



COMUNE DI SANT'AGOSTINO

Provincia di Ferrara

DOCUMENTO PROGRAMMATICO

SULLA SICUREZZA

*Il presente documento è predisposto in attuazione del punto 19 del
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
del*

*CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(Decreto legislativo 30 giugno 2003, n. 196)*

Indice del documento.

1.	SCOPO	3
2.	CAMPO DI APPLICAZIONE.....	3
3.	PRINCIPALI RIFERIMENTI LEGISLATIVI	3
4.	COMPOSIZIONE DEL DOCUMENTO	3
5.	I COMPITI DELLE SINGOLE FIGURE A PROTEZIONE DEI DATI PERSONALI.....	4
5.1	IL TITOLARE DEL TRATTAMENTO	4
5.2	IL RESPONSABILE DEL TRATTAMENTO	5
5.3	GLI INCARICATI DEL TRATTAMENTO	6
5.4	L'AMMINISTRATORE DI SISTEMA	6
6.	DATI AFFIDATI AD ENTI ESTERNI PER IL TRATTAMENTO DEI DATI all'esterno alla struttura	7
6.1	TRATTAMENTO DEI DATI AFFIDATI ALL'ESTERNO ALLA STRUTTURA	7
6.2	CRITERI PER LA SCELTA DEGLI ENTI TERZI PER IL TRATTAMENTO DEI DATI ALL'ESTERNO ALLA STRUTTURA	7
6.3	NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI ALL'ESTERNO ALLA STRUTTURA.....	7
7.	IDENTIFICAZIONE DELLE RISORSE DA PROTEGGERE	8
7.1	LUOGHI FISICI.....	8
7.2	RISORSE HARDWARE.....	8
7.3	RISORSE SOFTWARE.....	8
7.4	RISORSE DATI.....	8
8.	SISTEMA INFORMATIVO	18
9.	ANALISI DEI RISCHI.....	18
9.1	ANALISI DEI RISCHI SUI LUOGHI FISICI	20
9.2	ANALISI DEI RISCHI SULLE RISORSE HARDWARE	21
9.3	ANALISI DEI RISCHI SULLE RISORSE SOFTWARE.....	21
9.4	ANALISI DEI RISCHI SULLE RISORSE DATI	22
10.	MISURE DI SICUREZZA	22
10.1	MISURE DI SICUREZZA DI TIPO FISICO ADOTTATE.....	22
10.2	MISURE DI SICUREZZA DI TIPO LOGICO ADOTTATE	24
10.3	MISURE DI SICUREZZA DI TIPO ORGANIZZATIVO ADOTTATE	25
11.	CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI	26
11.1	SALVATAGGIO REGOLARE DEI DATI	26
11.2	PROCEDURE PER L'ARCHIVIAZIONE DEI SUPPORTI DI MEMORIZZAZIONE	26
11.3	PROCEDURE PER LA VERIFICA DELLA LEGGIBILITÀ DEI SUPPORTI DI MEMORIZZAZIONE	26
11.4	CRITERI PER L'ELIMINAZIONE DEI SUPPORTI DI MEMORIZZAZIONE OBSOLETI	26
11.5	MISURE PER LA CUSTODIA DEI SUPPORTI DI MEMORIZZAZIONE.....	26
11.6	PIANO DI CONTINUITÀ OPERATIVA	26
12.	PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI.....	27
13.	PERIODICITÀ DI REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	27

1. SCOPO

Il presente Documento Programmatico Sulla Sicurezza è adottato, in base alle disposizioni di cui al punto 19 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (nel seguito denominato più semplicemente DISCIPLINARE TECNICO) del CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (nel seguito denominato più semplicemente CODICE), per definire le politiche di sicurezza in materia di trattamento di dati personali, ed i criteri organizzativi per la loro attuazione.

In particolare nel Documento Programmatico Sulla Sicurezza vengono definiti i criteri tecnici e organizzativi per:

- a) la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
- b) i criteri e le procedure per assicurare l'integrità dei dati;
- c) i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
- d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

2. CAMPO DI APPLICAZIONE

Il Documento Programmatico Sulla Sicurezza, in raccordo con il Decreto legislativo 30 giugno 2003 n. 196, adottato dal COMUNE DI SANT'AGOSTINO, e del quale si richiamano tutte le definizioni e disposizioni, 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:

- Sensibili
- Giudiziari
- Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Il Documento Programmatico Sulla Sicurezza deve essere conosciuto ed applicato da tutti gli Uffici del COMUNE DI SANT'AGOSTINO.

3. PRINCIPALI RIFERIMENTI LEGISLATIVI

- CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, n. 174 - Supplemento ordinario n. 123/L)
- DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Allegato B)

4. COMPOSIZIONE DEL DOCUMENTO

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un Documento Programmatico Sulla Sicurezza contenente idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

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

Al fine di recepire completamente lo spirito con cui è stato varato il CODICE, il COMUNE DI SANT'AGOSTINO ha elaborato il seguente Documento Programmatico Sulla Sicurezza (nel seguito denominato più semplicemente DPSS), che testimonia lo sforzo fatto dall'Ente al fine di garantire la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.

Il documento parte innanzitutto dalla **Identificazione delle Risorse da proteggere**, risorse che hanno impatti con i problemi di sicurezza e svolgono un ruolo significativo nei processi di trattamento dei dati personali. L'**analisi dei Rischi** costituisce un punto fondamentale per affrontare in maniera definita e controllata le problematiche di sicurezza; rappresenta l'attività di raccolta ed analisi delle debolezze e lacune del rispetto del Codice all'interno dell'Ente. Successivamente all'analisi dei Rischi, si sono definite le **misure di sicurezza** (organizzative, fisiche e logiche) adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.

Vengono successivamente elencati i **criteri e le modalità per il ripristino dei dati** in caso di perdita dei dati dovuta, ad esempio, ad un guasto.

E' previsto un **Piano di Formazione degli Incaricati** per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni al sistema di elaborazione e gestione logica dei dati.

5. I COMPITI DELLE SINGOLE FIGURE A PROTEZIONE DEI DATI PERSONALI

5.1 IL TITOLARE DEL TRATTAMENTO

Il CODICE istituisce la figura del Titolare, identificandolo nella persona fisica, nella persona giuridica, nella pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali contenuti nelle banche dati del COMUNE DI SANT'AGOSTINO è il COMUNE DI SANT'AGOSTINO rappresentato nella persona del Sindaco pro-tempore del Comune stesso.

Il Titolare è responsabile di tutti gli adempimenti, non delegabili, relativi alle notificazioni al Garante, alle procedure di autorizzazione da parte del Garante, alla nomina dei Responsabili.

Il Titolare del trattamento affida ai Responsabili del trattamento dei dati il compito di porre in essere ogni misura tesa a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previa idonee istruzioni fornite con ogni mezzo ritenuto più idoneo.

Il Titolare del trattamento affida ai singoli Responsabili del trattamento l'onere di individuare, nominare ed indicare per iscritto uno o più Incaricati del trattamento.

5.2 IL RESPONSABILE DEL TRATTAMENTO

Il Responsabile è la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposto dal Titolare al Trattamento.

Sono considerati Responsabili del trattamento dei dati personali del COMUNE DI SANT'AGOSTINO i Responsabili di settore esistenti nelle articolazioni organizzative, ciascuno per il settore di competenza, che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo della sicurezza.

Il Responsabile del trattamento dei dati:

- Individua, nomina ed indica per iscritto uno o più Incaricati del trattamento;
- Redige ed aggiorna l'elenco dei propri Incaricati;
- Provvede, sulla base delle direttive impartite dal Titolare, ad attuare il trattamento o a dare istruzioni per il corretto trattamento dei dati personali eseguendo a tal fine gli opportuni controlli;
- Redige ed aggiorna ogni variazione dell'elenco delle tipologie dei trattamenti effettuati;
- Adotta le misure e dispone gli interventi necessari per la sicurezza della conservazione dei dati e per la correttezza dell'accesso;
- Cura i rapporti con gli interessati che esercitano i diritti di cui all'art.7 del CODICE;
- Informa il Titolare nella eventualità che si siano rilevati dei rischi;
- Collabora con il Titolare a predisporre le notificazioni iniziali e le eventuali e successive variazioni verificando l'esattezza e completezza dei contenuti.

I Responsabili del trattamento custodiscono gli elenchi e le lettere di incarico degli Incaricati nei rispettivi uffici in armadi chiusi a chiave.

Come previsto dal Codice, periodicamente almeno una volta all'anno, ogni Responsabile effettua la verifica delle condizioni di sussistenza dei profili di autorizzazione degli Incaricati che sono stati da lui nominati.

La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati, anche senza preavviso.

5.3 GLI INCARICATI DEL TRATTAMENTO

Ai Responsabili del trattamento è affidato il compito di nominare uno o più Incaricati del trattamento dei dati. La nomina di ciascun Incaricato del trattamento dei dati deve essere effettuata con atto scritto in cui sono specificati i compiti affidati, unitamente ad idonee ed analitiche istruzioni scritte.

Nel designare gli Incaricati del trattamento per iscritto e nell'impartire le istruzioni, il Titolare o il Responsabile, deve prescrivere che gli Incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.

Ad ogni incaricato va assegnata una parola chiave ed un codice identificativo personale. La nomina degli Incaricati decade per revoca o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

5.4 L'AMMINISTRATORE DI SISTEMA

Nonostante il CODICE non preveda più la figura dell'Amministratore di Sistema, il COMUNE DI SANT'AGOSTINO ritiene utile, in relazione alla complessità organizzativa dell'Ente, mantenerne la presenza per i trattamenti dei dati svolti con l'ausilio di strumenti elettronici.

Si intende per Amministratore di Sistema il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo degli elaboratori della rete e di consentirne l'utilizzazione.

L'Amministratore di Sistema del COMUNE DI SANT'AGOSTINO è individuato con apposito provvedimento del Sindaco.

E' compito dell'Amministratore di sistema:

- Curare l'applicazione delle misure di sicurezza e loro aggiornamenti;
- Attivare le credenziali di autenticazione agli Incaricati del trattamento, su indicazione del Responsabile del trattamento, per tutti i trattamenti effettuati con l'utilizzo di strumenti informatici;
- Disattivare i Codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore (in collaborazione con il Responsabile del Trattamento), oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 mesi;
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi;
- Conservare ed aggiornare gli elenchi delle risorse hardware e software di cui ai successivi paragrafi 7.2 e 7.3;
- Verificare periodicamente che l'aggiornamento automatico dei programmi antivirus avvenga regolarmente;
- Effettuare giornalmente il backup dei dati;
- Curare l'applicazione delle misure che costituiscono il "Piano di continuità operativa"
- Avanzare proposte di miglioramento generale del livello di sicurezza del sistema informativo.

6. DATI AFFIDATI AD ENTI ESTERNI PER IL TRATTAMENTO DEI DATI ALL'ESTERNO ALLA STRUTTURA

6.1 TRATTAMENTO DEI DATI AFFIDATI ALL'ESTERNO ALLA STRUTTURA

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, nominandoli Responsabili del trattamento.

In caso di trattamento dei dati affidati all'esterno della struttura:

- Se i soggetti terzi vengono nominati Responsabili, allora debbono essere specificati:
 - i soggetti interessati,
 - i luoghi dove fisicamente avviene il trattamento dei dati stessi
 - i Responsabili del trattamento
 - il tipo di trattamento effettuato
- Se i soggetti terzi non vengono espressamente nominati Responsabili del trattamento, i soggetti terzi devono intendersi autonomi titolari del trattamento (ai sensi dell'art. 28 del CODICE) e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

E' compito del Titolare del trattamento , attraverso la collaborazione dei responsabili interni, redigere e aggiornare, ad ogni variazione, l'elenco dei soggetti terzi che effettuano il trattamento dei dati in qualità di Responsabile del trattamento.

L'elenco dei soggetti terzi che effettuano il trattamento dei dati in qualità di Responsabile del trattamento deve essere conservato in luogo sicuro.

6.2 CRITERI PER LA SCELTA DEGLI ENTI TERZI PER IL TRATTAMENTO DEI DATI ALL'ESTERNO ALLA STRUTTURA

Il Titolare del trattamento può nominare Responsabile del trattamento dei dati all'esterno della struttura quei soggetti terzi che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento.

Il Responsabile del trattamento dei dati all'esterno della struttura deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dal CODICE e dal DISCIPLINARE TECNICO.

6.3 NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI ALL'ESTERNO ALLA STRUTTURA

Per ogni trattamento affidato ad un soggetto esterno nominato Responsabile del trattamento, il Titolare del trattamento deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

Il Responsabile esterno effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento e delle proprie istruzioni.

Il Responsabile esterno deve accettare la nomina, controfirmando per accettazione l'apposito modulo; copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

7. IDENTIFICAZIONE DELLE RISORSE DA PROTEGGERE

Le risorse coinvolte nel trattamento dei dati personali sono state divise in alcune categorie:

- **Luoghi Fisici.** Sono stati analizzati fisicamente tutti i luoghi in cui si svolge il trattamento dati, i luoghi ove si trovano i sistemi di elaborazione, i luoghi in cui sono conservati i dati.
- **Risorse hardware.** Sono state analizzate le apparecchiature elettroniche e i dispositivi utilizzati per la trasmissione e la comunicazione dei dati coinvolti nelle operazioni di trattamento e gli strumenti per consentire la conservazione e l'integrità dei dati.
- **Risorse software.** Sono stati analizzati i software applicativi mediante i quali vengono effettuati i trattamenti automatizzati.
- **Risorse dati.** Sono stati analizzati tutti gli archivi contenenti dati personali trattati siano essi in formato cartaceo che in formato elettronico.

7.1 LUOGHI FISICI.

I luoghi fisici in cui avvengono i trattamenti sono i seguenti:

- **MUNICIPIO** Piazza Marconi n. 2, SANT'AGOSTINO
- **ASILO NIDO** Corso Roma n. 1, SANT'AGOSTINO
- **CASA PROTETTA** Via Verdi n. 72, DOSSO
- **POLIZIA MUNICIPALE** Via Statale n. 142, SANT'AGOSTINO
- **MAGAZZINO COMUNALE** Via Campo Sportivo n. 5, SANT'AGOSTINO
- **BIBLIOTECA COMUNALE** Via Statale n. 191, SANT'AGOSTINO

7.2 RISORSE HARDWARE.

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle risorse hardware con cui viene effettuato il trattamento dei dati.

L'elenco delle risorse hardware è conservato, in luogo sicuro, a cura dell'Amministratore di sistema (codice documento:ALLEGATO 1)

7.3 RISORSE SOFTWARE

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle risorse software con cui viene effettuato il trattamento dei dati.

L'elenco delle risorse software è conservato, in luogo sicuro, a cura dell'Amministratore di sistema (codice documento:ALLEGATO 2).

7.4 RISORSE DATI

UFFICIO	BANCA DATI	MODALITÀ DI TRATTAMENTO	FINALITÀ DI INTERESSE PUBBLICO PERSEGUITO	DATI SENSIBILI E DATI GIUDIZIARI TRATTATI	TIPO DI OPERAZIONI ESEGUIBILI	
					TIPO DI TRATTAMENTO INTERNO	TIPO DI TRATTAMENTO ESTERNO

Sportello unico	Ascensori e montacarichi	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale DPR 162/99	Nessuno	Registrazione conservazione	Comunicazione DPR 162/99
	Agenzie d'affari, sostanze zuccherine, facchini, mestieri girovaghi, portieri, custodi	Cartaceo	Attività istituzionali DPR 311/2001	Giudiziari	Conservazione	Nessuno
	Attività di panificazione, attività artigianali	Cartaceo	Attività istituzionali DPR 327/80 1002/56	Nessuno	Registrazione conservazione	Comunicazione DPR 327/80 Regol. Comunale di Igiene
	Attività commerciali relative a edicole e rivendite di giornali	Cartaceo	Attività istituzionali L416/91 D lgs 170/01 Delib. G. Reg. 183/02	Giudiziari	Conservazione	Nessuno
	Attività commerciali di barbiere, parrucchiere ed estetiste	Cartaceo	Attività istituzionali L. 1/90 L.R. 12/93	Nessuno	Conservazione Modificazione	Comunicazione Regol. Comunale
	Pratiche per il rilascio di contributi comunali su finanziamenti alle imprese	Cartaceo	Benefici economici e abilitazioni. Regolamento comunale	Sensibili e Giudiziari	Registrazione conservazione elaborazione	Comunicazione Regol. Comunale
	Pratiche per autorizzazioni uso gas tossici	Cartaceo	Attività istituzionali R.D. 147/27	Giudiziari	Conservazione Modificazione	Comunicazione R.D. 147/27
	Pratiche per il rilascio di licenze noleggio trasporti con/senza conducente, trasporto scolastico	Cartaceo	Attività istituzionali DPR 480/01 L. 278/03	Giudiziari	Registrazione conservazione	Comunicazione DPR 481/01
	Produttori vitivinicoli	Cartaceo	Attività istituzionali Disposizioni annuali	Nessuno	Conservazione	Comunicazione Disposizioni annuali
	Commercio in sede fissa, su aree pubbliche. Esercizi di somministrazione di alimenti e bevande	Cartaceo e Informatico	Attività istituzionali D. lgs. 114/98 L. R. 12/99 L. R. 14/99 DPR 616/77 RD 773/31 DPR 311/01 LR 14/2003	Giudiziari	Registrazione conservazione	Comunicazione L. 310/93

	Pratiche per il rilascio di autorizzazioni sanitarie e pareri igienico-sanitari	Cartaceo	Attività istituzionali L. 327/80 Regolamento comunale	Nessuno	Registrazione conservazione	Comunicazione Regolamento comunale
	Manifestazioni locali, sagre, fiere	Cartaceo e Informatico	Attività istituzionali TULPS LR 12/2000 Regolamento comunale	Giudiziari	Conservazione Consultazione	Comunicazione TULPS LR 12/2000 Regolamento comunale
	Pratiche per il rilascio autorizzazioni per attività produttive	Cartaceo e Informatico	Attività istituzionali D. lgs. 114/98 L. R. 14/99 DPR 447/98 L.R. 14/03	Giudiziari	Registrazione conservazione	Comunicazione D. lgs. 114/98 L. R. 14/99 DPR 447/98 L.R. 14/03
Ambiente	Distribuzione chiavi per contenitore ad uso smaltimento rifiuti verdi	Informatico	Finalità in ambito amministrativo sociale	Nessuno	Conservazione	Nessuno
	Autorizzazioni scarico acque superficiali, corpo idrico	Cartaceo e Informatico	Attività istituzionali D.lgs. 152/99	Nessuno	Conservazione	Comunicazione D.lgs. 152/99
	Autorizzazioni emissioni in atmosfera	Cartaceo e Informatico	Attività istituzionali L.203/88	Nessuno	Conservazione	Comunicazione L.203/88
	Autorizzazioni abbattimento/potatura alberi	Cartaceo e Informatico	Attività istituzionali Regolamento del verde	Nessuno	Conservazione	Nessuno
	Associazioni ambientali	Cartaceo e Informatico	Attività istituzionali Regolamento consulta ambiente	Nessuno	Conservazione	Nessuno
	Comprensorio Panfilia - Bisana	Cartaceo e Informatico	Attività istituzionali Convenzione Panfilia – Bisana n° 18016/02	Nessuno	Conservazione	Comunicazione Convenzione Panfilia – Bisana n° 18016/02
	Urbanistica	Concessioni e autorizzazioni edilizie	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale L. 10/77 L. 47/35 L.R. 31/02	Nessuno	Registrazione conservazione consultazione
	Contributi per abbattimento di barriere architettoniche	Cartaceo	Finalità in ambito amministrativo e sociale L. 13/89	Sensibili	Conservazione	Comunicazione L. 13/89

	Notifiche atti notarili compravendita immobili	Cartaceo	Attività istituzionali L. 47/85	Nessuno	Conservazione	Nessuno
	Richieste di ricongiungimento familiare	Cartaceo	Cittadinanza, immigrazione e condizione dello straniero L. 40/98	Nessuno	Conservazione	Comunicazione L. 40/98
	Certificati di conformità degli impianti elettrici ed idraulici	Cartaceo	Attività di controllo e ispettive L. 46/90	Nessuno	Conservazione	Nessuno
	Insegne pubblicitarie	Cartaceo	Attività istituzionali Regolamento comunale	Nessuno	Conservazione	Nessuno
	Anagrafe cimiteriale	Cartaceo	Attività istituzionali DPR 285/90	Nessuno	Conservazione	Nessuno
	Opere in cemento armato o acciaio	Cartaceo	Attività istituzionali L. 1086/71 DPR 425/94	Nessuno	Registrazione Conservazione	Comunicazione L. 1086/71 DPR 425/94
	Certificati di destinazione urbanistica	Cartaceo	Attività istituzionali L. 47/85	Nessuno	Conservazione	Comunicazione L. 47/85
Anagrafe	Carte d'identità	Cartaceo e informatico	Finalità di pubblica sicurezza R.D. 773/31 R.D. 635/40	Sensibili	Registrazione Conservazione Elaborazione	Comunicazione R.D. 635/40
	Stato civile	Cartaceo e informatico	Finalità in ambito amministrativo e sociale DPR 396/00	Sensibili	Registrazione Conservazione Elaborazione Modificazione Utilizzo Consultazione	Comunicazione D.lgs 322/89 L.91/92 L.127/97 Art. 605 c.p.c.
	Anagrafe residenti, pensionati, cittadini stranieri	Cartaceo e informatico	Finalità in ambito amministrativo e sociale L. 1228/54 DPR 223/89 L. 470/88 L. 903/65	Nessuno	Registrazione Conservazione Elaborazione Modificazione Utilizzo Consultazione	Comunicazione DPR 394/99 D.M. 18/12/2000 L. 470/88 L. 903/65
	Anagrafe italiani residenti all'estero	Cartaceo e informatico	Finalità in ambito amministrativo e sociale L. 470/88	Nessuno	Registrazione Conservazione Elaborazione Modificazione Utilizzo Consultazione	Comunicazione L. 470/88
Segreteria	Elenco Consiglieri e Assessori	Cartaceo e informatico	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi DPR 570/60	Sensibili	Registrazione Conservazione Consultazione	Comunicazione Diffusione DPR 570/60

Dichiarazione redditi Consiglieri	Cartaceo	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi Statuto comunale	Nessuno	Conservazione Consultazione	Comunicazione Diffusione Statuto comunale
Autorizzazioni cimiteriali	Cartaceo	Funzioni istituzionali DPR 285/90	Nessuno	Registrazione Conservazione Consultazione	Nessuno
Contratti e convenzioni Modelli GAP	Cartaceo e informatico	Finalità in ambito amministrativo e sociale Attività di controllo e ispettive L. 726/82 L. 410/91	Nessuno	Registrazione Conservazione Consultazione	Comunicazione L. 726/82 L. 410/91
Protocollo	Cartaceo e informatico	Finalità in ambito amministrativo e sociale DPR 445/00	Sensibili	Registrazione Conservazione Consultazione Selezione	Nessuno
Delibere e determine	Cartaceo e informatico	Finalità in ambito amministrativo e sociale D.lgs 267/00	Sensibili Giudiziari	Conservazione	Comunicazione Diffusione D.lgs 267/00
Obiettori di coscienza	Cartaceo e informatico	Volontariato e obiezione di coscienza L. 230/98	Sensibili	Registrazione Conservazione Consultazione Organizzazione Utilizzo Selezione	Comunicazione L. 230/98
Deposito atti giudiziari	Cartaceo	Attività sanzionatorie e di tutela art. 140 C.P.C.	Giudiziari	Registrazione Conservazione	Comunicazione art. 140 C.P.C.
Registro notifiche	Cartaceo	Funzioni istituzionali	Sensibili Giudiziari	Registrazione Conservazione Consultazione Utilizzo	Comunicazione Funzioni istituzionali
Elenco debitori	Cartaceo	Materia tributaria e doganale DPR 600/73	Nessuno	Utilizzo	Diffusione DPR 600/73
Ordinanze	Cartaceo	Attività sanzionatorie e di tutela Finalità in ambito amministrativo e sociale D.lgs. 267/00	Sensibili	Conservazione Consultazione	Comunicazione In funzione dell'ordinanza
Decreti del Sindaco e del Segretario	Cartaceo e informatico	Finalità in ambito amministrativo e sociale D.lgs. 266/00	Nessuno	Conservazione Consultazione	Comunicazione Funzioni istituzionali

Leva	Liste di leva	Cartaceo e informatico	Finalità in ambito amministrativo e sociale Esercizio dei diritti politici e pubblicità dell'attività di determinati organi DPR 237/64 L. 269/91	Sensibili	Registrazione Conservazione Elaborazione Organizzazione Utilizzo	Comunicazione Diffusione DPR 237/64 L. 191/75
	Ruoli matricolari	Cartaceo	Finalità in ambito amministrativo e sociale Esercizio dei diritti politici e pubblicità dell'attività di determinati organi Regol. Reg. 1133/42 Circ. Min. 487/29	Sensibili	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Modificazione	Comunicazione Regol. Reg. 1133/42 Circ. Min. 487/29
Elettorale	Giudici popolari	Cartaceo e informatico	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi L. 287/51	Giudiziari	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Modificazione Selezione	Comunicazione Diffusione L. 287/51
	Liste e schedari elettorali	Cartaceo e informatico	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi Finalità in ambito amministrativo e sociale T.U. 223/67 Circ. 2600/L del 1986	Giudiziari	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Modificazione Selezione	Comunicazione T.U. 223/67 Circ. 2600/L del 1986
	Propaganda elettorale	Cartaceo e informatico	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi Finalità in ambito amministrativo e sociale L. 212/56 L. 130/75 Circ. 1943/V del 1980	Sensibili	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Consultazione Selezione	Comunicazione L. 212/56 L. 130/75 Circ. 1943/V del 1980

	Albo scrutinatori e presidenti di seggio	Cartaceo e informatico	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi L. 120/99 L. 53/90	Sensibili	Registrazione Conservazione Elaborazione Organizzazione Utilizzo Consultazione Selezione Modificazione	Comunicazione L. 120/99 L. 53/90
	Liste di candidati Sottoscrittori referendum Proposte di legge	Cartaceo	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi T.U. 223/67	Sensibili	Registrazione Conservazione	Comunicazione T.U. 223/67
Relazioni con il pubblico	Elenco utenti Segnalazioni dei Cittadini	Cartaceo e informatico	Finalità in ambito amministrativo e sociale Regol. URP art.18	Nessuno	Registrazione Conservazione Elaborazione Consultazione	Comunicazione Ad Enti competenti
	Elenco Associazioni	Cartaceo e informatico	Finalità in ambito amministrativo e sociale	Nessuno	Raccolta	Diffusione su sito comunale previo consenso informato dell'interessato
	Raccolta firme per Referendum	Cartaceo	Esercizio dei diritti politici e pubblicità dell'attività di determinati organi Finalità in ambito amministrativo e sociale L. 352/70 Regol. URP art. 3. c. 2	Sensibili	Raccolta	Comunicazione L. 352/70 Regol. URP art. 3. c. 2
LLPP	Appaltatore opere pubbliche e soggetti partecipanti alle gare	Cartaceo e informatico	Attività di controllo e ispettive L. 109/94	Giudiziari	Raccolta Conservazione Organizzazione	Comunicazione L. 109/94
	Anagrafe utenti servizio luci votive	Cartaceo e informatico	Attività di controllo e ispettive Del. Cons. Com. 6/03	Nessuno	Raccolta Conservazione Organizzazione Utilizzo Selezione	Comunicazione Del. Cons. Com. 6/03
Ragioneria	Anagrafe tributaria	Cartaceo e informatico	Materia tributaria e doganale Prevista dal diritto tributario comunale	Nessuno	Registrazione Conservazione Modificazione Organizzazione Elaborazione Utilizzo Selezione	Nessuno

	Archivio creditori / debitori	Cartaceo e informatico	Finalità in ambito amministrativo e sociale D.lgs 267/2000	Sensibili	Conservazione Modificazione Organizzazione Consultazione Utilizzo Selezione	Comunicazione D.lgs 267/2000
	Personale dipendente, amministratori, collaboratori	Cartaceo e informatico	Finalità in ambito amministrativo e sociale D.lgs 267/2000	Sensibili Giudiziari	Modificazione Organizzazione Consultazione Utilizzo	Nessuno
Polizia Municipale	Autorizzazioni per l'esercizio della pesca e dell'attività venatoria	Cartaceo	Finalità in ambito amministrativo e sociale DPR 616/77	Nessuno	Conservazione Modificazione Organizzazione Consultazione	Comunicazione DPR 616/77
	Comunicazione cessione fabbricati	Cartaceo	Cittadinanza, immigrazione e condizione dello straniero L. 191/78	Sensibili	Registrazione Conservazione	Comunicazione L. 191/78
	Cittadini extracomunitari assunti da ditte locali	Cartaceo	Cittadinanza, immigrazione e condizione dello straniero Attività di controllo e ispettive Attività sanzionatorie e di tutela D.lgs 50/48 D.lgs 286/98	Sensibili	Conservazione Organizzazione Selezione	Comunicazione D.lgs 50/48 D.lgs 286/98
	Contrassegni per invalidi	Cartaceo	Finalità in ambito amministrativo e sociale art.188 C.d.S.	Sensibili	Registrazione Conservazione Organizzazione	Nessuno
	Soggetti destinatari di atti amministrativi a seguito di violazioni varie	Cartaceo	Attività di controllo e ispettive Attività sanzionatorie e di tutela C.P.P. C.d.S. T.U.L.P.S.	Sensibili Giudiziari	Registrazione Conservazione	Comunicazione C.P.P. C.P.
	Dati anagrafici e di residenza	Cartaceo e Informatico	Attività di controllo e ispettive Attività sanzionatorie e di tutela Finalità in ambito amministrativo e sociale art. 201 C.d.S.	Nessuno	Registrazione Conservazione Elaborazione Modificazione Organizzazione Consultazione	Comunicazione art. 206 C.d.S.

Sociale	Richiedenti e assegnatari uso centri civici Sala riunioni San Carlo	Cartaceo	Funzioni istituzionali Regolamento per uso centri civici	Sensibili	Registrazione Conservazione Organizzazione Utilizzo	Nessuno
	Richiedenti assegni maternità, nucleo familiare, secondo figlio	Cartaceo e Informatico	Benefici economici e abilitazioni L. 448/98 L. 326/2003	Nessuno	Registrazione Conservazione Organizzazione Utilizzo Elaborazione	Comunicazione L. 448/98 L. 326/2003
	Albo beneficiari contributi	Cartaceo e Informatico	Benefici economici e abilitazioni DPR 118/2000	Nessuno	Conservazione Organizzazione Utilizzo Elaborazione	Diffusione DPR 118/2000
	Richiedenti contributo fondo sociale affitto	Cartaceo e Informatico	Benefici economici e abilitazioni L.R. 24/2001	Nessuno	Registrazione Conservazione Organizzazione Utilizzo Elaborazione	Comunicazione L.R. 24/2001
	Richiedenti e assegnatari edilizia residenziale pubblica	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale L.R. 24/2001	Nessuno	Registrazione Conservazione Organizzazione Utilizzo Elaborazione	Comunicazione Diffusione Regolamento assegnazione alloggi E.R.P.
	Richiedenti indennità di accompagnamento	Cartaceo e Informatico	Benefici economici e abilitazioni L. 388/2000	Sensibili	Conservazione Organizzazione Utilizzo Consultazione	Comunicazione L. 388/2000
	Partecipanti vacanze anziani	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale	Nessuno	Registrazione Conservazione Organizzazione Utilizzo Elaborazione	Comunicazione previo consenso informato dell'interessato
	Appaltatori servizi vari	Cartaceo	Finalità in ambito amministrativo e sociale Regolamento per la disciplina dei contratti L. 726/82 L. 410/91	Giudiziari	Registrazione Conservazione Organizzazione Utilizzo	Comunicazione L. 726/82 L. 410/91
	Appaltatore servizio pubblico e soggetti partecipanti alle gare	Cartaceo	Finalità in ambito amministrativo e sociale L. 726/82 L. 410/91	Giudiziari	Registrazione Conservazione Organizzazione Utilizzo Organizzazione	Comunicazione L. 726/82 L. 410/91
Casa Protetta	Utenti servizio casa protetta	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale Regolamento casa protetta	Nessuno	Registrazione Conservazione Organizzazione Utilizzo	Comunicazione Convenzione con USL per rimborso oneri sanitari
	Piani assistenziali e verifiche ospiti casa protetta	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale Dir. Reg. 1378/99	Sensibili	Registrazione Conservazione Utilizzo	Comunicazione Dir. Reg. 1378/99

Sport	Utilizzatori palestre e impianti sportivi	Cartaceo e Informatico	Attività sportive Regolamento per utilizzo palestre e impianti sportivi comunali	Nessuno	Registrazione Conservazione Organizzazione Utilizzo Elaborazione Selezione	Comunicazione Regolamento per utilizzo palestre e impianti sportivi comunali
	Associazioni sportive	Cartaceo	Attività sportive Regolamento concessione impianti sportivi	Nessuno	Conservazione Utilizzo	Nessuno
Biblioteca	Utenti servizio e utenti servizio Internet	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale Regolamento biblioteca	Nessuno	Registrazione Conservazione Utilizzo	Nessuno
Cultura	Associazioni culturali, ricreative, ecc. ed elenco invitati a manifestazioni	Cartaceo e Informatico	Attività ricreative e culturali	Nessuno	Registrazione Conservazione Utilizzo	Nessuno
	Richiedenti uso sala convegni	Cartaceo	Funzioni istituzionali Regolamento per uso centri civici	Sensibili	Registrazione Conservazione Organizzazione Utilizzo	Nessuno
Sanitario	Trattamento sanitario obbligatorio	Cartaceo	Finalità in ambito amministrativo e sociale L. 833/78	Sensibili	Registrazione Conservazione Organizzazione Utilizzo Elaborazione	Comunicazione L. 833/78
	Denunce infortuni sul lavoro	Cartaceo	Finalità in ambito amministrativo e sociale DPR 1124/65	Sensibili	Registrazione Conservazione Utilizzo	Comunicazione DPR 1124/65
	Anagrafe canina	Cartaceo e Informatico	Attività di controllo e ispettive L.R. 27/2000	Nessuno	Registrazione Conservazione Utilizzo Selezione Consultazione	Comunicazione L.R. 27/2000
Istruzione	Utenti asilo nido	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale Regolamento asilo nido	Sensibili	Registrazione Conservazione Utilizzo Selezione Consultazione	Nessuno
	Alunni fruitori mensa scolastica	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale Regolamento per i servizi di mensa e trasporto	Sensibili	Registrazione Conservazione Utilizzo Selezione Consultazione	Comunicazione Regolamento per i servizi di mensa e trasporto

Alunni fruitori trasporto scolastico	Cartaceo e Informatico	Finalità in ambito amministrativo e sociale Regolamento per i servizi di mensa e trasporto	Nessuno	Registrazione Conservazione Utilizzo Selezione Consultazione	Comunicazione Regolamento per i servizi di mensa e trasporto
Richiedenti borse di studio	Cartaceo	Benefici economici e abilitazioni L. 26/2001	Nessuno	Registrazione Conservazione Utilizzo Elaborazione	Nessuno
Richiedenti fornitura libri di testo	Cartaceo	Benefici economici e abilitazioni L. 448/98	Nessuno	Registrazione Conservazione Utilizzo Selezione Consultazione Elaborazione	Nessuno
Partecipanti corsi di nuoto	Cartaceo e Informatico	Attività sportive	Nessuno	Registrazione Conservazione Utilizzo Selezione Consultazione Elaborazione	Nessuno

8. SISTEMA INFORMATIVO

Il Sistema informativo si compone delle risorse hardware e software elencate negli allegati 1 e 2 al presente documento.

9. ANALISI DEI RISCHI

Il D. lgs. 196/2003 ha per finalità quella di garantire che “il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali”.

Sulla base di quanto prescritto da tale Codice, vengono individuati tre requisiti di sicurezza, che costituiscono il riferimento per valutare il proprio grado di corrispondenza rispetto a quanto indicato dal D. lgs. 196/2003.

I tre requisiti sono:

riservatezza: requisito specificatamente indicato nelle finalità del CODICE, si riferisce alla possibilità di intraprendere azioni in grado di proteggere i dati di natura personale e sensibile da modalità di trattamento non autorizzato che contemplano il rischio di accesso ai dati, e rientranti nelle seguenti categorie di attività specificatamente indicate dalla legge:

- raccolta,
- registrazione,
- organizzazione,
- conservazione,
- comunicazione,
- diffusione,
- selezione,

- estrazione,
- raffronto,
- interconnessione,
- utilizzo

integrità: tale requisito si riferisce alla possibilità di intraprendere azioni in grado di proteggere i dati di natura personale e sensibile da modalità di trattamento non autorizzate che contemplano il rischio di modifica delle informazioni, e rientranti nelle seguenti categorie di attività specificatamente indicate dalla Legge:

- elaborazione,
- modificazione,
- cancellazione,
- blocco,
- distruzione

disponibilità: tale requisito si riferisce alla necessità di intraprendere azioni in grado di proteggere dati di natura personale e sensibile, da possibili eventi che possono ridurre la capacità dell'azienda di assolvere alle finalità di trattamento per cui tali dati sono stati raccolti.

Tali requisiti forniscono quindi un punto di partenza per l'identificazione dei possibili attacchi, individuabili in base all'analisi dello scenario effettuata, e servono alla definizione dei criteri di protezione più adeguati a garantire tale necessità di protezione.

Per Analisi dei Rischi si intende l'attività di raccolta ed analisi delle minacce e delle vulnerabilità a cui sono soggette le risorse nel rispetto del CODICE.

Per ciascun dato è quindi necessario individuare ed analizzare i relativi rischi, anche accidentali.

Gli indici di rischio sono fissati mediante una scala semiquantitativa a 3 valori riportati nella successiva tabella.

Livello criticità	Descrizione
2	Rischio molto basso: identifica una minaccia remota e comunque rapidamente reversibile od ovviabile.
1	Rischio medio: superiore al precedente identificante una minaccia remota ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio.
0	Rischio alto: vengono individuati rischi che è sicuramente inaccettabile pensare di correre. Pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica, etc..) per abbattere il rischio e contenerlo in livelli accettabili.

9.1 ANALISI DEI RISCHI SUI LUOGHI FISICI

Controllo	Sede	Livello criticità	Misure adottate
Possibilità di intrusione / Furto	MUNICIPIO	2	<p>Durante il normale svolgimento dell'attività lavorativa, i locali sono sempre presidiati.</p> <p>Al termine dell'orario di lavoro, l'ingresso viene chiuso a chiave e i locali saranno presto protetti da un impianto d'allarme.</p> <p>Le finestre degli uffici ubicati al piano terra sono dotate di inferriate.</p> <p>I locali destinati ad ARCHIVIO non sono accessibili liberamente a tutti. Vengono tenuti chiusi a chiave e la chiave è custodita presso l'ufficio Segreteria.</p>
	ASILO NIDO	1	<p>Durante il normale svolgimento dell'attività lavorativa, i locali sono sempre presidiati.</p> <p>Al termine dell'orario di lavoro, l'ingresso viene chiuso a chiave.</p>
	CASA PROTETTA	2	<p>I locali sono sempre presidiati.</p> <p>Nelle ore notturne l'ingresso viene chiuso a chiave e i locali sono protetti da un impianto d'allarme.</p>
	POLIZIA MUNICIPALE	2	<p>Durante il normale svolgimento dell'attività lavorativa, i locali sono sempre presidiati.</p> <p>Al termine dell'orario di lavoro, l'ingresso viene chiuso da una saracinesca esterna.</p> <p>Non esistono finestre.</p>
	MAGAZZINO COMUNALE	1	<p>L'ufficio è situato al primo piano.</p> <p>L'ufficio o è presidiato o è chiuso a chiave.</p>
	BIBLIOTECA COMUNALE	2	<p>Durante il normale svolgimento dell'attività lavorativa, i locali sono sempre presidiati.</p> <p>Al termine dell'orario di lavoro, l'ingresso viene chiuso a chiave e i locali sono protetti da un impianto d'allarme collegato con le forze dell'ordine.</p> <p>Tutte le finestre al piano terra sono dotate di inferriate.</p>
Allagamenti	Tutte le sedi	2	<p>Non tutti gli elaboratori client sono sollevati da terra; questi, però, non contengono dati personali ma vengono utilizzati per accedere ai server.</p> <p>I server sono tutti sollevati da terra.</p>
Incendio	MUNICIPIO ASILO NIDO POLIZIA MUNICIPALE MAGAZZINO COMUNALE BIBLIOTECA COMUNALE	1	<p>I locali sono dotati di un idoneo numero di estintori.</p>

	CASA PROTETTA	2	I locali sono dotati di impianto antincendio con rilevatore fumi e segnalatori acustici.
Climatizzazione	MUNICIPIO	2	La sala server è dotata impianto di condizionamento ambientale, opportunamente dimensionato
Impossibilità di rilevare accessi non autorizzati	Tutte le sedi	2	Le sedi sono costantemente presidiate durante il normale svolgimento dell'attività lavorativa.
Verifica degli standard adottati	Tutte le sedi	2	Gli standard formalizzati vengono rispettati da tutti gli utenti
Impatti relativi alla Privacy	Tutte le sedi	2	Le modalità dei trattamenti avvengono nel rispetto della normativa vigente per la sicurezza fisica dei locali

9.2 ANALISI DEI RISCHI SULLE RISORSE HARDWARE

Controllo	Sede	Livello criticità	Misure adottate
Uso non autorizzato dell'hardware	Tutte le sedi	2	L'utilizzo dell'hardware è soggetto all'utilizzo di password
Manomissione/sabotaggio	Tutte le sedi	2	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici di fiducia.
Probabilità/frequenza di guasto	Tutte le sedi	2	L'hardware acquistato è di qualità e storicamente non ha mai dato problemi rilevanti.
Rischi connessi all'elettricità.	MUNICIPIO POLIZIA MUNICIPALE	2	Tutti gli elaboratori sono collegati ad un gruppo di continuità che fornisce energia di buona qualità e impedisce l'improvvisa assenza di corrente elettrica.

9.3 ANALISI DEI RISCHI SULLE RISORSE SOFTWARE

Controllo	Sede	Livello criticità	Misure adottate
Accesso non autorizzato alle basi dati connesse	Tutte le sedi	2	I software che trattano i dati controllano l'accesso tramite una finestra di autenticazione (finestra di Login).
Errori software che minacciano l'integrità dei dati	Tutte le sedi	2	I software sono utilizzati da parecchi anni e non hanno mai causato la perdita o il danneggiamento dei dati trattati
Presenza di codice non conforme alle specifiche del programma	Tutte le sedi	2	I programmi sono forniti da produttori che operano nel settore con la massima serietà da molti anni.
Aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti	Tutte le sedi	2	I programmi vengono aggiornati periodicamente, almeno ogni sei mesi.

9.4 ANALISI DEI RISCHI SULLE RISORSE DATI

Controllo	Sede	Livello criticità	Misure adottate
Accesso non autorizzato	Tutte le sedi	2	L'accesso alle risorse dati in formato elettronico avviene solo tramite gli elaboratori protetti da password. Ai documenti cartacei possono accedere solo i diretti incaricati.
Cancellazione non autorizzata di dati / manomissione di dati	Tutte le sedi	2	L'accesso agli elaboratori avviene solo tramite gli elaboratori protetti da password. Ai documenti cartacei possono accedere solo i diretti incaricati.
Perdita di dati	MUNICIPIO	2	I server hanno dischi mirrorati in alta affidabilità (tipo RAID1 o RAID5). Sono effettuate periodiche copie di backup.
Backup dei dati	Tutte le sedi	2	Il backup dei dati viene eseguito giornalmente.
Protezione da sw maligno	Tutte le sedi	2	Presente il software antivirus aggiornato giornalmente.

10. MISURE DI SICUREZZA

Al fine di assicurare

- l'integrità e la disponibilità dei dati,
- la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità ed impedirne la comunicazione e/o diffusione non autorizzata, il COMUNE DI SANT'AGOSTINO ha elaborato una precisa Politica di Sicurezza basata sull'adozione di misure di tipo fisico, logico ed organizzativo. Tali misure avranno il compito di garantire sia i minimi requisiti di sicurezza contemplati dal Codice, sia un livello idoneo di sicurezza relativamente alle tipologie dei dati trattati, alle modalità di trattamento ed agli strumenti utilizzati.

10.1 MISURE DI SICUREZZA DI TIPO FISICO ADOTTATE

Rientrano in tale categoria:

Misure di protezione delle aree e dei locali.

- MUNICIPIO

La sede sarà presto protetta da un sistema di allarme antintrusione. Durante l'orario di lavoro i locali sono costantemente presidiati dal personale.

Al termine dell'orario di lavoro, le porte di accesso vengono chiuse e nessun utente è ammesso, se non espressamente autorizzato.

I locali destinati ad ARCHIVIO non sono accessibili liberamente da tutti. Vengono tenuti chiusi a chiave e la chiave è custodita presso l'ufficio Segreteria.

In particolare, la sala server è sempre presidiata o chiusa a chiave.

- ASILO NIDO

Durante l'orario di lavoro i locali sono costantemente presidiati dal personale. Al termine dell'orario di lavoro, le porte di accesso vengono chiuse e nessun utente è ammesso, se non espressamente autorizzato.

- **CASA PROTETTA**

La sede è protetta da un sistema di allarme antintrusione. I locali sono costantemente presidiati dal personale.

Durante le ore notturne le porte di accesso vengono chiuse e nessun utente è ammesso, se non espressamente autorizzato.

- **POLIZIA MUNICIPALE**

Durante l'orario di lavoro i locali sono costantemente presidiati dal personale. Al termine dell'orario di lavoro, le porte di accesso vengono chiuse da una saracinesca esterna e nessun utente è ammesso, se non espressamente autorizzato. Non esistono finestre.

- **MAGAZZINO COMUNALE**

I locali sono presidiati o chiusi a chiave.

Durante l'orario di lavoro, i locali o sono presidiati oppure sono chiusi a chiave.

- **BIBLIOTECA COMUNALE**

La sede è protetta da un sistema di allarme antintrusione collegato con le forze dell'ordine. Durante l'orario di lavoro i locali sono costantemente presidiati dal personale.

Al termine dell'orario di lavoro, le porte di accesso vengono chiuse e nessun utente è ammesso, se non espressamente autorizzato.

Tutte le finestre al piano terra sono dotate di inferiate.

Accesso ai locali.

L'accesso del personale NON dipendente nei locali in cui vengono trattati dati personali è filtrato. Gli addetti sono tenuti ad effettuare vigilanza contro il rischio di accesso di persone non autorizzate. Al termine dell'orario di lavoro, l'accesso ai locali è consentito alle sole persone autorizzate; il personale addetto alle pulizie non ha comunque accesso a documenti contenenti dati personali.

Predisposizione di armadi non accessibili da personale non autorizzato.

Tutti i documenti cartacei contenenti dati personali (sensibili o giudiziari) sono conservati in armadi dotati di serratura. Le aree contenenti dati cartacei sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone non autorizzate e, di conseguenza, impedirne l'accesso stesso.

Misure per la protezione da accessi ai documenti cartacei

Quando gli atti e i documenti contenenti dati personali sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso alla sala server è consentito solo alle persone espressamente autorizzate. In assenza del personale autorizzato, la sala server è tenuta chiusa a chiave. L'ubicazione di stampanti ed apparecchi telefax tradizionali non consente ad esterni di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Misure di protezione da eventi di origine naturale o dolosa.

Sedi di:

- MUNICIPIO
- ASILO NIDO
- POLIZIA MUNICIPALE
- MAGAZZINO COMUNALE
- BIBLIOTECA COMUNALE

I locali sono dotati di estintori per la soppressione di focolai di incendio.

Non tutti gli elaboratori client sono sollevati da terra; questi, però, non contengono dati personali ma vengono utilizzati per accedere ai server.

I server sono tutti sollevati da terra in modo da evitare eventuali perdite di dati dovuti ad allagamenti, ecc.

Sede di:

- CASA PROTETTA

I locali sono dotati di impianto antincendio con rilevatore fumi e segnalatori acustici.

Continuità dell'alimentazione elettrica.

Sedi di:

- MUNICIPIO
- POLIZIA MUNICIPALE

Tutti gli elaboratori sono collegati ad un gruppo di continuità. Tale gruppo, garantisce stabilità alla tensione in ingresso e assicura un'autonomia temporale necessaria ad avviare le corrette procedure di spegnimento dell'elaboratore.

Climatizzazione dei locali.

La sala server è dotata impianto di condizionamento ambientale, opportunamente dimensionato.

10.2 MISURE DI SICUREZZA DI TIPO LOGICO ADOTTATE

Rientrano in tale categoria:

Misure per l'indicazione dei codici identificativi e delle parole chiave agli incaricati.

Agli incaricati saranno assegnate le credenziali di autenticazione consistenti in un codice per l'identificazione, che neppure in futuro potrà essere associato ad altre persone, unito a una parola chiave riservata conosciuta solamente dall'incaricato.

La parola chiave è composta da otto caratteri; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Agli incaricati saranno impartite le istruzioni necessarie per:

- assicurare la segretezza della componente riservata della credenziale
- custodire in modo diligente i dispositivi in possesso ed uso esclusivo dell'incaricato
- non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento
- cambiare autonomamente la componente riservata della credenziale

Misure per l'assegnazione ed autorizzazione degli elaboratori su cui effettuare i trattamenti.

Al fine di limitare l'accesso ai soli dati effettivamente necessari per effettuare le operazioni di trattamenti, ad ogni incaricato è stato assegnato un profilo di autorizzazione tramite il quale potrà accedere agli archivi in formato elettronico su cui operare i trattamenti.

Misure per la protezione da accessi accidentali ad informazioni riservate.

Ad ogni incaricato saranno assegnate le credenziali per l'autenticazione che consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.

Saranno impartite agli incaricati le istruzioni per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Misure di protezione da possibili danneggiamenti alle informazioni.

Al fine di rilevare immediatamente la presenza di codice maligno in un file, tutti gli elaboratori e i server sono dotati di programma antivirus che viene aggiornato automaticamente ogni giorno. L'Amministratore di Sistema periodicamente verifica che l'aggiornamento automatico avvenga regolarmente.

Misure di protezione da eventuali perdite di disponibilità dei dati.

L'integrità dei dati è garantita mediante idonee procedure di salvataggio periodico (backup). Detto salvataggio viene effettuato giornalmente.

Aggiornamento dei programmi software che trattano i dati personali.

Gli aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, sono effettuati almeno semestrale.

10.3 MISURE DI SICUREZZA DI TIPO ORGANIZZATIVO ADOTTATE

Rientrano in tale categoria:

Analisi dei Rischi e Documento Programmatico Sulla Sicurezza.

Sulla base dell'analisi dei rischi è stato redatto il presente documento programmatico sulla sicurezza. Il presente documento verrà rivisto ed aggiornato come previsto nel capitolo 13.

Piano di formazione degli incaricati.

E' stato predisposto un piano di formazione degli incaricati. Tale piano è illustrato nel presente DPSS al capitolo 12.

Piano di verifica delle misure adottate

La bontà delle misure adottate viene verificata periodicamente, almeno ogni sei mesi.

11. CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Al fine di assicurare il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento ed impedirne la comunicazione e/o diffusione non autorizzata, il COMUNE DI SANT'AGOSTINO ha elaborato i seguenti criteri e modalità.

11.1 SALVATAGGIO REGOLARE DEI DATI

Il salvataggio dei dati è una procedura che ricopre una funzione cruciale. Attraverso questa procedura, è possibile, in caso di guasto hardware dei dischi, "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo salvataggio.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza giornaliera.

11.2 PROCEDURE PER L'ARCHIVIAZIONE DEI SUPPORTI DI MEMORIZZAZIONE

I supporti di memorizzazione vengono etichettati con informazione per l'identificazione e conservati in cassaforte.

11.3 PROCEDURE PER LA VERIFICA DELLA LEGGIBILITÀ DEI SUPPORTI DI MEMORIZZAZIONE

I supporti di backup sono testati e verificati periodicamente con un apposito programma che verifica l'integrità dei dati registrati.

11.4 CRITERI PER L'ELIMINAZIONE DEI SUPPORTI DI MEMORIZZAZIONE OBSOLETI

I supporti rimovibili, se non utilizzati, sono distrutti o resi inutilizzabili.

Possono essere riutilizzati da altri incaricati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

11.5 MISURE PER LA CUSTODIA DEI SUPPORTI DI MEMORIZZAZIONE.

I supporti di memorizzazione utilizzati per l'attività di backup sono conservati in armadi ignifughi posti in locali distanti dalla sala server.

11.6 PIANO DI CONTINUITÀ OPERATIVA

L'obiettivo del piano di continuità operativa è quello di garantire la continuità del servizio informatico e la disponibilità delle informazioni, evitando o limitando i danni al patrimonio informativo a fronte di una emergenza.

Il piano di continuità operativa non deve essere inteso come misura alternativa a quelle di prevenzione, ma a completamento di queste ultime.

Allo scopo di gestire gli eventi critici e i disastri e garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, il COMUNE DI SANT'AGOSTINO ha adottato le seguenti misure:

- salvataggio regolare dei dati
- etichettatura dei supporti di memorizzazione con informazione per l'identificazione
- verifica dell'integrità dell'informazione memorizzata tramite apposito programma
- protezione fisica dell'accesso ai supporti di memorizzazione

- sicurezza durante il trasporto dei supporti di memorizzazione
- eliminazione dei supporti di memorizzazione e dell'informazione in essi contenuta.

12. PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Attualmente il COMUNE DI SANT'AGOSTINO prevede incontri formativi di sensibilizzazione, informazione e aggiornamento ai dirigenti, responsabili e incaricati sulla corretta modalità operativa per il trattamento dei dati e sui nuovi strumenti e /o misure di sicurezza implementati in azienda.

In particolare, sono stati previsti due moduli formativi:

Primo Modulo: Consapevolezza su sicurezza informatica e tutela dei dati

E' rivolto a tutto il personale del COMUNE DI SANT'AGOSTINO coinvolto nel trattamento dei dati personali (dirigenti, responsabili e incaricati).

Ha l'obiettivo di fornire una panoramica sul CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI e del DISCIPLINARE TECNICO, sensibilizzare i partecipanti sulle problematiche della sicurezza informatica, diffondere le politiche di sicurezza adottate dall'Ente.

Secondo Modulo: Panoramica sul "Codice in materia di protezione dei dati personali"

E' rivolto agli Amministratori e ai Responsabili del Trattamento dei Dati Personali.

L'obiettivo del modulo è quello di far conoscere agli Amministratori e ai Responsabili del COMUNE DI SANT'AGOSTINO le problematiche connesse alla tutela dei dati personali e informare gli stessi sulle opportune norme di comportamento e le relative responsabilità individuali.

Coerentemente con l'evoluzione degli strumenti tecnici adottati dal COMUNE DI SANT'AGOSTINO e/o all'insorgere di nuove disposizioni legislative in materia, nonché al momento dell'ingresso in servizio o in occasione di cambiamenti di mansioni, verranno istituiti nuovi incontri formativi. In ogni caso, almeno una volta l'anno, verrà comunque istituito un incontro per risensibilizzare gli incaricati sull'importanza di adottare le norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

13. PERIODICITÀ DI REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il Documento Programmatico Sulla Sicurezza deve essere sottoposto a revisione e aggiornato entro il 31 marzo di ogni anno. Trascorso tale termine deve essere oggetto di revisione per adeguarlo ad eventuali variazioni del livello di rischio a cui sono soggetti i dati personali e ad eventuali modifiche della tecnologia informatica.

Nell'attesa dell'adeguamento conservano validità le regole in vigore.

ALLEGATO 1)

COMUNE DI SANT'AGOSTINO

13.1 *RISORSE HARDWARE*

14. CODICE DOCUMENTO:

SCOPO DEL DOCUMENTO

Il presente documento contiene l'elenco delle risorse hardware con cui viene effettuato il trattamento dei dati.

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle risorse hardware con cui viene effettuato il trattamento dei dati, così come previsto dal Documento Programmatico Sulla Sicurezza (predisposto in attuazione del punto 19 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - Decreto legislativo 30 giugno 2003, n. 196).

ELENCO RISORSE HARDWARE

14.1.1 SEDE PRINCIPALE

Il sistema informativo è composto da:

- Un Server Dell Poweredge 1650 PIII con sistema operativo Windows Server 2000
- Un Server Compaq ML350 PIII utilizzato per l'applicazione Lotus Domino
- Un Router Zyxel "Prestige 200 series" per il collegamento a Internet
- Un Router "Centrecom AR300L" per assistenza da remoto
- Un Firewall Fortigate 60U
- 31 Personal Computer (di cui due portatili) collegati tramite rete locale con relative stampanti.

14.1.2

14.1.3 CASA PROTETTA

- Un personal computer portatile Compaq Armada con relativa stampante.

POLIZIA MUNICIPALE

- Due personal computer (collegati in rete interna) con relative stampanti;
- Un modem ISDN
- **Un firewall** in corso di installazione (pacchetto software MCAFEE)

14.1.4 MAGAZZINO COMUNALE

- Un personal computer con relativa stampante;

BIBLIOTECA COMUNALE

- Tre personal computer con relative stampanti;
- Un modem;

- Un Router per il collegamento alla Provincia per la gestione delle biblioteche tramite l'applicativo SEBINA;
- Un firewall in corso di installazione (pacchetto software MCAFEE).

ALLEGATO 2)

COMUNE DI SANT'AGOSTINO

14.2 RISORSE SOFTWARE

SCOPO DEL DOCUMENTO

Il presente documento contiene l'elenco delle risorse software con cui viene effettuato il trattamento dei dati.

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle risorse software con cui viene effettuato il trattamento dei dati, così come previsto dal Documento Programmatico Sulla Sicurezza (predisposto in attuazione del punto 19 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - Decreto legislativo 30 giugno 2003, n. 196).

14.2.1.1 *ELENCO RISORSE SOFTWARE*

- Sistemi operativi Windows 2000 o Windows XP;
- Antivirus MCAFEE (installato su tutti gli elaboratori);
- Office 2000 o in alternativa Word 2000;
- Applicativi della ditta ADS di Bologna per:
 1. Contabilità finanziaria
 2. Tributi ICI/TARSU
 3. Gestione Delibere / Determine
 4. Gestione Protocollo
 5. Servizi Demografici
 6. Lotus Notes
 7. URP / Procedimenti e pratiche L.241/90
- L'ufficio Urbanistica utilizza il programma ARCHIWIN 5.8.3 della ditta Geographis di Ferrara per le concessioni edilizie;
- L'ufficio Lavori Pubblici utilizza il programma STR della ditta Sistemi e Progetti di Ferrara (gestione progettazione lavori pubblici) e il programma AUTOCAD;
- L'ufficio Servizi Sociali utilizza il programma MS ACCESS di Castelnuovo Garfagnana (LU) per l'inventario dei beni.