COMUNE DI TRIUGGIO

Allegato n. 5

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Titolare del trattamento : Comune di Triuggio

Codice	Revisione	Data
Mod DPPS	4	28/11/2008

IL SINDACO
(Dr.Paolo Manzoni)

1. SCOPO DEL DOCUMENTO

Il presente Documento Programmatico sulla Sicurezza è adottato ai sensi dell'art. 34 del D.P.R. n° 196 del 30 giugno 2003 e Allegato B (Disciplinare Tecnico in materia di misure minime di sicurezza), per delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali.

2. CAMPO DI APPLICAZIONE

Il Documento Programmatico sulla Sicurezza adottato dall'Ente, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.
Il Documento Programmatico sulla Sicurezza riguarda tutti i dati personali:

- Personali
- Sensibili
- Giudiziari

Il Documento Programmatico sulla Sicurezza si applica al trattamento dei dati personali per mezzo di

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei)

Il Documento Programmatico sulla Sicurezza deve essere conosciuto ed applicato da tutti gli uffici dell'Ente, ad esclusione del sistema informatico della Biblioteca Comunale, nell'ambito delle attività di "Brianzabiblioteche" per le quali si fa riferimento al documento Programmatico per la Sicurezza dei dati adottato da "BrianzaBiblioteche".

3. RIFERIMENTI NORMATIVI

- Decreto Legislativo 29 dicembre 1992 n. 518 - tutela del diritto di autore sul software
- Legge 23 dicembre 1993 n. 547 - reati legati all'informatica - modifiche al Codice penale
- Direttiva UE 95/46/CE del 24 ottobre 1995 - tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- D.P.R. n. 196 del 30 giugno 2003 e suo Disciplinare Tecnico (Allegato B) - codice in materia di protezione dei dati personali

4. REVISIONE DEL DOCUMENTO

Il presente Documento Programmatico sulla Sicurezza (DPSS) , redatto nel mese di novembre anno 2008, verrà revisionato con frequenza almeno annuale, entro il 31 marzo di ogni anno, ed ogni qualvolta se ne evidenzi la necessità.

.

5. ELENCO DEI TRATTAMENTI PREVISTI SUI DATI PERSONALI

(punto 19.1 dell'Allegato B Disciplinare Tecnico in materia di misure minime di sicurezza)

In questa sezione è inserito l'elenco dei trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati trattati e della struttura (Settore, ufficio) interna od esterna che operativamente effettua il trattamento. Di seguito si descrivono le informazioni contenute nell'elenco. Si ritiene opportuno raccogliere le informazioni in tabelle.

Informazioni riportate

Per ciascun trattamento sono indicate le seguenti informazioni **(*=essenziali, **=ulteriori)**

Identificativo del trattamento(**): consiste in un codice che consente un'identificazione univoca e più rapida di ciascun trattamento, utile come riferimento nella compilazione delle altre tabelle

Descrizione sintetica(*): menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (fornitura di beni o servizi, gestione del personale, ecc.)e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori,fornitori, ecc.).

Natura dei dati trattati(*): tipologia dei dati trattati (personali, sensibili, giudiziari)

Banca dati(**): il nome o l'identificativo dell'eventuale banca dati (ovvero del database o dell'archivio informatico) in cui sono contenuti i dati che sono trattati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso elencare le banche.

Struttura di riferimento(*): indica la struttura (o reparto, funzione, ufficio, ecc.) all'interno della quale viene realizzato il trattamento. Sarà indicato sia un identificativo che la descrizione.

Descrizione degli strumenti elettronici utilizzati(*): va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi). (nota: indicare gli strumenti utilizzati per la gestione della banca dati (Database su Server di rete, vari tipi di file su PC in locale, ecc.)

Altre strutture che concorrono al trattamento(*): nel caso in cui un trattamento, per essere completato, comporti l'attività di diverse strutture è opportuno indicare oltre a quella che primariamente detiene la responsabilità dell'attività, anche quelle che concorrono, siano esse interne od esterne all'organizzazione comunale.

Luogo di custodia dei supporti di memorizzazione(**): contiene l'indicazione del luogo in cui risiedono fisicamente i dati, cioè dove si trova (in quale sede, centrale o periferica, presso quale fornitore di servizi, etc.) l'elaboratore sui cui i dati sono memorizzati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD-ROM, ecc.)

Tipologia di dispositivi di accesso(**): elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: personal computer, terminale non intelligente, palmare, telefonino, ecc.

Tipologia di interconnessione(**): descrizione sintetica e qualitativa della rete informatica che collega i dispositivi d'accesso utilizzati dagli incaricati ai dati se utilizzati: rete locale, extranet, Internet, ecc.

Incaricati (qui solo per semplicità di consultazione): elenco degli incaricati al trattamento per la banca dati

Responsabili (qui solo per semplicità di consultazione: elenco dei responsabili per la banca dati

Tabella 1 - Elenco dei trattamenti dei dati: informazioni di base

Identificativo del trattamento (**)	Descrizione Sintetica (*)	Natura dei dati trattati (*)	Banca dati (**)
DB_0001	Elettorale - elenco cittadini con diritto di voto	Giudiziari Sensibili	Elettorale WINSIC 2000
DB_0002	Incarichi elettorali Elenco scrutatori e presidenti di seggio	Giudiziari Sensibili	Elettorale (Applicativo WINSIC 2000)
DB_0003	Giudici popolari Elenco cittadini idonei alla carica di giudici popolari	Giudiziari Sensibili	Elettorale (Applicativo WINSIC 2000)
DB_0004	Liste di leva – Elenco cittadini iscritti alla leva militare e dei registri matricolari	Personali Giudiziari Sensibili	Leva (Applicativo WINSIC 2000)
DB_0005	Anagrafe - schede dell'anagrafe della popolazione residente	Personali Sensibili	Anagrafe (Applicativo WINSIC 2000)
DB_0006	AIRE schede dell'anagrafe della popolazione residente all'estero	Personali	Anagrafe (Applicativo WINSIC 2000)+Anagaire
DB_0007	Stato civile – Registri e atti nascita, matrimonio, morte	Personali Sensibili Giudiziari	Stato civile (Applicativo WINSIC 2000)
DB_0008	Anagrafe degli Amministratori Locali-	Giudiziari Sensibili	Delibere (Applicativo WINSIC 2000)
DB_0009	Cartellini carte d'identità	Personali	Cartellini carte identità (dati cartacei)

Identificativo del trattamento (**)	Descrizione Sintetica (*)	Natura dei dati trattati (*)	Banca dati (**)
DB_0010	Schede ISTAT (morte)	Personali Sensibili	Schede Istat di morte (dati cartacei)
DB_0011	Registro e Deposito atti giudiziari	Giudiziari Sensibili Personali	Atti giudiziari (dati cartacei)
DB_0012	Notificazione messi comunali - registro	Personali Giudiziari	Gestione Messi NT
DB_0013	Repertorio contratti	Personali Giudiziari	Contratti (Applicativo WINSIC 2000) Registro di repertorio
DB_0014	Atti notarili	Personali	Servernt file office
DB_0015	Verbali deliberazione giunta comunale e consiglio	Personali	Delibere (Applicativo WINSIC 2000)
DB_0016	Ordinanze	Giudiziari Sensibili	Delibere (Applicativo WINSIC 2000)
DB_0017	Determinazioni	Personali Giudiziari Sensibili	Delibere (Applicativo WINSIC 2000)
DB_0018	Protocollo	Personali Sensibili Giudiziari	ProNet (Applicativo WebSic 2000) Registro d'emergenza cartaceo
DB_0019	Fascicoli cause e vertenze	Personali Giudiziari sensibili	Cause e vertenze (dati cartacei)
DB_0020	Personale Banca dati rilevazione presenze,	Personali Sensibili Giudiziario	Riprese (Applicativo WINSIC 2000)
DB_0021	Compensi Personale-Amministratori	Personali Sensibili	Stipendi (Applicativo WINSIC 2000)
DB_0022	Fascicoli personale-	Personali Giudiziari Sensibili	Fascicoli Personale+Servernt File Office
DB_0023	Concorsi Pubblici - documentazione	Personali	Fascicoli concorsi pubblici Servernt File Office
DB_0024	Elenco Fornitori	Personali	Contabilità (Applicativo WINSIC 2000)
DB_0025	Tributi comunali (Ici-Tosap_ Tarsu)	Personali	Tributi (applicativo winSic200)+ Servernt (file Office)
DB_0026	Anagrafica Creditori	Personali	Contabilità(Applicativo WINSIC 2000)

Identificativo del trattamento (**)	Descrizione Sintetica (*)	Natura dei dati trattati (*)	Banca dati (**)
DB_0027	Dati catastali	Personali	Catasto 2000
DB_0028	Archivio utenti servizi tutela Minori	Personali Giudiziari Sensibili	Area minori
DB_0029	Relazioni PsicoSociali	Personali Sensibili Giudiziari	Servernt file office
DB_0030	Archivio utenti SAD- Sil e area handicap	Personali Sensibili Giudiziari	Servernt file office
DB_0031	Archivio ISEE	Personali sensibili	Servernt file office + Isee Inps
DB_0032	Dati relativi Tso	Personali Sensibili Giudiziari	Servernt file office
DB_0033	Archivio utenti beneficiari contributi comunali	Personali Sensibili	Servernt file office
DB_0034	Archivio assegnatari alloggi ERP	Personali Sensibili Giudiziario	Servernt file office
DB_0035	Cerimoniale nominativo associazioni. autorità locali, provinciali e regionali	Personali	Servernt file office
DB_0036	Assegnatari alloggi ERP	Personali Sensibili	Servernt file office
DB_0037	Beneficiari sportello affitti	Personali Sensibili	Servernt file office+ fsa regione
DB_0038	Graduatorie assegnazione alloggi ERP	Personali Sensibili	ERP Servernt (file office) + fsa-regione
DB_0039	Albo associazione volontariato	Personali Sensibili	Albo Volontariato Servernt(file office)
DB_0040	Banche dati pratiche concessione patrocinio/contributi – associazioni culturali, e di volontariato	Personali Sensibili	Servernt(file office)
DB_0041	Utenti iscritti servizi scolastici(mensa, trasporto, materne, corsi nuoto –pre-scuolaecc)	Personali Sensibili	Servernt file office+ bollette (applicativo WINSIC 2000)

Identificativo del trattamento (**)	Descrizione Sintetica (*)	Natura dei dati trattati (*)	Banca dati (**)
DB_0042	Elenchi assegnatari locali comunali (centri civici, palestre ecc)	Personali Sensibili Giudiziari	Servernt file office
DB_0043	Beneficiari contributi libro di testo	Personali	Servernet file office
DB_0044	Cimiteri (contratti, permessi seppellimento ecc)	Personali Sensibili	CRUX
DB_0045	Assegnatari orti comunali	Personali	Servernt file office
DB_0046	Pratiche edilizie	Personali	Pratiche edilizie (Applicativo WINSIC 2000)
DB_0047	Archivio frazionamenti	Personali	Archivio frazionamenti (cartaceo)
DB_0048	Banca dati lavori pubblici (gare, ditte ecc)	Personali Giudiziari	Servernt file office
DB_0049	Banca dati sportello unico attività produttive	Personali Sensibili Giudiziari	Spunico
DB_0050	Banca dati contestazione violazione codice della strada	Personali	Vigili (Applicativo WINSIC 2000)
DB_0051	Banca Dati incidenti stradali	Personali Sensibili Giudiziari	Aramix Web (provincia di Milano)
DB_0052	Banca dati cessione fabbricati	Personali	Cessione dei fabbricati (sw questura Milano)
DB_0053	Banca dati denunce infortunio	Personali Sensibili Giudiziari	Procedura vigili (Applicativo Winsic 2000)
DB_0054	Banca dati contrassegno invalidi	Personali Sensibili	Servernt File Office
DB_0055	Banca dati titolari autorizzazione commercio fisso	Personali	Servernt file office
DB_0056	Banca dati titolari pubblici esercizi	Personali Sensibili	Servernt file office
DB_0057	Banca dati commercio su aree pubbliche	Personali Sensibili	Servernt file office
DB_0058	Banca dati sanzioni amministrativa	Personali Sensibili	Servernt file office
DB_0059	Beneficiari contributi barriere architettoniche	Personali Sensibili	Servernt file office
DB_0060	Scritture private	Personali Sensibili Giudiziali	Servernt file office + registro di repertorio (cartaceo)

Identificativo del trattamento (**)	Descrizione Sintetica (*)	Natura dei dati trattati (*)	Banca dati (**)
DB_0061	Decreti del Sindaco	Personali Sensibili	Delibere (Applicativo Winsic 2000)+ Servernt file office
DB_0062	Elenco iscritti newsletter	Personali	Servernt file office
DB_0063	Pratiche richiesta contributo maternità e nucleo	Personali	Servent File Office
DB_0064	Pratiche Borse di studio	Personali	Servernt file Office
DB_0065	Dipendenti iscrizione sindacati	Personali Sensibili	Stipendi (applicativo WinSic 2000)
DB_0066	Albo beneficiari	Personali	Servernt file Office
DB_0067	Immagini registrate dal sistema di videosorveglianza	Personali	Server di registrazione
DB_0068	Piani attuativi - certificati urbanistici	Personali	Pratiche edilizie + servernt file office
DB_0069	Elenco utenti iscritti al servizio internet della biblioteca	Personali	File office pc biblioteca
DB_0070	Elenco utenti registrati al Portale del Cittadino	Personali	Database Server Pronet

Data di aggiornamento 28/11/2008

Tabella 2 - Elenco dei trattamenti dei dati: strutture di riferimento

Identificativo del trattamento	Struttura di riferimento (*)	Altre strutture che concorrono al trattamento (*)	Incaricati	Responsabili
DB_0001	Settore Amministrativo e della comunicazione		Sironi Maria Regina Bardone Elisabetta Bezzetto Miranda Vitali Daniela Colombo Rosaria Santambrogio M. Isabella Donghi Sonia La Mendola Giuseppe D'Angelo Elvira Villa Gianluca Tresca Nicola Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Castoldi Gianni Turconi Cristina Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	Rizzi Emanuela
DB_0002	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Donghi Sonia	Rizzi Emanuela
DB_0003	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Donghi Sonia	Rizzi Emanuela
DB_0004	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Donghi Sonia	Rizzi Emanuela
DB_0005	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Donghi Sonia La Mendola Giuseppe Villa Gianluca D'angelo Elvira Tresca Nicola	Rizzi Emanuela

			Doni Giuseppina Riva M.Grazia Bardone Elisabetta Santambrogio Fernanda Castoldi Gianni Turconi Cristina Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	
DB_0006	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Donghi Sonia	Rizzi Emanuela
DB_0007	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Donghi Sonia	Rizzi Emanuela
DB_0008	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Donghi Sonia Vitali Daniela Bezzetto Miranda Colombo Rosaria Castoldi Gianni Santambrogio M. Isabella La Mendola Giuseppe Villa Gianluca Tresca Nicola D'angelo Elvira Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Bardone Elisabetta Turconi Cristina Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	Rizzi Emanuela
DB_0009	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Donghi Sonia La Mendola Giuseppe Santambrogio M.	Rizzi Emanuela

			Isabella Tresca Nicola D'Angelo Elvira Villa Gianluca	
DB_0010	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria	Rizzi Emanuela
DB_0011	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Bezzetto Miranda Colombo Rosaria Vitali Daniela Santambrogio M. Isabella	Rizzi Emanuela
DB_0012	Settore Amministrativo e della Comunicazione		Santambrogio M. Isabella Bezzetto Miranda Colombo Rosaria Donghi Sonia La Mendola Giuseppe Tresca Nicola D'Angelo Elvira Villa Gianluca	Rizzi Emanuela
DB_0013	Settore Amministrativo e della Comunicazione		Bezzetto Miranda Colombo Rosaria Donghi Sonia	Rizzi Emanuela
DB_0014	Settore Amministrativo e della Comunicazione	Settore gestione del territorio	Bezzetto Miranda Colombo Rosaria Erba Ambrogio Pesce Laura De Melgazzi Flavia Cambiaghi Irma	Rizzi Emanuela
DB_0015	Settore Amministrativo e della Comunicazione	Settore Socio - educativo Settore Finanziario Settore Gestione del Territorio Settore Polizia Locale	Sironi Maria Regina Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Donghi Sonia Castoldi Gianni Vitali Daniela La Mendola Giuseppe D'Angelo Elvira Villa Gianluca Tresca Nicola Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Turconi Cristina Bardone Elisabetta Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	Rizzi Emanuela

DB_0016	Settore Amministrativo e della Comunicazione	Settore Socio-culturale Settore Finanziario Settore Gestione del Territorio Settore Polizia Locale	Sironi Maria Regina Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Donghi Sonia Castoldi Gianni La Mendola Giuseppe D'Angelo Elvira Villa Gianluca Tresca Nicola Vitali Daniela Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Turconi Cristina Bardone Elisabetta Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	Rizzi Emanuela
DB_0017	Settore Amministrativo e della Comunicazione	Settore Socio - educativo Settore Finanziario Settore Gestione del Territorio Settore Polizia Locale	Sironi Maria Regina Bardone Elisabetta Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Donghi Sonia Castoldi Gianni Vitali Daniela La Mendola Giuseppe D'Angelo Elvira Villa Gianluca Tresca Nicola Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Turconi Cristina Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	Rizzi Emanuela

DB_0018	Settore Amministrativo e della Comunicazione	Settore Socio - educativo Settore Finanziario Settore Gestione del Territorio Settore Polizia Locale	Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Donghi Sonia Castoldi Gianni La Mendola Giuseppe D'Angelo Elvira Villa Gianluca Tresca Nicola Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Bardone Elisabetta Turconi Cristina Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	Rizzi Emanuela
DB_0019	Settore Amministrativo e della comunicazione		Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Erba Ambrogio Vernaleone Paola La Mendola Giuseppe Doni Giuseppina	Rizzi Emanuela
DB_0020	Settore Amministrativo e della comunicazione		Bezzetto Miranda Donghi Sonia	Rizzi Emanuela
DB_0021	Settore Amministrativo e della comunicazione	Settore finanziario	Bezzetto Miranda Donghi Sonia Vernaleone Paola Di Girolamo Susanna Montrasio Corinna Colombo Rosaria	Rizzi Emanuela
DB_0022	Settore Amministrativo e della comunicazione		Bezzetto Miranda Colombo Rosaria Vernaleone Paola Di Girolamo Susanna Montrasio Corinna Erba Ambrogio Doni Giuseppina La Mendola Giuseppe	Rizzi Emanuela
DB_0023	Settore Amministrativo e della comunicazione		Bezzetto Miranda Colombo Rosaria Erba Ambrogio Doni Giuseppina	Rizzi Emanuela

			La Mendola Giuseppe Vernaleone Paola	
DB_0024	Settore Finanziario		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Donghi Sonia Castoldi Gianni La Mendola Giuseppe D'Angelo Elvira Villa Gianluca Tresca Nicola Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Turconi Cristina Bardone Elisabetta Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	Vernaleone Paola
DB_0025	Settore Finanziario		Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Donghi Sonia	Vernaleone Paola
DB_0026	Settore Finanziario		Sironi Maria Regina Vitali Daniela Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Donghi Sonia Castoldi Gianni La Mendola Giuseppe D'Angelo Elvira Villa Gianluca Tresca Nicola Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Turconi Cristina Bardone Elisabetta Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura	Vernaleone Paola

			De Melgazzi Flavia Villa Stefano	
DB_0027	Settore Finanziario		Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Donghi Sonia	Vernaleone Paola
DB_0028	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Colombo Lidia Fumagalli Liliana Diano Angelina Bardone Elisabetta	Doni Giuseppina
DB_0029	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Bardone Elisabetta	Doni Giuseppina
DB_0030	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Colombo Lidia Fumagalli Liliana Diano Angelina Bardone Elisabetta	Doni Giuseppina
DB_0031	Settore Socio-Educativo	Settore Amministrativo e della comunicazione	Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Bardone Elisabetta	Doni Giuseppina
DB_0032	Polizia Locale	Settore Socio-Educativo	Riva M.Grazia Santambrogio Fernanda Turconi Cristina Doni Giuseppina Tresca Nicola Villa Gianluca Casati Ettore	La Mendola Giuseppe
DB_0033	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Bardone Elisabetta	Doni Giuseppina

DB_0034	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Bardone Elisabetta	Doni Giuseppina
DB_0035	Settore Amministrativo e della comunicazione	Settore Socio-Educativo	Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Doni Giuseppina Bezzetto Miranda Colombo Rosaria Bardone Elisabetta	Rizzi Emanuela
DB_0036	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia	Doni Giuseppina
DB_0037	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Bardone Elisabetta	Doni Giuseppina
DB_0038	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Bardone Elisabetta	Doni Giuseppina
DB_0039	Settore Socio-Educativo	Settore Amministrativo e della comunicazione	Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Rizzi Emanuela Bezzetto Miranda Castoldi Gianni Bardone Elisabetta	Doni Giuseppina
DB_0040	Settore Socio-Educativo	Settore Amministrativo e della comunicazione	Riva M.Grazia Santambrogio Fernanda Turconi Cristina Castoldi Gianni Donghi Sonia Bezzetto Miranda Rizzi Emanuela Bardone Elisabetta	Doni Giuseppina

DB_0041	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Lissoni Marinella Saini Tiziana Bardone Elisabetta	Doni Giuseppina
DB_0042	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Castoldi Gianni Pesce Laura De Melgazzi Flavia Villa Stefano Erba Ambrogio Donghi Sonia Rizzi Emanuela Bardone Elisabetta	Doni Giuseppina
DB_0043	Settore Socio-Educativo		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Castoldi Gianni Donghi Sonia Bardone Elisabetta	Doni Giuseppina
DB_0044	Settore Gestione del Territorio		Pesce Laura De Melgazzi Flavia Villa Stefano Cambiaghi Irma Cazzaniga Stefano Tieghi Elio Donghi Sonia	Erba Ambrogio
DB_0045	Settore socio-culturale		Riva M.Grazia Santambrogio Fernanda Turconi Cristina Bardone Elisabetta Donghi Sonia	Doni Giuseppina
DB_0046	Settore Gestione del Territorio		Pesce Laura De Melgazzi Flavia Villa Stefano Cambiaghi Irma Cazzaniga Stefano Tieghi Elio Donghi Sonia	Erba Ambrogio
DB_0047	Settore Gestione del Territorio		Pesce Laura De Melgazzi Flavia Villa Stefano Cambiaghi Irma Cazzaniga Stefano Tieghi Elio	Erba Ambrogio

DB_0048	Settore Gestione del Territorio		Pesce Laura De Melgazzi Flavia Villa Stefano Cambiaghi Irma Cazzaniga Stefano Tieghi Elio	Erba Ambrogio
DB_0049	Settore Gestione del Territorio		Pesce Laura De Melgazzi Flavia Villa Stefano Cambiaghi Irma Cazzaniga Stefano Tieghi Elio Donghi Sonia La Mendola Giuseppe	Erba Ambrogio
DB_0050	Settore Polizia Locale		D'Angelo Elvira Villa Gianluca Tresca Nicola Donghi Sonia	La Mendola Giuseppe
DB_0051	Settore Polizia Locale		D'Angelo Elvira Villa Gianluca Tresca Nicola	La Mendola Giuseppe
DB_0052	Settore Polizia Locale		D'Angelo Elvira Villa Gianluca Tresca Nicola	La Mendola Giuseppe
DB_0053	Settore Polizia Locale		D'Angelo Elvira Villa Gianluca Tresca Nicola	La Mendola Giuseppe
DB_0054	Settore Polizia Locale		D'Angelo Elvira Villa Gianluca Tresca Nicola	La Mendola Giuseppe
DB_0055	Settore Polizia Locale		D?angelo Elvira Villa Gianluca Tresca Nicola	La Mendola Giuseppe
DB_0056	Settore Polizia Locale		D'angelo Elvira Villa Gianluca Tresca Nicola	La Mendola Giuseppe
DB_0057	Settore Polizia Locale		D'Angelo Elvira Villa Gianluca Tresca Nicola	La Mendola Giuseppe

DB_0058	Settore Polizia Locale		D'Angelo Elvira Villa Gianluca Tresca Nicola	La Mendola Giuseppe
DB_0059	Settore Socio - Educativo	Settore Gestione del Territorio	Pesce Laura De Melgazzi Flavia Villa Stefano Cambiaghi Irma Cazzaniga Stefano Tieghi Elio Erba Ambrogio Riva M.Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Bardone Elisabetta	Doni Giuseppina
DB_0060	Settore Amministrativo e della Comunicazione		Bezzetto Miranda Colombo Rosaria Donghi Sonia	Rizzi Emanuela
DB_0061	Settore Amministrativo e della Comunicazione		Sironi Maria Regina Bardone Elisabetta Vitali Daniela Bezzetto Miranda Colombo Rosaria Santambrogio M. Isabella Donghi Sonia La Mendola Giuseppe D'Angelo Elvira Villa Gianluca Tresca Nicola Doni Giuseppina Riva M.Grazia Santambrogio Fernanda Castoldi Gianni Turconi Cristina Di Girolamo Susanna Montrasio Corinna Villa Alessandro Vernaleone Paola Erba Ambrogio Cambiaghi Irma Tieghi Elio Cazzaniga Stefano Pesce Laura De Melgazzi Flavia Villa Stefano	Rizzi Emanuela
DB_0062	Settore Amministrativo e della Comunicazione		Donghi Sonia	Rizzi Emanuela

DB_0063	Settore Socio Educativo	Settore Amministrativo e della Comunicazione	Riva M.Grazia Santambrogio Fernanda Bardone Elisabetta Turconi Cristina Donghi Sonia	Doni Giuseppina
DB_0064	Settore Socio Educativo		Riva M- Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia	Doni Giuseppina
DB_0065	Settore Economico Finanziario		Di Girolamo Susanna Montrasio Corinna Villa Alessandro	Vernaleone Paola
DB_0066	Settore Economico Finanziario	Settore Socio Educativo	Di Girolamo Susanna Montrasio Corinna Villa Alessandro Riva M- Grazia Santambrogio Fernanda Turconi Cristina Donghi Sonia Bardone Elisabetta	Vernaleone Paola
DB_0067	Settore Polizia Locale		Tresca Nicola Villa Gianluca D'angelo Elvira Donghi Sonia	La Mendola Giuseppe
DB_0068	Settore Gestione del Territorio Gestione		Tiegi Elio Cazzaniga Stefano Cambiaghi Irma Villa Stefano Pesce Laura De Melgazzi Flavia	Erba Ambrogio
DB_0069	Settore Amministrativo e della Comunicazione		Castaldi Gianni Donghi Sonia	Rizzi Emanuela
DB_0070	Settore Amministrativo e della Comunicazione		Donghi Sonia	Rizzi Emanuela

Data di aggiornamento: 28/11/2008

Tabella 3 - Elenco dei trattamenti dei dati: strumenti utilizzati e ubicazione fisica dei supporti di memorizzazione

Identificativo del trattamento	**Descrizione degli strumenti utilizzati (*)**	**Tipologia di dispositivi di accesso** (**)	**Tipologia di interconnessione** (**)	**Luogo di custodia dei supporti di memorizzazione** (**)
DB_0001	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio servizi demografici
DB_0002	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio servizi demografici
DB_0003	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio servizi demografici
DB_0004	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio servizi demografici
DB_0005	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio servizi demografici
DB_0006	Database Server	Personal Computer	LAN+DB ministero	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio servizi demografici
DB_0007	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio servizi demografici

Identificativo del trattamento	Descrizione degli strumenti utilizzati (*)	Tipologia di dispositivi di accesso (**)	Tipologia di interconnessione (**)	Luogo di custodia dei supporti di memorizzazione (**)
DB_0008	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio segreteria
DB_0009	Archivio cartaceo			Armadio chiuso c/o Ufficio Servizi Demografici
DB_0010	Archivio cartaceo			Armadio chiuso c/o Ufficio Servizi Demografici
DB_0011	Archivio cartaceo			Armadio chiuso c/o Ufficio Segreteria
DB_0012	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Segreteria
DB_0013	Database Server+ File office	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Segreteria
DB_0014	Archivio cartaceo			Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Segreteria
DB_0015	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Uffici comunali
DB_0016	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Uffici comunali
DB_0017	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Uffici comunali
DB_0018	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio

				Segreteria
Identificativo del trattamento	**Descrizione degli strumenti utilizzati (*)**	**Tipologia di dispositivi di accesso** (**)	**Tipologia di interconnessione** (**)	**Luogo di custodia dei supporti di memorizzazione** (**)
DB_0019	Archivio cartaceo			Armadio Chiuso c/o Ufficio Segreteria
DB_0020	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Segreteria
DB_0021	Database Server+ file office	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Ragioneria
DB_0022	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Segreteria
DB_0023	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Segreteria
DB_0024	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Uffici Comunali
DB_0025	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Tributi
DB_0026	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Uffici Comunali
DB_0027	Database locale	Personal Computer	LAN	Pc Ufficio Tributi
DB_0028	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali

Identificativo del trattamento	Descrizione degli strumenti utilizzati (*)	Tipologia di dispositivi di accesso (**)	Tipologia di interconnessione (**)	Luogo di custodia dei supporti di memorizzazione (**)
DB_0029	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0030	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0031	File Office server	Personal Computer	LAN+ internet DB INPS	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0032	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0033	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0034	File Office server	Personal Computer	LAN+DB Regione Lombardia	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0035	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Uffici comunali
DB_0036	File Office server	Personal Computer	LAN+ internet Db ERP Regione Lombardia	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali

Identificativo del trattamento	Descrizione degli strumenti utilizzati (*)	Tipologia di dispositivi di accesso (**)	Tipologia di interconnessione (**)	Luogo di custodia dei supporti di memorizzazione (**)
DB_0037	File Office server	Personal Computer	LAN+intenet fsa Regione Lombardia	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0038	File Office server	Personal Computer	LAN+ internet DB ERP Regione Lombardia	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0039	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0040	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Uffici Comunali
DB_0041	Database Server+File Office server	Personal Computer	LAN +Db Sodexo	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Pubblica Istruzione .
DB_0042	File Office server	Personal Computer	LAN+	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Uffici Comunali
DB_0043	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Pubblica Istruzione
DB_0044	Dababase Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Tecnico e Segreteria
DB_0045	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali

Identificativo del trattamento	Descrizione degli strumenti utilizzati (*)	Tipologia di dispositivi di accesso (**)	Tipologia di interconnessione (**)	Luogo di custodia dei supporti di memorizzazione (**)
DB_0046	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Tecnico
DB_0047	Archivio Cartaceo	Personal Computer	Archivio cartaceo	Armadio chiuso c/o Ufficio Tecnico
DB_0048	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Tecnico
DB_0049	Dababase Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Tecnico
DB_0050	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0051	Dababase locale	Personal Computer	db provincia Milano	Pc Ufficio polizia locale Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0052	Database server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0053	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3

Identificativo del trattamento	Descrizione degli strumenti utilizzati (*)	Tipologia di dispositivi di accesso (**)	Tipologia di interconnessione (**)	Luogo di custodia dei supporti di memorizzazione (**)
DB_0054	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0055	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0056	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0057	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0058	File Office server e Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Tecnico c/o Ufficio e Polizia Locale sede di via 11 Settembre 2001, n.3
DB_0059	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi sociali
DB_0060	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Segreteria

Identificativo del trattamento	Descrizione degli strumenti utilizzati (*)	Tipologia di dispositivi di accesso (**)	Tipologia di interconnessione (**)	Luogo di custodia dei supporti di memorizzazione (**)
DB_0061	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Segreteria
DB_0062	File Office server	Personal Computer	LAN	Servernt(Locale CED
DB_0063	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Servizi Sociali
DB_0064	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Pubblica istruzione
DB_0065	Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Pubblica Ragioneria
DB_0066	File Office server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Pubblica Ragioneria
DB_0067		Personal Computer	Extranet	Pc Ufficio Polizia Locale Via 11 Settembre 2001, n.3
DB_0068	File Office server e Database Server	Personal Computer	LAN	Servernt(Locale CED) Fascicoli cartacei in armadi chiusi c/o Ufficio Tecnico

Identificativo del trattamento	Descrizione degli strumenti utilizzati (*)	Tipologia di dispositivi di accesso (**)	Tipologia di interconnessione (**)	Luogo di custodia dei supporti di memorizzazione (**)
DB_0069	File Office	Personal computer		PC Biblioteca Comunale Viale Indipendenza, 25 Fascicoli cartacei in armadi chiusi
DB_0070	Database Server	Personal computer	LAN	Server Pronet(Locale CED)

Data di aggiornamento:28/11/2008

6. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI

(punto 19.2 dell'Allegato B Disciplinare Tecnico in materia di misure minime di sicurezza)

In questa sezione è definita una mappa che associa ad ogni struttura (o reparto, dipartimento, ufficio) i trattamenti da questa effettuati, descrivendo sinteticamente l'organizzazione della struttura medesima e le relative responsabilità. Di seguito si descrivono le informazioni contenute nell'elenco. Si ritiene opportuno raccogliere le informazioni in tabelle.

Informazioni riportate

Per ciascuna struttura sono indicate le seguenti informazioni:
Struttura: contiene gli stessi identificativi utilizzati nella tabella 2 della sezione precedente (campo "Struttura di riferimento")

Responsabile della struttura: indica il ruolo del responsabile della struttura (non deve essere confuso il responsabile del trattamento ai sensi dell'art. 29 del Dlgs 196/2003)

Trattamenti operati dalla struttura: contiene, se necessario su più righe per ciascuna struttura, i trattamenti per i quali la struttura ha la primaria responsabilità

Compiti della struttura: contiene una descrizione sintetica dei compiti assegnati alla struttura in ciascuno dei trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)

Tabella 4 - Elenco delle strutture preposte ai trattamenti dei dati

Struttura	Responsabile della struttura	Trattamenti operati dalla struttura	Compiti della struttura
Settore Amministrativo e della Comunicazione	Rizzi Emanuela	Vedi Tabella 1	Servizio Affari generali e personale: Segreteria,Personale, Protocollo Contratti organizzazione , ecc. Servizio demografici Anagrafe, Elettorale, Leva Servizi informatici e della comunicazione Urp Servizi Informatici Biblioteca – cultura
Settore Economico Finanziario	Vernaleone Paola	Vedi tabella 1	Ragioneria Tributi Stipendi
Settore Gestione	Erba Ambrogio	Vedi tabella 1	Lavori pubblici Edilizia Privata

del Territorio			Ecologia
Struttura	Responsabile della struttura	Trattamenti operati dalla struttura	Compiti della struttura
Settore Socio-Educativo	Doni Giuseppina	Vedi tabella 1	Servizi Scolastici Trasporti, Mensa, ecc Servizi Sociali Area minori, sad , erp ecc Sport e Tempo Libero
Settore Polizia locale	La Mendola Giuseppe	Vedi tabella 1	Polizia Locale Commercio Videosorveglianza

Data di aggiornamento:28//11/2008

6.1 TITOLARE DEL TRATTAMENTO

Il Garante, ha identificato, nel caso della Pubblica Amministrazione, il titolare nello stesso Ente pubblico, come titolare del trattamento. Non è pertanto necessaria alcuna nomina per ciò che riguarda il titolare del trattamento, perché tale qualifica si desume dalla situazione di fatto.

6.2 RESPONSABILE DEL TRATTAMENTO

La legge prevede la possibilità di individuare, nell'ambito dell'organizzazione comunale, uno o più soggetti cui l'Ente (titolare del trattamento) delega le funzioni fondamentali ed i relativi poteri per la corretta attuazione degli obblighi di legge e per garantire l'effettuazione di trattamenti leciti e conformi ai principi della stessa legge. La nomina è tuttavia facoltativa: spetta al singolo Ente valutare l'opportunità di creare questa funzione.
Possono essere individuati anche più responsabili del trattamento, sia all'interno dell'Ente (ripartendo funzioni e poteri per aree), sia all'esterno (individuando quali responsabili anche società di servizi che svolgono particolari trattamenti per conto dell'Ente) .

La scelta del responsabile deve cadere su soggetti professionalmente idonei. In ogni caso sul titolare del trattamento permane un obbligo di vigilanza sull'operato del responsabile. La nomina deve essere deliberata dal soggetto titolare del relativo potere in base alle norme statutarie

Tabella 4.1 - Elenco dei responsabili dei trattamenti (suddivisi per strutture di riferimento)

Struttura	Responsabile trattamenti
Segretario Generale	Marchianò Vincenzo
Settore Amministrativo e della comunicazione	Rizzi Emanuela

Settore Economico Finanziario	Vernaleone Paola
Settore Gestione del Territorio	Erba Ambrogio
Settore Socio-Educativo	Doni Giuseppina
Settore Polizia Locale	La Mendola Giuseppe
Servizi Informatici e della comunicazione	Donghi Sonia

Data di aggiornamento 28/11/2008

6.3 INCARICATI

Il Codice sulla privacy (art. 30) impone all'Ente titolare del trattamento di designare gli "incaricati del trattamento" e di fornire a tutte queste persone incaricate del trattamento delle istruzioni scritte. La designazione e la definizione delle istruzioni viene compiuta dal titolare del trattamento o dal/i responsabile/i se nominato/i. Almeno una volta all'anno l'Ente deve verificare e, eventualmente, aggiornare l'elenco degli incaricati e dei relativi ambiti di trattamento consentiti (punti 14-15 e 27 del disciplinare tecnico). La finalità di queste istruzioni scritte è quella di individuare gli specifici trattamenti che l'incaricato può legittimamente effettuare conformemente alle proprie mansioni aziendali.
Pertanto, le istruzioni devono contenere l'individuazione delle banche dati cui l'incaricato può accedere, la definizione delle finalità per le quali si effettuano i trattamenti, l'eventuale ambito di comunicazione e/o diffusione all'esterno.
Inoltre, in forza degli specifici obblighi in materia di sicurezza imposti all'Ente dal Codice e dal disciplinare allegato al Codice, è necessario dettare anche prescrizioni puntuali sulle misure di sicurezza adottate a tutela dei dati: queste misure dovranno essere osservate da ogni singolo incaricato.
Dal punto di vista gestionale delle misure di sicurezza per i trattamenti informatici, le diverse mansioni (e di conseguenza le banche dati con le relative diverse finalità di trattamento) si concretizzano in un sistema di autenticazione all'accesso del sistema informatico che prevede diversi profili di autorizzazione (punti 12-13 e 14 del disciplinare tecnico).

(Nota: di seguito sono elencati gli incaricati del trattamento suddivisi per strutture di riferimento. Per ogni specifico trattamento si rimanda alla Tabella 2)

Tabella 4.2 - Elenco degli incaricati del trattamento (suddivisi per strutture di riferimento)

Struttura	Incaricati trattamento
Settore Amministrativo e della Comunicazione	Vitali Daniela Bezzetto Miranda Colombo Rosaria Donghi Sonia Santambrogio M. Isabella Sironi M.Regina Castaldi Gianni
Settore Economico finanziario	Di Girolamo Susanna Montrasio Corinna Villa Alessandro
Settore Gestione Territorio	Pesce Laura Costa Angelo Cambiaghi Irma Cazzaniga Stefano De Melgazzi Flavia Gioia Antonio Tieghi Elio Villa Stefano
Settore Socio-Educativo	Colombo Lidia Diano Angelina

	Fumagalli Liliana Turconi Cristina Lissoni Marinella Riva M.Grazia Saini Tiziana Santambrogio Fernanda Bardone Elisabetta
Polizia Locale	D'Angelo Elvira Villa Gianluca Tresca Nicola

Data di aggiornamento: 28/03/2008

6.4 CUSTODE DELLE CREDENZIALI DI AUTENTICAZIONE

Il disciplinare allegato al Codice (punto 10) ha confermato la necessità di introdurre nell'Ente la figura del "custode delle copie delle credenziali per l'autenticazione" nel caso di trattamenti informatici, figura già prevista ("custode delle parole chiave") dal precedente regolamento sulle misure di sicurezza (D.P.R. n. 318/99).
Questa figura svolge un ruolo fondamentale nella gestione delle misure minime di sicurezza di tipo informatico, assumendo dei precisi compiti operativi nella gestione, modifica e custodia delle password o parole chiave (che costituiscono la componente riservata delle credenziali per l'autenticazione) assegnate ai singoli incaricati del trattamento.
(Naturalmente tale figura può coincidere con un responsabile del trattamento)

Il custode delle password è stato individuato nella figura del responsabile dei servizi Informatici e della comunicazione Sig.ra Donghi Sonia

7. IDENTIFICAZIONE DELLE RISORSE DA PROTEGGERE

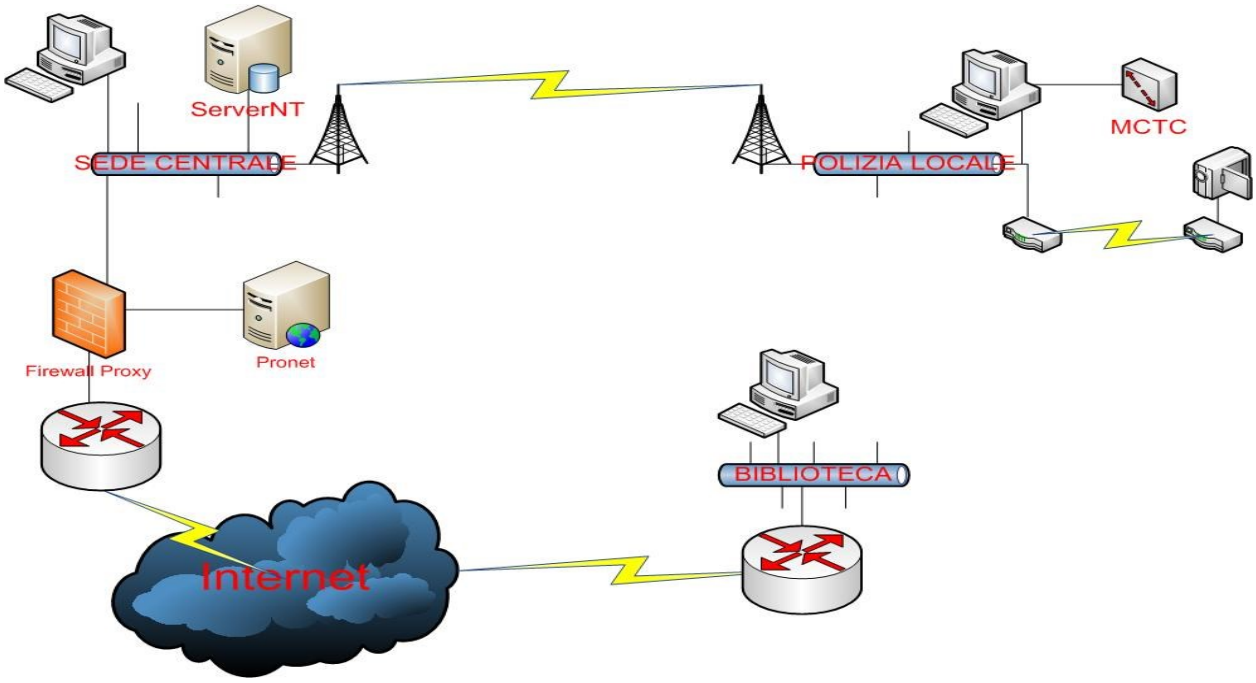
In questa sezione sono identificate e descritte tutte le risorse coinvolte nel sistema informatico dell'Ente oggetto dell'analisi dei rischi e che devono essere protette.

7.1 LUOGHI FISICI

Il Comune di Triuggio, consta delle seguenti sedi:

Sede Centrale del Comune in Via Vittorio Veneto n° 15 (Triuggio)
Sede della Polizia Locale in Via 11 Settembre n° 3 (Triuggio)
Sede della Biblioteca Civica in Viale Indipendenza n° 25 (Triuggio)

Le varie sedi constano di reti locali LAN Ethernet 10/100, collegate tramite differenti linee di comunicazione. Di seguito è riportato uno schema riassuntivo della rete locale dell'Ente:



I Server e il Firewall sono collocati nel LOCALE C.E.D. che si trova al piano primo dell'edificio di Via Vittorio Veneto n° 15. Il locale C.E.D. ospita gli apparati di rete. La sede della polizia locale possiede un armadi di permutazione chiusi a chiave e installato in un locale chiuso con porta blindata.
I 5 server di registrazione delle immagine delle videocamere sono collocati in armadi chiusi a chiavi nelle seguenti sedi:
- 1 Piazza della Chiesa Triuggio
- 2 Scuola Media Triuggio

- 3 Centro Civico via delle Grigne – Canonica
- 4 P-zza Don Baj – Tregasio
- 5 Via 11 Settembre 3 – sede Polizia locale

Mentre il Pc di collegamento è collocato presso la sede della Polizia Locale di Via 11 Settembre 36

Impianti di Sicurezza

L'intero stabile della sede centrale è protetto da un sistema di allarme anti-intrusione; il locale C.E.D. non possiede un proprio allarme anti-intrusione separato. Non esiste sistema antincendio; nel locale C.E.D. è stato installato nel 2006 un sistema di climatizzazione autonomo rispetto al resto dell'edificio al fine di garantire una temperatura costante. il locale C.E.D. è protetto da una porta blindata.

Nella sede della Polizia Locale esiste un allarme anti-intrusione per l'intero stabile L'armadio di rete e il server di registrazione della videosorveglianza è installato in un locale riservato e chiuso con porta blindata. Non esiste sistema antincendio.

Nella sede Biblioteca Comunale esiste un allarme anti-intrusione per l'intero stabile, non esiste sistema antincendio.

7.2 RISORSE HARDWARE

In questa sezione, saranno riportate le risorse hardware presenti nella sede costituente la rete informatica dell'Ente

(Sede Centrale)

N°2 Hub/Switch 10/100. collocati nell'armadio di permutazione
N° 1 HUb/Switch 10/100 collocato nel locale CED

N°1 Server **DC/DATI** (Primary Domain Controller del dominio Active Directory triuggio.local) Hewlett Packard Proliant ML350 con nome **SERVERNT** con la seguente configurazione HW:

Processore: 1 Intel Xeon 3 GHz
Memoria RAM : 1 GB espandibile a 8 GB
N° Dischi: 3 da 72 GB in configurazione RAID 5
Unità di backup : Quantum-Freecom SDLT 160/320 (160/320 GB)

N°1 Server **FIREWALL** (membro del nel dominio dominio Active Directory triuggio.local), Hewlett Packard LC3 con nome **PROXY** con la seguente configurazione HW:

Processore: 1 Intel Pentium III
Memoria RAM : 1 GB
N° Dischi: 3 da 9 GB in RAID-5
Unità di backup : Nessuna

(SEDE Centrale Zona DMZ)

N°1 Server **PROTOCOLLAZIONE** (Primary Domain Controller del dominio Active Directory dmztriuggio.local) Hewlett Packard Proliant ML350 con nome **PRONETSRV** con la seguente configurazione HW:

Processore: 1 Intel Xeon 3 GHz
Memoria RAM : 1 GB

N° Dischi: 3 da 72 GB in configurazione RAID 5
Unità di backup: DAT DDS4 (20/40 GB)

Per i 33 client di tutte le sedi, si riassumono di seguito le risorse hardware:

35 con la seguente configurazione HW
Processore: Celeron/Pentium IV/Pentiun Dual Core
Memoria RAM: 512 MB/1Gb

Sono inoltre presenti ulteriori risorse hardware:
N. 19 stampanti locali comprese le sedi periferiche (condivisioni non controllate)
N. 1 Plotter locale (condiviso in rete)
N.2 stampanti per etichette
N. 1 Scanner locale non condiviso in rete
N. 1 Router Internet HDSL collegato direttamente al Firewall per Rete Internet
N.1 Alvarion Breeze outdoor wireless point to point per il collegamento con gli uffici della polizia locale

(Sede Ufficio Polizia Locale)
N. 1 Switch
N. 1 Router ISDN utilizzato esclusivamente per collegamento alla Motorizzazione
N.1 Alvarion Breeze outdoor wireless point to point per il collegamento con la sede centrale

Videosorveglianza

5 server di registrazione(P.zza Chiesa Triuggio, P.zza Don Baj Tregasio, Scuola Media Triuggio, Centro civico via delle Grigne Canonica . sede polizia locale)
4 router ADSL x il collegamento con la sede dei vigili
n°1 Pc Processore Pentiun IV
n° 1 router ADSL per il collegamento al server di registrazione

(Sede Biblioteca Comunale)
N. 1 Switch
N. 2 Client
N. 1 Router ADSL per collegamento a Internet e al sistema bibliotecario esterno (il controllo di questa rete, del collegamento ad Internet e della banca dati è sotto la responsabilità del sistema bibliotecario esterno. La banca dati è situata presso il server centrale del sistema bibliotecario e vi si accede tramite sessioni Terminal Server.
N° 1 router Adsl per il collegamento a Internet del client destinato al servizio internet per gli utenti

7.3 RISORSE SOFTWARE

In questa sezione, saranno riportate le risorse software presenti nelle varie sedi fisiche costituenti la rete informatica dell'Ente.

(SEDE Centrale)

N°1 Server **DC/DATI** (Primary Domain Controller del dominio Active Directory triuggio.local) Hewlett Packard Proliant ML350 con nome **SERVERNT** con la seguente configurazione SW:

Sistema Operativo: Microsoft Windows 2003 Server Standard Edition

Servizi Attivi:

RDBMS Server: Microsoft SQL Server 2000
Controller Dominio Primario
File Server
WINS Server
DNS Primario Active Directory
DHCP Server
Backup Server (console Brightstore ARCServe Backup 11.1)
Server UPS (console gestione centrale UPS Winpower)
Antivirus console centralizzata Symantec Corporate Edition 10

N°1 Server **FIREWALL** (membro del nel dominio dominio Active Directory triuggio.local), Hewlett Packard LC3 con nome **PROXY** con la seguente configurazione SW:

Sistema Operativo: Microsoft Windows 2003 Server Standard Edition

Servizi Attivi:

Firewall implementato tramite Microsoft ISA Server 2004
Web Proxy implementato tramite Microsoft ISA Server 2004

(SEDE Centrale Zona DMZ)

N°1 Server **PROTOCOLLAZIONE** (Primary Domain Controller del dominio Active Directory dmztriuggio.local) Hewlett Packard Proliant ML350 con nome **PRONETSRV** con la seguente configurazione SW:

Sistema Operativo: Microsoft Windows 2003 Server Standard Edition

Servizi Attivi:

Web Server IIS 6.0
Web Server Pro.NET (protocollazione elettronica su IIS)
Applicativo Web Elettorale
Applicativo Portale servizi demografici

Per i 33 client di tutte le sedi, si riassumono di seguito le risorse software

33 con la seguente configurazione SW
Sistema Operativo: Microsoft Windows XP Professional
Office 2003
Applicativi gestionali

7.4 DATI

7.4.1 BANCHE DATI IN FORMATO ELETTRONICO

Tutte le banche dati sono in formato elettronico oppure misto. La maggior parte delle banche dati in formato elettronico prevede, comunque, il mantenimento di archivi cartacei le cui regole di custodia sono indicate nel paragrafo 7.4.3

7.4.2 COPIE DEGLI ARCHIVI ELETTRONICI (BACKUP)

(Vedi Tabella 3)

7.4.3 ARCHIVI CARTACEI

Archivi in formato esclusivamente in formato cartaceo

DB_0009
DB_0010
DB_0011
DB_0019
DB_0047

Per quanto riguarda la gestione degli archivi cartacei il comune ha adottato le seguenti regole:

- La documentazione corrente contenente dati personali, sensibili o giudiziari è conservata a cura del Responsabile del Settore in armadi e cassetti chiusi a chiave. Gli incaricati possono prelevare i documenti per il trattamento per il tempo necessario a tale operazione .Al termine del trattamento hanno il compito di riporli. E' inoltre compito dell'incaricato che preleva i documenti garantire che questi ultimi siano rinchiusi nel periodo di temporanea assenza dal posto di lavoro .
- la documentazione dell'archivio storico e di deposito è custodita in locali chiusi a chiave. Al predetto archivio può accedere il personale incaricato

7.4.3 COPIE DEGLI ARCHIVI ELETTRONICI (BACKUP)

(Vedi Tabella 7)

8. ANALISI DEI RISCHI

(punto 19.3 dell'Allegato B Disciplinare Tecnico in materia di misure minime di sicurezza)

Questa sezione rappresenta il nucleo fondamentale del documento, in quanto sulla base di questa valutazione l'Ente ha individuato le specifiche azioni da intraprendere. Sono individuati ed elencati i possibili rischi cui è esposto il sistema informatico dell'Ente

8.1 ELENCO RISCHI INDIVIDUATI

Per chiarezza le informazioni relative all'analisi dei rischi effettuata sono raccolte nella tabella successiva e contengono le seguenti informazioni essenziali:

Informazioni riportate

Elenco degli eventi: contiene l'elenco degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali

Impatto sulla sicurezza dei dati: contiene la descrizione delle principali conseguenze possibili per la sicurezza dei dati, legate al rischio individuato in relazione a ciascun evento e una valutazione della gravità delle stesse, anche in relazione alla probabilità stimata dell'evento. In questo modo consente di formulare un indicatore qualitativo di gravità omogeneo, per i diversi eventi che deve essere esplicitato

Riferimento alle misure d'azione: contiene il riferimento alla contromisura adottata o da adottare

Tabella 5- Elenco dei rischi individuati

Evento		**Impatto sulla sicurezza dei dati**		**Riferimento alle misure d'azione (già adottate o da adottare)**
		Codice Descrizione	**Gravità: Alta Media Bassa**	
Comportamento degli incaricati	Furto delle credenziali di autenticazione	DESC001	Media	MIS001, MIS002, MIS003
	Gestione dei documenti informatici	DESC02	Bassa	MIS002
	Carenza di consapevolezza disattenzione o incuria	DESC003	Alta	MIS004
	Comportamenti sleali e fraudolenti	DESC004	Media	MIS005, MIS006, MIS007, MIS028
	Errore materiale	DESC005	Bassa	MIS008, MIS009, MIS010
Eventi relativi agli strumenti	Azione di virus informatici	DESC006	Bassa	MIS011
	Spamming e tecniche di sabotaggio	DESC007	Media	MIS012, MIS013, MIS014
	Malfunziona-mento Indisponibilità o Degrado degli strumenti	DESC008	Bassa	MIS008, MIS009, MIS010, MIS015, MIS016, MIS017, MIS018, MIS019, MIS020, MIS021, MIS045, MIS046
	Accessi interni non autorizzati	DESC009	Bassa	MIS005, MIS009, MIS022, MIS023, MIS024, MIS025, MIS026, MIS027, MIS028,

				MIS029, MIS030, MIS031
	Accessi esterni non autorizzati	DESC010	Alta	MIS032, MIS033, MIS034, MIS035
	Intercettazione di informazioni in rete	DESC0010.1	Alta Vedi DESC009	MIS036
Eventi relativi al contesto	Accessi non autorizzati ai locali	DESC011	Bassa	MIS037, MIS038, MIS039
	Furto di strumenti contenenti dati	DESC012	Bassa	MIS018, MIS037, MIS038, MIS039
	Eventi distruttivi, naturali	DESC013	Alta	MIS040, MIS041, MIS042
	Guasto ai sistemi complementari (impianto elettrico , climatizzazione, etc)	DESC014	Bassa	MIS043
	Errori umani nella gestione della sicurezza fisica	DESC015	Bassa	MIS044

Data di aggiornamento: 25/112008

Tabella 5.1- Descrizione Impatto sicurezza dei dati

Codice Descrizione	Descrizione
DESC001	È stato individuato e nominato per iscritto il custode delle password (mettere in riferimenti della nomina Sono state impartire le opportune istruzioni agli incaricati affinché adottino tutte le necessarie cautele nell'uso dei dispositivi ad essi assegnati e per assicurare la segretezza delle password di accesso al Sistema e ai dati. Il sistema di autenticazione utilizzato (appartenenza ad un dominio Active Directory), costituisce un metodo relativamente sicuro di custodia e gestione delle credenziali di autenticazione degli utenti, per l'accesso alle risorse di rete. Anche il software per la gestione del protocollo assicura : (a) l'univoca identificazione ed autentificazione degli utenti; b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri; c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati; d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette da modifiche non autorizzate.
DESC002	In ogni documento informatico viene obbligatoriamente riportata, in modo

	facilmente leggibile, l'indicazione del soggetto che lo produce e quanto necessario per la formazione dei documenti. Per agevolare il processo di formazione dei documenti informatici e consentire la trattazione automatica dei dati in essi contenuti, l'amministrazione rende disponibili per via telematica, in modo centralizzato e sicuro, moduli e formulari elettronici validi ad ogni effetto di legge. Al fine di tutelare la riservatezza dei dati personali, i certificati e i documenti trasmessi all'esterno contengono solo i dati utilizzati ai fini del procedimento amministrativo e nei termini previsti dalla legge. Per la predisposizione dei documenti informatici si adottano formati che al minimo possiedono requisiti di leggibilità, interscambiabilità, non alterabilità durante le fasi di accesso e conservazione, immutabilità nel tempo del contenuto e della struttura, come specificato anche nell'articolo numero 8 del manuale di gestione. In via preferenziale si adottano i formati XML, PDF-A. La sottoscrizione dei documenti informatici è eseguita con una firma elettronica/digitale, basata su un certificato rilasciato da un certificatore accreditato e generata con un dispositivo sicuro, come specificato anche nell'articolo numero 9 del manuale di gestione. Per i documenti informatici che non necessitano di sottoscrizione, l'identificazione dei soggetti che li producono è assicurata della sistema informatico di gestione dei documenti oppure dal sistema di posta elettronica certificata. Per attribuire una data certa il documento informatico ci si avvale del servizio di marcatura temporale (time stamping) fornito dal certificatore accreditato. Tutti i documenti informatici ricevuti o prodotti dall'amministrazione sono soggetti a registrazione obbligatoria ad esclusione di quelli soggetti a particolare da parte dell'ente il cui elenco è allegato al Manuale di gestione del protocollo informatico ai sensi dell'art.53, comma 5 DPR 445/2000. L'operazione di modifica o di annullamento di una registrazione di protocollo è eseguita con le modalità di cui all'articolo 8 del Dpcm 31/10/2000 e all'articolo n. 23 del Manuale di gestione del protocollo informatico come di seguito specificato a) il tentativo di modifica di una delle informazioni generate, o assegnate, automaticamente dal sistema e registrate in forma non modificabile (numero di protocollo, data della registrazione), determina l'automatico e contestuale annullamento dell'intera registrazione; b) Le informazioni registrate in forma non modificabile (mittente, destinatario, oggetto) possono essere annullate per correggere errori intercorsi in sede di immissione di dati. In questo caso l'annullamento deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica. c) Solo al responsabile del servizio archivistico competono le funzioni di annullamento dei protocollo, come previsto dal manuale di gestione.
DESC003	L'Ente non ha attualmente adottato un regolamento per l'uso degli strumenti informatici da parte dei dipendenti e per garantire la sicurezza informatica
DESC004	Attraverso un sistema di controllo delle credenziali di autenticazione a livello centrale e la protezione delle risorse messe a disposizione dai server, l'Ente assicura l'adozione di una parte delle misure minime di sicurezza. In particolare con questo sistema quella parte che permette di evitare comportamenti più o meno consapevolmente fraudolenti. È sempre possibile rinforzare il sistema di controllo, attivando il monitoraggio delle operazioni di login, accesso ai file, ecc., che permettono di controllare quale utente ha commesso l'illecito.

	Non esistono disposizioni scritte per l'individuazione delle modalità con le quali il titolare può disporre dei dati e degli strumenti elettronici, in caso di impedimento o prolungata assenza dell'incaricato oppure di indifferibile intervento.
DESC005	Esiste una politica di backup delle banche dati che previene eventuali errori commessi dagli incaricati al trattamento. In caso di errore è possibile il recupero ripristinando completamente o in parte i dati Sono presenti politiche di Recovery specifiche per assicurare che le copie di backup costituiscano un valido mezzo per il recupero dei dati perduti (verifica logica delle copie e test sistematici di recupero dei dati), che consentano anche di valutare i tempi di recovery Al fine di garantire la non modificabilità delle operazioni di registrazioni del protocollo, il contenuto del registro informatico di protocollo al fine della giornata lavorativa è riversato su supporti riscrivibili e conservato a cura del Responsabile dei sistemi informativi, trimestralmente è riversato su supporti non riscrivibili, alla chiusura delle registrazioni il contenuto annuale del registro informatico di protocollo è riversato, in triplice copia, su un supporto informatico non riscrivibile di cui due copie vengono inviate al Responsabile del servizio archivistico secondo le modalità previste dal manuale di gestione del protocollo informatico, articoli 24 e 25.
DESC006	Esiste un sistema antivirus centralizzato che protegge il server e tutti i client della rete. Le parti antivirus client sono sottoposte al controllo e all'aggiornamento delle definizioni antivirus da una console centrale. Anche la possibilità di disattivazione di parti delle componenti antivirus dei client è bloccata attraverso il sistema centralizzato.
DESC007	La gestione delle caselle di posta elettronica avviene esternamente all'Ente. Presso la ditta ALFA.PI srl di Milano. L'adozione di strumenti antivirus sui singoli client, permette il blocco di codice pericoloso (almeno per quello intercettabile con le ultime versioni delle definizioni antivirus), contenuto in messaggi di posta elettronica. Sui sistemi server vengono regolarmente applicate le patch, disponibili per il Sistema Operativo, per il software applicativo generico e anche quelle necessario al software applicativo WinSic2000® A.P.Systems messe a disposizione dalla società A.P.Systems stessa (gestione dati). Sui client vengono regolarmente eseguiti gli aggiornamenti.
DESC008	Per quanto riguarda la disponibilità e l'integrità dei dati la situazione è la seguente: Tutti i server che forniscono servizi fondamentali: server dati, server web intranet, sono configurato con dischi in RAID. Non esiste nessun sistema di ridondanza hardware dei server, (a parte i sistemi RAID degli hard disk citati sopra). Politiche di Backup dei dati per quanto riguarda le procedure di backup dei dati contenuti nel Database del Sistema Informativo esiste la seguente politica:

	un backup giornaliero dal lunedì al sabato su nastro, utilizzando un ciclo di 6 supporti un backup giornaliero per ogni giorno della settimana su disco un backup settimanale su nastro, utilizzando un ciclo di 4/5 supporti un backup mensile su nastro, utilizzando il 4° o il 5° nastro del ciclo settimanale un backup annuale su nastro, utilizzando un ciclo di 1 supporto Esiste un piano che descrive il ciclo di sostituzione dei supporti utilizzati (vedere punto 9.5.3.5) Le copie di backup sono così conservate: in armadio dedicato ignifugo nel locale C.E.D. Nelle politiche di backup sopra elencate e specificate nella procedura PAU 01, sono compresi: il database del SIC + file dei sistemi + file utenti, depositati sul servernt Esiste una procedura per garantire l'integrità e la consistenza dei dati contenuti nei supporti magnetico utilizzati per le copie di backup (vedere punto 9.5.3.4) In caso di danneggiamento dei dati o degli strumenti di elaborazione esistono specifiche procedure interne di ripristino (vedere punto 9.5.4) È attualmente previsto un ciclo sistematico di pulizia delle unità di backup con apposito nastro (cleaning cartridge), ogni qualvolta il drive lo richieda (il dispositivo indica automaticamente quando eseguire la pulizia delle testine, rendendo visibile una spia luminosa sul suo pannello frontale). Non esiste a livello applicativo, almeno per quel che riguarda il funzionamento della rete (autenticazione, ecc.), una ridondanza capace di evitare completo disservizio in caso di malfunzionamento di uno dei server presenti, ma il sistema di backup e il relativo periodo di inattività dovuto al ripristino, è considerato accettabile dall'Ente. Non esiste una ridondanza per quel che riguarda l'accesso alla base dati (sistema in cluster, server ridondati fisicamente, ecc.), ma il sistema di backup e il relativo periodo di inattività dovuto al ripristino, è considerato accettabile dall'Ente.
DESC009	L'accesso alla rete LAN è gestito attraverso un Controller di dominio Active Directory. L'accesso alle risorse della rete LAN è governato da questo sistema di autenticazione centralizzato, quindi tutti gli utenti che accedono ai dati del Sistema Informativo sono protetti da questa appartenenza. L'accesso degli utenti alle risorse del sistema avviene tramite identificazione con un codice utente e una password (credenziali di autenticazione). È attivata sui client la sospensione automatica delle sessioni di lavoro con utilizzo di screensaver con relativa password. Questo aumenta la protezione da accessi da parte di utenti non autorizzati in caso di abbandono della postazione. L'esistenza di un dominio Active Directory, unita alla presenza di macchine con sistema operativo Microsoft Windows XP professional , permette di

	controllare con cura e produttività le politiche di sicurezza della rete e di imporre restrizioni ai client che evitino la creazione di buchi di sicurezza (situazioni anche inconsapevolmente create attraverso la costituzione di risorse condivise non controllate, l'installazione di software non approvato, ecc.). La password utente ha impostata una lunghezza minima, è gestita la possibilità di non riutilizzo della password alla scadenza, non vi sono regole per imporre la complessità della password, le password sono modificate dopo il primo rilascio e utilizzo. Esiste un periodo di 3 mesi, oltre il quale le credenziali non sono più valide (periodo di scadenza delle password). Esiste un istruzione operativa per la disabilitazione delle credenziale di autenticazione in caso di inutilizzo o perdita di qualità . L'accesso alle risorse di sistema, cioè alle risorse messe a disposizione dei server, quali repository di files condivisi, ecc., sono controllate in modo centralizzato con l'utilizzo di ACL (Access Control List) gestite dagli amministratori di sistema Le risorse utente, cioè le risorse messe a disposizione della rete dai singoli utenti, quali repository di files in condivisione per altri utenti, sono gestite con privilegi di accesso specifici, imposti da politiche implementate dagli amministratori (policy di dominio, ecc.) L'accesso al Database Comunale è gestito tramite strumenti di connessione al RDBMS presente, tramite credenziali note solo agli amministratori di sistema L'accesso alle procedure di gestione e trattamento dei dati SIC è effettuato attraverso delle apposite credenziali di autenticazione gestite dal software applicativo WinSic2000® A.P.Systems, conosciute dall'incaricato del trattamento stesso (è possibile per gli amministratori di rete bloccare o modificare le credenziali in caso di perdita di qualità o di inutilizzo, attraverso una procedura grafica di gestione, della stessa suite di applicativi). Per ogni maschera grafica e funzionalità, l'applicativo permette abilitazioni basate sull'utente, al fine di discriminare con cura l'accesso a determinati dati in base alle politiche di sicurezza in vigore.
DESC010	Di fatto le connessioni ad Internet così configurate sono ampiamente controllate. In particolare viene utilizzato un accesso ad Internet controllato da un Firewall che preclude grazie alle sue regole l'accesso alla rete LAN dal mondo Internet. Il server Proxy Web, che serve le richieste dei client interni, per la loro protezione e il controllo degli accessi verso il web è composto da sistema operativo Microsoft Windows 2003 con Microsoft ISA Server. Il server che si occupa dell'implementazione di un sistema Firewall che si frappone tra le risorse della rete locale ed il mondo Internet è composto da sistema operativo Microsoft Windows 2003 con Microsoft ISA Server. Esiste una DMZ, capace di pubblicare in sicurezza su Internet, pagine web con informazioni e servizi applicativi. Per la gestione della Posta elettronica sicura si utilizza un servizio di posta elettronica certificata conforme agli standard della rete nazionale delle pubbliche amministrazioni. L'Amministrazione si avvale di un servizio di "posta

	elettronica certificata" offerto da un soggetto in grado di assicurare la riservatezza e la sicurezza del canale di comunicazione; di dare certezza sulla data di spedizione e di consegna dei documenti, facendo ricorso al "time stamping" e al rilascio di ricevute di ritorno elettroniche: . Il server di posta certificata di cui si avvale l'amministrazione, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni: a) accesso alla Certification Authority per la verifica dei Message Autentication Code (MAC) presenti sui messaggi ricevuti; b) tracciamento delle attività nel file di log della posta; c) gestione automatica delle ricevute di ritorno. Lo scambio di documenti informatici soggetti a registrazione di protocollo avviene mediante messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni. I dati della segnatura informatica di protocollo di un documento informatico trasmesso ad un'altra pubblica amministrazione sono inseriti in un file conforme allo standard XML – XML 1.0. Le modalità di composizione dei messaggi protocollati, di scambio degli stessi e di notifica degli eventi sono conformi alle specifiche riportate nella Circolare AIPA 28/2001. L'operazione di ricezione dei documenti informatici comprende i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi. I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica. L'operazione di spedizione include la verifica della validità amministrativa della firma. Lo scambio di dati e documenti attraverso reti sicure, come la Rete nazionale delle pubbliche amministrazioni o le reti interne, può avvenire anche senza adottare le misure di sicurezza di cui al precedente comma in quanto esse non sono ritenute necessarie.
DESC010.1	Non esiste attualmente alcun tipo di crittografazione dell'informazione durante la trasmissione di rete (LAN). La LAN è comunque protetta da intrusioni esterne, le misure di controllo degli accessi dall'interni e la mancanza di punti rete non custoditi, assicurano una sufficiente protezione da intercettazioni dell'informazione.
DESC011	Esiste un sistema di sicurezza anti-intrusione per l'intero stabile. La porta di accesso al locale C.E.D. è blindata e vi sono disposizioni per la custodia ed il controllo delle chiavi di accesso. Vi sono disposizioni per la custodia delle chiavi di accesso ai server di registrazione della videosorveglianza
DESC012	Vedi DESC011
DESC013	Non esiste un sistema di sicurezza antincendio. È presente un sistema di condizionamento del locale C.E.D.
DESC014	Sono presenti 5 gruppi di continuità, uno per gli armadi di rete, 1 per ognuno dei server e 1 per le attrezzature della polizia locale.

DESC015	È stato individuato, nominato ed istruito un Responsabile del Sistema Informativo. Questo permette l'istruzione programmatica di una o più figure con adeguata professionalità, capaci di verificare periodicamente la sicurezza dell'intero sistema.

Data di aggiornamento: 28/11/2008

9. MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE PER IL TRATTAMENTO DEI DATI CON E SENZA STRUMENTI ELETTRONICI

(punto 19.4 dell'Allegato B Disciplinare Tecnico in materia di misure minime di sicurezza)

Scopo di questa sezione è evidenziare in quale maniera le misure minime di sicurezza vengono realizzate nella realtà tecnologica ed organizzativa dell'Ente per prevenire, contrastare o ridurre i rischi individuati nell'analisi dei rischi effettuata. Le misure si sintetizzano di seguito con una tabella e poi nei paragrafi specifici si descrivono in dettaglio.

Informazioni riportate

Per ciascuna misura sono indicate le seguenti informazioni:

Misura: la descrizione sintetica della misura di sicurezza

Rischio: per ogni misura è necessario indicare il riferimento all'elemento dell'analisi dei rischi che ha motivato l'adozione della misura in oggetto.

Database/trattamento interessato: riportare l'identificativo del (dei) database o dell'archivio informatizzato e dei trattamenti interessati per ciascuna delle misure adottate. È da notare che determinate misure possono non essere riconducibili a specifici trattamenti o basi di dati.

Riferimento Paragrafo DPS: contiene il riferimento eventuale al paragrafo del DPS (Documento Programmatico sulla Sicurezza) in cui è descritta in maniera analitica la misura stessa.

Data di effettività: per ogni misura è necessario indicare la data a partire dalla quale la misura è operativa o se già operativa la dicitura *standard* ("in essere").

Tabella 6 - Elenco delle misure di sicurezza adottate o da adottare

Codice Misura	Misura	Rischio (Codice Descrizione)	Riferimento Paragrafo DPS	Data di effettività
MIS001	Nomina del custode delle password	DESC001	9.2	(in essere)
MIS002	Istruzioni agli incaricati	DESC001	92	aggiornamento 30/3/2009
MIS003	Sistema di Autenticazione	DESC001	9.2	(in essere)
MIS004	Regolamento uso strumenti informatici	DESC002	9.6	30-3 2009
MIS005	Sistema controllo credenziali di autenticazione a livello centrale e sicuro	DESC003 DESC008	9.2	(in essere)
MIS006	Sistema di controllo e monitoraggio	DESC003	92	in essere
MIS007	Disposizioni uso dati titolare	DESC003	92	in essere
MIS008	Politica di Back Up banche dati RDBMS	DESC004 DESC007	9.5	(in essere)
MIS009	Politica di Back Up, gestione centralizzata e sicura banche dati di altro genere	DESC004 DESC007 DESC008	9.5	(in essere)
MIS010	Politica BackUp Recovery	DESC004 DESC007	95	(in essere)
MIS011	Sistema antivirus	DESC005	9.3	(in essere)
MIS012	Applicazione patch programmi servers	DESC006	9.4	(in essere)
MIS013	Applicazione patch programmi clients	DESC006	9.4	(in essere)

Codice Misura	Misura	Rischio (Codice Descrizione)	Riferimento Paragrafo DPS	Data di effettività
MIS014	Relazione conformità e-mail provider	DESC006	9.6	in essere
MIS015	Sistema RAID dischi server	DESC007	9.5.2	(in essere)
MIS016	Ulteriore ridondanza hardware dei server	DESC007	9.5.2	Non prevista
MIS017	Miglioramento politiche di Backup	DESC007	9.5.3	(in essere)
MIS018	Sicurezza copie di Back Up	DESC007 DESC011	9.5.3	(in essere)
MIS019	Integrità e consistenza dati supporti magnetico	DESC007	9.5.3	(in essere)
MIS020	Ridondanza Rete Applicativa	DESC007	9.5.2	Non prevista
MIS021	Ridondanza RDBMS	DESC007	9.5.2	(in essere)
MIS022	Accesso a rete utente + password	DESC008	9.2	(in essere)
MIS023	Utilizzo Sistemi operativi sicuri	DESC008	9.2	(in essere)
MIS024	ScreenSaver postazioni Server	DESC008	92	(in essere)
MIS025	ScreenSaver postazioni Client	DESC008	9.2	(in essere)
MIS026	Politiche credenziali autenticazione	DESC008	9.2	in essere
MIS027	Disabilitazione credenziali (organizzativo)	DESC008	9.2	(in essere)
MIS028	Protezione risorse servers	DESC003 DESC008	9.2	(in essere)
MIS029	Protezione risorse utente	DESC008	9.2	(in essere)
MIS030	Credenziali accesso aree dati A.P.Systems	DESC008	9.2	(in essere)

Codice Misura	Misura	Rischio (Codice Descrizione)	Riferimento Paragrafo DPS	Data di effettività
MIS031	Separazione rete fisica Ente da sottoreti a rischio	DESC008	9.3	
MIS032	Protezione Internet tramite Firewall	DESC009	9.3	(in essere)
MIS033	Navigazione Internet tramite Proxy Web	DESC009	9.6	(in essere)
MIS034	Implementazione Restrizioni navigazione Web	DESC009	9.6	(in essere)
MIS035	Regolamento consultazione log navigazione Web	DESC009	9.6	30/03/2009 Conforme linee guida del garante
MIS036	Necessità crittografazione della comunicazione di rete	DESC009.1	9.3	(in essere)
MIS037	Sistema anti-intrusione locale C.E.D.	DESC010 DESC011	9.1	(in essere)
MIS038	Porta Blindata locale C.E.D.	DESC010 DESC011	9.1	(in essere)
MIS039	Regolamento custodia chiavi locale C.E.D.	DESC010 DESC011	9.1 9.7.2 9.7.3	(in essere)
MIS040	Sistema antincendio locale C.E.D.	DESC012	9.1 9.5.1	
MIS041	Sistema condizionamento locale C.E.D.	DESC012	9.5.1	in essere
MIS042	Sistema antiallagamento locale C.E.D.	DESC012	9.1	
MIS043	Protezione guasto impianto elettrico (gruppi continuità)	DESC013	9.5	(in essere)

Codice Misura	Misura	Rischio (Codice Descrizione)	Riferimento Paragrafo DPS	Data di effettività
MIS044	Nomina responsabile C.E.D.	DESC014	9.2	(in essere)
MIS045	Registro emergenza protocollo informatico	DESC007	9.7.4	(in essere)
MIS046	Manutenzione Archivi	DESC007	9.7.5	(in essere)

Data di aggiornamento: 28/11/2008

9.1 SICUREZZA FISICA

In questa sezione sono definiti nel dettaglio i criteri tecnici ed organizzativi per la protezione delle aree e dei locali e le procedure di controllo accessi ai locali e alle aree stesse.

Sono stati adottati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali, in particolare sono state adottate le seguenti misure per la protezione fisica:

- la limitazione dell'accesso al data center (locale server) attraverso utilizzo di porta blindata, con accesso riservato e controllato agli uffici.
- presenza sistema allarme negli edifici collegato a una centrale di sorveglianza e ai Carabinieri
- chiusura degli uffici a chiave in assenza degli operatori comunali e comunque fuori orario di lavoro

9.2 SICUREZZA DEGLI ACCESSI

In questo paragrafo si indica la procedura di definizione delle credenziali di autenticazione, individuate tra le seguenti tipologie:

- Codice identificativo, più parola chiave
- Dispositivo di autenticazione (*smart card e simili*), più eventuale parola chiave
- Rilevazione biometrica (*es. impronta digitale*), più eventuale parola chiave

La modalità di attivazione, variazione e gestione delle credenziali e l'individuazione del custode delle credenziali (responsabilità della attuazione e della gestione). I Criteri di definizione dei profili di autorizzazione. L'Attribuzione, revoca ed aggiornamento dei profili di autorizzazione

Il sistema di autenticazione utilizzato dall'Ente per l'accesso alla rete e alle postazioni è il seguente: utente e password con controllo centralizzato attraverso la costituzione di un Dominio Microsoft Active Directory; il custode delle password individua i metodi da adottare a livello organizzativo per l'attivazione di un nuovo account,Istruzione operativa AU! la variazione e gestione delle credenziali, ed è responsabile della gestione di queste operazioni di amministrazione di rete. Sono stati costruiti i profili di autorizzazione (Access Control List) per le risorse di rete a livello di sistema operativo (accesso a files e risorse condivisi) e indicato ai dipendenti un comportamento da tenersi in rete ai fini di una corretta gestione.
Infine, vengono attuate immediatamente le operazioni organizzative per la disabilitazione delle credenziali in caso di perdita di qualità (licenziamento di dipendenti, smarrimento o divulgazione delle credenziali, ecc.).

Gestione delle password a livello di Sistema:

- definizione a livello di Sistema della lunghezza minima delle password che non può essere inferiore a n. 8 caratteri (minimo)
- definizione a livello di Sistema della possibilità di non riutilizzo della password alla scadenza e del periodo di scadenza della password
- impostazione della password del BIOS
- impostazione della password dello screensaver per server e client
- presenza di sistemi operativi sicuri (da Windows 2000 Professional in su) di tutte le postazioni
- sistemi di controllo e monitoraggio delle risorse di rete

Le credenziali di accesso al sistema di videosorveglianza sono gestite dal Responsabile del Settore Polizia Locale, secondo quanto stabilito dal vigente regolamento comunale per l'installazione e l'utilizzo di impianti di videosorveglianza del territorio

Per quanto riguarda il Software del protocollo informatico L'accesso in lettura e scrittura alle directory di rete utilizzate come deposito dei documenti è effettuato dal processo server dell'applicativo di protocollo informatico, mai dalle stazioni di lavoro.

9.2.1 MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

- Elenco del personale autorizzato al trattamento (INCARICATI)

E' presente un modulo di designazione ed istruzioni per gli incaricati del trattamento che viene fatto firmare al momento dell'assunzione; l'elenco del personale autorizzato al trattamento coincide con quello degli stessi incaricati al trattamento ed è riportato nelle tabelle 2 e 4.2.

- Definizioni dei criteri di assegnazione dei permessi di accesso ai dati

Il sistema di autenticazione utilizzato per l'accesso al database è il seguente: utente e password con controllo centralizzato tramite Amministratore NT e Ammin NET di A.P. Systems S.r.l. Il custode delle password è responsabile della gestione di queste operazioni: adottare i metodi a livello organizzativo per l'attivazione di nuovi account,(istruzione operativa…) la variazione e gestione delle credenziali ed è individuato quale amministratore degli accessi al database. Inoltre, costruisce i profili di autorizzazione (Access Control List) per l'accesso ai database (tramite disattivazioni e permessi per determinati menù delle procedure Winsic o altro).
Infine, vengono attuate immediatamente le operazioni organizzative per la disabilitazione delle credenziali in caso di perdita di qualità (licenziamento di dipendenti, smarrimento o divulgazione delle credenziali, ecc.).
Per gli applicativi Crux e Spunico il sistema di autenticazione delle credenziali è gestito direttamente attraverso delle funzioni dell'applicativo stesso, sono adottate gli stessi metodi organizzativi previsti nella procedura .

Per il protocollo informatico:

- Il livello di autorizzazione all'utilizzo del sistema di gestione informatica dei documenti è attribuito dal Responsabile del servizio archivistico;
- il controllo degli accessi ai dati di protocollo e alla base documentale da parte del personale dell'amministrazione è assicurato utilizzando USER Id e la PASSWORD assegnata ad ogni utente;
- Il servizio informatico assicura, la variazione sistematica delle password assegnate agli utenti per l'accesso alle funzioni del sistema
- ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è associata una Access Control List (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso. Per default il sistema segue la logica dell'organizzazione, nel senso che ciascun utente può accedere solamente ai documenti che sono stati assegnati alla sua struttura di appartenenza, o agli uffici ad esso subordinati;

- l'amministrazione adotta regole per l'accesso ai documenti sulla base della normativa vigente in materia di privacy .

9.3 SICUREZZA DELLA RETE CONTRO I RISCHI DI INTRUSIONI INTERNE ED ESTERNE

9.3.1 MISURE DI PROTEZIONE CONTRO I VIRUS INFORMATICI

All'interno dell'Ente esiste una gestione centralizzata del software Antivirus. È installata la parte centralizzata del sistema antivirus (Symantec Enterprise Manager), su tutti i Clients è installata la versione client dello stesso antivirus, gestita centralmente dalla console.

9.3.2 MISURE DI PROTEZIONE CONTRO INTRUSIONE DA RETE INTERNET

E' presente un Firewall costituito da un server con sistema operativo Microsoft Windows Server 2003 Server Standard Edition firewall implementato con Microsoft Isa Server 2004 .. Esiste una separazione della rete fisica dell'Ente da sottoreti a rischio, quindi non si ritiene necessità la crittografazione della comunicazione in LAN.

9.4 SICUREZZA DELLA VULNERABILITÀ DEGLI STRUMENTI ELETTRONICI

Periodicamente vengono controllati ed effettuati gli update, i relativi aggiornamenti (processo di applicazione delle patch per il software e l'hardware) sui servers e sui clients per la correzione dei difetti (bugs), tutto ciò per evitare la vulnerabilità.

9.5 CRITERI E PROCEDURE PER ASSICURARE DISPONIBILITÀ ED INTEGRITÀ DEI DATI *(punto 19.5 dell'Allegato B Disciplinare Tecnico in materia di misure minime di sicurezza)*

9.5.1 IMPIANTI DI SICUREZZA DEI LOCALI (CLIMATIZZAZIONE, …)

Sono presenti i seguenti impianti di sicurezza
- Sistema di allarme con apparti volumetrici
- Contratto con istituto di vigilanza
- Per la sede centrale sistema di climatizzazione

9.5.2 POLITICHE DI RIDONDANZA E CONTINUITÀ DEL SERVIZIO

È presente 1 gruppo di continuità (UPS), installato per tutti i server e apparati di rete del C.E.D.
Da ciò si può dedurre che tutti i servizi fondamentali, forniti dal Centro di Elaborazione sono protetti contro sbalzi e cadute di tensione improvvisi.

9.5.3 POLITICHE DI BACKUP

In questo paragrafo si definiscono nel dettaglio le politiche adottate dall'Ente al fine di garantire la disponibilità dei dati a seguito di eventuale distruzione o danneggiamento dei dati stessi e/o degli strumenti elettronici utilizzati per il trattamento.

Le politiche e le procedure si sintetizzano di seguito con una tabella e poi nei paragrafi specifici si descrivono in dettaglio.
Per quanto riguarda il protocollo informatico
Il responsabile del Servizio informatico garantisce la puntuale esecuzione delle operazioni di backup trimestrale dei dati e dei documenti registrati, su supporti informatici non riscrivibili, da parte di personale appositamente autorizzato, come previsto dal Manuale di gestione articoli numero 24 e 25 e dal piano di conservazione
Ogni operazione di manutenzione o di backup effettuata sul sistema che ospita la base documentale e sul sistema di protocollo informatico è registrata su un file di log periodicamente controllato.
Le copie di backup dei dati e dei documenti prodotte in almeno tre copie sono conservate a cura del Responsabile del servizi informativi, dal Responsabile del servizio archivistico e in un luogo diverso dalla sede dell'amministrazione a cura di un soggetto terzo con il quale si è stabilita la convenzione per la conservazione, come previsto dal Manuale di gestione
Per l'archiviazione ottica dei documenti si utilizzano i supporti di memorizzazione digitale che consentono la registrazione mediante la tecnologia laser (DVD-R).
La conservazione dei documenti digitali e dei documenti analogici (che comprendono quelli su supporto cartaceo) avviene nei modi e con le tecniche specificate nel piano di conservazione (Documento n.) e nella deliberazioni CNIPA 11/04
Il riferimento temporale, inteso come l'informazione, contenente la data e l'ora in cui viene ultimato il processo di conservazione digitale, associata ad uno o più documenti digitali, è generato secondo i canoni di sicurezza
Informazioni riportate

Identificativo Database: contiene l'identificativo del data base o dell'archivio interessato.

Dati sensibili o giudiziari contenuti: contiene l'elenco dei dati sensibili o giudiziari contenuti nel database o archivio.

Criteri individuati per il salvataggio (procedure operative in essere): contiene una descrizione della tipologia di salvataggio e della frequenza con cui viene effettuato.

Ubicazione di conservazione delle copie: contiene l'indicazione del luogo fisico in cui sono custodite le copie dei dati salvate.

Struttura operativa o persona incaricata del salvataggio: contiene il nominativo della struttura/persona incaricata di effettuare il salvataggio e/o di controllarne l'esito o del coordinatore del gruppo preposto.

Tabella 7 - Elenco delle politiche di backup adottate o da adottare

Identificativo Database	Dati personali sensibili o giudiziari contenuti	Criteri per il salvataggio	Ubicazione di conservazione delle copie	Struttura operativa incaricata al salvataggio
DB_0001	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0002	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0003	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0004	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0005	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.

		DESC007		
DB_0008	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0008	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_00013	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0015	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0016	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0017	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.

		nella tabella 5.1 colonna DESC007		
DB_0018	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0020	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0021	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0022	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0023	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0024	Vedi Tabella 1	Per questa banca dati,si faccia	Nastri conservati in armadio di sicurezza	Responsabile C.E.D.

		riferimento a quanto descritto nella tabella 5.1 colonna DESC007	ignifugo	
DB_0025	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0026	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0027	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0028	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0029	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.

DB_0030	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0031	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0032	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0033	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0034	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0035	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.

		5.1 colonna DESC007		
DB_0036	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0037	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0038	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0039	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0040	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0041	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.

		quanto descritto nella tabella 5.1 colonna DESC007		
DB_0042	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0043	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0044	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0045	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0046	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0048	Vedi Tabella 1	Per questa	Nastri conservati	Responsabi

		banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	in armadio di sicurezza ignifugo	le C.E.D.
DB_0049	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0050	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0051	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0052	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0053	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.

		colonna DESC007		
DB_0054	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0055	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0056	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0057	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0058	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0059	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.

		descritto nella tabella 5.1 colonna DESC007		
DB_0060	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0061	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0062	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0063	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0064	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0065	Vedi Tabella 1	Per questa banca	Nastri conservati in armadio di	Responsabile C.E.D.

		dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	sicurezza ignifugo	
DB_0066	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0067	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0068	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.
DB_0070	Vedi Tabella 1	Per questa banca dati,si faccia riferimento a quanto descritto nella tabella 5.1 colonna DESC007	Nastri conservati in armadio di sicurezza ignifugo	Responsabile C.E.D.

Data di aggiornamento: 28/11/2008

9.5.3.1SISTEMA E SUPPORTI DI BACKUP UTILIZZATI

Il sistema utilizzato per l'esecuzione delle procedure di backup attualmente è il software applicativo Brightstor ArcServer Backup server (con IDR).
I supporti utilizzati sono i seguenti:

- lettore nastro tipo Hewlett Packard StorageWorks DLT VS80
- solo per gli adempimenti relativi al protocollo per l'archiviazione ottica dei documenti si utilizzano i supporti di memorizzazione digitale che consentono la registrazione mediante la tecnologia laser (DVD-R)

Per maggiori specifiche sul numero dei dispositivi utilizzati, cicli di sostituzione, metodologie di utilizzo nel tempo, , si faccia riferimento alla tabella 5.1, colonna con identificativo DESC007.

9.5.3.2 CRITERI E PROCEDURE PER IL SALVATAGGIO

Per maggiori specifiche sui criteri e procedure di backup, si faccia riferimento alla tabella 5.1, colonna con identificativo DESC007.

9.5.3.3 PROCEDURA PER LA CUSTODIA E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI UTILIZZATI PER IL BACKUP DEI DATI

Il processo di custodia dei supporti di backup delle banche dati viene così gestito:
I nastri sono custoditi in un armadio di sicurezza ignifugo.
Nelle politiche di backup sono compresi: il database del Sistema Informativo + file di sistema + file utenti
L'accesso ai nastri avviene solamente da parte del personale addetto
Per maggiori specifiche sulle procedure e sulla custodia dei supporti, si faccia riferimento alla tabella 5.1, colonna con identificativo DESC007.

9.5.3.4PROCEDURA PER LA VERIFICA DELLA REGISTRAZIONE DEI BACKUP

La verifica della corretta esecuzione dei backup avviene sia attraverso il software di backup, che attraverso i tools dei differenti sistemi applicativi: log dei backup di Sql per quel che riguarda la copia dei dati su server stesso, interfaccia grafica del sistema di backup per la verifica della corretta esecuzione del processo di backup Le operazioni di verifica fisica, vengono eseguite giornalmente. Con cadenza mensile, viene anche verificata la correttezza logica dei dati oggetto di backup, con prova di restore e verifica dell'integrità dei dati (con metodologie a campionamento).

9.5.3.5 UTILIZZO E RIUTILIZZO DEI SUPPORTI RIMOVIBILI

La procedura di dismissione dei supporti non più utilizzati è la seguente: distruzione fisica prima della dismissione per evitarne la lettura a personale non autorizzato che potrebbe recuperarli. Il ciclo di sostituzione dei supporti per

evitare l'invecchiamento e conseguente impossibilità di recupero avviene ogni 12 mesi circa mentre, i cicli di pulizia delle unità nastro con apposite cleaning cartridge vengono effettuati unicamente quando richiesto dal dispositivo di backup (il dispositivo stesso richiede ciclo di pulizia quando necessario attraverso un led lampeggiante posto sulla parte frontale del server).

9.5.4 CRITERI E PROCEDURE DI DISASTER RECOVERY

In questo paragrafo si definiscono nel dettaglio le politiche adottate dall'Ente al fine di garantire il ripristino dei dati e degli strumenti elettronici a seguito di eventuale distruzione o danneggiamento degli stessi. Le politiche e le procedure si sintetizzano di seguito con una tabella e poi nei paragrafi specifici si descrivono in dettaglio.

Informazioni riportate

Identificativo Database: contiene l'identificativo del data base o dell'archivio interessato.

Procedure definite: contiene l'indicazione delle procedure che assicurino in tempi certi il ripristino dei sistemi (la normativa prevede un tempo non superiore a 7 giorni)

Periodicità delle prove :contiene la periodicità prevista per l'effettuazione delle verifiche delle procedure attivate

Tabella 8 - Elenco delle politiche di disaster recovery adottate o da adottare

Identificativo Database	Procedure definite	Periodicità delle prove
DB_0001	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0002	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0003	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0004	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0005	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0006	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0007	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0013	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0014	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0015	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0016	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0017	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0018	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0020	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0021	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0022	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0023	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0024	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0025	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0026	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0027	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0028	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0029	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0030	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0031	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0032	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0033	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0034	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0035	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0036	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0037	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg

DB_0038	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0039	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0040	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0041	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0042	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0044	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0045	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0046	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0048	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0049	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0050	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0051	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0052	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0053	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0054	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0055	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0056	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0057	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0058	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0059	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0060	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0061	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0062	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0063	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0064	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0065	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0066	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0067	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0068	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0069	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg
DB_0070	Si faccia riferimento al par. 9.5.4.1	1 / 90 gg

Data di aggiornamento: 28/11/2008

9.5.4.1 PROCEDURE DI RIPRISTINO DEFINITE

In caso di disastro che danneggia gravemente il sistema informativo il responsabile dei sistemi informatici provvede a ripristinare il funzionamento delle apparecchiature guaste facendo intervenire delle ditte specializzate

In questa parte descriviamo sommariamente tutte le risorse considerate indispensabili, cioè non facilmente ricostruibili in caso di fault del servizio o dell'intero server, successivamente le procedure individuate per il ripristino della condizione di funzionamento. Come descritto meglio in tabella 5.1 alla colonna DESC007,

Elenco risorse da proteggere	
Servizi	**Risorse**
RDBMS	Viene effettuato un backup dei databases presenti nel RDBMS . L'esportazione dei dati avviene tramite

	comandi di sql e genera files per ogni singolo database nella cartella su disco del server "d:\…\backup\t". Viene creato un file di log (exports.log) con indicazione dei tempi e dell'esito per ogni operazione di esportazione; L'operazione sopra elencata viene eseguita automaticamente tramite una schedulazione di sistema operativo, prima dell'esecuzione del backup su nastro. Con quanto descritto sopra, viene creata un'unica posizione che contiene tutto ciò di cui si ha bisogno per un corretto ripristino del RDBMS. Di questa posizione viene poi eseguito un backup su nastro con le modalità descritte nella tabella 5.1 colonna DESC007.
Domain Controller	L'elenco di risorse di cui eseguire backup su nastro, comprende anche dati di sistema operativo tra i quali quelli necessari al ripristino delle funzionalità del dominio.
File Server	L'elenco di risorse di cui eseguire backup su nastro, comprende anche i file degli utenti, presenti in determinate cartelle del server (es: tutto quanto contenuto nella cartella "documenti utenti", quanto contenuto in alcune cartelle dell'amministratore del server: documenti, desktop, …). Posizioni dove gli utenti sanno di poter salvare file il cui contenuto sarà sottoposto a backup su nastro.
WINS Server	Sebbene la ricostruzione del servizio wins per una rete così semplice non costituisca particolari problemi, oltre a non costituire punto di fallimento determinante per un corretto funzionamento dei servizi fondamentali, l'elenco di risorse di cui eseguire backup su nastro, comprende anche dati di sistema operativo tra i quali quelli necessari al ripristino del servizio wins.
DNS Server (AD)	L'elenco di risorse di cui eseguire backup su nastro, comprende anche dati di sistema operativo tra i quali quelli necessari al ripristino del servizio dns (legato al corretto funzionamento del dominio).
DHCP Server	Sebbene la ricostruzione del servizio dhcp per una rete così semplice non costituisca particolari problemi, oltre a non costituire punto di fallimento determinante per un corretto funzionamento dei servizi fondamentali, l'elenco di risorse di cui eseguire backup su nastro, comprende anche dati di sistema operativo tra i quali quelli necessari al ripristino del servizio dhcp.
Web Server Pro.NET	Sebbene la parte web del sito che permette il corretto funzionamento della protocollazione elettronica sia di semplice ricostruzione (si tratta di un setup seguito da alcuni dati di configurazione), l'elenco di risorse di cui eseguire backup su nastro, comprende anche la cartella con i dati indispensabili per il corretto ripristino

	del servizio di protocollazione sono invece già compresi nel backup dei databases del RDBMS e nell'elenco delle risorse di cui eseguire backup su nastro, in cui è compresa la cartella contenente tutti gli allegati di protocollazione (documenti protocollati, documenti scannerizzati, …).
Backup Server	Il sistema di backup può essere installato e riconfigurato in breve tempo, sfruttando l'operazione di backup del catalogo del sistema di backup, sui nastri.
Antivirus Norton	N/A
Firewall	Viene eseguito uno script di backup presente sul firewall unicamente in caso di modifica dei parametri di configurazione di uno dei servizi forniti. Lo script esegue il backup di tutti i files di configurazione necessari al ripristino delle funzionalità del server. Il file viene copiato sul server centrale e compreso nell'elenco di risorse di cui eseguire backup su nastro.
Sistema Operativo	L'elenco di risorse di cui eseguire backup su nastro, comprende anche i dati di sistema operativo necessari al ripristino delle parti fondamentali del sistema (System Files, Registry, Active Directory, WINS, DHCP, IIS, TS Licensing, …).

Metodologie di ripristino	
Tipologia	**Procedura**
Standard	È sempre necessario avere un backup standard delle risorse considerate indispensabili al corretto ripristino dei servizi. Almeno per un ripristino in tempi brevi di quelli fondamentali e successivamente di quelli meno urgenti. Con questa metodologia sarà necessario: • reinstallare il sistema operativo e tutti i driver necessari (operazione che unitamente alla presenza dei dischi di installazione forniti con il server risulta piuttosto semplice e relativamente veloce) • eseguire tutti i service pack e aggiornamenti del sistema operativo • poi per ogni servizio eseguire le procedure specifiche **Servizi** **Procedure** **RDBMS** Restore della cartella descritta nell' "Elenco risorse da proteggere", parte **"RDBMS" +** Installare il RDBMS in modo standard e poi far puntare al file di configurazione recuperato dal backup, verificando che l'albero delle directory con le varie directory coincida con quanto scritto nel file di configurazione **+** eseguire il servizio **Domain Controller** Il ripristino di questo componente è compreso nel ripristino da nastro dei dati del sistema operativo. **File Server** Eseguire il restore della parte descritta nell' "Elenco risorse da proteggere", parte **"File Server"**. **WINS Server** Il ripristino di questo componente è compreso nel ripristino da nastro dei dati del sistema operativo. **DNS Server (AD)** Il ripristino di questo componente è compreso nel ripristino da nastro dei dati del sistema operativo. **DHCP Server** Il ripristino di questo componente è compreso nel ripristino da nastro dei dati del sistema operativo. **Web Server Pro.NET** Se non ancora presente, installare IIS 6 sul server **+** Installare il componente WebSicDotNet A.P.Systems in modalità standard **+** eseguire il restore della parte descritta nell' "Elenco risorse da proteggere", parte **"Web Server Pro.NET"**. **Backup Server** Installazione del software di backup secondo modalità standard, creazione dei processi di backup.

	Antivirus Norton Installazione del software Symantec Norton Antivirus Console Centrale. **Firewall** Installazione del sistema operativo + restore dei file di configurazione nelle posizioni originali. **Sistema Operativo** Il ripristino delle condizioni del sistema operativo è compreso nel ripristino da nastro dei dati del sistema operativo. **NOTA: chiaramente i passi descritti potrebbero essere eseguiti in questo modo: installare tutti i software necessari nelle loro posizioni originali e poi eseguire un unico restore di tutto il nastro su destinazioni originali, verificando poi il funzionamento di ogni servizio.** Con le politiche di backup assunte, si accetta come massimo tempo di perdita di dati 1 giorno (l'intervallo minimo di backup considerato come compromesso tra prestazioni e sicurezza è di un giorno). Con questa metodologia, si assumere che il tempo di ripristino, almeno per i servizi fondamentali è di 18 ore.

9.6 SICUREZZA DELLA LICEITÀ DELL'UTILIZZO DI STRUMENTI QUALI INTERNET E POSTA ELETTRONICA

Questa misura di sicurezza consiste nell'applicazione del regolamento definito dall'Ente in cui sono indicate le regole per l'utilizzo di tutti gli strumenti informatici e quindi anche di Internet e della Posta Elettronica sul posto di lavoro.

9.7 SICUREZZA PER I TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI INFORMATICI

In questa sezione sono definite nel dettaglio le misure di sicurezza adottate o da adottare per il trattamento dei dati senza l'ausilio di strumenti elettronici.

In particolare sono descritte:

- Procedure e modalità per l'organizzazione degli archivi cartacei ad accesso autorizzato
- Modalità di custodia dei dati particolari durante l'utilizzo
- Modalità di identificazione e registrazione degli accessi ai dati particolari dopo l'orario di chiusura

9.7.1 PROCEDURE E MODALITÀ PER L'ORGANIZZAZIONE DEGLI ARCHIVI CARTACEI

I documenti gestiti in forma cartacea sono gestiti in fascicoli cartacei .
La formazione di un nuovo fascicolo avviene attraverso la registrazione delle seguenti informazioni:

1. Indice classificazione
2. Oggetto fascicolo
3. Data di apertura
4. Ufficio procedente
5. Livello riservatezza

9.7.2 MODALITÀ DI CUSTODIA DEI DATI

Presso la sede comunale di Triuggio è situato l'archivio storico contenente i documenti sino all'anno 1966 e l'archivio di deposito contenente i documenti fino all'anno .2003
I locali sono chiusi a chiave e le chiavi sono depositate presso l'Ufficio Segreteria,
La documentazione corrente è conservata da ogni Servizio che tenuto all'archiviazione ed all'adeguata custodia per i relativi documenti in formato cartaceo, che dovranno essere conservati in armadi chiusi a chiave la tipologia degli atti di propria competenza che devono essere custoditi.

9.7.3 MODALITÀ DI IDENTIFICAZIONE E REGISTRAZIONE DEGLI ACCESSI DOPO L'ORARIO DI CHIUSURA

Ogni dipendente che accede agli edifici comunali è tenuto all'identificazione tramite badge personale e la relativa procedura di timbratura.

9.7.4 REGISTRO DI EMERGENZA

In condizioni di emergenza si applicano le modalità di registrazione e di recupero dei dati descritte all'articolo 63 del DPR 445/2000 e a quanto previsto nel manuale di gestione del protocollo informatico.

- sul registro di emergenza sono riportate la causa, la data e l'ora d'inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;
- per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'ente;
- le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico utilizzando un'apposita funzione di recupero dei dati, senza ritardo rispetto al ripristino delle funzionalità del sistema; durante la fase di recupero, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero in emergenza, pertanto i documenti registrati in emergenza avranno due numeri: uno quello di emergenza e l'altro quello del protocollo generale

9.7.5 TENUTA DELL'ARCHIVIO INFORMATICO

Il Responsabile del procedimento di conservazione digitale (Conservatore) sulla base di quanto specificato nel manuale di gestione e nel piano di conservazione:

a) adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza;
b) definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;
c) verifica periodicamente con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti

10. PREVISIONE DEGLI INTERVENTI FORMATIVI (PIANO DI FORMAZIONE)
(punto 19.6 dell'Allegato B Disciplinare Tecnico in materia di misure minime di sicurezza)

Obiettivo della formazione è fornire a tutti gli incaricati dei trattamenti un'informazione approfondita sul D.Lgs. 196/2003 e sui contenuti del Documento Programmatico per la sicurezza.
In particolare ad ogni revisione del documento e comunque ogni anno, tutti gli incaricati saranno istruiti sui rischi connessi al trattamento e sulle misure adottate per prevenire i possibili danni.

Corsi	***Data prevista***
La privacy nel Comune	***entro il 31/12/2009***

11. TRATTAMENTI AFFIDATI ALL'ESTERNO
(punto 19.7 dell'Allegato B Disciplinare Tecnico in materia di misure minime di sicurezza)

Obiettivo di questa sezione è redigere un quadro sintetico delle attività trasferite a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Informazioni riportate

Per ciascun trattamento sono indicate le seguenti informazioni

Attività esternalizzata: contiene l'identificativo dell'attività che è stata oggetto di delega a terzi

Descrizione sintetica: contiene una descrizione sintetica dell'attività

Dati personali, sensibili o giudiziari interessati: contiene l'elenco dei dati personali, sensibili
o giudiziari oggetto di trattamento per la realizzazione dell'attività delegata

Soggetto delegato: riporta l'identificativo della società o del consulente a cui è stato affidato
l'incarico

Descrizione dei criteri per garantire l'adozione delle misure: perché sia garantito un adeguato
trattamento dei dati è necessario che il soggetto esterno a cui viene affidato il trattamento

si assuma alcuni impegni su base contrattuale

Il soggetto cui le attività sono affidate dichiara:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate;

In questa casella sono riportati gli impegni contrattualmente assunti nel caso specifico.

Tabella 10 - Elenco dei trattamenti affidati all'esterno

Attività delegata	Descrizione sintetica	Dati personali, sensibili o giudiziari interessati	Soggetto esterno delegato	Definizione dei criteri per l'adozione delle misure minime
Servizio Tesoreria	Servizio Tesoreria	personali	Banca di Credito Cooperativo - TRIUGGIO	Comunicazione responsabilità Trattamento dei dati
Esattoria	Servizio di Esattoria	personali	Esatri - Milano	Comunicazione responsabilità Trattamento dei dati
Servizio diattività di data entry e di pianificazione e controllo dei dati finanziari	Front Office ufficio Anagrafe	personale giudiziario sensibile	Ditta Claro s.a.s Airuno	Comunicazione responsabilità Trattamento dei dati
Assistenza Software	Manutenzione e aggiornamento software	Accesso banca dati SIC	AP.Systems. srl Magenta	Comunicazione responsabilità Trattamento dei dati
Assistenza Software Sportello Unico Attività produttive	Manutenzione e aggiornamento software	Accesso banca dati SIC	Ced Camere Milano	Comunicazione responsabilità Trattamento dei dati
Assistenza software CRUX(gestione cimiteri)	Manutenzione e aggiornamento software	Accesso banca dati SIC	Starch srl Ornago	Comunicazione responsabilità Trattamento dei dati

Assistenza hardware	Manutenzione Hardware	Accesso al SIC	Elettrodata 8 srl Dolzago	Comunicazione responsabilità Trattamento dei dati
Assistenza hardware server + impianto videosorveglianza	Manutenzione Hardware	Accesso al SIC	AP.Systems. srl Magenta	Comunicazione responsabilità Trattamento dei dati
Servizio Area Minori	Servizio area minori	Personali Sensibili Giudiziari	Coop. CTA Milano	Comunicazione responsabilità Trattamento dei dati
Servizio Assistenza alunni disabili nelle scuole	Assistenza alunni disabili	Personali sensibili	Coop City Service Busto Arsizio	Comunicazione responsabilità Trattamento dei dati
Servizio gestione cimiteri	Gestione cimiteri	Personali Sensibili	Coop Il Ponte Albiate	Comunicazione responsabilità Trattamento dei dati
Servizio Refezione scolastica	Servizio refezione scolastica – gestione presenze e pagamenti	Personali sensibili	Ditta Sodexho Cinisello Balsamo	Comunicazione responsabilità Trattamento dei dati
Servizio pulizia Edifici Comunale	Pulizia Edifici Comunali		Coop. Il Ponte -Albiate	Comunicazione responsabilità Trattamento dei dati
Aggiornamento nuovo catasto Edilizio – Recupero arretrato catastale	Aggiornamento nuovo catasto Edilizio – Recupero arretrato catastale	Personali	So.Ge,S.T. SEREGNO	Aggiornamento nuovo catasto Edilizio – Recupero arretrato catastale
Manutenzione e servizio hosting Sito comune	Manutenzione e servizio hosting Sito comune	personali	Alfa.pi srl Milano	Comunicazione responsabilità Trattamento dei dati

Data di aggiornamento: 28/11/2008

12. PIANO DI VERIFICHE DELLE MISURE ADOTTATE

In questa sezione è riportato per mezzo di una tabella il quadro che identifica la periodicità dei controlli sulle misure previste nel documento programmatico secondo quanto indicato dalla normativa (Disciplinare Tecnico Allegato B DLgs 196/2003).

Informazioni riportate

Per ogni misura da verificare sono riportate le seguenti informazioni:

Misure da verificare: riporta la denominazione delle misure da verificare

Descrizione sintetica: contiene la descrizione sintetica del controllo

Tipologia dei dati : indica la natura dei dati (sensibili, giudiziari)

Periodicità: contiene le date previste per il controllo

Riferimento al Disciplinare Tecnico: indica il punto del Disciplinare Tecnico Allegato B del Dlgs 196/2003

Tabella 11 - Elenco delle verifiche previste per il trattamento con strumenti elettronici

TRATTAMENTO CON L'AUSILIO DI STRUMENTI ELETTRONICI

MISURE DA VERIFICARE	DESCRIZIONE SINTETICA	Tipologia dei dati	CADENZA	Riferimento nel Disciplinare Tecnico Allegato B del DL 196/2003
Credenziali di autenticazione	disattivazione in caso di mancato utilizzo dei medesimi per un periodo superiore ai 6 mesi		6 mesi	7
Credenziali di autenticazione	disattivazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali		sempre	8
Codice per l'identificazione	una volta assegnato, non può essere assegnato ad altri incaricati		sempre	6
Parola chiave	per il trattamento di dati personali deve essere modificata ogni sei mesi		6 mesi	5
Parola chiave	per il trattamento di dati sensibili deve essere modificata ogni tre mesi	Dati sensibili e giudiziari	3 mesi	5
Profili di autorizzazione	possono essere individuati per singolo incaricato o per classi omogenee di incaricati		sempre	13
Profili di autorizzazione	verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione		1 anno	14

Lista degli incaricati autorizzati	può essere redatta anche per classi omogenee di incarico		1 anno	15
Antivirus	efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.		6 mesi	16
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici		1 anno	17
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici	Dati sensibili e giudiziari	6 mesi	17
Backup	salvataggio dei dati con frequenza settimanale		7 giorni	18
Ripristino accesso dati	Ripristino accesso dati in caso di danneggiamento degli stessi o degli strumenti elettronici	Dati sensibili e giudiziari	massimo 7 giorni	23
DPS	Documento Programmatico sulla sicurezza		1 anno (entro 31/3)	19
Sistemi antintrusione	Protezione contro l'accesso abusivo nel caso di trattamento di dati sensibili		sempre	20
Custodia dei supporti rimovibili di memorizzazione	istruzioni organizzative e tecniche per la loro custodia e utilizzo		sempre	21
Riutilizzo dei supporti di memorizzazione	se non utilizzati devono essere distrutti o resi inutilizzabili, controllo sulla non recuperabilità delle informazioni precedentemente contenute		sempre	22

Tabella 12 - Elenco delle verifiche previste per il trattamento senza l'ausilio di strumenti elettronici

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

MISURE DA VERIFICARE	DESCRIZIONE MISURA	Tipologia dei dati	CADENZA	Riferimento nel Disciplinare tecnico
Istruzioni scritte	Finalizzate al controllo e custodia dei documenti		sempre	27
Profili di autorizzazione	Individuazione dell'ambito del trattamento consentito agli incaricati, individuati anche per classi omogenee		1 anno	27
Procedure di controllo e custodia	Al fine di non consentire l'accesso a persone prive di autorizzazione	Dati sensibili e giudiziari	sempre	28
Accesso controllato agli archivi	Le persone ammesse dopo l'orario di chiusura devono essere identificate e registrate	Dati sensibili e giudiziari	sempre	29
Autorizzazione preventiva all'accesso	qualora gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di incaricati alla vigilanza	Dati sensibili e giudiziari	sempre	29