

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi dell'art.19 all. B al
D.Lgs 196/2003 "Codice in materia di trattamento dei dati personali"

Introduzione:

Il presente documento riguarda il **piano operativo annuale delle misure di sicurezza** per l'anno in corso, secondo quanto previsto dal D.Lgs 196/2003 "Codice in materia di trattamento dei dati personali", allo scopo di minimizzare i rischi di distruzione, perdita anche accidentale che il trattamento dei dati personali (in particolare quelli sensibili) inevitabilmente comporta.

Contenuti del Documento Programmatico sulla Sicurezza:

Vengono elencati nell'ordine i seguenti criteri:

- A) *Criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;*
- B) *Criteri tecnici ed organizzativi per assicurare l'integrità dei dati trattati senza l'ausilio di strumenti elettronici (in forma cartacea);*
- C) *Criteri tecnici ed organizzativi per assicurare l'integrità dei dati trattati con strumenti elettronici;*
- D) *Sistema di autenticazione informatica per la sicurezza del trattamento dei dati;*
- E) *Elenco dei trattamenti di dati personali, delle banche dati e delle strutture preposte ai trattamenti;*
- F) *Trattamenti all'esterno;*
- G) *Interventi formativi;*

A) CRITERI TECNICI ED ORGANIZZATIVI PER LA PROTEZIONE DELLE AREE E DEI LOCALI INTERESSATI DALLE MISURE DI SICUREZZA, NONCHÉ LE PROCEDURE PER CONTROLLARE L'ACCESSO DELLE PERSONE AUTORIZZATE AI LOCALI MEDESIMI

1. Protezione delle aree e dei locali interessati
 - 1.1. I server sono collocati in un apposito locale (denominato *sala server*)
 - 1.2. La sala server è dotata di:
 - a) Impianto elettrico a norma;
 - b) Gruppo di continuità che permette la regolare chiusura delle operazioni in corso sul server in caso di mancanza improvvisa di energia elettrica;
 - 1.3. L'accesso alla sala server è limitato ai soli amministratori di sistema o alle persone espressamente autorizzate dagli stessi, per il tempo strettamente necessario allo svolgimento dei compiti eventualmente assegnati (es. manutenzione software e/o hardware del server).
 - 1.4. In assenza del personale autorizzato, la sala server viene mantenuta chiusa a chiave. La chiave è custodita dai Responsabili della sicurezza dei dati e di sistema.

CRITICITA':

CRITICITÀ:	MISURA DI SICUREZZA	IN PREVISIONE DAL
La sala server non è dotata di rilevatore di presenza remoto (allarme antifurto). Data la presenza di finestre, l'intrusione dall'esterno è possibile.	Estensione dell'impianto antifurto già esistente nei restanti locali comunali nell'interno della sala server.	30.9.2005

B) CRITERI TECNICI ED ORGANIZZATIVI PER ASSICURARE L'INTEGRITÀ DEI DATI TRATTATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (IN FORMA CARTACEA)

1. Conservazione dei dati personali:
 - 1.1. Le banche dati costituite in forma cartacea sono conservate presso i rispettivi uffici comunali in appositi archivi organizzati.
 - 1.2. I documenti contenenti dati personali sono custoditi in armadi ignifughi, dotati di chiusura a chiave in custodia esclusivamente al personale incaricato del trattamento;
2. Conservazione dei dati sensibili:
 - 2.1. Le banche dati contenenti dati sensibili sono conservate in cassaforte di sicurezza ubicata presso l'ufficio segreteria.
 - 2.2. In nessun caso sono riportati dati sensibili su documenti o contenitori esposti alla vista, anche involontaria, di persone non autorizzate.
3. Accesso ai locali
 - 3.1. Ogni ufficio dispone di uno o più accessi comunque dotati di chiusura a chiave. Le chiavi degli uffici sono conservate in locale non accessibile al pubblico.
 - 3.2. Le chiavi di accesso all'ufficio servizi sociali e polizia locale sono custodite esclusivamente dai responsabili, in considerazione del fatto che all'interno dei suddetti locali sono conservati dati sensibili e/o giudiziari.
 - 3.3. L'accesso agli uffici comunali è protetto da allarme antintrusione attivato e disattivato manualmente dal personale e collegato alla centrale dell'istituto di vigilanza. La sede municipale è altresì controllata esternamente dallo stesso istituto due volte ogni notte.
 - 3.4. Al di fuori dei normali orari di apertura al pubblico, l'accesso agli uffici è inibito dalla chiusura automatica (programmata) della porta principale e consentito esclusivamente dall'interno con apertura manuale oppure, dall'esterno, solo al personale comunale in possesso delle relative chiavi.
4. Protezione dei locali
 - 4.1. All'interno della sede municipale sono ubicati in posizione evidente e agevolmente raggiungibile gli estintori antincendio. Il numero e la dislocazione sono conformi alla normativa in materia e la loro efficacia viene semestralmente verificata da ditta incaricata.
 - 4.2. Il piano seminterrato della sede municipale, che ospita l'archivio storico e corrente, è stato "compartimentato" a termini della normativa antincendi con apposite porte REI. All'esterno dell'edificio è inoltre presente un pulsante che permette, in caso di incendio, di togliere energia elettrica all'intera sede municipale.

CRITICITÀ':

CRITICITÀ':	MISURA DI SICUREZZA	IN PREVISIONE DAL
Il locale archivio al piano seminterrato non è dotato di rilevatore di presenza remoto (allarme antifurto). Data la presenza della porta di accesso dal corridoio di ingresso al municipio (luogo di transito), l'intrusione è possibile.	Estensione dell'impianto antifurto già esistente nei restanti locali comunali nell'interno del locale archivio.	30.9.2005

C) CRITERI TECNICI ED ORGANIZZATIVI PER ASSICURARE L'INTEGRITÀ DEI DATI TRATTATI CON STRUMENTI ELETTRONICI

1. Sicurezza del software

- 1.1. Presso ciascun ufficio è consentita l'installazione esclusiva delle seguenti categorie di software:
 - a) Software commerciale dotato di licenza d'uso (esempio: pacchetti di office automation)
 - b) Software gestionale realizzato specificatamente per l'Amministrazione Comunale dalle ditte specializzate nel settore della P.A. (es: applicativi in uso al personale)
 - c) Software gestionale realizzato specificatamente dagli organi centrali della Pubblica Amministrazione (es. Istat, INPS, Ministeri ..)
- 1.2. L'eventuale installazione di software diversi deve essere preventivamente valutata e autorizzata dai responsabili della sicurezza.
- 1.3. Al fine di prevenire ed evitare la diffusione di virus informatici, il software viene installato solo da supporti fisici originali dei quali è ben nota la provenienza.

CRITICITÀ:	MISURA DI SICUREZZA	IN PREVISIONE DAL
Le licenze di MS Office installate sui diversi PC sono state acquistate con regolare licenza d'uso, di cui alcune non sono però più reperibili in archivio e sono comunque riferite a pochi PC.	Nel corso del 2005 e 2006 verranno reperiti i fondi necessari all'acquisto delle licenze mancanti, che saranno conservate in cassaforte.	parte: 1.1.2006 parte: 31.12.2006

2. Integrità dei dati

- 2.1. Gli amministratori di sistema sono i responsabili incaricati del backup dei dati conservati sui server.
- 2.2. Sul server Windows:
 - a) Il salvataggio dei dati viene eseguito quotidianamente, ad eccezione della domenica, con procedura automatica impostata sul server per iniziare alle ore 23,00.
 - b) I dati vengono salvati su un supporto a nastro che viene inserito manualmente nel drive ogni mattina, a cura del personale. Esiste pertanto una cassetta per ogni giorno feriale.
 - c) E' inoltre previsto di predisporre una procedura giornaliera suppletiva di salvataggio su uno dei PC della rete per supplire a situazioni di guasto del sistema di salvataggio DAT su Server;
 - d) I dati salvati riguardano gli applicativi di più recente installazione presso gli uffici comunali, sia con riferimento all'ambiente di programma che con riferimento alle banche dati. La procedura di backup è configurata in modo da restituire il risultato del savataggio evidenziando eventuali file non salvati con indicazione dell'anomalia riscontrata.
 - e) Il server è dotato di un gruppo di continuità che assicura l'alimentazione elettrica in caso di perdita di energia sulla rete
 - f) Una volta alla settimana, una copia dei dati viene trasferita nella cassetta di sicurezza situata presso la tesoreria comunale (edificio separato dalla sede municipale).
 - g) Le cassette con i salvataggi quotidiani sono conservate in apposito armadio ignifugo ubicato presso l'ufficio segreteria (locale separato dal locale server).

CRITICITÀ:	MISURA DI SICUREZZA	IN PREVISIONE DAL
Il server Windows 2000 ha raggiunto il limite di disponibilità di spazio fisico ed è stato già implementato ove possibile (doppio processore, ampliamento RAM e dischi ecc.): viste le necessità degli uffici di installare nuovi applicativi e tenuto conto dell'aumento dei dati, il rischio di collasso del sistema è probabile.	Nel corso del 2005 è previsto l'acquisto di un nuovo server.	1.12.2005

2.3. Sul server Novell:

Il dispositivo DAT sul server è guasto. Vista la scarsa movimentazione di dati e ricordato che questo sistema è destinato allo spegnimento con recupero dei dati e loro ripristino sul server Windows 2000, si è adottata la procedura di cui ai punti seguenti:

- a) E' attivata una procedura giornaliera di salvataggio su uno dei PC della rete in modo da garantire maggior sicurezza e facilità di ripristino dei dati e disporre comunque di una copia per ogni giorno; la procedura viene attivata alle ore 20.00.
- b) I dati salvati riguardano gli applicativi di meno recente installazione presso gli uffici comunali (in via di dismissione) con riferimento alle sole banche dati generate o aggiornate quotidianamente. Vengono comunque salvati archivi documentali in formato Word ed Excel tuttora in uso e residenti su tale server;
- c) Le cassette con i salvataggi quotidiani sono conservate in apposito armadio ignifugo ubicato presso l'ufficio segreteria (locale separato dal locale server).

CRITICITÀ:	MISURA DI SICUREZZA	IN PREVISIONE DAL
Su alcuni PC non è previsto il salvataggio dei dati creati in locale. Questi ultimi non costituiscono comunque banche dati. E' stata valutata la possibilità di effettuare copie sul server (vedi DPS 2004) ma manca disponibilità di spazio fisico.	Nel corso del 2005 è previsto l'acquisto di un nuovo server: Verrà a quel punto effettuata nuova valutazione.	1.12.2005

2.4. In casi particolari, il backup viene effettuato localmente nell'ambito di taluni uffici. In questo caso l'incaricato effettua le seguenti operazioni:

- a) Esecuzione quotidiana del backup, eventualmente tramite procedure automatiche
- b) Copia del risultato di backup sul server allo scopo di consentirne il salvataggio quotidiano con le modalità di cui ai punti precedenti.

2.5. Ulteriori accorgimenti a tutela del trattamento di dati sensibili, consentono:

- a) il salvataggio temporaneo automatico con periodicità inferiore a 10 minuti
- b) il salvataggio eventuale su hard disk del PC con registrazione protetta da password scelta dall'utente
- c) compressione dei dati elaborati in appositi file di tipo "zip" per eventuale invio all'indirizzo e-mail noto e certo (certificato);

E' inoltre prevista, entro il 2005, l'introduzione della posta certificata e della firma elettronica sui documenti trasmessi via e-mail;

- 2.6. In caso di trattamenti di dati personali affidati all'esterno della struttura (ad es. per manutenzione delle banche dati ad opera della ditta cui è affidata l'assistenza del software) verranno adottati i seguenti criteri da adottare per garantire l'adozione delle misure minime di sicurezza:
- Ove possibile, l'invio dei dati avviene in modalità ftp con trasferimento dei dati direttamente sul sito del destinatario in forma compressa e con password;
 - Se inviati con posta elettronica, i file vengono opportunamente compressi ed inviati solo a destinatario certo e, quando possibile, a casella di posta elettronica certificata;
 - Ad ogni destinatario dei dati viene richiesta apposita dichiarazione in cui viene attestato il rispetto delle disposizioni in materia di sicurezza nel trattamento dei dati;
3. Sistema di monitoraggio
- 3.1. Attraverso apposito sistema di monitoraggio di Windows 2000 server (gestione eventi e definizione delle regole di protezione sugli oggetti) è stato realizzato un sistema di controllo e verifica della sicurezza del sistema informatico, a livello di sistema, di gestione delle basi dati e delle applicazioni.
- 3.2. Il sistema di controllo suddetto è in grado di registrare:
- gli accessi, riusciti e falliti, a livello di sistema, su tutti i file del sistema stesso;
 - gli accessi in lettura e scrittura effettuati su tutti i file del sistema;
4. Interventi di ripristino dei dati
- 4.1. In caso di necessità, il ripristino dei dati è previsto entro le 24 ore successive a cura dei responsabili della sicurezza
- 4.2. Qualora non fosse possibile procedere al ripristino dei dati memorizzati con l'ultimo salvataggio, si procederà al restore dell'ultimo nastro utile. Nella peggiore delle ipotesi verranno ripristinate le banche dati memorizzate sul supporto trasferito nella cassetta di sicurezza. I dati ripristinati non avranno quindi età superiore a 7 giorni
5. Protezione dai rischi di intrusione (Antivirus)
- 5.1. Il server è dotato di sistema antivirus Norton Antivirus Corporart Edition 2000 che aggiorna automaticamente le firme dei virus e le rende disponibile per l'aggiornamento anche ai PC della rete; la procedura è automatica;
- 5.2. Gli elaboratori ed i server di rete sono protetti contro il rischio di intrusione mediante apposito software antivirus (Norton Antivirus). Dai PC, viene effettuato l'aggiornamento automatico programmato del software antivirus con connessione automatica al sistema antivirus presente sul server;
- 5.3. In caso di segnalazione di rischi di intrusioni probabili e non debellate dal sistema antivirus in uso, viene scaricato ed installato su ogni PC l'apposito tool reso disponibile per la protezione dal nuovo virus dal sito della Symantec.
- 5.4. Il programma antivirus è configurato in modo da procedere alla scansione sia in entrata che in uscita di ogni messaggio di posta elettronica esterna e relativi allegati. Outlook è altresì in grado di bloccare messaggi in transito sulla posta elettronica interna qualora rilevi la possibile "inattendibilità" di detti allegati.
- 5.5. In mancanza di procedure di installazione automatiche, gli incaricati del trattamento sono stati istruiti per effettuare l'aggiornamento del software antivirus sulle postazioni di lavoro di propria competenza, con cadenza settimanale.
- 5.6. E' prevista l'installazione generalizzata di strumenti Anti spyware: in particolare si prevede l'installazione generalizzata dello strumento Anti Spyware di Microsoft per ora nella versione beta1 (l'uso di tale strumento, attualmente gratuito, verrà valutato in accordo ai cambiamenti di proposta commerciale da parte di Microsoft); si fa menzione di questo SW proprio per la massima integrazione e flessibilità che consente ovviamente negli ambienti Microsoft.

5.7 Dal mese di luglio 2004 è attiva la nuova connessione HDSL. A maggior garanzia di sicurezza per i dati presenti sul sistema informativo, è altresì attivo un firewall, a protezione dagli accessi non consentiti dall'esterno (Attribuzione dinamica degli indirizzi IP).

CRITICITÀ:	MISURA DI SICUREZZA	IN PREVISIONE DAL
Attualmente la connessione HDSL presenta frequenti problemi di funzionamento, con conseguenti disservizi e ritardi anche nelle procedure FTP sugli applicativi.	Attivare una connessione ADSL, più semplificata dal punto di vista dei dispositivi tecnici a corredo (router ecc) e meno a rischio di malfunzionamenti.	1.7.2005
Non su tutti i PC è già attiva la scansione antivirus programmata e l'installazione di strumenti Anti Spyware.	Estendere le procedure di cui ai punti 5.2 e 5.6 a tutti i PC	31.12.2005

3. Prevenzione della vulnerabilità degli strumenti (patch)

- 6.1. Gli aggiornamenti dei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti sono effettuati automaticamente
- 6.2. La connessione ad internet costantemente attiva su tutti i PC consente di scaricare in tempo reale le patch messe a disposizione da Microsoft e dalla ditta produttrice del software applicativo in uso

D) SISTEMA DI AUTENTICAZIONE INFORMATICA PER LA SICUREZZA DEL TRATTAMENTO DEI DATI

1. Controllo degli accessi

- 1.1. L'accesso alla rete di sistema può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password ("*credenziali di autenticazione*");
- 1.2. Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato "*profilo*", rispetto alle risorse del sistema informatico. A ciascun profilo è associato un *gruppo* di utenti, che condividono gli stessi privilegi di accesso ed utilizzo;
- 1.3. Fin nel dettaglio delle voci di menu delle diverse applicazioni, ad ogni nome utente sono associati diversi livelli di accesso (nessuno, sola lettura, modifica), così da limitare in maniera trasparente, intuitiva e sicura la visibilità e la modifica delle banche dati;
- 1.4. Gli applicativi relativi ai servizi demografici e finanziari disciplinano inoltre ad un ulteriore livello l'accesso degli utenti in modalità sola lettura, abilitando alla modifica dei dati unicamente il personale responsabile dei relativi trattamenti;
- 1.5. Gli applicativi utilizzati per il trattamento dei dati possono sfruttare l'autenticazione di cui al punto 1.1, oppure richiedere a loro volta un nome utente e/o una password
- 1.6. Il nome utente non può essere assegnato ad altri incaricati, neppure in tempi diversi
- 1.7. Gli amministratori provvedono, con cadenza almeno semestrale, alla verifica degli elenchi degli utenti ed alla disattivazione delle utenze:
 - a) Non utilizzate da oltre sei mesi (a meno che trattasi di credenziali preventivamente autorizzate per soli scopi di gestione tecnica);
 - b) Che abbiano perso le qualità che consentono all'incaricato l'accesso ai dati personali;

2. Password

- 2.1. Una prima password viene richiesta all'utente al momento dell'accensione del PC, limitando di fatto l'accesso immediato alla macchina ("*password del BIOS*");
- 2.2. Una volta avuto accesso alla macchina, viene richiesto l'inserimento del nome utente e di un'ulteriore password (diversa dalla precedente). Il nome utente è preconfigurato per delimitare l'ambito di accesso dell'utente così connesso ai diversi ambienti della rete aziendale (dalla posta elettronica all'accesso a cartelle condivise);
- 2.3. La password del BIOS e quella di accesso alla rete:
 - a) Non devono derivare dal nome utente o dai dati personali dell'utente né contenere riferimenti agevolmente riconducibili all'incaricato;
 - b) Devono avere lunghezza minima di otto caratteri oppure, qualora lo strumento non lo permetta, da un numero di caratteri pari al massimo consentito;
 - c) Sono strettamente personali: l'utente è tenuto a non comunicarle a terzi ed a non annotarle in vicinanza della propria postazione di lavoro o comunque in luoghi incustoditi;
- 2.4. Le password in uso vengono modificate dai responsabili della sicurezza con cadenza trimestrale, comunicate agli incaricati e da questi ultimi modificate al primo utilizzo.
- 2.5. Le password non possono essere assegnate ad altri incaricati, neppure in tempi diversi.

3. Copie delle credenziali

- 3.1. La custodia delle copie delle credenziali si rende necessaria per assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
- 3.2. I soggetti incaricati della loro custodia sono i responsabili della sicurezza dei dati e del sistema informativo, individuati dal titolare, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
- 3.3. Le copie delle credenziali sono memorizzate su file accessibile esclusivamente ai soggetti incaricati della custodia.

4. Individuazione dei rischi

- 4.1. I responsabili della sicurezza dei dati e del sistema informativo provvedono ad informare tempestivamente i responsabili del trattamento dati di ogni eventuale problema di sicurezza di cui dovessero venire a conoscenza;
- 4.2. I soggetti responsabili del trattamento provvederanno di conseguenza, anche per tramite dei responsabili della sicurezza, a informare tempestivamente gli incaricati:
 - a) della presenza di virus negli elaboratori dell'ufficio;
 - b) di prassi da parte del personale non conformi alle disposizioni di sicurezza;
 - c) della periodica necessità di variazione delle parole chiave da parte degli incaricati;
 - d) della disponibilità di programmi di aggiornamento relativi all'antivirus;
 - e) della perdita delle qualità che consentono all'incaricato l'accesso ai dati personali
- 4.3. I responsabili del trattamento, in caso di necessità, provvederanno ad organizzare iniziative per l'illustrazione e la diffusione degli accorgimenti da adottare in tema di sicurezza.
- 4.4. Per evitare accessi non autorizzati ai computer incustoditi, i PC vengono automaticamente bloccati dopo un periodo di inattività superiore ai 30 minuti. Lo sblocco è possibile solo reinserendo la password di rete del relativo utente.

CRITICITÀ:	MISURA DI SICUREZZA	IN PREVISIONE DAL
Non su tutti i PC è attivo il blocco automatico in caso di prolungata inattività. Durante l'assenza del personale (es: pausa pranzo), il PC rimane acceso ed incustodito: il rischio di intrusione è elevato.	Attivare il blocco automatico dopo 30 min di inattività su tutti i PC.	30.9.2005

SCHEMA DEL SISTEMA DI AUTORIZZAZIONE:

L'accesso alle banche dati è così tutelato:

1. Accensione PC → viene richiesta la password del Bios

↓
Accesso consentito alla macchina solo in locale: nessuna banca dati contenente dati personali disponibile.

2. Connessione alla rete → viene richiesto nome utente + password di rete

↓
Accesso alla rete: posta elettronica, cartelle condivise: nessuna banca dati contenente dati personali disponibile.

↓
Accesso alle banche dati Sicra (anagrafe, tributaria, finanziaria): disciplinato in base al profilo utente (nessuno, modifica, o solo lettura)

3. Connessione agli applicativi Lotus (protocollo, delibere) → viene richiesta password di rete

F) TRATTAMENTI DI DATI AFFIDATI ALL'ESTERNO

Per l'esercizio delle proprie attività istituzionali, il Comune può affidare a terzi funzioni o servizi che contemplano necessariamente il trattamento di dati personali, sensibili e/o giudiziari.

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 al Codice per il trattamento dei dati personali;
2. di ottemperare agli obblighi previsti per la protezione dei dati personali;
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrando le procedure già in essere
4. di aver adottato il Documento Programmatico della Sicurezza (in caso di trattamenti effettuati tramite strumenti elettronici) previsto dal D.Lgs 196/2003
5. di impegnarsi a relazione annualmente sugli aggiornamenti apportati al suddetto DPS.
6. di riconoscere il diritto del Comune a verificare periodicamente l'applicazione delle norme di sicurezza adottate

Nella tabella sono riportati gli impegni allo stato attuale contrattualmente assunti e per i quali è già stato emesso provvedimento di nomina a responsabile del trattamento:

ATTIVITÀ'	DESCRIZIONE DEL TRATTAMENTO	DATI PERSONALI	DATI SENSIBILI / GIUDIZIARI	SOGGETTO
MANUTENZIONE E ASSISTENZA SOFTWARE	Manutenzione ed assistenza del software applicativo in uso presso il Comune	Tutti i dati contenuti nelle banche dati del sistema informativo comunale	Tutti i dati contenuti nelle banche dati del sistema informativo comunale	SAGA SPA di Orzinuovi (BS)
CONSULENZA SISTEMA INFORMATIVO COMUNALE	Manutenzione del software	Tutti i dati contenuti nelle banche dati del sistema informativo comunale	Tutti i dati contenuti nelle banche dati del sistema informativo comunale	GFC srl di Osnago
TESORERIA COMUNALE	Tenuta e gestione della tesoreria comunale	Anagrafe creditori/debitori del Comune		Deutsche Bank spa di Lecco
MENSA SCOLASTICA	Gestione del servizio di somministrazione pasti agli alunni, insegnanti, dipendenti comunali presso gli istituti scolastici	Nominativi degli utenti	Dati sulla salute, sulle convinzioni religiose di utenti con particolari necessità dietetiche.	SERIST di Cinisello B. (MI)
PUBBLICHE AFFISSIONI	Gestione servizio affissione negli spazi pubblici e riscossione della relativa imposta	Anagrafica degli utenti	Dati giudiziari per la riscossione coattiva	TRE ESSE ITALIA di Supino (FR)
RISCOSSIONE TARSU	Riscossione tassa per il servizio di raccolta dei rifiuti solidi urbani ed assimilabili agli	Anagrafica dei contribuenti	Dati giudiziari per la riscossione coattiva	RILENO di Lecco

	urbani			
VISITE MEDICHE D.LGS 626/94	Controlli medici periodici e visite preassunzione del personale comunale	Dati del personale comunale	Dati relativi alla salute	Economie Ambientali di Lecco
SERVIZIO ASSISTENZA DOMICILIARE	Fornitura di personale ausiliario per servizio assistenza domiciliare	Dati anagrafici utenti del servizio	Dati relativi alla salute, convin- zioni religiose, abitudini sessuali	Coop. Soc. Età Insieme di Milano
SERVIZIO ASSISTENZA EDUCATIVA	Fornitura di persona- le educativo rivolto a minori, nuclei fami- liari, soggetti rischio emarginazione	Dati anagrafici utenti del servizio	Dati relativi alla salute, convin- zioni religiose, abitudini sessuali	Coop. Soc. Età Insieme di Milano
TRASPORTO DISABILI E ANZIANI	Servizio con personale volontario presso centri sociali, sanitari ecc.	Dati anagrafici utenti del servizio	Dati relativi alla salute	Associazione di Volontariato il Pellicano di Osnago (LC)

G) INTERVENTI FORMATIVI

1. Gli interventi formativi rivolti agli incaricati del trattamento avranno come contenuti:
 - 1.1. Renderli edotti dei rischi che incombono sui dati e delle misure disponibili per prevenire eventi dannosi;
 - 1.2. I profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
 - 1.3. Le responsabilità che derivano dalla non corretta o insufficiente applicazione delle misure di sicurezza
 - 1.4. Le cautele da adottare per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
 - 1.5. Le istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
2. La formazione è programmata:
 - 2.1. Al momento dell'ingresso in servizio;
 - 2.2. In occasione di cambiamenti di mansioni
 - 2.3. In occasione dell'introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
3. Ogni anno vengono programmate modalità ed entità dell'intervento formativo che può consistere in:
 - 3.1. Giornate di studio o seminari destinati collettivamente agli incaricati ed ai responsabili;
 - 3.2. Attività ristrette di formazione per gruppi di utenti;
 - 3.3. Aggiornamenti rivolti ai soli responsabili;
 - 3.4. Divulgazione materiale informativo agli interessati riferito alle novità o migliorie in materia di sicurezza
4. In sede di prima applicazione del presente documento, ai responsabili ed agli incaricati dei trattamenti è stata consegnata copia del "Memorandum in materia di sicurezza nel trattamento di dati personali".
5. Tenuto conto della precedente formazione attuata nel 2003 e nel 2004 a favore di tutto il personale comunale, per l'anno 2005 la formazione sarà programmata ai sensi del precedente punto 2 e verrà assicurata dal referente interno dell'ente in materia di privacy.