



**COMUNE DI  
VEDUGGIO CON COLZANO**  
Provincia di Milano

**SERVIZIO  
AMMINISTRATIVO - INFORMATICO**

**DOCUMENTO  
PROGRAMMATICO  
SULLA SICUREZZA  
DEI DATI INFORMATICI**

Approvato con delibera di G.C. n° 8 del 25/01/2005  
Modificato con delibera di G.C. n° 30 del 17/03/2006

## INDICE

1 - INTRODUZIONE .....	pag.	3
2 - ASPETTI GENERALI		
2.1 - Contenuti.....	pag.	4
2.2 - Responsabilità .....	pag.	4
2.3 - Applicabilità.....	pag.	5
2.4 - Validità.....	pag.	5
2.5 - Revisione.....	pag.	5
3 - STRUTTURA ORGANIZZATIVA		
3.1 - Identificazione dei trattamenti.....	pag.	6
3.2 - Titolare del trattamento dei dati personali .....	pag.	6
3.3 - Responsabile del trattamento dei dati informatici.....	pag.	6
3.4 - Amministratore della sicurezza e password.....	pag.	7
3.5 - Incaricato del trattamento dei dati.....	pag.	7
3.6 - Incaricato dei back-up.....	pag.	7
4 - SICUREZZA DEI DATI		
4.1 - Analisi dei rischi.....	pag.	8
4.2 - Misure di sicurezza.....	pag.	8
4.3 - Misure di sicurezza fisiche.....	pag.	9
4.4 - Misure di sicurezza logiche .....	pag.	9
4.5 - Misure di sicurezza organizzative .....	pag.	12
5 - FORMAZIONE		
5.1 - Piano di formazione .....	pag.	15

## ALLEGATI

- A) Elenco dei trattamenti, unità organizzative coinvolte e incaricati
- B) Elenco delle apparecchiature server
- C) Elenco delle apparecchiature hardware in dotazione ai servizi e agli uffici
- D) Elenco dei software installati sul server e sulle singole postazioni

## 1 - INTRODUZIONE

Il presente documento è adottato dal comune di Veduggio con Colzano allo scopo di descrivere e pianificare, attraverso la rilevazione delle risorse attinenti il patrimonio informatico ed una analisi dei rischi cui lo stesso è soggetto, le misure di sicurezza fisiche, logiche ed organizzative adottate o da adottare per la sicurezza e integrità dei trattamenti effettuati mediante strumenti automatizzati, individuati come necessari per l'attività e che contengono dati personali soggetti all'applicazione del Dlgs 30/06/2003 n. 196 "Codice in materia di protezione dei dati personali".

Le misure individuate sono tali da soddisfare i requisiti generali del Dlgs 196/2003 e le misure minime di sicurezza descritte nell'allegato B del medesimo decreto legislativo.

## **2 - ASPETTI GENERALI**

### **2.1 - Contenuti**

Secondo quanto disposto dall'allegato B) del Dlgs 196/2003 il presente documento definisce, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità:

- a. l'elenco dei trattamenti di dati personali;
- b. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- c. l'analisi dei rischi che incombono sui dati;
- d. 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;
- e. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- f. 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;
- g. 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.

### **2.2 - Responsabilità**

Il Titolare del trattamento dei dati personali (di seguito Titolare) ed il Responsabile del trattamento dei dati informatici (di seguito Responsabile) assicureranno che il programma di sicurezza sia adeguatamente sviluppato, realizzato e gestito secondo quanto indicato nel presente documento con lo scopo di:

- a. minimizzare le possibilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati personali o comunque critici per le funzioni istituzionali;
- b. minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali.

### **2.3 - Applicabilità**

Le norme indicate nel presente documento si applicano a tutti i trattamenti eseguiti nell'ambito dell'ente e sono da considerarsi vincolanti anche nei rapporti contrattuali relativi a trattamenti eseguiti da altri soggetti esterni cui vengano conferiti incarichi in materia di informatizzazione.

### **2.4 - Validità**

Il presente documento è valido per un anno dalla data della sua emissione o dalla sua ultima revisione e comunque non oltre il 31 marzo di ogni anno.

Entro tale data dovrà essere effettuato quanto previsto dal successivo punto 2.5.

### **2.5 - Revisione**

La revisione del documento avviene obbligatoriamente:

- a. alla scadenza del periodo di validità, allo scopo di valutare l'adeguatezza del documento anche in considerazione dell'evoluzione tecnologica;
- b. ogni qualvolta dovessero cambiare le strutture dei dati o le apparecchiature oggetto delle misure di sicurezza;
- c. ad ogni modifica della struttura organizzativa cui è demandata la responsabilità della sicurezza;
- d. ad ogni controllo periodico cui le misure di sicurezza sono sottoposte per verificarne la validità ed efficacia. In tal caso la revisione del documento riporterà gli esiti di tale controllo ed eventuali riferimenti alla documentazione prodotta.

La nuova versione del documento riporterà, in modo sintetico, un verbale del processo di revisione che ha portato alla sua emissione con l'indicazione delle motivazioni.

### **3 - STRUTTURA ORGANIZZATIVA**

#### **3.1 - Identificazione dei trattamenti**

Presso il comune di Veduggio con Colzano vengono eseguiti trattamenti dei dati previsti dalla Legge 196/2003 e cioè operazioni o complesso di operazioni, svolte con l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, l'interconnessione, la comunicazione, la diffusione, la cancellazione di dati personali, trattamenti tutti finalizzati all'attività istituzionale dell'ente.

L'elenco completo dei trattamenti, le unità organizzative coinvolte e i relativi incaricati sono riportati nell'allegato A) al presente documento.

#### **3.2 - Titolare del trattamento dei dati personali**

Titolare del trattamento dei dati oggetto del presente documento è il Comune di Veduggio con Colzano nella persona del Sindaco pro-tempore.

Il Titolare identifica i trattamenti necessari allo svolgimento dei processi dell'ente, definisce le modalità e le finalità degli stessi e la natura dei dati trattati. Il Titolare è inoltre responsabile dell'osservanza di tutte le normative di legge in materia di dati personali.

Il Titolare emana il Documento Programmatico sulla sicurezza e vigila sulla sua applicazione.

#### **3.3 - Responsabile del trattamento dei dati informatici**

Il Responsabile del trattamento dei dati informatici è individuato nella persona del Responsabile del servizio informatico dell'ente.

Il Responsabile ha il compito di attuare le normative di legge e le prescrizioni di sicurezza indicate nel presente documento per quanto attiene il trattamento dei dati personali definiti dal Titolare come funzionali allo svolgimento dei processi dell'Ente, ivi incluso quanto attiene alla gestione tecnica delle risorse informatiche ed allo sviluppo e manutenzione delle funzionalità applicative degli stessi.

Il Responsabile rileva e propone al Titolare le esigenze di atti formali nei confronti dell'Autorità Garante della Privacy.

Egli nomina incaricati di trattamento le persone fisiche che accedono ai dati, assegnando loro, ove lo ritenga opportuno, anche delle responsabilità specifiche in relazione ai diversi trattamenti effettuati.

Il responsabile viene nominato mediante comunicazione scritta da parte del Titolare e la comunicazione dovrà essere controfirmata per accettazione.

### **3.4 - Amministratore della sicurezza e delle password**

L'amministratore della sicurezza e delle password (di seguito custode delle password) è nominato dal titolare e nel comune di Veduggio con Colzano viene identificato con la figura del Responsabile.

Il custode delle password ha il compito di assicurare la disponibilità dei dati e degli strumenti informatici in caso di prolungata assenza dell'incaricato che renda indispensabile od indifferibile intervenire per esclusive necessità di operatività e sicurezza del sistema. La custodia delle copie delle password è organizzata garantendo la relativa segretezza .

### **3.5 - Incaricato del trattamento dei dati**

L'incaricato del trattamento dei dati (di seguito incaricato) opera in accordo con le mansioni ed istruzioni affidate, eseguendo le operazioni necessarie per l'esecuzione dei trattamenti specificati.

L'incaricato viene nominato mediante comunicazione scritta dal Responsabile e la comunicazione dovrà essere controfirmata per presa visione. Nella lettera di nomina dovranno essere indicati in dettaglio i trattamenti e gli archivi cui l'incaricato è autorizzato ad accedere.

### **3.6 - Incaricato dei back-up**

Il Responsabile provvede a nominare mediante comunicazione scritta:

- a. l'incaricato dell'esecuzione dei back-up nel caso di una sua prolungata assenza:
- b. l'incaricato dell'esecuzione dei back-up per i trattamenti eseguiti in uffici esterni privi di collegamento alla rete informatica.

## 4 - SICUREZZA DEI DATI

### 4.1 - Analisi dei rischi

Per ciascun tipo di trattamento dei dati vengono adottate misure di sicurezza adeguate.

I singoli rischi sono raggruppati come segue:

- **rischi per la riservatezza dei dati**  
le informazioni devono essere accessibili ed utilizzate solo da persone autorizzate e per fini conformi all'attività istituzionale dell'ente;
- **rischi per l'integrità dei dati**  
i dati devono essere esatti, aggiornati e corrispondenti alla realtà proteggendoli da qualsiasi forma di alterazione non controllata;
- **rischi per la disponibilità**  
l'accesso ai dati deve poter avvenire ogni qual volta ve ne sia necessità in conformità alle esigenze dei trattamenti;
- **rischi di uso improprio**  
l'accesso ai dati deve avvenire esclusivamente per i fini definiti dal titolare da parte di soggetti adeguatamente autorizzati e istruiti.

### 4.2 - Misure di sicurezza

In considerazione dei rischi individuati vengono indicate le misure di sicurezza adottate nel rispetto degli obblighi di legge.

Le misure di sicurezza sono divise in:

- **misure di sicurezza fisiche**  
riguardano la sicurezza passiva e il controllo degli accessi ai locali contenenti le apparecchiature ed i supporti di memorizzazione informatici;
- **misure di sicurezza logiche**  
riguardano il controllo dell'accesso alle piattaforme, agli archivi, ai database e alle applicazioni con il compito di segnalare una intrusione in atto e di richiedere l'intervento del responsabile e/o di un tecnico in grado di bloccare l'intrusione;
- **misure di sicurezza organizzative**  
riguardano le modalità per garantire la corretta funzionalità delle misure fisiche e logiche e di assicurare in tempi brevi l'intervento del responsabile e/o dei tecnici.

### **4.3 - Misure di sicurezza fisiche**

Le macchine server del comune di Veduggio con Colzano, (vedi all. B), sono:

- AS 400/series (per gestione software contabilità finanziaria e personale);
- server IBM (per gestione posta in arrivo e in partenza);
- server HP (server primario per gestione di tutta la rete informatica).

Le stesse sono collocate in un locale esclusivamente destinato allo scopo posto al piano ammezzato dell'edificio comunale.

Questo locale è dotato di

- impianto elettrico a norma;
- un gruppo di continuità che permette il salvataggio dei dati e il mantenimento in funzione per un periodo di tempo limitato anche in caso di black out (solo per As400 IBM).

Non è dotato di:

- impianto di condizionamento;
- impianto antifurto.

Il locale è accessibile esclusivamente al responsabile del trattamento dei dati informatici, all'amministratore della sicurezza e password, all'incaricato dell'esecuzione dei back-up nonché ai tecnici di società esterne che operano per l'ente esclusivamente per la necessaria manutenzione delle componenti hardware e software di loro competenza.

In assenza del personale la sala viene mantenuta chiusa a chiave.

I supporti di back up vengono conservati in una cassetta di sicurezza custodita in apposito armadio blindato, munito di serratura di sicurezza, posto nell'ufficio.

Le chiavi dell'armadio vengono custodite dal responsabile e dagli addetti all'ufficio servizi demografici.

Non esistono armadi che contengono gli apparati di rete.

Le singole apparecchiature sono date in dotazione agli uffici e ai servizi secondo quanto indicato nell' all. C).

### **4.4 - Misure di sicurezza logiche**

#### **a) sicurezza del software**

Presso ciascun ufficio e su ogni postazione di lavoro è consentita esclusivamente l'installazione delle seguenti quattro categorie di software:

- software commerciale, ancorché gratuito, dotato di apposita licenza d'uso;

- software gestionale realizzato specificatamente per l'amministrazione comunale da ditte specializzate nel settore della pubblica amministrazione;
- software realizzato internamente per soddisfare eventuali esigenze particolari del singolo servizio;
- software scaricato via internet o posta elettronica, realizzato e trasmesso da altri enti della pubblica amministrazione (regione, provincia, prefettura, ministeri, ecc.) per la trasmissione on-line delle relative informazioni.

L'eventuale installazione di software diversi da quelli citati deve essere preventivamente valutata ed autorizzata dal Responsabile.

Il software installato sulla rete e sulle singole postazioni è in dotazione ai servizi e agli uffici secondo quanto indicato nell'allegato D).

Al fine di prevenire ed evitare la diffusione di virus informatici il software deve venir installato solo da supporti fisici originari, dei quali sia nota la provenienza o scaricato, se nel caso, dai siti ufficiali degli enti e delle società titolari dei diritti.

La rete informatica e le singole postazioni sono protette dal programma antivirus Trend Micro NetSuite gestito dal server con aggiornamenti giornalieri.

Le postazioni ubicate presso il centro culturale sono protette con antivirus Norton con aggiornamento giornaliero.

Per quanto riguarda l'accesso ad internet ed alla posta elettronica gestita con il programma Lotus Notes, la sicurezza è garantita direttamente dal provider che provvede ad un controllo della posta in arrivo e da un firewall Soho, interposto tra la rete interna e quella esterna, in grado di filtrare e prevenire gli accessi non autorizzati ed indesiderati alla rete comunale. Tra il firewall e il server esiste un'ulteriore password per garantire in maniera ottimale la protezione della Intranet.

Ogni due mesi viene effettuato uno scandisk del server.

#### **b) integrità dei dati**

Il Responsabile mantiene l'elenco (all. C) di tutte le attrezzature informatiche dei singoli uffici, dello scopo a cui sono destinati, della loro locazione fisica, delle misure di sicurezza su di esse adottate e delle eventuali misure di adeguamento pianificate. Tale elenco viene aggiornato con cadenza semestrale o in occasione di consistenti modifiche nella dotazione delle attrezzature stesse.

In fase di installazione e configurazione del sistema di archiviazione dei file sono stati definiti i volumi logici o le aree di disco da sottoporre ai backup sui vari server.

Ogni incaricato deve collocare i propri documenti nelle apposite cartelle mappate su server.

Le operazioni di backup vengono effettuate così come segue:

- per i dati gestiti su as400 viene effettuato un backup automatico giornaliero su nastro che viene cambiato ogni giorno. Con cadenza settimanale viene effettuato un ulteriore backup automatico e il relativo nastro viene depositato in una cassetta di sicurezza presso la locale filiale del Banco Desio;
- per i dati gestiti sui server gli stessi vengono salvati su cartelle protette da accessi autorizzati. Viene effettuato un backup automatico giornaliero su nastri che vengono cambiati ogni giorno. Con cadenza settimanale viene effettuato un ulteriore backup manuale a cura del responsabile e i relativi nastri vengono depositati in una cassetta di sicurezza presso la locale filiale del Banco Desio;
- nel centro culturale esterno alla rete informatica comunale, le operazioni di backup vengono effettuate settimanalmente con procedura manuale o automatica.

Qualora l'incaricato non provveda a collocare i documenti nelle cartelle su server ma sul proprio Personal computer sarà responsabile dell'eventuale perdita dei dati dovuta a malfunzionamento o rottura della macchina.

#### **c) sistema di monitoraggio**

Attraverso appositi file di log presenti sul server è stato realizzato un sistema di controllo e verifica della sicurezza del sistema informatico. Tali file raccolgono le informazioni relative al funzionamento del Sistema Operativo del server, su eventuali virus e sull'invio e ricezione della posta elettronica.

Il sistema di controllo è in grado di registrare:

- gli accessi riusciti e falliti;
- gli accessi in lettura e scrittura;
- gli accessi in lettura e scrittura sui singoli archivi.

#### **d) controllo degli accessi**

L'accesso diretto ai server è consentito esclusivamente al Responsabile, ai soggetti incaricati dallo stesso quali sostituti in caso di assenza, ai tecnici di società esterne che operano per l'ente esclusivamente per il software di propria competenza.

L'accesso al server da parete dei tecnici di società esterne è consentito, esclusivamente per software di propria competenza o per interventi sulla rete informatica anche tramite collegamento diretto in teleassistenza previo accordi stipulati tra le parti e identificazione dei soggetti tramite apposite credenziali.

L'accesso alla rete informatica avviene esclusivamente attraverso un profilo di abilitazione che prevede per ciascun soggetto abilitato (di seguito utente) una propria identificazione tramite un nome utente (user-id) ed una password.

Per ciascun utente vengono definiti:

- il trattamento e/o gli archivi presenti sul server per cui viene data abilitazione di accesso;
- gli eventuali diritti di detta abilitazione (sola lettura, lettura e scrittura, ecc.).

A ciascun profilo di abilitazione è associato un gruppo di utenti che condividono gli stessi privilegi di accesso e di utilizzo.

Il custode delle password custodisce un elenco aggiornato contenente i nomi e le qualifiche degli utenti autorizzati.

Esso provvede inoltre:

- a definire il nome utente e la password per il primo accesso;
- a consegnare agli utenti il nome utente e la password assegnati;
- a definire i gruppi necessari per rispettare i privilegi di utilizzo.

Le password devono essere sostituite da parte dai singoli utenti con una frequenza non superiore a tre mesi.

La definizione della password deve tener conto delle seguenti regole minime:

- deve essere alfanumerica, di non meno di otto caratteri;
- non deve essere composta utilizzando il nome utente;
- non deve essere ottenuta anagrammando la precedente.

Il custode delle password imposta il sistema in modo da forzare l'utente :

- a cambiare obbligatoriamente la password ogni tre mesi;
- a non poter utilizzare la stessa password.

Il nome utente e la password sono strettamente personali. L'utente è tenuto

- a comunicare a la propria password in busta chiusa e ad ogni cambio della stessa esclusivamente al custode delle password;
- a non annotare la password stessa su supporti posti in vicinanza della propria postazione di lavoro o comunque incustoditi.

La busta contenente le password verrà conservata in cassaforte.

La violazione della segretezza della password costituisce infrazione grave alle disposizioni di sicurezza.

#### **4.5 - Misure di sicurezza organizzative**

##### **a) controllo dei back up**

Il Responsabile è chiamato a verificare la corretta esecuzione dei backup, a mantenere un elenco dei back up effettuati, a conservare i supporti in appositi

armati in modo da garantirne la sicurezza.ed a richiamare gli incaricati, nel caso, alla tempestiva esecuzione di tali adempimenti anche a mezzo di comunicazione scritta.

#### **b)nomina degli incaricati**

Il Responsabile provvede alla nomina degli incaricati per il trattamento dei dati informatici e per l'esecuzione dei backup, a definire le diverse responsabilità e all'assegnazione dei relativi compiti.

Qualora si faccia ricorso a soggetti esterni all'ente per l'assistenza alla rete informatica con accesso a trattamento dei dati, il Responsabile provvede al relativo incarico definendo compiti e limiti dell'accesso.

#### **c)individuazione dei rischi e prevenzione dei danni**

Il Responsabile provvede ad informare tempestivamente gli incaricati:

- della presenza di virus nei personal computers in dotazione agli uffici;
- dell'utilizzo, da parte del personale, di procedure non conformi alle disposizioni sulla sicurezza;
- della periodica necessità di variazione della password;
- della disponibilità di programmi di aggiornamento relativi ad antivirus;
- del mancato rispetto di quanto previsto dalle norme contenute nel predetto documento.

In caso di continua inadempienza da parte degli incaricati il Responsabile provvederà a darne comunicazione scritta al Titolare.

Il responsabile provvede ad organizzare iniziative per illustrare e diffondere gli accorgimenti da adottare in tema di sicurezza.

#### **d) verifica ed aggiornamento del Documento sulla sicurezza**

Il Responsabile provvede periodicamente:

- a presentare al titolare una relazione sull'andamento dei processi relativi alla sicurezza;
- alla verifica delle norme contenute nel presente documento in rapporto all'efficacia delle contromisure adottate.

In particolare provvederà periodicamente a verificare:

- gli accessi fisici ai locali dove sono poste le apparecchiature server e/o dove si svolgono trattamenti informatici di qualsiasi genere;
- la corretta gestione dei codici identificativi personali e delle password;
- la corretta gestione dei profili di accesso degli incaricati;
- le procedure relative al controllo dell'integrità dei dati e al loro aggiornamento;
- la sicurezza delle trasmissioni in rete di dati personali;
- le modalità di conservazione dei back up;

- le modalità di ripristino dei back up;
- le modalità di reimpiego dei supporti di memorizzazione;
- il livello di formazione e il grado di apprendimento degli incaricati.

Il responsabile provvede ad aggiornare il presente documento a cadenza annuale e comunque ogni qualvolta si apportino consistenti variazioni al sistema informatico, alle strutture o a qualunque altro elemento o se ne dovesse ravvisare l'opportunità e/o la necessità in dipendenza di eventi non considerati nel documento stesso.

## **5 - FORMAZIONE**

### **5.1 - Piano di Formazione**

Il Titolare, in accordo col responsabile, provvede annualmente alla stesura di un piano di formazione su quanto oggetto del presente documento e su eventuali aggiornamenti dovuti a modifiche di legge, a cui gli incaricati e il personale addetto sono tenuti a partecipare.

**ALLEGATI:**

- A) Elenco dei trattamenti, unità organizzative coinvolte e incaricati
- B) Elenco delle apparecchiature server
- C) Elenco delle apparecchiature hardware in dotazione ai servizi e agli uffici
- D) Elenco dei software installati sul server e sulle singole postazioni