COMUNE DI BUTTAPIETRA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI[1]

(ai sensi del punto 19 del Disciplinare tecnico in materia di misure minime di sicurezza - Allegato B del D.lgs. 196/03 "Codice in materia di protezione dei dati personali")

2009

INDICE

PREMESSA....4

INTRODUZIONE....5

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI....6

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI....7

3. ANALISI DEI RISCHI....8

3.1. IDENTIFICAZIONE DELLE RISORSE DA PROTEGGERE....8
3.1.1. Hardware....8
3.1.2. Software....9
3.1.3. Supporti Dati....10
3.2. VALUTAZIONE DELLE MINACCE E DELLA VULNERABILITÀ DEI BENI....10
3.2.1. Penetrazione logica....10
3.2.2. Penetrazione sulle reti di telecomunicazioni....11
3.2.3. Guasti tecnici delle apparecchiature....12
3.2.4. Errori umani....12
3.2.5. Minacce fisiche....13
3.3. INDIVIDUAZIONE DELLE CONTROMISURE....13
3.4. DEFINIZIONE DELLE POLITICHE DI SICUREZZA....14
3.4.1. Classificazione delle informazioni....15
3.4.2. Protezione fisica delle risorse....15
3.4.2.1. Classificazione delle aree aziendali....15
3.4.2.2. Controllo dell'accesso alle aree critiche....15
3.4.2.3. Sicurezza fisica (impianti)....16
3.4.3. Protezione logica delle informazioni....16
3.4.3.1. Controllo degli accessi alle informazioni....16
3.4.3.2. Mantenimento dell'integrità e riservatezza delle informazioni....16
3.4.3.3. Sicurezza dei PC e dei Server....16
3.5. NORME PER IL PERSONALE....17
3.5.1. Utilizzo delle risorse informatiche....17
3.5.2. Accesso ai sistemi e ai dati....17
3.5.3. Uso delle credenziali di autenticazione....17
3.6. GESTIONE DEGLI INCIDENTI....18
3.7. MANUTENZIONE DEI SISTEMI HARDWARE E SOFTWARE....18
3.7.1. Le apparecchiature....18
3.7.2. Il software....19

4. MISURE DI GARANZIA DELL'INTEGRITA' E DELLA DISPONIBILITA' DEI DATI. PROTEZIONE DELLE AREE E DEI LOCALI AI FINI DI CUSTODIA E ACCESSIBILITA' DEI DATI. 20

4.1. ELENCO DELLE RISORSE DA PROTEGGERE. 20
4.2. IDENTIFICAZIONE ED AUTORIZZAZIONE. 20
4.3. INDIVIDUAZIONE DELL'ESPOSIZIONE AL RISCHIO. 20
4.3.1. Il livello delle minacce ai suddetti beni. 20
4.3.2. Il livello di vulnerabilità dei suddetti beni. 22
4.4. SICUREZZA ED INTEGRITÀ DEI DATI. 24
4.5. SICUREZZA DELLA RETE. 29
4.6 TRASMISSIONE DEI DATI. 29
4.7. SICUREZZA FISICA. 32

5. CRITERI E MODALITA' PER IL RISPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO.....34

6. IL PROGRAMMA DI FORMAZIONE DEGLI INCARICATI.....35

6.1 PIANO DI FORMAZIONE. 35

7. CRITERI DA ADOTTARE PER GARANTIRE L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTI DI DATI PERSONALI AFFIDATI ALL'ESTERNO DELLA STRUTTURA.....37

8. IL PIANO DI VERIFICHE E DI AGGIORNAMENTO PERIODICO DEL MANUALE 38

PREMESSA

Il presente Documento Programmatico sulla Sicurezza è stato redatto il 17 maggio 2004 ai sensi del punto 19 del Disciplinare tecnico in materia di misure minime di sicurezza – Allegato B del Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” (di seguito Codice), e aggiornato il 21 marzo 2007 nelle sole parti che elencano i sistemi operativi dei clients, e le stampanti in dotazione agli uffici comunali.

INTRODUZIONE

Il Documento Programmatico sulla Sicurezza (in seguito DPS) è redatto ai sensi del punto 19 del Disciplinare tecnico in materia di misure minime di sicurezza – Allegato B al D.lgs. 196/03 "Codice in materia di protezione dei dati personali. Il DPS costituisce il progetto "sicurezza" del trattamento dei dati all'interno del Comune.

Il DPS del Comune di Buttapietra si articola in otto capitoli:

1. Il primo capitolo è dedicato all'elenco dei trattamenti di dati personali effettuato dal comune;
2. Il secondo capitolo analizza la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. Il terzo capitolo è dedicato all'analisi dei rischi attraverso il quale vengono messi in evidenza i rischi legati al trattamento dei dati personali, in particolare quelli definiti sensibili;
4. Il quarto capitolo esamina le principali 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;
5. Il quinto capitolo prende in esame i criteri e le modalità per il ripristino delle disponibilità dei dati in seguito a distruzione o danneggiamento;
6. Il sesto capitolo è dedicato al programma di formazione degli incaricati;
7. Il settimo capitolo si occupa della 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;
8. L'ottavo capitolo è dedicato al piano di verifiche e di aggiornamento del documento stesso. Il DPS deve essere aggiornato entro il 31 marzo di ciascun anno.

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Il Comune di Buttapietra effettua i seguenti trattamenti di dati sensibili:

- Dati dei dipendenti

- Dati provenienti da curricula

- Dati contenuti nei registri di Stato Civile (ad es. matrimonio celebrato con rito cattolico o con altro culto ammesso dallo Stato)

- Dati di cittadini trattati dai Servizi Sociali e dall'Area Vigilanza.

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

Il Comune di Buttapietra ha nominato un responsabile interno del trattamento e un responsabile esterno (vedi allegato di dettaglio e nomine).

Le strutture individuate, preposte al trattamento, sono le seguenti:

- Area amministrativa
- Area economico-finanziaria
- Area tecnica: edilizia pubblica; edilizia privata
- Area vigilanza

Per ogni area è stato individuato un responsabile.

Gli incaricati del trattamento sono stati nominati analizzando l'area di appartenenza e individuando l'ambito del trattamento consentito agli addetti dell'unità medesima.

Per il dettaglio dell'ambito di trattamento si rimanda alle lettere di incarico.

3. ANALISI DEI RISCHI

3.1. IDENTIFICAZIONE DELLE RISORSE DA PROTEGGERE.

3.1.1. Hardware

La rete locale del Comune Di Buttapietra, situata in Buttapietra (Vr), è composta da:

- N.22 (ventidue) pc clients, di marche e modelli diversi, tutti IBM compatibili.
- N.1 (una) stampante HP 4000 (c/o ufficio ragioneria).
- N.1 (una) stampante HP LaserJet 6L (c/o ufficio assist. Sociale)
- N. 1 (una) stampante HP LaserJet 6P (c/o ufficio tecnico)
- N. 1 (una) stampante HP Laserjet 1150 (c/o ufficio vigili)
- N.1 (una) stampante Epson Stylus Color 1520 (c/o ufficio tecnico)
- N.1 (una) stampante Epson LQ 2080 (aghi) (c/o uffici demografici)
- N.1 (una) stampante Epson LQ 2180 (aghi) (c/o ufficio tributi)
- N.1 (una) stampante Epson LQ 2090 (aghi) (c/o uffici demografici)
- N. 1 (una) stampante Epson LX 1170 (aghi) (c/o ufficio vigili)
- N.1 (una) stampante HP LaserJet 1200 (c/o uffici demografici)
- N. 1 (una) stampante CANON Pixma iP4200 (c/o ufficio tecnico)
- N. 1 (una) stampanet CANON Pixma iP4000 (c/o ufficio segret. Com.le)
- N.1 (uno) hub 3COM 16 porte
- N.1 (uno) switch NetGear 16 porte
- N.1 (uno) modem/router ADSL in comodato Telecom.
- N.1 (uno) firewall Symantec 200R
- N.1 (uno) server IBM XSeries 225 Xeon 1,67 Ghz-1GB Ram - 3x36 SCSI Disk in RAID 5 hardware, Server Windows 2003 appartenente al dominio

NT, configurato come file server per la condivisione di tutte le cartelle di lavoro del comune. Su questo server sono stati spostati tutti i dati del vecchio server HP E50.

L'infrastruttura fisica della rete si basa su cablaggio strutturato UTP cat.5 e switch Ethernet/FastEthernet (3com e NetGear).

Non esiste alcuna connettività in fibra ottica.

Non è presente alcun collegamento in radiofrequenza

Non sono impostate VLAN sugli hub/switch.

Non è presente alcun apparato di management di rete né a livello software né a livello di connettività/rete fisica agli switch

A tale infrastruttura sono collegati gli elaboratori ed altri apparati di rete. La struttura logica si basa sul protocollo TCP/IP. Il network ID è costituito da una classe C su indirizzi ip 10.0.0.X.

Non vi sono server DHCP in quanto le macchine client e server hanno indirizzi ip fissi.

Un elenco dettagliato dell'hardware viene fornito in allegato, assieme al diagramma della struttura logica e fisica della rete LAN.

3.1.2. Software

Sistema operativo NT Server 4.0 sul server controllore di dominio.

Sistema operativo Windows 2003 Server, sul server file server IBM xSeries.

Sistema operativo Windows XP su tutte le 20 macchine clients.

Symantec Antivirus Enterprise Editing 8.6, installato sul server Windows 2003.

Halley, sistema che gestisce contabilità, anagrafe, rilevazione presenze.

Altro software per la gestione dell'ICI.

Autocad Light

GPE (gestione pratiche edilizie)

Programma S7 (gestione pratiche pensionistiche, TFR)

Norton Antivirus 2006.

Utilità varie quali Winzip, Acrobat, Nero, degimp (fotoritocco), programmi di masterizzazioni. Installati sui PC.

3.1.3. Supporti Dati

Hard disk installati sui PC e sui Server; CD-ROM applicativi e Sistemi Operativi; cassette per backup; dischetti.

3.2. VALUTAZIONE DELLE MINACCE E DELLA VULNERABILITÀ DEI BENI.

3.2.1. Penetrazione logica

Tale tipo di minaccia, nel caso in oggetto, è legato alla possibilità di utenti non autorizzati dei Personal Computer di accedere alla rete, alle applicazioni su di essa disponibili ed ai dati presenti sui Server o sui PC stessi, nonché alla possibilità di accedere ai dati ed alle applicazioni direttamente attraverso la console di uno dei Server.

Un'altra minaccia logica è data dai virus informatici introdotti inavvertitamente dagli utenti attraverso programmi e dati di provenienza non controllata o non controllabile.

Un’ulteriore minaccia logica è legata alla navigazione su Internet ed alla possibilità, attraverso il browsing di un sito WWW, di attivare più o meno consapevolmente script o applicazioni malevole che verrebbero eseguite sul PC da cui si effettua la navigazione.

3.2.2. Penetrazione sulle reti di telecomunicazioni.

La natura permanente e l’indirizzo IP fisso del collegamento ad Internet tramite ADSL Telecom espongono la rete locale (LAN) del Comune alla possibilità di studio e tentativo di accesso remoto attraverso Internet, alla possibilità di attacchi DOS (Denial of Service) volti alla interruzione delle funzionalità proprie dei PC, dei Server o delle applicazioni di rete, portati attraverso il "bombardamento" mediante pacchetti di dati opportunamente creati per sfruttare i difetti dei sistemi operativi o di una delle applicazioni di rete.

La navigazione sul World Wide Web avviene attraverso un Firewall Symantec 200R. Le singole stazioni di lavoro hanno quindi accesso diretto ad Internet, rimangono esposte solo ai rischi indiretti legati alla navigazione Web (pagine Web malevoli, con script e applet dai contenuti incontrollabili).

Sempre tramite il firewall Symantec 200R, i clients si collegano al provider che mantiene le cassette postale del personale del Comune di Buttapietra. La posta viene pertanto prelevata dal provider e portata sui pc del Comune di Buttapietra solo su esplicita richiesta dei client. Pertanto, ogni tentativo di accesso via SMTP da parte di terzi (o di bombardamento spamming) è vano non consentito.

Non sono presenti collegamenti modem da pc pertanto ogni tentativo d’accesso di accesso tramite le linee di fonia non è fattibile.

3.2.3. Guasti tecnici delle apparecchiature.

Le minacce legate ai guasti tecnici delle apparecchiature sono da individuare in:

a) **Guasto di uno dei Personal Computer (non relativo al disco fisso)** che porti all'inutilizzabilità dell'apparecchiatura con conseguente interruzione del lavoro tramite essa eseguito. Non comporta perdita di dati, a parte quelli in elaborazione al momento del guasto e non salvati sul disco fisso o su altro supporto.

b) **Guasto di uno dei Server (non relativo al disco fisso)** che porti alla sua inutilizzabilità o inaccessibilità sulla rete locale, con conseguente blocco di tutte le attività legate alle applicazioni che si trovano sul Server.

c) **Guasti ai dischi fissi dei PC e dei Server**. Sicuramente la peggiore minaccia in quanto possono portare alla perdita dei dati in essi salvati.

d) **Guasti alle periferiche (stampanti, router, switch, unità a nastro).** Possono portare ad un più o meno lungo periodo di inutilizzo di tali risorse, causando anche l’interruzione del normale lavoro. Il guasto dell'unità a nastro utilizzata per il backup dei dati può causare un'ulteriore minaccia indiretta per l'integrità dei dati salvati sui dischi fissi.

3.2.4. Errori umani.

Le minacce di questo tipo sono legate ad imperizia, imprudenza o inaccortezza degli operatori, oltre ad una possibilità statistica di errore anche da parte del personale meglio preparato. I danni possono andare dalla perdita del lavoro in esecuzione al

momento dell'errore fino alla cancellazione di dati importanti dai supporti di memorizzazione (dischi fissi) o al danneggiamento delle apparecchiature.

3.2.5. Minacce fisiche.

Le minacce di questo tipo riguardano l'accesso fisico di persone non autorizzate ai locali o alle postazioni di lavoro e la sicurezza fisica delle apparecchiature rispetto agli impianti di alimentazione, di condizionamento e di protezione antincendio. Nel primo caso, il pericolo riguarda la possibilità di furto delle apparecchiature e/o dei supporti di memorizzazione o l'utilizzo non autorizzato degli stessi. Nel secondo caso il pericolo riguarda l'integrità fisica stessa delle apparecchiature e delle altre risorse aziendali.

3.3. INDIVIDUAZIONE DELLE CONTROMISURE.

Un sistema di contromisure adeguato alle necessità deve quindi comprendere:

a) Messa in sicurezza dei locali con un sistema che impedisca accessi non autorizzati al di fuori del normale orario di lavoro.

b) Sistema di protezione dell'alimentazione dei Server.

c) Sistema antincendio.

d) Sistema di protezione delle reti locali dai tentativi di accesso non autorizzato attraverso Internet (Firewall) ed altri collegamenti di rete remota (controllo degli accessi).

e) Installazione di un sistema di protezione dai virus e suo aggiornamento costante.

f) Operazioni di backup periodico dei dati dei Server ed, eventualmente, dei PC.

g) Attivazione di un sistema di controllo degli accessi al sistema informativo del tipo "nome utente/password".

h) Messa in sicurezza dei Server (blocco della console).

i) Sensibilizzazione del personale ai rischi della "navigazione" su Internet e alle necessarie prudenze.

3.4. DEFINIZIONE DELLE POLITICHE DI SICUREZZA

Con la definizione delle Politiche di Sicurezza si prende atto della valutazione del rischio e si definisce la risposta adeguata alle necessità messe in luce nei paragrafi precedenti fissando obiettivi che verranno perseguiti nel Piano Operativo, che si articola nei capitoli successivi.

La sicurezza deve inoltre essere considerata, da tutti i dipendenti, parte integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione.

Un sistema di sicurezza è un insieme di misure fisiche, logiche ed organizzative integrate, volte a ridurre la probabilità di danni ad un livello e ad un costo ragionevole.

Le Politiche di Sicurezza si basano sul principio che le risorse informatiche (dati, risorse hardware e software) sono un patrimonio che deve essere protetto dal momento in cui viene creato/installato, durante il suo utilizzo, fino al momento in cui viene distrutto. Devono essere portate a conoscenza, per le parti di pertinenza, delle società esterne che interagiscono con il Comune, le quali devono accettarne i contenuti ed impegnarsi a rispettarle.

Le Politiche di Sicurezza devono essere aggiornate con periodicità annuale per riflettere eventuali nuovi indirizzi, evoluzioni e normative in materia di sicurezza.

3.4.1. Classificazione delle informazioni.

I dati trattati dal Comune hanno natura di dati personali (ai sensi dell'art. 4 lett. b) del Codice), dati identificativi (ai sensi dell'art. 4 lett. c) del Codice), dati sensibili (ai sensi dell'art. 4 lett. d) del Codice) e di dati giudiziari (ai sensi dell'art. 4 lett. e) del Codice).

3.4.2. Protezione fisica delle risorse.

3.4.2.1. Classificazione delle aree aziendali.

Il Comune Di Buttapietra è composto da un edificio a 3 livelli con uffici e locali accessibili al pubblico, da uffici e locali accessibili al solo personale dipendente e da uffici e locali accessibili solo al personale dipendente dotato di particolari autorizzazioni.

3.4.2.2. Controllo dell'accesso alle aree critiche.

Le postazioni di lavoro dotate di PC e soprattutto l'area ove sono situati i Server non sono accessibili al pubblico se non accompagnato da personale del Comune.

Analoghe misure sono prese per i luoghi ove vengono maneggiati e custoditi i supporti cartacei delle informazioni.

Gli atti e i documenti contenenti i dati sono conservati in archivi ad accesso selezionato e inoltre, per i documenti contenenti dati sensibili sono stati previsti archivi ad accesso controllato.

3.4.2.3. Sicurezza fisica (impianti).

Si è provveduto ad adottare le necessarie misure antincendio, di salvaguardia elettrica e, ove divenisse necessario, di condizionamento.

3.4.3. Protezione logica delle informazioni.

3.4.3.1. Controllo degli accessi alle informazioni.

L'accesso alle informazioni è protetto dalle credenziali di autenticazione costituite da un codice di identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solamente dal medesimo. Inoltre è stato previsto un sistema di autorizzazione contenenti appositi "profili" per l'accesso controllato ai dati ed alle applicazioni del sistema informativo.

3.4.3.2. Mantenimento dell'integrità e riservatezza delle informazioni.

La protezione dai virus informatici viene garantita attraverso l'utilizzo di un software antivirus (Symantec Antivirus Enterprise Editing 8.6) con aggiornamenti giornalieri gestiti centralmente attraverso un Server di rete. Tale protezione è garantita a livello file system. Tutti i pc client del Comune sono automaticamente aggiornati, in caso di aggiornamenti delle definizioni dei virus, dal server centralizzato

Sono attive procedure di salvataggio di sicurezza (backup) dei dati. Le copie di sicurezza vengono poste in luogo sicuro ed al di fuori della portata del pubblico o di personale non autorizzato.

3.4.3.3. Sicurezza dei PC e dei Server.

I PC sono protetti da accessi non autorizzati al sistema operativo locale quanto alla rete.

L'accesso all'utilizzo della console dei Server è protetto e permesso al solo Amministratore di Sistema.

3.5. NORME PER IL PERSONALE.

3.5.1. Utilizzo delle risorse informatiche.

Il personale dipendente utilizzerà le risorse informatiche a cui ha accesso attenendosi alle istruzioni di incarico e autorizzazione ricevute.

3.5.2. Accesso ai sistemi e ai dati.

L’accesso ai sistemi e ai dati sarà definito dal Responsabile insieme al Titolare del trattamento, al fine di individuare categorie omogenee di incaricati avente le necessarie autorizzazione a trattare particolari dati.

3.5.3. Uso delle credenziali di autenticazione.

Il personale è tenuto, durante l'utilizzo degli strumenti elettronici aziendali, all'utilizzo dello specifico codice identificativo e della parola chiave (password) assegnati. Il codice identificativo e la password sono strettamente personali e riservati ed è responsabilità del personale farne uso accorto.

La parola chiave dovrà essere composta da almeno otto caratteri, non dovrà contenere riferimenti agevolmente riconducibili all’incaricato e dovrà essere modificata dall’incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi (in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave dovrà essere modificata ogni tre mesi).

3.6. GESTIONE DEGLI INCIDENTI.

Qualsiasi incidente che dovesse accadere al sistema informativo dovrà essere comunicato agli incaricati della gestione e manutenzione degli strumenti elettronici, che interverranno prontamente avvisando il Responsabile del trattamento dei dati personali.

3.7. MANUTENZIONE DEI SISTEMI HARDWARE E SOFTWARE.

3.7.1. Le apparecchiature.

I PC, i Server e le periferiche, se utilizzati in maniera appropriata, hanno una vita media in genere superiore alla loro obsolescenza tecnica, ossia è più probabile che la loro sostituzione sia dovuta a fattori di prestazioni insufficienti dovute al rapido evolversi della tecnologia che a gravi malfunzionamenti meccanici, elettrici o elettronici. La manutenzione dei sistemi hardware riguarda quindi principalmente la sostituzione di materiale di consumo (nastri o toner per stampante, floppy disks, ecc.) e la pulizia periodica delle parti esposte all'ambiente esterno (tastiere, mouse, monitor). Gli interventi di manutenzione dovuti a guasti sono di ordine straordinario e comportano nella maggioranza dei casi la sostituzione di una parte o dell'intera apparecchiatura. Di conseguenza, gli interventi di manutenzione in seguito a guasti vanno gestiti tenendo presente la criticità delle singole apparecchiature e quindi, nel caso in oggetto, prevedendo necessariamente un contratto di assistenza tecnica per i Server, eventualmente estendibile ai PC ed alle periferiche.

3.7.2. Il software.

Per quel che riguarda i sistemi operativi dei PC e dei Server, la manutenzione consiste nel mantenerli aggiornati tramite l'installazione delle correzioni (patch, service packs, ecc.) rilasciate periodicamente dalle case produttrici.

Per quel che riguarda i programmi di protezione dai virus informatici, la manutenzione riguarda il continuo aggiornamento delle tracce virali al fine di mantenere efficace la protezione.

Per gli altri programmi applicativi vale il discorso fatto per i sistemi operativi.

Periodicamente tutti i prodotti software possono presentare la necessità di essere sostituiti da nuove versioni degli stessi ed è solitamente possibile farlo attraverso procedure di aggiornamento (upgrade) del software preesistente. In questo caso l'impatto sull'operatività è minimo. In altri casi è necessario procedere alla sostituzione integrale del pacchetto software con conseguente necessità di ripristinare le procedure di utilizzo adattandole al nuovo software.

4. MISURE DI GARANZIA DELL'INTEGRITA' E DELLA DISPONIBILITA' DEI DATI. PROTEZIONE DELLE AREE E DEI LOCALI AI FINI DI CUSTODIA E ACCESSIBILITA' DEI DATI.

4.1. ELENCO DELLE RISORSE DA PROTEGGERE.

Come prima cosa viene prodotto un elenco dettagliato delle risorse hardware e software da allegare al Documento Programmatico sulla Sicurezza.

4.2. IDENTIFICAZIONE ED AUTORIZZAZIONE.

Si procede poi all'assegnazione d'identificativi univoci ai PC ed ai Server ed alla distribuzione di codici identificativi e parole chiave (username e password) univoci agli operatori dei PC ed all'amministratore di sistema per l'accesso ai Server (come previsto dal Disciplinare tecnico in materia di misure minime di sicurezza). Sui PC e sui Server vengono quindi attivate le misure di sicurezza atte ad impedire l'accesso ai dati ed ai servizi locali e di rete ad utenti non autorizzati (username e password, blocco della console dei Server, autenticazione ai servizi di rete).

4.3. INDIVIDUAZIONE DELL'ESPOSIZIONE AL RISCHIO.

4.3.1. Il livello delle minacce ai suddetti beni.

a) **Penetrazione logica**. Il livello di tale minaccia è basso, in quanto le apparecchiature sono utilizzate solo da personale incaricato ed autorizzato il quale, durante l'orario di lavoro, è sempre presente nei locali e quindi controlla l'utilizzo delle stesse. L'accesso diretto alla console dei Server è poi limitato

anche dal fatto che essi si trovano in un unico locale non utilizzato dal personale per il normale lavoro e chiuso a chiave. L'accesso diretto alla console dei Server è protetto dal blocco della stessa che richiede l'esecuzione di una procedura di autenticazione. Al di fuori dell'orario di lavoro l'accesso ai PC è protetto tramite le misure di sicurezza fisica.

Un certo grado di minaccia è legato ad un uso malevolo dell'autorizzazione all'accesso alle risorse da parte di personale autorizzato, che potrebbe aver maturato motivi di rivalsa nei confronti del Comune. Tale minaccia è minimizzata dalla puntuale ed efficiente organizzazione degli incarichi ed autorizzazioni all'utilizzo degli elaboratori che riducono il campo d'azione dei singoli operatori non privilegiati.

L'unico vero fattore di rischio è l'introduzione di virus informatici attraverso la posta elettronica o software e dati di provenienza esterna e l'attivazione inconsapevole di applicazioni malevole durante la navigazione su Internet.

Il livello di tale minaccia viene ridotto attraverso l'utilizzo di appositi software antivirus e la sensibilizzazione del personale ai rischi della navigazione su Internet, oltre che tramite la limitazione delle possibilità di navigazione mediante misure tecniche (filtraggio via firewall) ed organizzative (policy aziendali).

b) Penetrazione sulle reti di telecomunicazioni. Il livello di tale minaccia è medio-basso. Si ha la certezza statistica che prima o poi l'indirizzo IP pubblico sarà assoggettato a scansione e a tentativo di intrusione attraverso Internet. E' altresì vero che una scansione risulta difficoltosa a causa della traduzione dell'intera rete locale sul singolo indirizzo IP pubblico.

Sono state adottate anche una serie di misure volte a ridurre i rischi di penetrazione attraverso il collegamento ad Internet (Firewall).

c) **Guasti tecnici delle apparecchiature**. Il livello di tale minaccia è in costante evoluzione ed è legato a diversi fattori, quali la qualità delle apparecchiature, la loro età, il livello di utilizzazione e la frequenza e tempestività dei lavori di manutenzione. Nella situazione in oggetto tale minaccia può definirsi ridotta al minimo possibile. Le apparecchiature sono state rinnovate, vengono utilizzate in maniera appropriata ed è in essere un contratto di manutenzione ed assistenza per la tempestiva risoluzione dei guasti tecnici. Le accurate politiche di backup contribuiscono a minimizzare ulteriormente i rischi già ridotti legati ad un eventuale guasto.

d) **Errori umani**. Il livello di tale minaccia è minimo, per quanto ineliminabile, per la competenza e professionalità del personale addetto.

e) **Minacce fisiche**. Gli uffici dove avviene il trattamento dei dati sono sorvegliati dal personale dipendente durante tutto l'orario di lavoro; durante i restanti periodi sono protetti attraverso allarme o mediante chiusura delle porte di accesso.

4.3.2. Il livello di vulnerabilità dei suddetti beni.

a) **Penetrazione logica**. La penetrazione logica riguarda i sistemi operativi e le applicazioni presenti sui calcolatori.

I sistemi operativi Windows XP/NT/2000/2003, sia Server che workstation, offrono invece solide garanzie di sicurezza logica, impedendo validamente l'accesso alla stazione di lavoro ad utenti non autorizzati.

b) **Penetrazione sulle reti di telecomunicazioni**. Alla penetrazione attraverso le reti di telecomunicazioni sono esposti tutti i PC ed i Server in quanto dotati del protocollo TCP/IP. La vulnerabilità di tali apparecchiature, con sistema operativo Windows NT/XP/2000/2003, ad un attacco DOS (Denial of Service) è elevata, così come la loro vulnerabilità a virus informatici (che costituiscono pericolo anche per i dati contenuti nei PC), la maggioranza dei quali sono appositamente studiati per colpire i prodotti della Microsoft.

c) **Guasti tecnici delle apparecchiature**. La vulnerabilità delle apparecchiature ai guasti tecnici è abbastanza bassa, in quanto si tratta di macchine progettate per un lavoro prolungato e con un numero limitato di organi meccanici, maggiormente esposti al logorio dell'uso. Tra essi sono tuttavia compresi i dischi fissi dei PC e dei Server i quali, una volta superato il periodo di vita media delle loro parti meccaniche (cuscinetti, testine), sono estremamente vulnerabili e soprattutto mettono in pericolo i dati in essi immagazzinati. Per quanto riguarda i guasti di natura elettrica, la vulnerabilità maggiore è quella degli alimentatori degli elaboratori, il guasto dei quali però, al di là di un fermo macchina per manutenzione, non comporta, se non in rari casi, danni anche alle informazioni immagazzinate nei dischi fissi.

d) **Errori umani**. La vulnerabilità delle apparecchiature agli errori umani è bassa, in quanto l'interazione degli addetti al trattamento con la parte fisica degli elaboratori si limita alle periferiche (mouse, tastiera, schermo, ecc.); tale interazione, al di là del tasto di accensione, risulta nulla con il corpo macchina e con le parti più importanti di un elaboratore.

   All'opposto, la vulnerabilità dei dati agli errori umani è totale, in quanto sono proprio essi l'oggetto dell'azione costante di elaborazione, modifica, immagazzinamento e richiamo da parte degli operatori.

e) **Minacce fisiche**. La vulnerabilità può considerarsi media considerando i tipi di serrature di sicurezza adottate.

4.4. SICUREZZA ED INTEGRITÀ DEI DATI.

E' attivo un sistema di salvataggio, con periodicità giornaliera, dei dati immagazzinati sui Server. Il salvataggio avviene su 5 cassette giornaliere, per un totale di 1 settimana di storico (1 backup al giorno per ogni giorno lavorativo).
Il backup avviene sul server IBM. Sul nastro viene copiato l’intero contenuto del server.

E’ attivo un sistema Antivirus per i PC e per la rete dotato di procedure di aggiornamento dello stesso: Symantec Norton Antivirus Enterprise 8.6.

Di seguito si elencano le norme a cui attenersi per evitare rischi provocati dai virus informatici (tali norme verranno distribuite al personale incaricato del trattamento dei dati):

Fattori di incremento del rischio e comportamenti da evitare

I seguenti comportamenti, comportano un incremento dei livelli di rischio informatico:

a) riutilizzo di dischetti già adoperati in precedenza

b) uso di software gratuito (o shareware) prelevato da siti internet o in allegato a riviste o libri

c) uso di dischetti preformattati

d) collegamento in rete, nel quale il client avvia solo applicazioni residenti nel proprio disco rigido

e) collegamento in rete, nel quale il client avvia anche applicazioni residenti sul disco rigido del Server

f) uso di modem per la posta elettronica e prelievo di file da BBS o da servizi commerciali in linea o da banche dati

g) ricezione di applicazioni e dati dall'esterno, Amministrazioni, fornitori, ecc.

h) utilizzo dello stesso computer da parte di più persone

i) collegamento in Internet con download di file eseguibili o documenti di testo da siti WEB o da siti FTP

l) collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi

m) file allegati di posta elettronica.

Norme basilari di comportamento

Al fine di evitare problemi correlati ad infezioni informatiche, dovranno essere rispettate almeno le seguenti prescrizioni:

a) i floppy disk, sia quando vengono forniti sia quando vengono ricevuti, devono essere sottoposti a scansione da parte del programma antivirus

b) è obbligatorio sottoporre a controllo tutti i floppy disk di provenienza incerta prima di eseguire o caricare uno qualsiasi dei files in esso contenuti

c) non si deve utilizzare il proprio "disco sistema" su di un altro computer se non in condizione di "protezione in scrittura"

d) proteggere in "scrittura" tutti i propri floppy disk di sistema o contenenti programmi eseguibili

e) se si utilizza un computer che necessita di un "bootstrap" da floppy, usare un floppy disk protetto in scrittura

f) non attivare mai da floppy un sistema basato su hard disk a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto

g) limitare la trasmissione di files eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computers in rete

h) non utilizzare i Server di rete come stazione di lavoro

i) non aggiungere mai dati o files ai floppy disk contenenti programmi originali.

Regole operative

1. Tutti i computer dell'Azienda devono essere dotati di programmi antivirus.
2. Il Responsabile deve assicurarsi che i computer delle società esterne, qualora interagiscano con proprio sistema informatico, siano dotati di adeguate misure di protezione antivirus.

3. Il personale delle ditte addette alla manutenzione dei supporti informatici devono usare solo dischetti preventivamente controllati e certificati singolarmente ogni volta.
4. Ogni PC deve essere costantemente sottoposto a controllo anti-virus.
5. I dischetti provenienti dall' esterno devono essere sottoposti a verifica da attuare con un PC non collegato in rete (macchina da quarantena), ed inoltre devono essere individuate le aree dell'Amministrazione che, in relazione alla loro particolare attività, sono da considerare a più alto rischio nei riguardi dell'infezione da virus.
6. All'atto della individuazione di una infezione il virus deve essere immediatamente rimosso.
7. Tutti gli utenti del sistema informatico devono sapere a chi rivolgersi per la disinfezione e l'informazione dell'infezione deve essere mantenuta riservata.
8. Il personale deve essere a conoscenza che la diffusione dei virus è punita dall'art. 615 quinquies del Codice Penale.
9. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.

Caratteristiche di base del software antivirus

Il software antivirus deve essere sottoposto a costante e frequente aggiornamento (almeno due volte al mese) ed in particolare:

a) gli aggiornamenti devono essere resi disponibili non solo per posta ma anche tramite BBS o Internet
b) deve essere particolarmente efficace contro i virus della nostra area geografica

c) deve poter effettuare automaticamente una scansione ogni volta che viene avviato un programma

d) deve poter effettuare una scansione automatica del floppy disk

e) deve accorgersi del tentativo di modificare le aree di sistema

f) deve essere in grado di effettuare scansioni a intervalli regolari e programmati

g) deve essere in grado di effettuare la scansione all'interno dei file compressi

h) deve mantenere il livello di protezione in tempo-reale

i) deve eseguire la scansione in tempo-reale

l) deve poter eseguire la rimozione del codice virale in automatico

m) in caso di impossibilità di rimozione i file non pulibili devono essere spostati una subdirectory predefinita,

n) deve essere attivo nella protezione per Applet di ActiveX e Java contenenti codice malizioso

o) deve essere in grado di effettuare la rilevazione la pulizia dei virus da Macro sconosciute

p) deve essere in condizione di rilevare e rimuovere i virus da macro senza file pattern con un grado di riconoscimento superiore al 97 %

q) deve essere in grado di riconoscere i codici virali anche in file compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo.

Considerato che in sistemi basati su reti locali o su reti geografiche, aumenta il pericolo di diffusione dei virus, ove possibile il sistema antivirus deve essere centralizzato e predisposto a svolgere almeno le funzioni di:

1. distribuzione degli aggiornamenti sia dei motori di scansione che degli eventuali file “pattern”
2. controllo e monitoraggio degli eventi virali
3. automatico spostamento in directory di “quarantena” di virus informatici risultati non pulibili
4. avviso all’amministratore di sistema di rilevazione di virus e indicazione del file “infetto”.

4.5. SICUREZZA DELLA RETE.

E’ attivo un sistema di filtraggio del traffico da e per Internet sul sistema che fa da Firewall (Symantec 200R) posto tra la rete locale e il router di collegamento ad Internet.

Tale apparato è il “default gateway” della rete locale, ossia il punto di contatto di questa con altre reti (Internet previo instradamento attraverso modem ADSL Telecom).

4.6 TRASMISSIONE DEI DATI.

I dati inviati tramite reti aperte sono protetti con opportuni standard di sicurezza come lo standard SSL 2.0 e 3.0.

Il protocollo SSL è uno standard per autenticare l'accesso ai Server tramite un meccanismo a chiave pubblica (RSA) e per scambiare in modo sicuro una chiave di crittografia tra client e server.

L'SSL, nello schema ISO-OSI, si posiziona al di sopra del livello di trasporto in modo da rendersi indipendente dall'applicazione che lo utilizza.

Il protocollo SSL permette una connessione sicura TCP/IP sicura sulla base di tre proprietà:

- le entità di comunicazione possono autenticarsi a vicenda utilizzando la crittografia a chiave pubblica:
- la confidenzialità dei dati trasmessi è garantita dall'utilizzo di una chiave di sessione generata durante l'interazione tra le parti nella prima fase del protocollo;
- l'integrità dei dati è garantita dall'utilizzo del Message Authentication Code (MAC).

L'instaurazione di una connessione sicura mediante SSL comporta una procedura di scambio messaggi fra client e server (handshaking) che si articola nei seguenti nove passi nella versione 3.0 del protocollo (la versione 2.0, che non effettua l'autenticazione del client, non prevede i passi 6 e 7):

1. Client hello: il client invia una challenge phrase al server e comunica la scelta di un algoritmo a chiave privata per lo scambio dei messaggi (DES, RC2 o RC4), di un algoritmo a chiave pubblica per lo scambio delle chiavi di sessione (RSA, Diffie-Hellman, Fortezza-KEA) e di un algoritmo di hashing (MD5).
2. Server hello: il server invia al client il proprio server certificate (ottenuto da una CA), fornisce il proprio acknowledgment ai protocolli scelti dal cliente

genera un connection identifier da usarsi nella successiva fase di comunicazione, client-server.

3. Client master key: il client verifica il server certificate inviatogli dal server (i certificati sono memorizzati nel browser per connessioni successive), genera una master session key usata come chiave generatrice di una coppia di chiavi simmetriche (una per le comunicazioni in uscita e l'altra per le comunicazioni in entrata) e la crittografa con la server public key contenuta nel public server certificate; il tutto è inviato al server.
4. Client finished: il Client, dopo aver inviato il messaggio cifrato, termina la propria sessione crittografando con la propria client-read key (server-write key) il connection identifier inviatogli dal server e si pone in attesa del messaggio server finished.
5. Server verifier: il server decrittografa la master session key inviatagli con la propria server private key, genera la coppia di chiavi simmetriche di sessione (lato server) e invia al client la challenge phrase iniziale crittografata con la server-write (Client-read) key; a questo punto il server è autenticato.
6. Request certificate: il server chiede che il client presenti un valìdo Client certificate e invia al clìent una nuova challenge phrase crittografata con la server-write (clìent-read) key.
7. Client certificate: il client invia al server una response phrase costruita crittografando, con la clìent-write key, la client public key unita all'hash (crittografato, come firma elettronica, con la client private key) della challenge phrase unita alla server public key; il server ricalcola 1'hash e lo

confronta con quello ricavato decrittografando con la client public key la firma elettronica contenuta nella response phrase (il client è ora autenticato).

8. Server finished: il server termina la propria sessione inviando al client un session identifier (un numero univoco generato ìn modo casuale), utilizzabile in ogni altra sessione per evìtare ulteriori handshaking che rallenterebbero la performance sul sistema.
9. Start communication sessions: ogni altra sessione client-server si instaurerà utilizzando le chiavi di sessione e i relativi algoritmi di crittografia simmetrici (più veloci di quelli asimmetrici) precedentemente definiti.

Al termine della procedura di autenticazione si è formato un canale sicuro in cui tutti i dati in transito vengono criptati secondo la chiave di sessione e non utilizzando la coppia di chiavi in possesso dalle due parti. Questo modo di operare porta a una comunicazione più veloce, visto che la dimensione della chiave di sessione è nettamente inferiore a quella delle chiavi segrete.

Nonostante il keyspace sia in tal modo diminuito, la sicurezza della comunicazione non viene meno, perché l'utilizzo di una chiave di sessione è limitata appunto a quel particolare scambio di informazioni e il numero di tentativi necessari per la scoperta della chiave occuperebbero un tempo troppo elevato rispetto al tempo in cui tale chiave viene utilizzata.

4.7. SICUREZZA FISICA.

Gli uffici sono disposti in due palazzine (P.zza Roma, 2 e Largo XXV Aprile, 2). In questo caso la sicurezza fisica è garantita dalle porte di accesso che presentano opportune serrature.

Accesso dei dipendenti e collaboratori: tutti i dipendenti e gli amministratori hanno le chiavi.

In conclusione l'analisi del rischio ha evidenziato una situazione di bassa esposizione per quel che riguarda:

a) Accesso non autorizzato ai dati del sistema informativo.

b) Danneggiamento dei dati e delle risorse di elaborazione da parte del personale addetto.

c) Obsolescenza delle apparecchiature e relativo aumento di incidenza dei guasti.

d) Esposizione ai virus informatici.

Un livello di rischio più elevato è legato invece ai seguenti fattori:

a) Penetrazione informatica attraverso la rete del sistema informativo.

5. CRITERI E MODALITA' PER IL RISPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

DISASTER RECOVERY. In caso di crash dei sistemi, il Comune Di Buttapietra è in grado di ripristinare i dati entro i termini stabiliti dalla legge.

6. IL PROGRAMMA DI FORMAZIONE DEGLI INCARICATI

6.1 PIANO DI FORMAZIONE.

Gli incaricati saranno formati dal Responsabile che potrà avvalersi anche di figure professionali esterne al Comune. La formazione è programmata al momento dell'ingresso in servizio degli incaricati, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.Tale Piano andrà aggiornato con cadenza annuale e tutte le volte che si renda necessario da una nuova disposizione di legge.

Il Piano dovrà prevedere:

- Un'analisi dettagliata delle vigenti disposizioni di legge, aggiornate mano a mano che entrano in vigore.
- Un'ampia rassegna delle disposizioni legislative in materia di tutela dei dati e di criminalità informatica.
- L'analisi dettagliata del Disciplinare tecnico in materia di misure minime di sicurezza.
- Un profilo degli uomini coinvolti nella tutela dei dati personali e delle loro responsabilità.
- Principi di diligenza secondo il codice civile: i profili di responsabilità penale e civile. L'inversione dell'onere della prova.
- Un'analisi approfondita degli apprestamenti di sicurezza, sia a livello di misure minime che di misure appropriate.

- Gli adempimenti ex D.lgs. 196/03 “Codice in materia di protezione dei dati personali”: notificazioni, rapporti con gli interessati, trasferimento dei dati da e per l’estero, rapporti con il Garante, incaricati, informative, consenso.
- Il D.lgs. 518/92 “Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore.
- La legge 547/93 “Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica
- La Direttiva UE 95/46/CE del 24 ottobre 1995. Direttiva “relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”.

7. CRITERI DA ADOTTARE PER GARANTIRE L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTI DI DATI PERSONALI AFFIDATI ALL'ESTERNO DELLA STRUTTURA

Vedi dichiarazione allegata fornita dai responsabili esterni.

8. IL PIANO DI VERIFICHE E DI AGGIORNAMENTO PERIODICO DEL MANUALE

Le verifiche del Piano di Sicurezza si focalizzeranno sulle seguenti tematiche:

- L'accesso fisico ai locali ove si svolge il trattamento automatizzato.
- La gestione delle parole chiave e dei profili di accesso degli incaricati.
- Le procedure atte a verificare l'integrità e l'aggiornamento dei dati personali.
- La sicurezza delle trasmissioni in rete.
- Le modalità di conservazione dei documenti, non soggetti a trattamento automatizzato.
- Le modalità di reimpiego di supporti di memorizzazione.
- Il livello di formazione ed il grado di apprendimento degli incaricati.

Sarà cura del Responsabile effettuare tali verifiche almeno 1 volta l'anno.

Il presente documento consta di 40 (quaranta) pagine, viene finito di redigere il 31 marzo 2009 e dovrà essere aggiornato entro il 31 marzo 2010 ai sensi del punto 19 dell'Allegato tecnico in materia di misure minime di sicurezza (Allegato B del D.lgs. 196/03 "Codice in materia di protezione dei dati personali").

Buttapietra, li 31 marzo 2009

Il Titolare del Trattamento

_____

Il Responsabile del Trattamento

_____