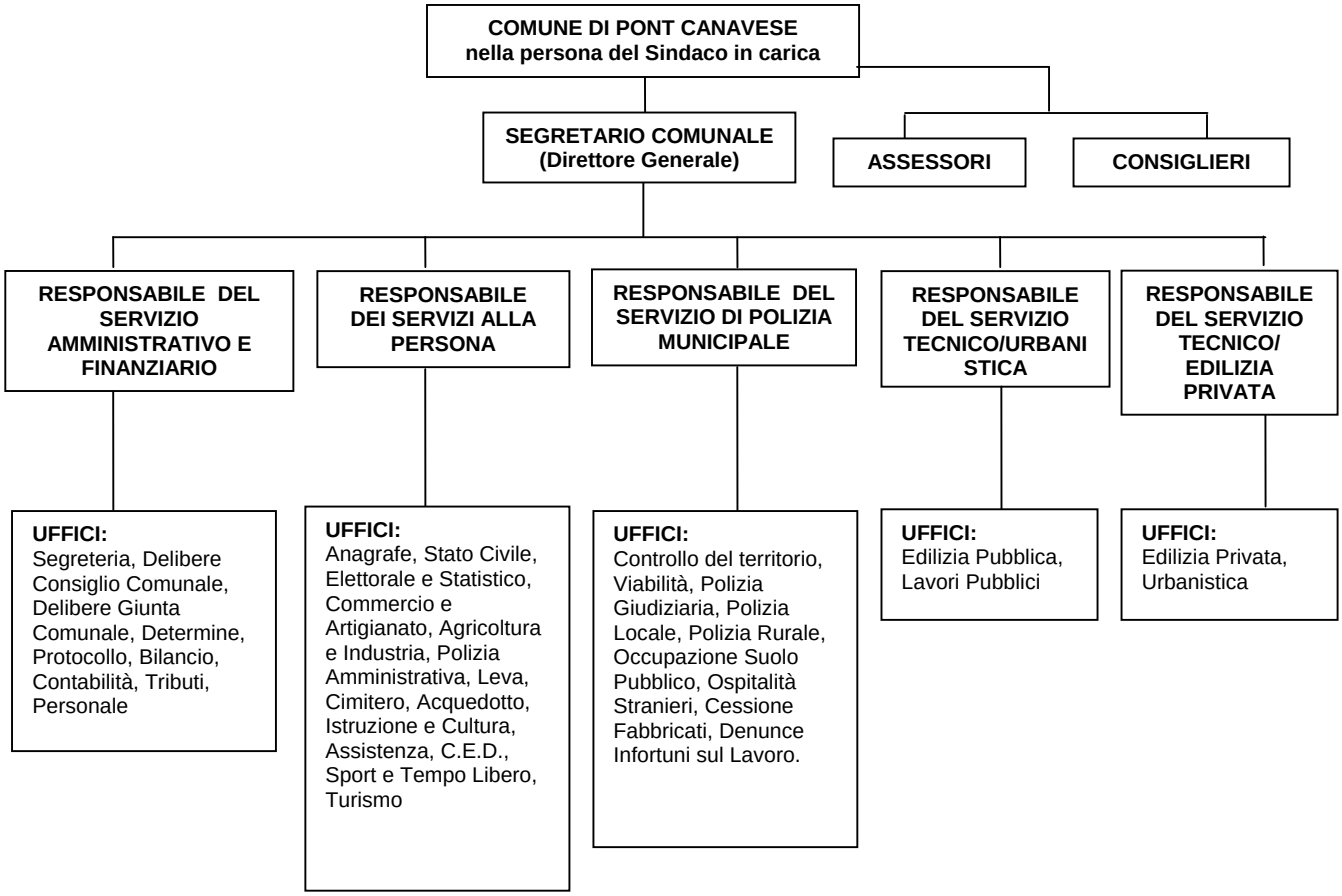
Trattamenti	Dati	A	B	C	D	E	F	G
Dati comuni (anagrafici, retributivi, curriculari) dei dipendenti	**comuni**	X		X	X			X
Dati comuni di persone giuridiche fruitori/ beneficiari di servizi	**comuni**	X		X	X			
Dati comuni dei cittadini fruitori/ beneficiari di servizi	**comuni**	X		X	X			
Dati economici dei fornitori	**comuni**	X		X	X			
Dati comuni dei cittadini	**comuni**	X		X	X			
Dati eventualmente sensibili dei dipendenti	**sensibili**	X		X	X			
Dati sensibili dei cittadini fruitori/ beneficiari di servizi	**sensibili**	X		X	X		X	
Dati sensibili dei cittadini	**sensibili**	X		X	X			

Il colore rosso evidenzia le intersezioni "tipi di dati/strumenti utilizzati" che presentano il maggior livello di rischio; il verde connota le situazioni a minor rischio; il giallo quelle a rischio intermedio.

A – Schedari ed altri supporti cartacei
B – Elaboratori centrali
C – Elaboratori server di rete
D – Elaboratori fissi in rete privata
E – Elaboratori portatili in rete privata
F – Elaboratori in rete pubblica
G - Elaboratori in altre sedi

2. COMPITI, RESPONSABILITA' E SICUREZZA (regola 19.2)

Per il trattamento dei dati personali il Comune di Pont Canavese si è dotato di un'organizzazione che rispecchia l'organigramma funzionale:[ss4]



Organigramma della sicurezza

Il comune di Pont Canavese ha nominato, attribuendo loro incarichi di natura organizzativa e direttiva, i seguenti responsabili, che a loro volta hanno provveduto ad attribuire gli incarichi ai sotto elencati signori:

- TITOLARE

COMUNE DI PONT CANAVESE
Marco Balagna – Sindaco in carica;

- RESPONSABILI

Maria Teresa Grandi
responsabile del trattamento dei dati personali di cittadini, fruitori di servizi, fornitori e dipendenti;

Paolo Coppo
responsabile del trattamento dei dati personali di cittadini, fruitori di servizi, fornitori e dipendenti;

[ss5]

Ivana Roncaglione Tet
responsabile del trattamento dei dati personali di dipendenti, cittadini, fruitori di servizi e fornitori e incaricata della produzione e custodia delle copie di sicurezza dei dati;

Bruno Madlena
responsabile del trattamento dei dati personali di fornitori, cittadini e fruitori di servizi e Amministratore di sistema;

Adriano Mattiuz
responsabile del trattamento dei dati personali di fornitori, cittadini e fruitori di servizi e custode della copia di sicurezza della password di Amministratore di sistema.

- INCARICATI

Elvira Cosco, Susanna Chiri, Flora Capello, Franca Mosca, Raffaella Picheca
incaricate del trattamento dei dati relativi ai servizi alla persona quali: Anagrafe, Stato Civile, Elettorale e Statistico, Commercio e Artigianato, Agricoltura e Industria, Polizia Amministrativa, Leva, Cimitero, Acquedotto, Istruzione e Cultura, Assistenza, C.E.D., Sport e Tempo Libero, Turismo;

Germana Edantippe, Jessica Podio
incaricate del trattamento dei dati relativi ai servizi Amministrativi e finanziari quali: Segreteria, Delibere Consiglio Comunale, Delibere Giunta Comunale, Determine, Protocollo, Bilancio, Contabilità, Tributi, Personale;

Lauretta Nardo
incaricate del trattamento dei dati relativi ai servizi di Segreteria, Delibere Consiglio Comunale, Delibere Giunta Comunale, Determine e Protocollo;

Romina Bugni
incaricata del trattamento dei dati relativi ai servizi di Ufficio Tecnico di Edilizia Privata e Urbanistica;

Anna Airoldi
incaricata del trattamento dei dati relativi ai servizi di Ufficio Tecnico di Edilizia Pubblica e Lavori Pubblici;
[ss6]
Massimo Lucco Castello, Giuseppe Perono Garoffo
incaricati del trattamento dei dati relativi ai servizi di polizia municipale quali Controllo del territorio, Viabilità, Polizia Giudiziaria, Polizia Locale, Polizia Rurale, Occupazione Suolo Pubblico, Ospitalità Stranieri, Cessione Fabbricati, Denunce Infortuni sul Lavoro;

Laura Balagna, Fiorentina Bausano, Paolo Coppo, Raffaele Costa, Silvana Ferrero, Giovanni Gallo Lassere, Mario Faletti, Massimo Motto, Luca Panier Suffat, Donatella Maria Perono, Mauro Piccolo, Pietro Oberto, Vincenzo Lechiara, Dante Barinotto, Lorenzo Feira, Piero Giovanni Querio
incaricati del trattamento dei dati personali di cittadini, fruitori di servizi, fornitori e dipendenti;

ESTERNI

Kibernetes
responsabile della gestione delle reti, del sistema informativo, delle procedure di ripristino dei dati e degli applicativi Microsoft di base installati nei client;
responsabile della manutenzione dei software per la gestione di servizi demografici, contabilità finanziaria e controllo di gestione, personale e stipendi, ufficio tecnico, bollettazione acqua, protocollo.

WinXPal
responsabile della manutenzione dei software per la gestione cimiteriale, gestione tributi e ufficio tecnico, Polizia Municipale e contravvenzioni, cessione fabbricati, delibere e determine, gestione attività economiche e produttive.

Siteck
Responsabile della gestione ICI.

Cabril Service Srl
Responsabile della manutenzione del software per la gestione delle presenze del personale.

Secure Group
Responsabile della gestione dei firewall e della sicurezza della rete comunale e della rete della biblioteca.

E-public
Responsabile della gestione del server su cui risiede il sito internet del comune e la posta elettronica che viene giornalmente scaricata.

Giorgio Pozzi
Responsabile della gestione e manutenzione del sistema di smistamento della posta elettronica.

Comunità Montana Valli Orco e Soana
responsabile della gestione del Servizio Associato di Polizia Municipale.

Elementi di sicurezza

Per quanto riguarda i dati personali trattati dal **Titolare**, i trattamenti avvengono ad opera:

- del **Titolare**;
- dei responsabili;
- degli incaricati;
- di soggetti esterni.

Sia a livello direttivo che a livello operativo, il trattamento dei dati personali viene dunque effettuato solo da soggetti che abbiano ricevuto un formale incarico scritto, con il quale siano stati indicati gli ambiti di responsabilità ovvero i trattamenti consentiti. Oltre alle istruzioni generali, su come devono essere trattati i dati personali, ai soggetti che effettuano i trattamenti sono state fornite istruzioni in merito ai seguenti punti:

- modalità di reperimento e di manipolazione dei documenti contenenti dati sensibili e modalità da osservare per la custodia degli stessi e per la loro archiviazione al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti;
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti;
- modalità di accesso alle password master o di sistema, affidate e custodite dai responsabili dei sistemi informatici, ai vari livelli di responsabilità;
- prescrizione di non lasciare incustoditi e accessibili gli elaboratori, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di custodia ed utilizzo dei supporti rimovibili contenenti dati personali;
- obblighi di aggiornamento, utilizzando il materiale e gli strumenti forniti dal **Titolare**, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, esterni all'organizzazione del **Titolare**, è stato prescritto che, in caso di intervento, non debbano effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o la manutenzione del sistema.
Le lettere di comunicazione dell'ambito dei trattamenti consentiti e le comunicazione di nomina dei responsabili sono raccolte in modo ordinato a cura del **Titolare** che così dispone di un "mansionario della privacy".
Periodicamente, con cadenza annuale, si procede ad aggiornare la tipologia dei dati a cui gli incaricati sono autorizzati ad accedere e l'ambito dei trattamenti che essi sono autorizzati ad effettuare, anche al fine di verificare se sussistono le condizioni che hanno giustificato tali autorizzazioni.
La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione e manutenzione degli strumenti elettronici e agli incaricati del trattamento di dati e documenti cartacei.

Di norma, i soggetti esterni ai quali vengano affidati dei trattamenti, sono considerati responsabili esterni. Tuttavia, in alcuni casi, detti soggetti sono considerati Titolari autonomi di trattamento.
Questa scelta viene effettuata per evitare di nominare responsabili esterni in modo surrettizio, a causa dell'impossibilità che in taluni casi si potrebbe manifestare per il **Titolare** di impartire direttive e vigilare tramite verifiche periodiche sull'operato del soggetto esterno.

Organizzazione e Responsabilità

Il modello adottato dal **Titolare** per la tutela dei dati personali prevede, oltre al **Titolare**, le figure dei Responsabili del trattamento, degli Incaricati del trattamento e dell'Amministratore di Sistema.

Compiti e responsabilità di detti soggetti sono specificatamente definiti nei rispettivi atti di nomina, conservati a cura del **Titolare**.

I Responsabili del trattamento, scelti – come richiesto dall'art. 29 del Codice – tra persone dotate di esperienza, capacità ed affidabilità, hanno il compito di attuare e di far applicare gli adempimenti e le norme del Codice. Essi devono, con la massima diligenza:

- adottare ogni misura necessaria o utile a garantire la sicurezza dei dati personali oggetto dei trattamenti;
- designare, con lettera di incarico contenente specifiche istruzioni, gli incaricati del trattamento dei dati personali e vigilare sulla loro attività;
- comunicare agli interessati tutte le prescrizioni dalla vigente normativa;
- collaborare con il **Titolare** nel rispondere ad ogni richiesta del Garante per la protezione dei dati personali;
- provvedere a rispondere ad ogni richiesta ex art.7 del Codice attinente alla propria funzione fornendo riscontro all'interessato;
- eseguire ogni provvedimento del Garante.

L'amministratore di sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse di elaborazione e di telecomunicazione del **Titolare**.

Ad esso competono i seguenti compiti:

- gestire le richieste di abilitazione e accesso ai sistemi;
- comunicare ai richiedenti l'esito o eventuali problemi riguardanti le loro richieste;
- tenere traccia di ogni abilitazione/user richiesta per ogni singolo utente.
- attribuire ai soggetti autorizzati ad accedere alle banche dati, un codice identificativo personale (user-id) per l'utilizzazione dello strumento elettronico;
- assegnare la prima password di accesso alla rete, password che sarà modificata dagli utenti al primo accesso;
- assegnare e gestire i codici identificativi personali (user-id) in modo che ne sia prevista la disattivazione in caso di mutamento o perdita dell'incarico o della mansione che consentiva l'accesso allo strumento elettronico o in caso mancato utilizzo per un periodo superiore a 6 mesi (artt. 7-8 allegato B D.Lgs. 196/2003);
- utilizzare un sistema di autorizzazione individuando per ogni incaricato, o per classi omogenee di incaricati, un profilo di autorizzazione;
- periodicamente e almeno una volta all'anno, verificare con la Direzione del Personale la sussistenza delle condizioni per la conservazione dei profili di autorizzazione (artt. 12-13-14 allegato B D.Lgs. 196/2003);
- proteggere i dati personali contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615 quinquies c.p. mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale (art. 16 allegato B D.Lgs.196/2003) o trimestrale per trattamento di dati sensibili e giudiziari (art. 17 allegato B D.Lgs. 196/2003);
- impartire istruzioni organizzative e tecniche per il salvataggio dei dati con frequenza almeno settimanale (art. 18 allegato B D.Lgs. 196/2003);
- assistere il **Titolare** e i Responsabili nell'attuazione pratica delle procedure in essere in materia di sicurezza e di accesso ai dati e agli strumenti;
- assistere il **Titolare** e i Responsabili nell'attuazione di tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati memorizzati;

- assistere il **Titolare** e i Responsabili nella gestione sicura dei supporti e delle aree di memoria già utilizzati per il trattamento dei dati, provvedendo affinché le informazioni precedentemente contenute non siano recuperabili, o siano distrutte;
- assistere, ove richiesto, il **Titolare** e i Responsabili in sede di verifica preliminare dell'affidabilità dei fornitori di servizi in termini di sicurezza informatica e di garanzia di continuità del servizio;
- verificare periodicamente la sussistenza della affidabilità di cui al punto precedente, in capo ai predetti fornitori di servizi.

Soggetti cui competono i trattamenti

Per ciascuno dei trattamenti elencati, il **Titolare** ha individuato l'unità organizzativa cui compete il trattamento stesso e l'incaricato di riferimento, ed inoltre le unità organizzative, o gli esterni, che concorrono al trattamento. Questi elementi sono riportati nella tabella che segue:

Trattamenti effettuati	Struttura di riferimento/ responsabile o incaricato	Strutture esterni e/o concorrenti
Trattamento giuridico ed economico del personale	Segretario Comunale Maria Teresa Grandi	Kibernetes
Adempimenti connessi con l'esercizio dei diritti sindacali	Segretario Comunale Maria Teresa Grandi	Cabril Service
Rilevazione stato di salute e idoneità alla mansione	Medico competente	
Gestione organizzativa del personale	I responsabili dei servizi	
Valutazione e selezione del personale	Segretario Comunale Maria Teresa Grandi	
Gestione Anagrafe e stato civile	Servizi alla persona Bruno Madlena	Kibernetes
Gestione Servizi elettorali	Servizi alla persona Bruno Madlena	Kibernetes
Fornitura di servizi socio assistenziali	Servizi alla persona Bruno Madlena	
Fornitura di servizi TSO e ASO	Servizi alla persona Bruno Madlena	
Fornitura di servizi di trasporto	Servizi alla persona Bruno Madlena	
Fornitura di servizi di mensa	Servizi alla persona Bruno Madlena	
Fornitura di servizi sport, cultura e tempo libero	Servizi alla persona Bruno Madlena	
Concessione di licenze per attività economiche produttive	Servizi alla persona Bruno Madlena	
Concessione licenze per Es. Pubblici	Servizi alla persona Bruno Madlena	
Concessione di licenze edilizie	Anna Airoldi, Romina Bugni	
Riscossione sanzioni	Polizia Municipale Adriano Mattiuz	WinXPal
Riscossione tributi	Servizio Amministrativo Ivana Roncagliene Tet	WinXPal
Altre finalità di rilevante interesse pubblico	Segretario Comunale Maria Teresa Grandi	
Gestione del protocollo	Servizio Amministrativo Ivana Roncagliene Tet	Kibernetes
Gestione delibere e determine	Servizio Amministrativo Ivana Roncagliene Tet	WinXPal
Produzione di stampati	Servizio Amministrativo Ivana Roncagliene Tet	
Elaborazione bandi, gare e capitolati	Responsabili dei Servizi	
Valutazione di offerte, proposte e fornitori	Responsabili dei Servizi	

Acquisto di beni e di servizi	Responsabili dei Servizi	
Gestione dei fornitori e dei relativi pagamenti	Servizio Amministrativo Ivana Roncagliene Tet	Kibernetes
Gestione del contenzioso	Segretario Comunale Maria Teresa Grandi	
Gestione contabile e amministrativa generale	Servizio Amministrativo Ivana Roncagliene Tet	Kibernetes
Trasferimenti da e verso altri Enti della Pubblica amministrazione	Segretario Comunale Maria Teresa Grandi	
Rendicontazione di dati e attività	Segretario Comunale Maria Teresa Grandi	
Acquisizione di dati da Internet e gestione servizi via Internet	Servizi alla persona Bruno Madlena	epublic

3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (regola 19.3)

Premessa
Il **Titolare** è consapevole:

- dell'importanza e del valore dei dati personali, dei dati industriali, delle informazioni e del know-how, i quali costituiscono una componente essenziale del proprio patrimonio;
- degli impatti derivanti da incidenti o errori in tema di sicurezza dei dati, nonché dalla eventuale perdita di riservatezza e integrità dei dati e/o dalla indisponibilità dei beni;
- della necessità di ridurre al minimo accettabile i danni derivanti da incidenti o errori in tema di sicurezza dei dati;
- delle leggi e delle disposizioni comunitarie vigenti in materia di sicurezza dei dati;
- dell'importanza del ruolo del personale nell'ambito della riduzione dei rischi errori in tema di sicurezza dei dati;
- dell'importanza della formazione e del coinvolgimento del personale in tutti gli aspetti inerenti la sicurezza dei dati.

Per tale motivo intende adottare tutte le misure di sicurezza e di prevenzione atte a ridurre al minimo i rischi, in grado di assicurare la protezione dei dati e degli strumenti di trattamento da minacce reali e potenziali, capaci di rispondere a situazioni di crisi in maniera efficace per assicurare la continuità dei servizi e della produzione aziendale.

Valutazioni di carattere generale concernenti i rischi che incombono sui dati
In questa prima parte viene formulata una valutazione sul grado di rischio legato alla gestione dei dati e agli strumenti utilizzati per i trattamenti.

La stima del rischio che grava su un determinato trattamento di dati è infatti il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti esterni, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- quelli legati alle caratteristiche degli strumenti utilizzati per effettuare i trattamenti .

Il grado di rischio insito nella tipologia del dato è dunque stimato combinando il grado di interesse potenziale da parte per i soggetti terzi con la pericolosità per la privacy dell'interessato. Ciò è schematizzato nella tabella che segue:

GRADO DI INTERESSE PER TERZI					
	MOLTO ALTO				
	ALTO		Dati comuni di persone giuridiche fruitori/beneficiari di servizi		Dati sensibili dei cittadini fruitori/beneficiari di servizi
	MEDIO	Dati comuni dei dipendenti e candidati	Dati comuni dei cittadini	Dati comuni dei cittadini fruitori/beneficiari di servizio	Dati sensibili relativi ai dipendenti
	BASSO				Dati sensibili relativi ai cittadini
		BASSO	**MEDIO**	**ALTO**	**MOLTO ELEVATO**

PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO

Livello di rischio relativo ai dati

■ Alto ▣ Medio ☐ Basso

Per quanto concerne gli strumenti impiegati per i trattamenti, le componenti di rischio possono essere suddivise in:

- rischi relativi al comportamento degli operatori;
- eventi e rischi relativi agli strumenti;
- eventi e rischi relativi al contesto.

Nella seguente tabella si evidenziano i fattori di rischio cui sono soggetti gli strumenti con cui vengono effettuati i trattamenti.
Il simbolo "X", qualora non sia grassettato, indica che l'esposizione al rischio è modesta.
La sua grassettatura indica invece una esposizione al rischio più elevata.

		A	B	C	D	E	F	G
Comportamento	Furto di credenziali di autenticazione			x	X	X		X
	Carenza di consapevolezza, incuria disattenzione	X		x	X	X		X
	Comportamenti sleali o fraudolenti			x	X	X		X
	Errore materiale	x		x	x	x		x
	Rischio legato ad atti di sabotaggio	X		X	X	X		X
Strumenti	Azione di virus e codici malefici			x	x	x		x
	Spamming o altri sabotaggi			x	x	x		x
	Malfunzionamenti o degrado			x	x	x		x
	Accessi non autorizzati			x	X	X		X
	Intercettazione di informazioni in rete			X	x	x		
Contesto	Accessi non autorizzati a locali controllati	X		x	x	x		
	Asportazione e furti di strumenti			x	x	X		X
	Eventi distruttivi, di qualsiasi natura	X		x	x	x		x
	Guasti a sistemi complementari			x	x	x		
	Errori nella gestione della sicurezza	x		X	X	X		X

Legenda degli strumenti utilizzati per il trattamento:
A – Schedari ed altri supporti cartacei
B – Elaboratori centrali
C – Elaboratori server di rete
D – Elaboratori fissi in rete privata
E – Elaboratori portatili in rete privata
F – Elaboratori in rete pubblica
G - Elaboratori client in altre sedi

L'Analisi del Rischio secondo la ISO/IEC 27001:2005

L'Analisi del Rischio è un processo formale e strutturato attraverso il quale si identificano i rischi e si determina la loro ampiezza.
Questo significa che attraverso l'analisi del rischio è possibile definire le esigenze di sicurezza e individuare le più appropriate misure da adottare al fine di prevenirli o di ridurre il loro impatto.
L'analisi del rischio può essere effettuata in molti modi, adottando metodi diversi che si basano su concetti analoghi. La scelta qui effettuata è quella di fare riferimento il più possibile a standard ufficialmente definiti e riconosciuti; pertanto si è adottato come modello di riferimento quello previsto dalle norme ISO.

La norma **ISO/IEC 27001:2005 Sistemi** di **Gestione** per la **Sicurezza** delle **Informazioni (SGSI)** tratta l'analisi del rischio richiamando la metodica e le definizioni riportate nella **Guida ISO/IEC 73:2002.**

Vediamo di seguito le principali definizioni:

- **rischio:** combinazione della probabilità di un evento e della sua conseguenza.
- **probabilità:** frequenza teorica con la quale un evento si verifica.
- **evento:** verificarsi di un insieme di circostanze.
- **conseguenza:** esito di un evento.
- **minaccia:** possibile causa di evento indesiderato che può comportare danni ad un sistema o a una organizzazione.
- **vulnerabilità:** debolezza insita in un bene, in un processo, in un sistema, che può essere sfruttata da una minaccia per generare un evento indesiderato.
- **accettazione del rischio:** decisione di accettare un rischio.
- **mitigazione del rischio:** limitazione delle conseguenze di un evento.
- **riduzione del rischio:** diminuzione della probabilità e delle conseguenze.
- **trasferimento del rischio:** condivisione con altro soggetto dell'onere derivante da un rischio.

Per ogni minaccia considerata è stato calcolato un indice di rischio che è una funzione della probabilità di accadimento, della vulnerabilità del Titolare a quella minaccia e dell'ipotetico valore del danno.
A fronte dell'indice di rischio calcolato per ciascuna minaccia, viene pertanto proposto il criterio di gestione del rischio (accettare, mitigare, ridurre, trasferire) e vengono valutate e scelte le più opportune contromisure da adottare.

Classificazione e conseguenze delle minacce
Le minacce possono essere distinte in:

- naturali
  - terremoto
  - incendio
  - alluvione
  - esplosione
  - fulmine
  - smottamenti
- tecniche
  - blackout elettrici
  - corto circuiti
  - rottura apparati di alimentatore
  - rottura di dischi o supporti di memorizzazione
  - malfunzionamento, degrado o indisponibilità degli strumenti
  - guasti ai sistemi complementari (impianto elettrico, climat.)
- comportamentali interni
  - imprudenza, imperizia, negligenza
  - installazione/uso di software non autorizzato
  - uso di risorse aziendali per attività illegali/illecite
  - uso di risorse aziendali per profitto personale
  - furto fisico, sabotaggio, distruzione di strumenti
  - furto elettronico, sabotaggio, distruzione/diffusione dati o di software
  - comportamenti sleali o fraudolenti
  - errori materiali
  - installazione/uso di strumenti o periferiche non autorizzati
- comportamentali esterni
  - attacchi di virus/trojan/worms
  - accessi logici e fisici non autorizzati

- spamming e altre tecniche di sabotaggio
- attacchi su bug di web server
- denial of service
- buffer overflow attacks
- exploits dovuti a scripting/mobile code (Java, Javascripts...)
- attacchi dovuti a debolezza del protocollo
- attacchi dovuti a password non sicure (furto credenziali).

Minacce naturali:
Le conseguenze delle minacce naturali possono riguardare:

- il patrimonio informativo, conservato su carta e/o a livello informatico
- le infrastrutture
- le strutture
- l'hardware
- il software

e comportano essenzialmente la distruzione o la perdita di dati.

Minacce tecniche:
Le conseguenze delle minacce tecniche possono riguardare:

- le infrastrutture: difetti di costruzione, installazione o funzionamento di parti automatiche in movimento, difetti di chiusura di infissi, ecc.
- le strutture: vizi e difetti nella costruzione o nel funzionamento di armadi, cassaforti, contenitori, ecc.
- l'hardware: difetti di costruzione, assemblaggio, installazione, manutenzione ecc.
- il software: difetti ed errori di produzione, installazione, configurazione, manutenzione, aggiornamento, ecc.

e possono comportare:

- distruzione, danneggiamento, perdita di dati
- alterazione dei dati
- accesso ai dati non consentito.

Minacce dovute a comportamenti umani:
Le conseguenze delle minacce dovute a comportamenti umani possono riguardare, a secondo della loro particolare natura:

- ✓ minacce di tipo fisico, accidentali:
  - infrastrutture: accesso non autorizzato o inconsapevole, ecc.
  - strutture: danneggiamento fortuito di un dispositivo di sicurezza, ecc.
  - hardware: distruzione o danneggiamento fortuito, uso senza istruzioni, uso eccessivamente intenso di apparati, ecc.
  - software: distruzione e danneggiamento, errori nell'installazione, utilizzo improprio, conflitto tra programmi, ecc.
  - patrimonio informativo: smarrimento di un fascicolo, alterazione casuale di documenti, fortuito trattamento non consentito di dati personali, ecc.

- ✓ minacce di tipo fisico, volontarie:
  - infrastrutture: accesso non autorizzato doloso, distruzione, danneggiamento, scassinamento di porte o cancelli, atti vandalici ecc.
  - strutture: furto, scassinamento, sabotaggio, ecc.
  - hardware: distruzione o danneggiamento dolosi, uso volutamente lesivo, volontario mancato rispetto delle istruzioni, sabotaggio, ecc.
  - software: distruzione o danneggiamento doloso, utilizzo improprio o doloso, cancellazione volontaria, ecc.

- risorse professionali: minacce al personale, pressioni ecc.
- patrimonio informativo: accesso doloso ai dati, trattamento erroneo, consentito, non conforme o eccedente le finalità della raccolta, ecc.

✓ minacce di penetrazione logica, accidentali:
- software: intercettazioni accidentali, accesso non consentito a un programma o ad un file, ecc.
- risorse professionali: introduzione di alterazioni o vizi di procedura, di errori nella gestione dei dati, perdita dell'integrità dei dati nello svolgimento di un compito particolare, ecc.
- patrimonio informativo: accesso involontario ai dati, alterazione, distruzione, danneggiamento, perditadell'integrità, trattamento erroneo, non consentito, non conforme o eccedente le finalità della raccolta, ecc.

✓ minacce di penetrazione logica, volontarie:
- hardware: monitoraggio indebito o alterazione della trasmissione dati effettuata da router e server, ecc.
- software: intercettazioni, virus, trojan horse, intrusioni, ecc.
- risorse professionali: possibili intimidazioni, pressioni, ricatti, ecc.
- patrimonio informativo: accesso doloso ai dati, alterazione, distruzione, danneggiamento, perditadell'integrità, trattamento erroneo, non consentito, non conforme o eccedente le finalità della raccolta, ecc.

Minacce e loro conseguenze sui dati

Nella tabella che segue sono riportate le principali minacce, con l'indicazione delle conseguenze che dette minacce possono avere sui dati e sulla sicurezza dei trattamenti.

Tipo	Minacce	Conseguenze sui dati o sulla sicurezza dei trattamenti
Comportamento di soggetti interni, accidentali o volontari	Ingressi non autorizzati a locali/aree ad accesso ristretto	Danneggiamento hardware e software; possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Sottrazione di documenti contenenti dati	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati e documenti non consentita
	Carenza di consapevolezza, disattenzione, incuria	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Comportamenti sleali o fraudolenti	Acquisizione di dati da utilizzare con vantaggio personale (comunicazione informazione a concorrenti, atti di sabotaggio)
	Ignoranza procedurale	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Errore o disattenzione	Possibilità di distruzione, perdita, modifica di dati non prevista (es. chiusura di computer mentre è in corso l'aggiornamento patch)
	Errore nella gestione della sicurezza	Danneggiamento hardware e software distruzione,perdita di dati (es. strumento elettronico incustodito durante la sessione di trattamento dati)
	Uso illegittimo di strumenti	Possibilità di utilizzo dei dati ad uso personale, consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Installazione non autorizzata di strumenti	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita, comunicazione o diffusione illegittima di dati
	Danneggiamento degli strumenti o apparati	Possibilità di distruzione, perdita, modifica di dati non prevista
	Furto di strumenti e apparati	Possibilità di consultazione non autorizzata; comunicazione o diffusione illegittima di dati
	Installazione o produzione di copie di dati abusive	Acquisizione di dati da utilizzare con vantaggio personale e/o comunicazione o diffusione illegittima di dati
	Uso improprio del software	Possibilità di distruzione, perdita, modifica di dati non prevista
	Furto o disinstallazione di software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Danneggiamento del software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Installazione non autorizzata di software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita, comunicazione o diffusione illegittima di dati
	Erronea abilitazione all'accesso	Possibilità da parte di soggetti non incaricati di consultare, distruggere, modificare, comunicare, diffondere dati
	Modifica non controllata	Possibilità di modifica di dati non consentita
	Cancellazione	Possibilità di distruzione o perdita di dati non prevista
	Distruzione	Possibilità di distruzione o perdita di dati non prevista
	Diffusione illegittima	Possibilità di comunicazione o diffusione di dati non autorizzata
	Altri atti di sabotaggio	Possibilità di utilizzo dei dati ad uso personale, consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita; comunicazione o diffusione di dati non autorizzata
	Sottrazione delle credenziali di autenticazione	Possibilità di accesso non consentito, distruzione, perdita, modifica di dati con responsabilità attribuita ad altri

Comportamento di soggetti esterni, accidentali o volontari	Azione di virus informatici o di altri programmi dannosi	Danneggiamento software e/o accesso non consentito, distruzione, perdita, modifica,invio di dati a terzi
	Spamming o altre tecniche di sabotaggio	Intasamento/blocco della casella postale con possibile perdita di dati
	Accessi esterni, fisici e logici, non autorizzati	Possibilità da parte di terzi non autorizzati di consultare, distruzione, modificare, comunicare, diffondere dati
	Ingressi non autorizzati a locali/aree ad accesso ristretto	Danneggiamento hardware e software; possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Intercettazioni di informazioni in rete	Possibilità di accesso non consentito,distruzione, perdita, modifica di dati, comunicazione a terzi
	Sottrazione delle credenziali di autenticazione	Possibilità di accesso non consentito, distruzione, perdita, modifica di dati con responsabilità attribuita ad altri
	Uso illegittimo di strumenti	Possibilità di utilizzo dei dati ad uso personale, consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Danneggiamento degli strumenti	Possibilità di accesso non consentito, distruzione, perdita modifica di dati, comunicazione a terzi
	Furto o disinstallazione di software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Danneggiamento del software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Furto di strumenti e apparati	Possibilità di consultazione non autorizzata; comunicazione o diffusione illegittima di dati
	Installazione non autorizzata di strumenti	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita, comunicazione o diffusione illegittima di dati
	Installazione non autorizzata di software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita, comunicazione o diffusione illegittima di dati
	Installazione o produzione di copie abusive	Acquisizione di dati da utilizzare con vantaggio personale e/o comunicazione o diffusione illegittima di dati
	Altre intercettazioni	Possibilità di accesso non consentito, modifica di dati con responsabilità attribuita ad altri; comunicazione o diffusione illegittima di dati
	Altri atti di sabotaggio	Possibilità di uso dei dati ad uso personale, consultazione non autorizzata; distruzione, perdita, modifica illecita; comunicazione o diffusione di dati non autorizzata
	Furto di credenziali di autenticazione	Accesso non consentito, distruzione, perdita, modifica, diffusione di dati con responsabilità attribuita ad altri
Tecniche	Dismissione, rottamazione o Interruzione d'uso	Possibilità di consultazione e comunicazione di dati riservati contenuti su strumenti informatici dismessi o in assistenza per manutenzione
	Interventi di Manutenzione	Possibilità di consultazione e comunicazione di dati riservati da parte di chi esegue aggiornamenti, integrazioni, modifiche ai programmi
	Interruzione d'uso del sfwr	Impossibilità di consultazione e di trattamento di dati
	Interruzione della connessione	Rallentamento o blocco dell'attività operativa, con necessità di ricorso ad altri canali di comunicazione
	Malfunzionamento, degrado,	Distruzione, perdita, modifica di dati
	Guasto tecnologico	Possibilità di distruzione, perdita, modifica di dati o di comunicazione illegittima a terzi
	Guasto a sistemi complement.	distruzione e perdita di dati
Naturali	Terremoto o smottamento	Danneggiamento hardware e software, distruzione, perdita di dati
	Incendio, fulmine	Danneggiamento hardware e software, distruzione, perdita di dati
	Esplosione	Danneggiamento hardware e software, distruzione, perdita di dati
	Alluvione, allagamento	Danneggiamento hardware e software, distruzione, perdita di dati

4. MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI (regola 19.4)

Nel presente paragrafo vengono elencate le possibili misure di sicurezza atte a garantire:

- la protezione delle aree e dei locali nei quali si svolgono i trattamenti;
- la corretta archiviazione e custodia di atti, documenti e supporti;
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

ELENCO DELLE POSSIBILI MISURE DI SICUREZZA	
1. **MISURE MINIME**	
1.1.	**Uso di procedure di autenticazione**
1.1.1	Obbligo di unicità e segretezza delle credenziali
1.1.2	Obbligo di diligente custodia delle credenziali con specifiche prescrizioni
1.1.3	Modifica periodica delle password (6 mesi; 3 per dati sensibili)
1.1.4	Disattivazione password non utilizzate per 6 mesi
1.1.5	Divieto di lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro
1.1.6	Adozione di procedura per l'accesso in caso di assenza dell'incaricato
1.2.	**Individuazione dei profili di autorizzazione**
1.2.1	Analisi e definizione dei profili
1.2.2	Revisione almeno annuale della sussistenza dei profili di autorizzazione
1.3.	**Revisione almeno annuale degli ambiti dei trattamenti consentiti agli incaricati**
1.4.	**Protezione di dati e strumenti elettronici da trattamenti illeciti e da accessi non consentiti**
1.4.1	Adozione di sistemi antivirus
1.4.2	Adozione di sistemi firewall
1.4.3	Aggiornamento semestrale dei suddetti apparati o sistemi software
1.4.4	Aggiornamento annuale (semestrale per i dati sensibili) dei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggere i difetti
1.5.	**Produzione almeno settimanale delle copie di sicurezza almeno una volta a settimana**
1.5.1	Definizione di procedure per il salvataggio dei dati
1.5.2	Definizione di procedure per garantire il ripristino dei dati in caso di danneggiamento degli stessi
1.6.	**Istruzioni per la gestione di supporti rimovibili contenenti dati sensibili o giudiziari**
1.6.1	Istruzioni per la custodia e l'uso dei supporti
1.6.2	Istruzioni per la distruzione o il riutilizzo dei supporti
1.7.	**Adozione di misure e procedure per garantire il ripristino dei dati sensibili in massimo 7 gg**
1.8.	**Disgiungimento o cifratura di dati idonei a rivelare lo stato di salute o la vita sessuale**
1.9.	**Acquisizione delle dichiarazioni di conformità per installazioni concernenti la sicurezza**
1.10.	**Istruzioni per il controllo e la custodia di dati e documenti cartacei**
1.10.1	Istruzioni per il controllo e la custodia di dati comuni e documenti cartacei
1.10.2	Istruzioni per il controllo e la custodia di dati sensibili o giudiziari e documenti cartacei
1.10.3	Istruzioni per la gestione e l'accesso agli archivi contenenti dati sensibili
1.11.	**Produzione e aggiornamento dell'elenco dei trattamenti effettuati**
1.12.	**Protezione di aree e locali rilevanti ai fini della custodia e accessibilità dei dati**
1.13.	**Definizione di criteri e controlli sull'operato di affidatari esterni dei dati**
1.14.	**Attività di formazione programmate**

ALTRE MISURE
2. Misure organizzative
2.1. Adozione di procedure formali per la produzione e gestione delle copie di sicurezza
2.2. Adozione del registro delle copie
2.3. Copie di sicurezza giornaliere
2.4. Copie di sicurezza conservate in altra sede
2.5. Procedure di Disaster recovery e business continuity
2.6. Piano di prevenzione virus
2.7. Procedure rigorose per l'installazione del software
2. 8. procedure rigorose per la manutenzione dei sistemi
2. 9. Redazione di mansionari
2.10. Procedure di accesso e uso dei sistemi informativi
3. Misure fisiche
3.1. Vigilanza della sede
3.2. Ingresso della sede presidiato
3.3. Identificazione dei visitatori
3.4. Registrazione dei visitatori
3.5. Sistemi di allarme e sorveglianza
3.6. Adozione di sistemi di autenticazione degli accessi
3.7. Custodia di documenti e atti in classificatori e armadi ignifughi
3.8. Deposito di password o dei dati in cassaforte
3.9. Custodia dei supporti magnetici in contenitori sigillati
3.10. Esistenza di dispositivi antincendio
3.11. Sistemi di continuità dell'alimentazione elettrica
3.12. Rilevatori di gas
3.13. Locali dotati di serratura e distribuzione oculata delle chiavi
4. Misure logiche
4.1. Adozione di sistemi automatici di controllo password
4.2. antivirus aggiornato quotidianamente
4.3. Controllo delle funzionalità e dell'integrità del Firewall
4.4. Adozione di sistemi antispamming
4.5. Cifratura dei dati sensibili o pericolosi per la Privacy degli interessati
4.6. Cifratura delle trasmissioni
4.7. Annotazione della fonte dei dati
4.8. Rilevazione delle intercettazioni
4.9. Verifiche periodiche di rispetto delle finalità dei trattamenti e della non eccedenza dei trattamenti
4.10. Verifiche automatizzate dei requisiti dei dati
4.11. Controllo dei supporti inviati in manutenzione
4.12. Limitazione e identificazione degli incaricati che effettuano la trasmissione dei dati
5. Altre misure
5.1 Affidamento in outsourcing
5.2 Stipula di coperture assicurative
5.3 Sviluppo clima positivo
5.4 Adozione della politica delle scrivanie pulite

Le misure adottate dal **Titolare** sono commisurate all'indice di rischio (**IR**) definiti al precedente punto. Di seguito si procede perciò alla descrizione:

- delle misure che risultano già adottate alla data del presente documento;

- delle eventuali ulteriori misure atte ad incrementare la sicurezza nei trattamenti, la cui adozione sia stata programmata entro un arco di tempo ragionevole (indicativamente entro la fine del corrente anno 2009).

Protezione di aree e locali

La sede del Comune è ubicata in un edificio di tre piani fuori terra indipendente su tre lati. Al complesso si accede tramite androne sorvegliato nelle ore diurne dagli stessi dipendenti che svolgono la loro funzione al piano terreno. Gli uffici sui tre piani sono così distribuiti:

- Piano terreno:
  - servizio alla persona (Anagrafe, Stato Civile, Elettorale e Statistico, Commercio e Artigianato, Agricoltura e Industria, Polizia Amministrativa, Leva, Cimitero, Acquedotto, Istruzione e Cultura, Assistenza, C.E.D., Sport e Tempo Libero, Turismo)
- Piano primo:
  - servizio amministrativo e finanziario (Segreteria, Delibere Consiglio Comunale, Delibere Giunta Comunale, Determine, Protocollo, Bilancio, Contabilità, Tributi, Personale)
  - servizio di Polizia municipale (Controllo del territorio, Viabilità, Polizia Giudiziaria, Polizia Locale, Polizia Rurale, Occupazione Suolo Pubblico, Ospitalità Stranieri, Cessione Fabbricati, Denunce Infortuni sul Lavoro)
  - Ufficio del Segretario Comunale
  - Ufficio del Sindaco
- Piano secondo:
  - Servizio Tecnico (Edilizia privata, Edilizia Pubblica, Urbanistica, Lavori Pubblici)

Al piano terra vi è un locale adibito al servizio riscossioni (gestito da Equitalia) e ad incontri di sindacati e patronati al servizio dei cittadini. Tali enti esterni non interferiscono in alcun modo con l'attività comunale, essendo il locale separato dagli uffici ove si svolgono i trattamenti e avendo in comune con essi solo l'androne di accesso.
Agli uffici del piano terreno si accede tramite porta a vetri. Il primo locale è dotato di front desk con banchi reception per le relazioni con il pubblico. Agli altri uffici del piano terreno si accede attraversando ulteriori porte.
Agli uffici del primo piano si accede tramite ascensore o scalinata interna; ad ogni ufficio è dedicata una stanza. Agli uffici operativi si accede dal corridoio, utilizzato anche come sala d'attesa, al quale si accede
varcando una porta sul pianerottolo.
Agli uffici del secondo piano si accede tramite ascensore o scalinata interna; anche in questo piano ogni ufficio è separato dall'altro e l'ingresso è consentito tramite una porta che conduce ad un corridoio che funge anche da sala di aspetto.
Ogni ufficio è stato arredato con armadi e cassetti, taluni dei quali chiudibili a chiave.
Gli uffici vengono regolarmente chiusi a chiave fuori dagli orari di lavoro. Invece durante l'orario di operatività la sede è sempre presieduta.
La Sala Consiglio è ubicata in una palazzina adiacente all'edificio comunale, in piazza XXV Aprile, sede del locale Poliambulatorio.
Tutti i locali sono protetti da un sistema di antifurto sonoro collegato con i Carabinieri.
Con determinazione n. 369 del 16/09/2008 è stato affidato alla Ditta Lanponet di Cuorgnè l'installazione di un impianto di videosorveglianza presso il palazzo municipale con registrazione delle immagini su un pc installato presso il Servizio Tributi.

LE SEDI DISTACCATE

Biblioteca Civica (via Carlo Alberto Dalla Chiesa n. 3)
La Biblioteca civica è ubicata al primo piano di una palazzina il cui piano terreno è adibito a locali commerciali.

L'ingresso al pubblico è indipendente e avviene tramite scala interna o rampa per i disabili disposta sul lato nord della palazzina.
La biblioteca dispone anche di un altro accesso (nell'ala vecchia dell'edificio), ma quest'ultimo non è utilizzato dal pubblico e viene aperto dai funzionari solo in caso di necessità.
I locali sono protetti da antifurto sonoro.

Ufficio turistico (piazza Craveri n. 8)
L'Ufficio Turistico, situato al piano terreno di una palazzina interamente di proprietà del comune, è composto da due locali: il primo è adibito a ricezione del pubblico, il secondo, situato al piano intermezzo, è adibito a vetrina e deposito di materiale informativo. Al piano superiore è situata la sede di una associazione.

Custodia e archiviazione di atti, documenti e supporti
Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti (CD, dischetti, …), si è provveduto ad istruire gli incaricati affinché essi adottino precise procedure atte a salvaguardare la riservatezza dei dati ivi contenuti.

Agli incaricati sono state date disposizioni, per iscritto, di accedere ai soli dati personali, prelevando dagli archivi i relativi atti e documenti, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. In caso di dubbio, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile dei trattamenti, o direttamente al **Titolare**.

Gli incaricati devono inoltre custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi ricollocarli nell'archivio al termine di tale ciclo.
Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari, tuttavia di norma non trattati. Agli incaricati viene prescritto, in questi casi, di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione.
Al fine di porre in essere le suddette misure di protezione dei dati personali, gli incaricati sono stati dotati di:

- classificatori, cassetti e armadi non accessibili (dotati di serratura);
- contenitori chiusi per i supporti magnetici;

I documenti, soprattutto se contenti eventuali dati sensibili o, a maggior ragione, dati giudiziari, sono riposti, a cura dei diretti interessati, negli appositi dispositivi protetti prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi, i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli nei giorni successivi.
Al termine del trattamento, l'incaricato ripone nell'archivio gli atti, i documenti ed i supporti non più necessari per lo svolgimento delle proprie mansioni lavorative.

Per quanto concerne l'archiviazione, già si è detto che il **Titolare** ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali.
Ovviamente, particolari cautele sono previste per l'archiviazione di documenti, atti e supporti eventualmente contenenti dati sensibili o giudiziari.

Misure logiche di sicurezza
Gli strumenti elettronici utilizzati dal Comune per effettuare i trattamenti di dati personali sono di proprietà della stessa.
Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), sono state adottate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone affinché a ciascuno strumento elettronico possa accedere solo chi è autorizzato;
- realizzazione e gestione di un sistema di autorizzazioni, al fine di individuare le tipologie di dati ai quali i singoli incaricati possono accedere ed i tipi di trattamenti che su di essi sono autorizzati ad effettuare;
- adozione di un sistema di controllo degli accessi;
- registrazione degli accessi;
- realizzazione, gestione e periodico aggiornamento di un sistema di protezione degli strumenti e dei dati da malfunzionamenti, da attacchi informatici e da programmi che contengono codici maliziosi (virus);
- prescrizione di opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD, …), nei quali siano contenuti dati personali;
- annotazione della fonte dei dati;
- annotazione del responsabile di ciascuna operazione;
- rilevazione di intercettazioni;
- monitoraggio continuo delle connessioni di rete;
- verifiche periodiche su dati o trattamenti non consentiti o non corretti;
- verifiche automatizzate dei requisiti dei dati;
- controllo sull'operato degli addetti alla manutenzione;
- controllo dei supporti consegnati in manutenzione;
- verifica periodica della leggibilità dei supporti.

Più in particolare:
Tutti gli incaricati e il sindaco hanno una credenziale di autenticazione composta da userID e password. Assessori e consiglieri hanno una password comune che abilita l'accesso ad una unica cartella di documenti comuni.
La password abilita l'accesso al dominio di rete ed agli applicativi.
Tutte le password sono di almeno otto caratteri, non sono riconducibili all'utilizzatore e vengono cambiate ogni tre mesi a cura degli incaricati e su segnalazione automatica di scadenza ad opera dei server.
Il sistema di autenticazione è impostato su due livelli:
- il primo consiste nell'abilitazione ai servizi di rete e abilita l'accesso agli applicativi Windows;
- il secondo abilita l'accesso ad alcuni applicativi residenti sul server Linux.
[ss7]L'amministratore di sistema ha una credenziale che lo abilita a qualsiasi tipo di intervento su tutti gli applicativi e su entrambi i server.
Ad ogni credenziale è abbinato un preciso profilo di autorizzazione che abilita o meno l'accesso agli applicativi e, nell'ambito di ogni applicativo, alle operazioni ed ai trattamenti consentiti ad ogni incaricato.
L'amministratore di sistema definisce con i responsabili dei servizi i profili di autorizzazione.
Poichè tutti documenti sono organizzati in cartelle accessibili da profili e ambiti di incarico omogenei, in funzione del servizio di appartenenza, considerato anche che l'amministratore di sistema può intervenire per modificare all'occorrenza le credenziali, non viene tenuta copia delle password in uso.
Viene mantenuta una copia della password dell'amministratore di sistema in busta chiusa riposta in cassaforte, le cui chiavi sono custodite dal Comandante dei Vigili Urbani.
Il sistema antivirus in uso è Trend Micro ed è installato sia sul server della sede che sul server della biblioteca; l'aggiornamento è automatico e gli aggiornamenti sono rilasciati dal server ai client in tempo reale.
I firewall (hardware con software a bordo) hanno anche funzionalità di antivirus di primo livello.
Il sistema di posta, a cura del provider, è protetto da un sistema antivirus e anti spamming.

I client della sede non hanno restrizioni di accesso ad Internet, mentre restrizioni significative sono state applicate ai client della biblioteca che vengono utilizzati dai cittadini, anche minori.
Poichè per gli accessi pubblici ad Internet della biblioteca sussistono gli stessi obblighi previsti per gli Internet Point, vengono conservati i log di accesso e gli identificativi degli utenti.
Nuove utenze
L'attivazione di nuove utenze, in caso di assunzione o di trasferimento di un dipendente, avviene su comunicazione dell'Ufficio del Personale al Responsabile per la sicurezza dei Sistemi Informativi.
La tipologia di profilo da assegnare sul sistema gestionale viene indicata dal responsabile del serizio cui appartiene il nuovo utente e il Responsabile dei Sistemi Informativi procede all'attivazione dell'utenza (e del nuovo profilo di posta) con il profilo richiesto.

Disposizioni generali sull'uso degli elaboratori

Agli incaricati sono state impartite precise istruzioni in merito ai seguenti punti:

- Dovere di custodire eventuali dispositivi di accesso agli strumenti informatici, attribuiti agli incaricati a titolo di possesso ed uso esclusivo. La custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici (viene prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo come se fosse una carta di credito). In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza all'amministratore di sistema, o alle altre persone che sono state a tale fine indicate al momento dell'attribuzione del dispositivo.
- Obbligo di non lasciare incustodito e accessibile lo strumento elettronico, sia durante una sessione di trattamento che in ipotesi di breve assenza.
- Dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (username), attribuite.
- Attenzione e impegno a non lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale scopo, per evitare errori o dimenticanze, è stato inserito lo screen saver automatico che si attiva dopo 5 minuti di non utilizzo, con password segreta per la ripresa del lavoro.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'incaricato stesso;
- i caratteri che costituiscono la singola password, secondo buona norma, siano per almeno un quarto e per non più della metà di natura numerica;
- le password non devono essere comunicate a nessuno, ma scritte e consegnate in busta chiusa al Titolare per garantire in casi di emergenza il regolare svolgimento delle attività lavorative.

Le password sono conservate a cura di un incaricato.

Custodia dei supporti

Per quanto concerne i supporti rimovibili (floppy disk, dischi ZIP, CD, …), contenenti dati personali, la norma impone particolari cautele nell'ipotesi in cui contengano dati sensibili o giudiziari.
E' stata tuttavia data disposizione di estendere tali accorgimenti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento che:

- i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti;
- essi devono essere conservati in cassetti chiusi a chiave, quando non utilizzati.

Una volta cessate le ragioni per la conservazione dei dati, vengono adottati opportuni accorgimenti, finalizzati a rendere non intelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti.
Tali supporti vengono quindi formattati più volte, o eventualmente distrutti.

Riepilogo delle misure adottate e da adottare per contrastare i rischi

Nella tabella che segue vengono riportati i fattori di rischio individuati e, per ciascuno di essi, vengono indicate le corrispondenti contromisure adottate per ridurre la probabilità di accadimento dell'evento dannoso o per ridurre gli effetti che l'evento dannoso potrebbe causare ai dati, o agli strumenti, o ai trattamenti.

	Minacce	Gestione	Misure di sicurezza già adottate	Misure di sicurezza da adottare
Comportamento di interni	Ingressi non autorizzati a locali/aree ad accesso ristretto	Accettare	**1.10 dati e doc. cartacei** **1.12 protezione aree e locali** 2.9 mansionari 2.10 procedure d'uso dei sistemi 3.2 ingresso presidiato 3.5 allarmi 3.13 locali chiusi a chiave	Attuazione della politica della "scrivania pulita"
	Sottrazione di documenti contenenti dati	Accettare	**1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 2.9 mansionari 2.10 procedure d'uso dei sistemi 3.2 ingresso presidiato 3.5 allarmi 3.13 locali chiusi a chiave 5.3 clima positivo	Attuazione della politica della "scrivania pulita"
	Carenza di consapevolezza, disattenzione, incuria	Accettare	**1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.10 dati e doc. cartacei** **1.14 formazione** 2.3 copie giornaliere 4.9 verifiche periodiche 5.3 clima positivo	
	Comportamenti sleali o fraudolenti	Mitigare	**1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** 2.3 copie giornaliere 4.9 verifiche periodiche 5.3 clima positivo	Adozione regolamento di disciplina sull'uso degli strumenti informatici
	Ignoranza procedurale	Accettare	**1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.10 dati e doc. cartacei** **1.14 formazione** 2.3 copie giornaliere 4.9 verifiche periodiche	
	Errore o disattenzione	Accettare	**1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.10 dati e doc. cartacei** **1.14 formazione** 2.3 copie giornaliere 4.9 verifiche periodiche	
	Errore nella gestione della sicurezza	Accettare	**1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.9 redazione di mansionari 2.10 procedure uso sistemi 4.9 verifiche periodiche	
	Uso illegittimo di strumenti	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** 2.3 copie giornaliere 4.9 verifiche periodiche	

Installazione non autorizzata di strumenti	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.9 redazione di mansionari 2.10 procedure uso sistemi 4.9 verifiche periodiche	
Danneggiamento degli strumenti o apparati	Accettare	**1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.10 procedure uso sistemi 4.9 verifiche periodiche 5.3 clima positivo	
Furto di strumenti e apparati	Accettare	**1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 3.2 ingresso presidiato 3.5 allarmi 3.13 locali chiusi a chiave 5.3 clima positivo	
Installazione o produzione di copie di dati abusive	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.5 copie di sicurezza** 2.3 copie giornaliere 2.10 procedure uso sistemi 4.9 verifiche periodiche 5.3 clima positivo	
Uso improprio del software	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.10 procedure uso sistemi 4.9 verifiche periodiche	
Furto o disinstallazione di software	Accettare	**1.1 procedure credenziali** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 3.2 ingresso presidiato 3.13 locali chiusi a chiave 5.3 clima positivo	
Danneggiamento del software	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.10 procedure uso sistemi 4.9 verifiche periodiche	
Installazione non autorizzata di software	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.10 procedure uso sistemi 4.9 verifiche periodiche	
Erronea abilitazione all'accesso	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.9 redazione di mansionari 2.10 procedure uso sistemi 4.9 verifiche periodiche	

	Modifica non controllata	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.9 redazione di mansionari 2.10 procedure uso sistemi 4.9 verifiche periodiche	
	Cancellazione	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.9 redazione di mansionari 2.10 procedure uso sistemi 4.9 verifiche periodiche	
	Distruzione	Accettare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.9 redazione di mansionari 2.10 procedure uso sistemi 4.9 verifiche periodiche	
	Diffusione illegittima	Mitigare	**1.2 profili di autorizzazione** **1.3 ambiti di incarico** **1.5 copie di sicurezza** **1.14 formazione** 2.3 copie giornaliere 2.9 redazione di mansionari 2.10 procedure uso sistemi 4.11 controllo supporti manut. 4.9 verifiche periodiche	Adozione regolamento di disciplina sull'uso degli strumenti informatici Aggiornamento formazione
	Altri atti di sabotaggio	Mitigare	**1.1 procedure credenziali** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 3.2 ingresso presidiato 3.13 locali chiusi a chiave 3.5 allarmi 5.3 clima positivo	
	Sottrazione delle credenziali di autenticazione	Accettare	**1.1 procedure credenziali** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 3.13 locali chiusi a chiave 4.11 controllo supporti manut. 5.3 clima positivo	
Comportamento di est	Azione di virus informatici o di altri programmi dannosi	Accettare	**1.4 protezione strumenti** **1.5 copie di sicurezza** **1.13 controllo tratt. esterni** 2.3 copie giornaliere 2.6 piano di prevenzione virus 4.2 agg. quotidiano antivirus 4.4 antispamming	Diffusione istruzioni e piano di prevenzione virus
	Spamming o altre tecniche di sabotaggio	Accettare	**1.4 protezione strumenti** **1.5 copie di sicurezza** 2.3 copie giornaliere 4.2 agg. quotidiano antivirus 4.4 antispamming	Istruzioni specifiche per la posta
	Procurato malfunzionamento, degrado, degli strumenti	Accettare	**1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 2.7 procedure installaz. sw 2.8 procedure manutenzione 3.2 ingresso presidiato 3.5 allarmi 3.13 locali chiusi a chiave	

e r n i	Accessi esterni fisici e logici, non autorizzati	Mitigare	**1.4 protezione strumenti** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 2.6 piano di prevenzione virus 2.7 procedure installaz. sw 2.8 procedure manutenzione 3.1 vigilanza sede 3.2 ingresso presidiato 3.5 allarmi 3.13 locali chiusi a chiave 4.2 agg. quotidiano antivirus 4.4 antispamming	Potenziamento delle misure fisiche di controllo
	Ingressi non autorizzati a locali/aree ad accesso ristretto	Mitigare	**1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 3.1 vigilanza sede 3.2 ingresso presidiato 3.5 allarmi 3.6 autenticazione accessi 3.13 locali chiusi a chiave	Potenziamento delle misure fisiche di controllo
	Intercettazioni di informazioni in rete	Accettare	**1.4 protezione strumenti** 2.6 piano di prevenzione virus 2.7 procedure installaz. sw 2.8 procedure manutenzione 4.2 agg. quotidiano antivirus 4.8 rilevazione intercettazioni 4.12 limitazione incaricati	
	Sottrazione delle credenziali di autenticazione	Accettare	**1.1 procedure credenziali** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 3.13 locali chiusi a chiave 4.11 controllo supporti manut.	
	Uso illegittimo di strumenti	Accettare	**1.1 procedure credenziali** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 2.7 procedure installaz. sw 2.8 procedure manutenzione 3.13 locali chiusi a chiave 3.2 ingresso presidiato 3.13 locali chiusi a chiave 4.11 controllo supporti manut.	
	Danneggiamento degli strumenti	Accettare	**1.1 procedure credenziali** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 2.8 procedure manutenzione 3.13 locali chiusi a chiave 3.1 vigilanza sede 3.2 ingresso presidiato 3.5 allarmi	
	Furto o disinstallazione di software	Accettare	**1.1 procedure credenziali** **1.12 protezione aree e locali** 2.7 procedure installaz. sw 2.8 procedure manutenzione 3.13 locali chiusi a chiave	
	Danneggiamento del software	Accettare	**1.1 procedure credenziali** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 2.7 procedure installaz. sw 2.8 procedure manutenzione 3.13 locali chiusi a chiave 4.11 controllo supporti manut.	
	Furto di strumenti e apparati	Ridurre Trasferire	**1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 3.1 vigilanza sede 3.2 ingresso presidiato 3.5 allarmi 3.13 locali chiusi a chiave	Potenziamento delle misure fisiche di controllo Stipula coperture assicurative

	Installazione non autorizzata di strumenti	Accettare	**1.1 procedure credenziali** **1.12 protezione aree e locali** 2.8 procedure manutenzione 3.13 locali chiusi a chiave	
	Installazione non autorizzata di software	Accettare	**1.1 procedure credenziali** **1.12 protezione aree e locali** 2.7 procedure installaz. sw 2.8 procedure manutenzione	
	Installazione o produzione di copie abusive	mitigare	**1.1 procedure credenziali** **1.2 profili di autorizzazione** 2.7 procedure installaz. sw 2.8 procedure manutenzione 3.13 locali chiusi a chiave	Potenziamento delle misure fisiche di controllo
	Altre intercettazioni	Accettare	**1.4 protezione strumenti** 2.7 procedure installaz. sw 2.8 procedure manutenzione 4.8 rilevazione intercettazioni 4.12 limitazione incaricati	
	Altri atti di sabotaggio	Ridurre Trasferire	**1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 2.7 procedure installaz. sw 2.8 procedure manutenzione 3.1 vigilanza sede 3.2 ingresso presidiato 3.5 allarmi 3.13 locali chiusi a chiave	Potenziamento delle misure fisiche di controllo Stipula coperture assicurative
	Furto di credenziali di autenticazione	Accettare	**1.1 procedure credenziali** **1.5 copie di sicurezza** **1.12 protezione aree e locali** 2.3 copie giornaliere 3.8 deposito in cassaforte 3.13 locali chiusi a chiave 4.11 controllo supporti manut.	
tecniche	Dismissione, rottamazione o Interruzione d'uso	Accettare	**1.1 procedure credenziali** **1.6 gestione supporti** 2.7 procedure installaz. sw 2.8 procedure manutenzione 4.11 controllo supporti manut.	
	Interventi di Manutenzione	Accettare	**1.1 procedure credenziali** **1.6 gestione supporti** 2.7 procedure installaz. sw 2.8 procedure manutenzione 4.11 controllo supporti manut.	
	Interruzione d'uso del sfwr	Accettare	2.7 procedure installaz. sw 2.8 procedure manutenzione 5.1 affidamento in outsourcing	
	Interruzione della connessione	Ridurre	2.8 procedure manutenzione	Backup delle connessioni
	Guasto tecnologico	Accettare	2.8 procedure manutenzione 5.1 affidamento in outsourcing	
	Guasto ai sistemi complementari	Accettare	2.8 procedure manutenzione 3.11 sistemi di continuità	
naturali	Terremoto o smottamento	Mitigare trasferire	2.4 copie in altra sede 2.5 disaster recovery 3.7 armadi ignifughi	stipula coperture assicurative
	Incendio, fulmine	Mitigare trasferire	2.4 copie in altra sede 2.5 disaster recovery 3.7 armadi ignifughi 3.10 dispositivi anti incendio	Potenziamento dispositivi prevenzione stipula coperture assicurative
	Esplosione	Ridurre trasferire	2.4 copie in altra sede 2.5 disaster recovery 3.7 armadi ignifughi 3.10 dispositivi anti incendio	stipula coperture assicurative
	Alluvione, allagamento	Ridurre trasferire	2.4 copie in altra sede 2.5 disaster recovery 3.7 armadi ignifughi	stipula coperture assicurative

Conclusioni

Le misure procedurali, fisiche, logiche di sicurezza, atte alla protezione dei dati e alla sicurezza dei trattamenti, di cui è dotato il **Titolare**, appaiono nel loro complesso più che adeguate al fine di

garantire la necessaria sicurezza ai dati personali oggetto di trattamenti. Per l'anno 2009, oltre a quanto indicato come misure da adottare, sono previsti ulteriori interventi finalizzati all'aggiornamento ed alla manutenzione generale del sistema di sicurezza.

5. CRITERI E MODALITÀ DI RIPRISTINO DEI DATI (regola 19.5)

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, sono stati previsti metodi e strumenti atti a garantire il loro ripristino in tempi brevi, comunque entro due giorni lavorativi.
A tale proposito sono previsti:

- operazioni periodiche di salvataggio dei dati;
- procedure di custodia dei backup;
- piani, anche non formalizzati, di continuità operativa;

Documenti cartacei
I documenti cartacei, e gli eventuali supporti diversi da quelli elettronici, contenenti dati personali, vengono accuratamente conservati negli armadi ubicati nei vari uffici.
I documenti cartacei e gli eventuali supporti diversi da quelli elettronici vengono archiviati solo in originale.

Dati contenuti su supporti elettronici
Le copie di sicurezza dei dati contenuti sul server Linux sono effettuate tramite uno streaming (su cassetta), una volta alla settimana, automaticamente. Viene utilizzata una serie di 6 cassette. Tutte le cassette vengono conservate in cassaforte.
Una volta al giorno (da lunedì a venerdì) viene effettuata una copia automatica su hard disk esterno con metodo differenziale. Il sabato viene effettuata la stessa copia ma con metodo incrementale.
Le copie del server della biblioteca vengono effettuate una volta al giorno su hard disk esterno (da lunedì a sabato) sia con metodo differenziale che con metodo incrementale.
Una volta all'anno viene generata una copia generale di tutti gli archivi che fotografa la situazione alla data di effettuazione. Tale copia viene conservata a cura dell'amministratore di sistema.[ss8]

Procedure di ripristino
Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti, sono state impartite le seguenti istruzioni:

- avvertire il Responsabile per la sicurezza dei Sistemi Informativi, che ha in custodia i supporti con le copie di sicurezza;
- chiedere l'immediato intervento dei responsabili esterni per:
  - sostituire, se necessario, l'intero hardware;
  - reinstallare tutti i dati contenuti nei supporti di sicurezza;
  - reinstallare i programmi danneggiati o distrutti;
  - aggiornare i sistemi operativi una volta reinstallati.

In ogni caso, il ripristino dei dati e dei sistemi deve avvenire entro due giorni lavorativi.
E' inoltre stato dato incarico al responsabile dei sistemi informatici di suggerire ogni altra misura opportuna al fine di evitare eventi di perdita e di danneggiamento degli strumenti elettronici e dei dati in essi contenuti.
La manutenzione delle procedure di ripristino viene effettuata in modo adeguato ad opera degli incaricati senza soluzione di continuità.

6. INTERVENTI FORMATIVI (regola 19.6)

Al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o in occasione dell'introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali, e comunque con frequenza annuale, sono previsti interventi formativi degli incaricati del trattamento, finalizzati a renderli edotti dei seguenti aspetti:

- eventuali aggiornamenti nella disciplina sulla protezione dei dati personali, in particolare per quanto concerne il proprio ambito di responsabilità;
- responsabilità nell'esercizio del proprio ruolo e rischi che incombono sui dati (con specificazione delle sanzioni connesse, penali e disciplinari);
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure di sicurezza adottate dal **Titolare**;
- invito a segnalare eventuali disfunzioni dei sistemi operativi;
- invito a richiedere ad un responsabile, in caso di dubbio, se un dato possa avere o meno natura sensibile o giudiziaria.

Gli interventi formativi possono avvenire sia all'interno, a cura del **Titolare** o di un incaricato per la sicurezza dei dati o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati. In ogni caso, sono previste riunioni periodiche per fare il punto sull'evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali.
Nel corso degli anni, il Titolare ha svolto le seguenti attività formative:

- **anno 2006**: sessioni di formazione tradizionali in aula per responsabili e incaricati, con un consulente esterno;
- **anno 2007**: sono state effettuate sessioni formative di approfondimento sulle linee guida in materia di trattamento dei dati dei lavoratori e sull'utilizzo della posta elettronica e di internet negli ambienti di lavoro. A detta sessione hanno partecipato gli incaricati addetti alla gestione del personale e tutti i responsabili. Inoltre, tutti gli incaricati hanno partecipato ad un incontro formativo sul Provvedimento 19/04/2007, n.17 "Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali";
- **anno 2009**: è previsto l'aggiornamento tramite un sistema di "help desk" on line per mezzo del quale sarà possibile: proporre domande, quesiti, dubbi interpretativi o applicativi; consultare le risposte ricevute, in forma scritta; consultare una sezione di FAQ; consultare, organizzati in una apposita sezione, il testo delle leggi, dei provvedimenti, dei codici deontologici; proporre domande e dubbi in merito alla scelta di apparati di sicurezza.

Un importante strumento formativo adottato è lo stesso Documento Programmatico sulla Sicurezza, che è stato usato come testo di auto apprendimento ed è messo a disposizione di tutti gli incaricati ed i responsabili.

7. AFFIDAMENTO DI TRATTAMENTI ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE (regola 19.7)

In conformità a quanto previsto dal D.lgs. 196/2003, per i trattamenti affidati all'esterno della struttura del **Titolare**, si sono adottati criteri atti a verificare che il soggetto destinatario abbia adottato misure di sicurezza conformi a quelle minime previste dagli articoli da 33 a 35 D.Lgs. 196/2003 e dal disciplinare tecnico allegato al codice.
A tal fine, sono state impartite istruzioni al soggetto esterno destinatario, affinché venga rispettato quanto prescritto dal D.lgs. 196/2003, se il terzo destinatario è italiano; dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

Inoltre, nel caso di destinatario italiano, ad esso viene richiesto che:

- rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico;

oppure

- consegni una copia del documento programmatico sulla sicurezza redatto, ovvero consegni una copia del certificato di conformità rilasciato da chi ha curato la progettazione e l'attuazione delle misure minime di sicurezza, nel caso in cui il destinatario abbia affidato a soggetti esterni tali compiti.

In ogni caso, è sempre previsto che debba rispettare specifiche clausole contrattuali, preventivamente convenute, al fine di disciplinare gli aspetti legati alla gestione dei dati personali ed in particolare al fine di limitare il trattamento dei dati affidati a quanto strettamente necessario ed in conformità a quanto indicato nelle informative date agli interessati.
Allo stato attuale, sono affidati all'esterno i trattamenti indicati al punto "**organigramma della Privacy**".

8. CIFRATURA O SEPARAZIONE DEI DATI IDENTIFICATIVI (regola 19.8)

Il **Titolare** non cripta archivi, né tratta archivi criptati da terzi.

9. CONTROLLO PERIODICO SULLO STATO DELLA SICUREZZA

Criteri generali di controllo
Al responsabile della sicurezza dei trattamenti è affidato il compito di verificare l'aggiornamento delle misure di sicurezza, al fine di proporre l'adozione di strumenti e conoscenze resi disponibili dal progresso tecnico, che consentano:

- di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati;
- di prevenire l'accesso non autorizzato;
- di evitare trattamenti non consentiti.

A tale fine, è previsto che:

- per singoli investimenti, i responsabili delle unità organizzative debbano ottenere l'autorizzazione del Responsabile Privacy o del **Titolare**;
- annualmente venga organizzata una riunione dei responsabili con il **Titolare** per discutere degli investimenti fatti e di quelli futuri.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il **Titolare**, il responsabile e le eventuali ulteriori persone da questi appositamente incaricate provvedono periodicamente, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento;

- verificare le procedure di archiviazione e custodia di atti, documenti e supporti;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate;
- controllare l'integrità dei dati e delle loro copie di backup;
- verificare la sicurezza delle trasmissioni in rete;
- controllare che i supporti magnetici non più riutilizzabili vengano distrutti;
- verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, il **Titolare** procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono più stati utilizzati.

Infine, con frequenza annuale, il **Titolare** svolge internamente, o con affidamento a società specializzata, un audit di sicurezza.
Con tale termine si intende l'attività di verifica, che potrà avvenire in modo estemporaneo, anche con verifiche casuali e non annunciate. Obiettivo dell'audit di sicurezza è di verificare che tutte le misure adottate, sia quelle tecnologiche che quelle organizzative, svolgano correttamente le funzionalità per cui sono state adottate.

Controlli specifici
I controlli specifici che il **Titolare** effettua, anche in modo occasionale e senza preavviso, hanno l'obiettivo di:

- ridurre i rischi di errore, furto, frode e/o uso scorretto degli impianti da parte delle persone interne all'organizzazione del Titolare o di esterni affidatari dei dati;
- far sì che gli utenti siano consapevoli delle minacce alla sicurezza e che siano idoneamente dotati per il sostegno e l'attuazione della politica per la sicurezza nello svolgimento delle proprie attività;
- minimizzare i danni provocati da incidenti e malfunzionamenti della sicurezza, monitorandoli per instaurare un processo di miglioramento continuo;
- prevenire:
  - l'accessi fisici non autorizzati,
  - danni al patrimonio informativo,
  - perdita, danno o compromissione di beni
  - interruzione delle attività;
- impedire la compromissione e/o il furto delle informazioni e degli strumenti di elaborazione delle informazioni;
- assicurare corrette operazioni di gestione e manutenzione degli strumenti di elaborazione;
- minimizzare il rischio di guasti e avarie ai sistemi;
- proteggere l'integrità del software, dei dati e dei documenti;
- mantenere l'integrità e la disponibilità delle informazioni e dei servizi di comunicazione;
- assicurare la salvaguardia delle informazioni nelle reti e nelle infrastrutture di supporto;
- prevenire perdite, modifiche o usi scorretti delle informazioni scambiate tra le unità organizzative interne o con altre organizzazioni;
- controllare l'accesso a dati e documenti;
- assicurare che i diritti di accesso ai sistemi siano conformi a quanto previsto, distribuiti e mantenuti in modo appropriato;
- prevenire accessi da parte di utenti non autorizzati;
- assicurare la protezione dei servizi di rete;
- prevenire accessi non autorizzati ai computer e ai dati contenuti nei sistemi;
- individuare attività non autorizzate;
- prevenire perdite, modifiche o usi impropri dei dati;
- proteggere la riservatezza, l'autenticità o l'integrità delle informazioni;
- assicurarsi che i progetti IT e le attività di sostegno siano gestiti in sicurezza;
- mantenere la sicurezza dei software e delle informazioni dei sistemi;

Ruolo del personale nella sicurezza

I ruoli e le responsabilità del personale sono esplicitati nel manuale della qualità e nei documenti operativi dei processi produttivi.

Tutto il personale viene informato e aggiornato in materia di sicurezza dei sistemi informativi.

Il personale ha altresì ricevuto precise istruzioni in merito a intercettare e formalizzare:

- incidenti,
- nuove o non ancora identificate minacce
- vulnerabilità e debolezze (reali o potenziali),
- malfunzionamenti o anomalia del software;

trasmettendone prontamente i contenuti al Direttore dei Sistemi Informativi, il quale provvede a definire tipo, gravità, entità, costi e possibile ricorsivitàdell'accaduto, avviando le necessarie azioni.

Sicurezza fisica e ambientale

Data la particolare localizzazione geografica e struttura del fabbricato non si ritengono necessari ulteriori protezioni per quanto concerne gli eventi naturali.

Tutti i cavi dati sono stati inseriti all'interno di appositi canaline protette da eventuali manomissioni.

La manutenzione dei sistemi informatici è affidata ad aziende qualificate cui sono state impartite specifiche prescrizioni di sicurezza.

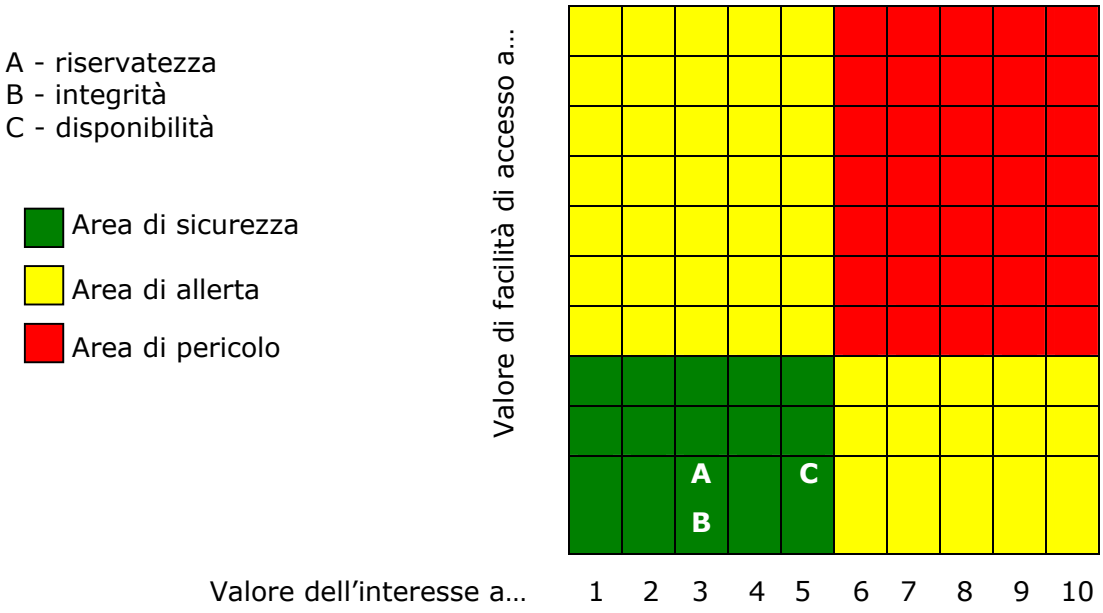
Nel caso in cui fosse necessario, per qualsiasi motivo, asportare parti critiche dei sistemi (per riparazioni o sostituzioni) l'amministratore interno di sistema da giustificazione alla Direzione per ottenere le necessarie autorizzazioni. Le componenti asportate o dimesse dovranno vengono svuotate dei dati o delle componenti critiche prima di consentirne l'uscita. Nel caso di hard djsk o supporti elettronici contenenti dati, questi sono cancellati e i supporto riformattato più volte.

VALUTAZIONE DEI RISCHI E CONCLUSIONI

Il **Titolare** protegge in modo adeguato i dati dal rischio di violazione della riservatezza, dell'integrità e della disponibilità. In particolare, i sistemi adottati per quanto riguarda le copie di sicurezza e i metodi di ripristino proteggono adeguatamente dal rischio di perdita dei dati. Considerata la tipologia dei dati trattati e i trattamenti effettuati, utilizzando come criterio di misura una scala da 1 a 10, si ritiene che:

- il livello di interesse da parte di un soggetto terzo a conoscere i dati del **Titolare** al fine di trarne indebito vantaggio, sia pari a 3
- il livello di interesse da parte di un qualsiasi soggetto ad alterare i dati al fine di danneggiare il **Titolare** sia pari a 3;
- il livello di interesse da parte di un qualsiasi soggetto a distruggere questi dati al fine di danneggiare il **Titolare** sia pari a 5.

Incrociando questa valutazione con una analoga valutazione sulla facilità (10 = massima facilità) con la quale è possibile accedere ai dati per conoscerli, alterarli, distruggerli (valutata sempre 2) si ottiene la seguente matrice delle probabilità



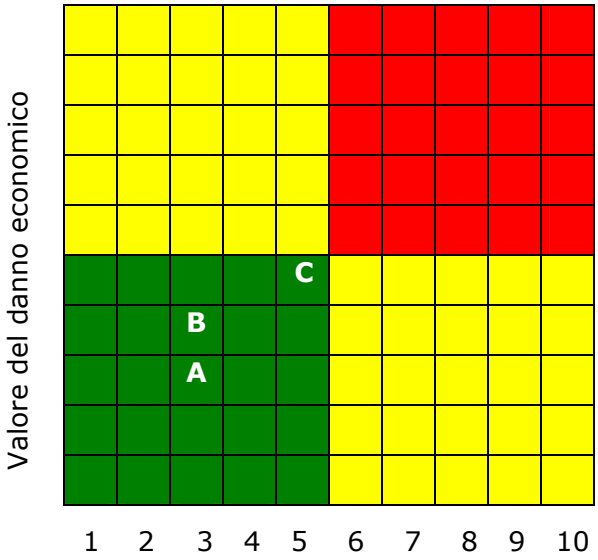
In considerazione di quanto esposto ne deriva che:

1) la probabilità di accesso non autorizzato (violazione della riservatezza) è intorno al 3%;
2) la probabilità di trattamenti non consentiti (violazione dell'integrità) è intorno al 3%;
3) la probabilità di distruzione e/o perdita dei dati (perdita della disponibilità) è intorno al 5%.

Infine, incrociando i valori di rischio in precedenza definiti con la valutazione della dimensione del danno economico conseguente la violazione della riservatezza, o dell'integrità, nonché la perdita della disponibilità (valutazione espressa sempre con un valore compreso un una scala da 1 a 10, dove 10 esprime il massimo danno), si ottiene la seguente matrice che rappresenta la mappa dei valori di rischio:

A - riservatezza
B - integrità
C - disponibilità

Area di basso rischio
Area di medio rischio
Area di alto rischio



DICHIARAZIONI D'IMPEGNO E FIRMA

Il presente documento, redatto nel mese di marzo 2009, è costituito da 53 pagine, compreso l'indice, e viene firmato in calce da **Marco Balagna**, Sindaco in carica.

L'originale del presente documento viene custodito presso la sede del **Titolare**, per essere esibito in caso di controlli.
Una sua copia verrà consegnata a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

Pont Canavese, 23 marzo 2009

Il Sindaco

……

INDICE