

# 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;
    - c) allarme antintrusione
  - 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.

| CRITICITÀ:   | MISURA DI SICUREZZA | IN PREVISIONE DAL |
|--|---------------------|-------------------|
| La porta di accesso al locale server non è sufficientemente resistente agli urti e potrebbe aprirsi se soggetta a spinta energica. | Sostituire la porta | 31.12.2009        |

## **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. Il locale è altresì dotato di allarme antintrusione.

## 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.
- 1.4. I sistemi operativi e i pacchetti MS Office installati su tutti i PC della rete sono dotati di regolare licenza e sono stati uniformati verso Windows XP Professional e MS Office 2003;

| CRITICITÀ:   | MISURA DI SICUREZZA   | IN PREVISIONE DAL |
|--|---|-------------------|
| Con Provvedimento generale pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana – Serie generale n. 58 del 10/03/2007 il Garante per la protezione dei dati personali ha prescritto ai datori di lavoro alcune misure per conformare alle vigenti disposizioni in materia di privacy il trattamento dei dati personali effettuato per verificare il corretto utilizzo, nel rapporto di lavoro, della Posta elettronica e di Internet. | Approvazione di un <i>"disciplinare interno per l'utilizzo di internet e della posta elettronica da parte dei dipendenti"</i> che soddisfi quanto previsto dal Garante. | 31.12.2008        |

### 2. Integrità dei dati

- 2.1. Gli amministratori di sistema sono i responsabili incaricati del backup dei dati conservati sui server.
- 2.2. Sui server Windows 2000 e SBS 2003:
  - 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) 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 salvataggio evidenziando eventuali file non salvati con indicazione dell'anomalia riscontrata.
  - d) Il server è dotato di un gruppo di continuità che assicura l'alimentazione elettrica in caso di perdita di energia sulla rete
  - e) Una volta alla settimana, una copia dei dati viene trasferita nella cassetta di sicurezza situata presso la tesoreria comunale (edificio separato dalla sede municipale).
  - f) Le cassette con i salvataggi quotidiani sono conservate in apposito armadio ignifugo ubicato presso l'ufficio segreteria (locale separato dal locale server).

2.3. I server sono protetti dalle variazioni non idonee di caratteristiche elettriche dell'alimentazione da UPS.

| CRITICITÀ:  | MISURA DI SICUREZZA                                      | IN PREVISIONE DAL |
|---|--|-------------------|
| L'UPS in uso ha registrato un numero significativo di situazioni dove le caratteristiche elettriche non erano idonee. Come misura temporanea è stata abbassata la soglia di sensibilità dell'UPS stesso a protezione dell'ups stesso. | Verifica del funzionamento dell'alimentazione elettrica. | 30.6.2009         |

2.4. Il server Novell è stato definitivamente dismesso. Dei dati contenuti nello stesso è stata fatta copia in data 4.8.2006 sul server SBS2003, in file compresso MSBackup.

2.5. 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.

| CRITICITÀ:   | MISURA DI SICUREZZA   | IN PREVISIONE DAL |
|--|---|-------------------|
| Alcune banche dati installate direttamente dagli utenti potrebbero essere memorizzate localmente su PC sui quali non è prevista una procedura di backup: rischio di perdita dei dati | Ricognizione degli applicativi in uso presso gli utenti e trasferimento degli archivi su server. Qualora non sia possibile predisporre una procedura automatica per tale salvataggio, si istruiranno gli addetti ad effettuare manualmente una copia su server dell'archivio, con cadenza adeguata alla frequenza di aggiornamento dei dati | 31.12.2009        |

2.5. Ulteriori accorgimenti, disponibili su MS Word e MS Excel, 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" con password per eventuale invio all'indirizzo e-mail noto e certo (certificato);

E' inoltre prevista, entro il 2008, 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:

- a) 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;

- b) Se inviati con posta elettronica, i file vengono opportunamente compressi con password ed inviati solo a destinatario certo e, quando possibile, a casella di posta elettronica certificata;
- c) 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:

L'attuale sistema di monitoraggio attivato sui server con l'apposito "Visualizzatore eventi" prevede al momento un controllo e verifica della sicurezza del sistema informatico a livello di sistema, di gestione delle basi dati e delle applicazioni, ed è in grado di registrare:

- gli accessi da parte degli utenti, riusciti e falliti;
- gli accessi in lettura e scrittura effettuati dagli utenti sui propri files;

escludendo comunque dal sistema di controllo la partizione C:\ del server SBS2003 su cui è installato il sistema operativo. Non sono state inoltre attivate interamente tutte le funzionalità potenziali, in quanto verrebbe altrimenti generato un file di log troppo grande per poter essere conservato e consultato.

Preso inoltre atto che il Provvedimento del Garante del 27.11.2008 (in vigore dal 1.7.2009) prevede che l'operato degli amministratori di sistema debba essere assimilato a quello dei responsabili del trattamento dei dati (vista le capacità di interazione con il sistema che questi hanno) si renderà pertanto necessario attivare il monitoraggio degli accessi dell'amministratore in genere e su tutti gli oggetti e gli ambienti, con conseguente ingenti dimensioni dei file di log generati.

Tenuto quindi conto della normativa attuale e di quella a breve in vigore, si rende necessario predisporre uno studio di fattibilità per dotarsi degli strumenti idonei a garantire la memorizzazione e la gestione dei file di log generati dai controlli richiesti.

| CRITICITÀ:  | MISURA DI SICUREZZA   | IN PREVISIONE DAL |
|---|---|-------------------|
| Il "disciplinare interno per l'utilizzo di internet e della posta elettronica da parte dei dipendenti" di cui alla lettera C punto 1, prevederà che le attività sull'uso del servizio di accesso ad internet vengano automaticamente registrate attraverso i file di log e siano conservate per un periodo di un mese. I dischi dell'attuale server SBS 2003 non hanno capacità di memorizzazione così ampia. | All'attuale sistema di protezione firewall (per il controllo degli accessi non autorizzati dall'esterno) verrà aggiunta la funzione di proxy (per tracciare gli accessi ad internet da parte degli utenti nei termini e nelle modalità previste dal decreto del garante). | 1.7.2009          |

### 4. Interventi di ripristino dei dati

4.1. In caso di necessità, il ripristino dei dati è previsto entro le 24 ore successive all'avvenuta conoscenza della perdita, 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 Windows SBS 2003 è dotato di sistema antivirus Symantec Multi-tier Protection ver. 11.0.2 che distribuisce ed aggiorna automaticamente le firme dei virus e le protezioni (trojan, dialer, spyware, jokes, altro) ai client della rete dotati di sistema operativo Windows XP.

| CRITICITÀ:   | MISURA DI SICUREZZA   | IN PREVISIONE DAL |
|--|---|-------------------|
| Il server Windows 2000 è ancora dotato di sistema antivirus Norton Antivirus Corporate Edition 2002 per i client Windows 98 che sono stati dismessi. | Sottoporre al sistema Symantec Multi-tier la gestione del server Win 2000 e dei client ad esso collegati. | 1.6.2009          |

5.3 A maggior garanzia di sicurezza per i dati presenti sul sistema informativo, è stato attivato su piattaforma Linux un firewall (IPCOP 1.4.x aggiornato all'ultima versione disponibile) a protezione dagli accessi non consentiti dall'esterno e da intrusioni di hacker o di ambienti software evoluti capaci di mettere a repentaglio la sicurezza dei dati. L'accesso esterno al firewall, per manutenzione e monitoraggio, è protetto da password e criptato.

Sui computer è altresì attivo un firewall locale, previsto già sulla piattaforma Microsoft.

5.4 Con cadenza settimanale, anche ai fini della normativa in materia di sicurezza legata alla carta di identità elettronica, viene consultato il firewall per rilevare eventuali rischi di intrusione, porvi rimedio ed aggiornare le regole antintrusione.

5.5 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 sul sito della Symantec per la protezione dal nuovo virus.

5.6 In caso l'amministratore di sistemi rilevi situazioni anomale, in aggiunta alla protezione Symantec di cui al punto precedente, viene utilizzato lo strumento BitDefender disponibile online su internet.

5.6 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. L'antispamming è gestito direttamente da MS Outlook, che utilizza il proprio filtro per destinare lo spam nella casella di "posta indesiderata" (autolearning).

6. 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:

| CRITICITÀ:  | MISURA DI SICUREZZA   | IN PREVISIONE DAL |
|---|---|-------------------|
| La segnalazione automatica di disponibilità di aggiornamenti che compare sui video dei client, necessita di essere espressamente accettata: non tutti gli utenti sono stati sensibilizzati sulla necessità di confermare l'installazione degli aggiornamenti. | Istruzione degli addetti affinché procedano tempestivamente e correttamente all'installazione degli aggiornamenti proposti dal sistema. | 30.6.2009         |

## 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. Accesso remoto da parte di utenti

- 2.1 Per esigenze di manutenzione, è stata attivata una funzionalità di assistenza remota da parte di personale accreditato (es. amministratore di sistema; ditte produttrici degli applicativi, fornitori) in modalità protetta e dove richiesto, crittografata.

| CRITICITÀ:   | MISURA DI SICUREZZA  | IN PREVISIONE DAL |
|--|--|-------------------|
| L'accesso da remoto da parte di alcuni fornitori di applicativi avviene con lo strumento UltraVNC Server che al momento viene utilizzato in modalità non criptata. | Individuare uno strumento che consenta ai fornitori di accedere da remoto in modalità esclusivamente criptata. | 30.9.2009         |

- 2.2 Gli utenti della Polizia Locale sono abilitati ad accedere in modalità remota da un PC situato presso il comune di Lomagna (convenzionato) in modalità protetta e criptata terminal server. A maggior protezione delle banche dati, gli applicativi ed i dati della polizia locale sono stati isolati sul solo server Windows 2000.

### 3. Password

- 3.1. Una prima password viene richiesta all'utente al momento dell'accensione del PC, limitando di fatto l'accesso immediato alla macchina (*"password del BIOS"*).

| CRITICITÀ:   | MISURA DI SICUREZZA                       | IN PREVISIONE DAL |
|--|---|-------------------|
| Non tutti i PC hanno attivata la richiesta della password del BIOS | Ripristino della richiesta su ogni client | 30.6.2009         |

- 3.2. 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);
- 3.3. La password del BIOS e quella di accesso alla rete:
- Non devono derivare dal nome utente o dai dati personali dell'utente né contenere riferimenti agevolmente riconducibili all'incaricato;
  - Devono avere lunghezza minima di otto caratteri oppure, qualora lo strumento non lo permetta, da un numero da caratteri pari al massimo consentito; devono essere alfanumeriche con caratteri sia minuscoli che maiuscoli.
  - 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;
- 3.4. Le password hanno scadenza trimestrale: il sistema invita automaticamente l'utente a modificare la propria password. Tale scadenza temporale è applicata anche per le password di accesso agli applicativi che consentono la configurazione di tale automatismo (Sicra, Polcity).

| CRITICITÀ:   | MISURA DI SICUREZZA   | IN PREVISIONE DAL |
|--|---|-------------------|
| Non si ha la certezza che le password di accesso agli applicativi abbiano le caratteristiche (lunghezza minima, caratteri alfanumerici ecc) previste dalla legge | Ricognizione delle password in utilizzo e sensibilizzazione degli utenti in merito                    | 1.7.2009          |
| E' possibile che i fornitori degli applicativi abbiano conoscenza delle credenziali per l'accesso da remoto con diritti di amministratore                        | Fornire le credenziali autorizzando l'accesso di volta in volta e senza rivedere note le credenziali. | 1.7.2009          |

3.5. Le password non possono essere assegnate ad altri incaricati, neppure in tempi diversi.

#### 4. Copie delle credenziali

- 4.1. La custodia delle copie delle credenziali si rende necessaria esclusivamente qualora l'accesso ai dati ed agli strumenti elettronici sia consentito esclusivamente mediante uso di password non gestibili né dall'utente né dagli amministratori di sistema (es: "quantità di informazione" per INA-SAIA, assegnate dal Ministero dell'Interno e non modificabili).
- 4.2. Per le restanti password, la procedura prevede che a fronte della perdita della password da parte dell'utente o a fronte della necessità di intervento da parte dell'amministratore, quest'ultimo è in grado di modificare la password di accesso, di assegnare una password "di cortesia" e di imporre al sistema la richiesta di una nuova password per l'accesso successivo. Viene in tal modo superata la necessità per gli amministratori di disporre di copia delle password degli utenti.

#### 5. Individuazione dei rischi

- 5.1. 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;
- 5.2. I soggetti responsabili del trattamento provvederanno di conseguenza, anche per tramite dei responsabili della sicurezza, a informare tempestivamente gli incaricati:
- della presenza di virus negli elaboratori dell'ufficio;
  - 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
- 5.3. 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.
- 5.4. Per evitare accessi non autorizzati ai computer incustoditi, i PC vengono automaticamente bloccati dopo un periodo di inattività superiore ai 10 minuti. Lo sblocco è possibile solo reinserendo la password di rete del relativo utente.

|  |
|--|
| <u>SCHEMA DEL SISTEMA DI AUTORIZZAZIONE:</u> |
|--|

***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.

**3. Connessione agli applicativi → viene richiesta ulteriore password:**

Sicra (anagrafe, tributi, finanziaria),  
Lotus Notes (protocollo, delibere),  
Polcity (polizia),  
AIRE, INA-SAIA: sono vincolati alle credenziali di accesso da parte dell'operatore dei Servizi Demografici; dove previsto dagli ambienti forniti dal Ministero dell'Interno si richiedono credenziali di accesso gestite conformemente alla normativa di Legge.

## 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:

| <b>ATTIVITÀ'</b>                   | <b>DESCRIZIONE DEL TRATTAMENTO</b>   | <b>DATI PERSONALI</b>   | <b>DATI SENSIBILI / GIUDIZIARI</b>  | <b>SOGGETTO</b>                      |
|------------------------------------|--|---|---|--------------------------------------|
| 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)           |
| MANUTENZIONE E ASSISTENZA SOFTWARE | Manutenzione ed assistenza del software applicativo in uso presso l'ufficio Polizia Locale | Tutti i dati contenuti nelle banche dati del sistema informativo comunale |   | OPEN SOFTWARE SRL di Mirano (VE)     |
| ASSISTENZA SOFTWARE                | Assistenza del software applicativo per la gestione delle retribuzioni                     | Tutti i dati contenuti nelle banche dati del sistema informativo comunale | Riferiti al personale dipendente (Rilevazione assenze e permessi per malattie, aspettative, rappresentatività sindacali, visite mediche di idoneità, denunce di infortunio sul lavoro, trattenute per adesioni sindacali e per scioperi (salute; opinioni sindacali, religiose, filosofiche, politiche; abitudini sessuali). Emolumenti per familiari (salute). | MCP ITALIA di Porto San Giorgio (AP) |
| MANUTENZIONE E ASSISTENZA          | Manutenzione ed assistenza del   | Tutti i dati contenuti nelle  |   | STARCH srl di Ornago (MI)            |

|  |   |   |  |   |
|--|---|---|--|---|
| SOFTWARE UTC                             | software applicativo in uso presso l'ufficio tecnico comunale   | banche dati del sistema informativo comunale                              |  |   |
| 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                                    |  | Credito Valtellinese di Sondrio                             |
| 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. | SerCar di Alzano Lombardo (BG)                              |
| PUBBLICHE AFFISSIONI                     | Gestione servizio affissione negli spazi pubblici e riscossione della relativa imposta                                      | Anagrafica degli utenti   | Dati giudiziari per la riscossione coattiva  | CESFIL s.p.a. di Arcore (MI)                                |
| RISCOSSIONE RUOLI COATTIVI               | Riscossione somme a ruolo per TIA e sanzioni codice della strada  | Anagrafica dei contribuenti   | Dati giudiziari per la riscossione coattiva  | RILENO di Lecco   |
| 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, convinzioni religiose, abitudini sessuali                           | Coop. Soc. Nuovo Impegno ONLUS di Brescia                   |
| SERVIZIO ASSISTENZA EDUCATIVA            | Fornitura di personale educativo rivolto a minori, nuclei familiari, soggetti rischio emarginazione                         | Dati anagrafici utenti del servizio                                       | Dati relativi alla salute, convinzioni religiose, abitudini sessuali                           | Coop. Soc. Nuovo Impegno ONLUS di Brescia                   |
| SERVIZIO ASSISTENZA TRASPORTO SCOLASTICO | Fornitura di personale per la sorveglianza degli alunni durante il trasporto scolastico                                     | Dati anagrafici utenti del servizio                                       |  | Coop. Sociale LA COMETA di Casatenovo (LC)                  |
| SERVIZIO PRESCUOLA                       | Fornitura di personale per la sorveglianza degli alunni durante il prescuola scuola primaria                                | Dati anagrafici utenti del servizio                                       |  | Coop. Sociale EIDOS a r.l. ONLUS di Oggiona S. Stefano (VA) |
| TRASPORTO DISABILI E                     | Servizio con personale volontario   | Dati anagrafici utenti del servizio                                       | Dati relativi alla salute  | Associazione di Volontariato Io                             |

|                            |  |  |  |                            |
|----------------------------|--|--|--|----------------------------|
| ANZIANI                    | presso centri sociali, sanitari ecc.   |  |  | per Osnago                 |
| SITO COMUNALE E NEWSLETTER | Manutenzione ed implementazione sito web comunale ed indirizzario newsletter | Anagrafe utenti, associazioni e iscritti alla newsletter |  | V.I.P. srl di Oggiono (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, 2004 e 2005 a favore di tutto il personale comunale, anche per l'anno 2009, come per il 2006, 2007 e 2008, la formazione sarà programmata ai sensi del precedente punto 2 e verrà assicurata dal referente interno dell'ente in materia di privacy.