



COMUNE DI FUCECCHIO

Documento Programmatico per la Sicurezza (DPS) 2011

Decreto legislativo 30.06.03 n.196
Codice in materia di protezione dei dati personali

Allegato 1 alla Deliberazione di approvazione della Giunta comunale

SOMMARIO

Conformemente a quanto prescrive il punto 19. del Disciplinare Tecnico, Allegato B al D. Lgs.196/2003, il presente Documento Programmatico per la Sicurezza è così strutturato:

Premessa.....	3
1. Distribuzione dei compiti e delle responsabilità	4
2. Architettura della rete e mappatura delle sedi	5
3. Formazione.....	9
4. Salvataggio dei dati e ripristino.....	10
5. Analisi dei rischi e delle misure di sicurezza adottate e da attuare.....	11
Allegato A – Scheda di rilevazione dei trattamenti e delle banche dati dei settori (ad integrazione del DPS).....	18

La documentazione di dettaglio relativa alle misure preventive per l'accesso dei locali è conservata agli atti del Ced.
L'elenco dei trattamenti è approvato dai responsabili di settore, delegati dalla Giunta comunale con deliberazione n.81/2010, ad esercitare le competenze assegnate al Titolare del trattamento dalle vigenti norme al titolare del trattamento dei dati.

Premessa

L'osservanza del Codice sulla Privacy (D.Lgs.196/2003) rappresenta, oltre che un obbligo, una vera e propria opportunità per la protezione dei dati a fronte di uno scenario in cui crescono sempre più i rischi di perdita di dati legati alle "aggressioni" informatiche, con il conseguente pericolo di sospensione dei servizi e di costi gravosi per la ricostruzione degli archivi elettronici.

Il diritto alla riservatezza ed alla protezione dei dati si presenta come un bene prezioso della personalità, un diritto essenziale, la cui garanzia si attua mediante comportamenti finalizzati a costituire una "rete di protezione" attorno ai dati personali oggetto del trattamento, onde assicurare che, a seguito dell'intervenuto trattamento, la sfera soggettiva dell'interessato non sia violata o indebitamente invasa.

Privacy e sicurezza sono aspetti assolutamente coincidenti. Come afferma il Garante della Privacy, "la sicurezza non è contraddittoria alla privacy ma è invece l'unica minima garanzia e speranza che io possa avere che siano tutelati i dati dei cittadini nel contesto di così crescente bulimia e richiesta di dati. L'unica garanzia che io possa dare ai miei cittadini è che il Ced protegga le informazioni..." (Convegno "Sicurezza, privacy, efficienza dei servizi" – 22 novembre 2007).

Si tratta quindi, non solamente di adempiere ad un obbligo di legge, ma di individuare idonee misure organizzative e tecniche ed al contempo di aumentare la cultura della sicurezza nell'ente e la responsabilizzazione dell'intera struttura organizzativa

Tale è la finalità di questo documento, ossia quella di definire il quadro delle misure di sicurezza, organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato dal Comune ed affinché siano adottati gli accorgimenti opportuni per **ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.**

Il Documento Programmatico per la Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali. Riguarda il trattamento di tutti i dati personali (comuni, sensibili e giudiziari) effettuato per mezzo di strumenti elettronici di elaborazione e di strumenti non elettronici di elaborazione (cartacei, audio, visivi, audiovisivi, etc.).

Il presente Documento Programmatico sulla Sicurezza si applica a tutti gli elaboratori elettronici e supporti cartacei, a tutte le sedi, tutti i locali, tutti gli Incaricati, gli eventuali Responsabili, i Titolari del trattamento ed a tutto il personale coinvolto, a vario titolo, nel trattamento dati effettuati per nome e conto del Comune di Fucecchio.

Quadro normativo di riferimento

- Decreto Legislativo 196 del 30.6.2003 (codice della privacy) in materia di protezione dei dati personali
- Allegato B al D.Lgs. 196/2003 (Disciplinare Tecnico in Materia di Misure Minime di Sicurezza)
- Regolamento per il trattamento dei dati sensibili e giudiziari, approvato con deliberazione del Consiglio comunale n.4 del 20.1.2006
- Regolamento sul rapporto tra i cittadini e l'amministrazione comunale nello svolgimento delle attività e dei procedimenti amministrativi, contenente la disciplina del trattamento dei dati personali e della tutela della riservatezza (Titolo IV)", approvato con deliberazione del Consiglio comunale n.86 del 28 novembre 2008 e modificato con deliberazione di Consiglio Comunale n. 91 del 19.11.2010
- Direttive in materia di protezione dei dati personali approvata con deliberazione della Giunta n.81 del 26 marzo 2010

1. Distribuzione dei compiti e delle responsabilità

La Giunta comunale, con deliberazione n.81 del 26/3/2010, ha delegato ai responsabili dei settori dell'ente, ciascuno per i trattamenti e le banche dati di competenza della struttura diretta, l'esercizio delle competenze assegnate al Titolare del trattamento dalle vigenti norme al titolare del trattamento dei dati.

Ruolo	Cognome e nome	Mansione ricoperta
DELEGATI DALLA GIUNTA A SVOLGERE LE COMPETENZE ASSEGNATE DALLA LEGGE AL TITOLARE	Fattori Fera	Dirigente Settore 1
	Buti Cristina	Dirigente Settore 2
	Savini Giorgio	Dirigente Settore 3
	Comuniello Antonio	Dirigente Settore 4
	Cheti Alberto	Dirigente Settore 5
	Dini Roberto	P.O. Polizia municipale
AMMINISTRATORE DI SISTEMA	Menichetti Monica	Informatico del Ced
	Santarneckchi Carla	Informatico del Ced

2. Architettura della rete e mappatura delle sedi

Gli uffici comunali sono dislocati in sette sedi: il palazzo comunale e sei sedi remote che, ad eccezione dell'ufficio di Querce, sono collegate tra loro tramite ponti radio.

Tutti i dipendenti dotati di PC sono collegati alla rete Intranet, dalla quale possono accedere alle applicazioni dell'Ente e ad un server contenente due cartelle per ognuno; una cartella con l'accesso riservato solo al dipendente ed una dove possono accedere tutti. I dipendenti accedono ad Internet da un unico punto con connessione a 2Mb, filtrati da un firewall.

La posta elettronica è gestita internamente; ad ogni dipendente è assegnata una casella individuale; esistono caselle non nominali corrispondenti a figure istituzionali e liste di distribuzione.

Attualmente è presente un sistema centralizzato di autenticazione/autorizzazione per l'accesso alla rete: Dominio Windows 2000 utilizzato per autenticare gli utenti di risorse condivise su rete come cartelle e stampanti.

Nei personal computer con sistema Windows 2000 e XP, è stato utilizzato il sistema nativo di autenticazione tramite username e password. La validità della password è di tre mesi trascorsi i quali il sistema automaticamente chiede il rinnovo della stessa direttamente all'utente.

Le procedure applicative non utilizzano questo sistema centralizzato, ma possiedono un proprio sistema di autenticazione ed autorizzazione degli utenti.

Ad ogni singolo utente possono essere assegnate più credenziali, diverse fra loro, a seconda delle procedure applicative alle quali accede.

I server che fanno parte di questa architettura di rete sono indicati nella tabella di seguito riportata.

L'accesso alla sala macchine dei server centrali è consentito con digitazione password su centralina elettronica. Le misure preventive adottate per l'accesso ai locali sono documentate in dettaglio e conservate agli atti del CED.

Sedi comunali:

Palazzo Comunale -Via Lamarmora, 34
Casa Banti - Piazza La Vergine, 21
Polizia Municipale - Via Cesare Battisti, 71
Cantiere Comunale - Via dei Rosai, 1
Complesso Parco Corsini (Biblioteca, Museo, CIAF, Tinaia e Frantoio) - Piazza Vittorio Veneto, 26/A
Servizi Sociali - Vicolo delle Carbonaie, 1
Ufficio decentrato di Querce - Via di Ferretto 3

I server che fanno parte della architettura di rete sono indicati nella tabella di seguito riportata.

Descrizione	Configurazione HW	Configurazione SW	Locale
Server 01 (Artemis)	HP PROLIANT DL 380 3.00 Ghz Ram 2 Gb HD 80 Gb	Win 2003 Srv SP2 Domain Controller DNS Antivirus Server (T.Micro) Tomcat (Delibere) Web Server IIS Infoweb Front End Term Talk Server Cedaf (Applicazione)	Locale server
Server 02 (Chibi01)	HP PROLIANT DL 380 2.80 Ghz Ram 1 Gb HD 800 Gb	Win 2000 ADV Srv SP4 Cluster File server	Locale server
Server 03 (Chibi02)	HP PROLIANT DL 380 2.80 Gz Ram 1 Gb HD 34 Gb	Win 2000 ADV Srv SP4 Cluster File server	Locale server
Server 04 (APPL)	HP PROLIANT DL 380	Linux Application Insiel	Locale server
Server 05 (DB)	HP PROLIANT DL 380	Linux, Oracle Db server Insiel Db Cedaf (concessioni edilizie)	Locale server

Descrizione	Configurazione HW	Configurazione SW	Locale
Server 06 (Sweb)	HP PROLIANT DL 585 2.01 Ghz Ram 2 Gb HD 70 Gb	Windows 2003 Srv Sever Stand Alone (DMZ) Web Server IIS (Sito) Tomcat (sincronizzazione dati)	Locale server
Server 07 (Spro)	HP ML350	Linux Server Proxy SQUID	Locale server
Server 08 (BKVERIT AS)	HP ML310 2.53 Ghz Ram 524 Mb HD 110 Mb	Windows 2000 Backup Veritas	Locale server
Server 09 BCK3	HP Proliant DL180G6 E5504 2 GHZ Ram 4 GB HD 750GB x 3	Linux CentOS 5 Software BackupPC	Locale server
Server 10 Esx1 (Virtualizz azione)	HP PROLIANT DL 585 8 CPU x 2,009 Ghz	Server di posta Sql Server 2005 Wsus Domain controller DHCP DNS Concilia Tributi Patrimonio Intranet Syslog	Locale server

Descrizione	Configurazione HW	Configurazione SW	Locale
Server 11 Protocollo (Virtualizzazione)	HP PROLIANT DL585 G7	Server dedicato alla procedura Padoc	Locale server

Tipo di connessione ad internet	Tramite ponti radio con la rete del Circondario Empolese-Valdelsa
Tipo di Firewall	Router Board 750G
Tipo di Antivirus	Trend Micro Officescan
Frequenza di aggiornamento dell'Antivirus	Giornaliera
Elenco dei sistemi di Backup	BKVeritas e Server BCK3
Frequenza con cui vengono eseguiti i Backup	Giornaliera
Frequenza con la quale vengono cambiate le password	ogni 3 mesi

3. Formazione

Figure interessate	Personale coinvolto	Periodo	Note
Responsabili e incaricati	In occasione dell'adozione del disciplinare per l'uso delle risorse informatiche, previsto per il 2011, il Settore 1 organizzerà la formazione dei responsabili e degli incaricati, compatibilmente con la programmazione operativa degli uffici.	Nel corso del 2011	Se gli incaricati sono stagisti o collaboratori a tempo determinato si prevede la consegna di un piccolo decalogo per la sicurezza informatica al momento dell'ingresso in servizio da parte dell'Ufficio Personale

4. Salvataggio dei dati e ripristino

- ✓ Le copie di sicurezza delle banche dati informatiche a livello centralizzate sono a cura del CED.
- ✓ Sono presenti due sistemi di backup, uno su nastro ed uno su disco.
- ✓ Su un apposito server viene effettuato il backup "Backup pc" delle cartelle pubbliche e private (nel Comune è presente una sun contenente due cartelle per ogni utente, una il cui contenuto è visibile a tutti ed una visibile solo al proprietario), server APPL, server DB, server posta mentre su nastro le configurazioni di tutti i restanti server mediante il programma Veritas.
- ✓ Nell'eventualità di una perdita accidentale dei dati, è assicurato il ripristino dei dati dal giorno in cui è stato effettuato l'ultimo salvataggio.

SCHEMA DELLA SEZIONE SALVATAGGI

Banca Dati	Dispositivo di backup	Politiche di backup
Tutte le banche dati mappate	Nastro e disco	Salvataggio giornaliero. Ogni giorno viene fatto un backup incrementale con inizio dopo la mezzanotte, mentre la domenica un backup full di tutti i server. La copia su nastro è garantita per 2 mesi, quella su disco 30 giorni

5. Analisi dei rischi e delle misure di sicurezza adottate e da attuare

Macro area	Evento	Probabilità P	Danno probabile	Gravità G	Valutazione del rischio R = PxG	Misure attuate	Misura da attuare
		1=trascurabile 2 =bassa 3 =media 4 =elevata		1 = lieve 2 = reversibile 3 = parzialmente irreversibile 4 = irreversibile	R≤3 basso 4≤R≤8 moderato R≥9 elevato		
COMPORAMENTI DEGLI OPERATORI	furto di credenziali di autenticazione	1	Accesso a banche dati contenenti dati personali.	3	3	<p><i>Sistema di autenticazione alla rete conforme alla normativa:</i> Le credenziali per l'accesso alla rete ed alle singole banche dati sono conosciute solo dal titolare che deve provvedere a non divulgarle o lasciarle incustodite. La password di accesso alla rete ha validità 90 giorni; in prossimità della scadenza l'utente viene avvertito dal sistema della necessità di cambiare la propria password. Per l'accesso alle banche dati ogni procedura prevede un accesso tramite utente/password e la possibilità di avere diversi profili utente a seconda delle competenze in ambito di trattamento.</p>	<p>-Introduzione di un disciplinare per l'uso delle risorse informatiche e formazione per favorire una maggiore consapevolezza da parte del personale sui rischi e sulle misure di sicurezza da osservare nell'uso della posta elettronica, di Internet e della Intranet comunale.</p> <p>- Revisione dei profili di accesso alle procedure di anagrafe e di finanziaria ed il controllo dei log di accesso ad ogni procedura (già avviato nel 2010) tramite un programma di gestione log installato su un server virtuale (syslog), secondo le direttive del Garante della privacy.</p>
	carezza di consapevolezza, disattenzione o incuria	1	Accesso a banche dati contenenti dati personali.	3	3	Formazione dei dipendenti.	
	comportamenti sleali o fraudolenti	1	Accesso a banche dati contenenti dati personali.	3	3	Formazione dei dipendenti.	
	errore materiale	1	Perdita o indisponibilità di dati.	3	3	Formazione dei dipendenti Ripristino dei sistemi operativi.	

Macro area	Evento	Probabilità P	Danno probabile	Gravità G	Valutazione del rischio R = PxG	Misure attuate	Misura da attuare
		1=trascurabile 2 =bassa 3 =media 4 =elevata		1 = lieve 2 = reversibile 3 = parzialmente irreversibile 4 = irreversibile	R≤3 basso 4≤R≤8 moderato R≥9 elevato		
EVENTI RELATIVI AGLI STRUMENTI	azione di <i>virus</i> informatici o di codici malefici	1	Malfunzionamento degli applicativi SW	2	2	<p><i>Antivirus:</i> Su ogni Server e su ogni PC client connesso ad Internet è installato un software antivirus (Trend Micro OfficeScan) L'aggiornamento delle licenze antivirus avviene annualmente, mentre l'aggiornamento della definizione di virus viene effettuato quotidianamente.</p> <p>Sono stati installati i seguenti server: -WSUS (Windows Server Update Services) per assicurare l'aggiornamento dei sistemi operativi sui server e su tutte le postazioni; - proxy server per proteggere la rete comunale da violazioni esterne e per impostare limitazioni interne alla navigazione su Internet.</p> <p>Nel 2009 è stato avviato un piano pluriennale di acquisti per sostituire i PC con sistema operativo Windows 2000.</p>	<p>-Attivazione del proxy e definizione modalità di gestione (anche sulla base del disciplinare interno che sarà adottato nel 2011).</p> <p>-Proseguimento del piano pluriennale per sostituire i PC con sistema operativo Windows 2000.</p>

Macro area	Evento	Probabilità P	Danno probabile	Gravità G	Valutazione del rischio R = PxG	Misure attuate	Misura da attuare
		1=trascurabile 2 =bassa 3 =media 4 =elevata		1 = lieve 2 = reversibile 3 = parzialmente irreversibile 4 = irreversibile	R≤3 basso 4≤R≤8 moderato R≥9 elevato		
	spamming o altre tecniche di sabotaggio	1	Download di software nocivi che possono, in tutto o in parte, danneggiare le banche dati	2	2	Sul Server di Posta è istallato Clam , SpamAssassin , Amavisd-New e sqlgrey . Si tratta di programmi open source che funzionano rispettivamente da antivirus ed antispam. Gli aggiornamenti dei programmi vengono eseguiti periodicamente.	

Macro area	Evento	Probabilità P	Danno probabile	Gravità G	Valutazione del rischio R = PxG	Misure attuate	Misura da attuare
		1=trascurabile 2 =bassa 3 =media 4 =elevata		1 = lieve 2 = reversibile 3 = parzialmente irreversibile 4 = irreversibile	R≤3 basso 4≤R≥8 moderato R≥9 elevato		
	malfunzionamento, indisponibilità o degrado degli strumenti	1	Indisponibilità degli strumenti.	2	2	<p>I tecnici incaricati della gestione e manutenzione degli strumenti elettronici intervengono al bisogno; le anomalie possono essere evidenziate in vari modi:</p> <ul style="list-style-type: none"> - guasti individuati attraverso malfunzionamenti del sistema - anomalie riscontrate durante le fasi di controllo preventivo previste per gli apparati in questione - anomalie riscontrate sui server dal programma di controllo nagios <p>Le funzionalità vengono ripristinate entro le otto ore per i guasti bloccanti ed entro le 24 ore per i guasti non bloccanti (oppure per il tempo minimo necessario per il reperimento di pezzi da sostituire)</p>	<p>-Definizione più accurata dei controlli preventivi e relative competenze.</p> <p>-Negli anni 2011, 2012, 2013 è prevista una graduale ristrutturazione della rete nel palazzo comunale che prevede due centri stella per piano che si ricongiungono alla sala macchine. Precisamente nel 2011 sarà riorganizzato il piano secondo e la mansarda.</p> <p>-E' previsto nel 2011 l'ampliamento della banda della comunale per aumentare il livello di continuità operativa.</p>
EVENTI RELATIVI AGLI STRUMENTI	accessi esterni non autorizzati	1	Trasmissione incontrollata di dati all'esterno.	3	3	E' presente un firewall programmato in modo da rendere improbabile attacchi esterni al pc.	

Macro area	Evento	Probabilità P	Danno probabile	Gravità G	Valutazione del rischio R = PxG	Misure attuate	Misura da attuare
		1=trascurabile 2 =bassa 3 =media 4 =elevata		1 = lieve 2 = reversibile 3 = parzialmente irreversibile 4 = irreversibile	R≤3 basso 4≤R≤8 moderato R≥9 elevato		
	intercettazione di informazioni in rete	1	Trasmissione incontrollata di dati all'esterno.	3	3	E' presente un firewall programmato in modo da rendere improbabile attacchi esterni alla rete.	Entro il 2011 sarà installato un nuovo programma per la creazione ed il controllo delle credenziali di accesso ai server da parte delle ditte esterne. Questo programma permetterà direttamente al personale del ced una razionalizzazione e controllo degli accessi.
EVENTI RELATIVI AL CONTESTO	accessi non autorizzati a locali/reparti ad accesso ristretto	1	Furto di attrezzature o accesso ai PC client; furto di documenti cartacei.	3	3	In ogni edificio l'accesso ai locali è protetto da porte con chiusura a chiave. Il rischio di accesso ai singoli vani può essere definito basso, atteso che gli stessi sono dotati di porte con chiusura e l'ingresso di terzi estranei avviene solo previa accettazione e controllo.	

Macro area	Evento	Probabilità P	Danno probabile	Gravità G	Valutazione del rischio R = PxG	Misure attuate	Misura da attuare
		1=trascurabile 2 =bassa 3 =media 4 =elevata		1 = lieve 2 = reversibile 3 = parzialmente irreversibile 4 = irreversibile	R≤3 basso 4≤R≥8 moderato R≥9 elevato		
	asportazione e furto di strumenti contenenti dati	1	Accesso e/o trasmissione di dati a persone non autorizzate.	3	3	In ogni edificio l'accesso ai locali è protetto da porte con chiusura a chiave. Il rischio di accesso ai singoli vani può essere definito basso, atteso che gli stessi sono dotati di porte con chiusura e l'ingresso di terzi estranei avviene solo previa accettazione e controllo.	
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	1	Perdita completa o parziale dei dati residenti su strumenti elettronici; perdita di documenti cartacei.	4	4		- Per evitare la perdita della posta dovuta a malfunzionamenti di Outlook Express, è prevista la completa sostituzione di questo programma con Mozilla Thunderbird. Nell'anno 2011 è prevista una riorganizzazione delle cartelle private e pubbliche che permetta di accedere ai dati richiesti con maggiore facilità e logica. E' previsto il trasferimento dei server di back up in locali distanti dalla sala macchine per evitare la completa perdita di dati e configurazioni dei server nel caso di danneggiamenti nella sala macchine.

Macro area	Evento	Probabilità P	Danno probabile	Gravità G	Valutazione del rischio R = PxG	Misure attuate	Misura da attuare
		1=trascurabile 2 =bassa 3 =media 4 =elevata		1 = lieve 2 = reversibile 3 = parzialmente irreversibile 4 = irreversibile	R≤3 basso 4≤R≥8 moderato R≥9 elevato		
EVENTI RELATIVI AL CONTESTO	Guasto ai sistemi complementari (impianto elettrico, climatizzazione)	1	Perdita completa o parziale dei dati residenti su strumenti elettronici; perdita di documenti cartacei.	3	3	Ogni server è dotato di un gruppo di continuità con shutdown automatico attivato dopo 10 minuti di black-out all'alimentazione.	
	Errori umani nella gestione della sicurezza fisica	1	Perdita completa o parziale dei dati residenti su strumenti elettronici; perdita di documenti cartacei.	4	4	Formazione degli incaricati	-Introduzione di un disciplinare per l'uso delle risorse informatiche e formazione per favorire una maggiore consapevolezza da parte del personale sui rischi e sulle misure di sicurezza da osservare nell'uso della posta elettronica, di Internet e della Intranet comunale.

Allegato A – Scheda di rilevazione dei trattamenti e delle banche dati dei settori (ad integrazione del DPS)

SETTORE _____ **SERVIZIO** _____ **RESPONSABILE DEL TRATTAMENTO** _____

Descrizione	Tipologia trattamento	Tipo banca dati/archivio	Banca dati sul PC di incaricati	Eventuali responsabili esterni	Tipologia dati ¹
		Informativo e/o cartaceo	Sì/no		

Misure di sicurezza aggiuntive rispetto a quelle previste dal DPS

¹ P=Personale, S=Sensibile, G=Giudiziario