DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

(Misure di sicurezza per il trattamento di dati personali – artt. da 33 a 36 del Decreto Legislativo 30/06/2003 n. 196)

Approvato con Delibera di Giunta n. xx del xx/xx/xxxx

SEZIONE 1: GENERALITA'

Introduzione

Il D.lgs. 30 giugno 2003 n.196 garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e alla identità delle persone.
I principi fondamentali del codice in materia di protezione dei dati personali (d'ora in avanti "codice sulla privacy") in cui anche il Comune di Sesto Fiorentino si riconosce, sono:

- **Principio di necessità nel trattamento dei dati**: i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità
- **Principio di trasparenza**: il titolare del trattamento deve manifestare all'esterno e far conoscere una serie di elementi caratterizzanti la propria attività di trattamento: da qui l'esigenza di provvedere alla notifica al Garante, nei casi previsti dal decreto all'art. 37, e quella di fornire l'informativa all'interessato;
- **Adozione delle misure minime,** di cui agli artt. 33-36 e all'Allegato B (disciplinare tecnico in materia di misure minime di sicurezza) che devono essere adottate obbligatoriamente;
- **Adozione di misure di sicurezza idonee** per la protezione dei dati personali: tali misure sono quelle che devono essere valutate in *process* e adattate continuamente anche in base alle conoscenze acquisite con il progredire delle tecnologie, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, 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

Oggetto e obiettivi

Il "*Documento programmatico sulla sicurezza dei dati"* rappresenta lo *standard di sicurezza* dei dati trattati sugli elaboratori del Comune di Sesto Fiorentino ed è quindi lo strumento chiave per gestire al meglio tutti gli aspetti relativi alla sicurezza informatica dei dati e delle risorse di elaborazione che necessitano di protezione. Il presente documento viene aggiornato in caso di cambiamenti degli standard di sicurezza adottati.

Comunque, entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige (o aggiorna) anche attraverso il responsabile (se designato), il documento programmatico sulla sicurezza. Il presente documento contiene idonee informazioni riguardo a (vedi art. 19 – allegato B):

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;

- 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;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
- la previsione di interventi formativi degli incaricati del trattamento
- 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.

Il presente documento programmatico sulla sicurezza descrive le misure da adottare o già in atto al fine di:

- garantire che le informazioni siano accessibili solo alle persone autorizzate (riservatezza)
- salvaguardare l'esattezza e completezza delle informazioni e dei metodi per la loro elaborazione (integrità)
- garantire che gli utenti autorizzati abbiamo accesso alle informazioni nel momento in cui lo richiedono (disponibilità)
- garantire la sicurezza nella trasmissione dei dati
- garantire, ove richiesto, la provenienza dei dati (autenticità).

Lo scopo è di adottare criteri per il trattamento dei rischi residui: procedere non solo all'eliminazione dei rischi monitorati, ma anche alla loro riduzione o in alternativa al trasferimento degli stessi a terzi.

I rischi in generale sono imputabili a fattori quali:

- **l'inaffidabilità:** cioè la non garanzia di corretto funzionamento (hardware o software)
- **l'esposizione alle intrusioni informatiche**
- **l'errore umano.**

Il Comune di Sesto Fiorentino intende la sicurezza del proprio Sistema Informativo Automatizzato non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali", ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".

La sicurezza dei dati trattati presso il Comune di Sesto Fiorentino non dipende solo dall'utilizzo di misure di sicurezza a carattere tecnico, ma anche dalla adozione di **regole organizzative e comportamentali** seguite da tutto il personale e definite nel presente "*Documento programmatico sulla sicurezza*" ed in più precise istruzioni scritte dettagliate fornite ai dipendenti.

Tale regole comportamentali sono supportate da una **idonea formazione degli incaricati al trattamento**, pianificata fin dall'ingresso in servizio.

Campo di applicazione

Il Documento programmatico sulla sicurezza si applica a tutte le attività svolte all'interno del **Comune di Sesto Fiorentino** che abbiano un impatto sulle attività di trattamento dei dati personali.

Per quanto riguarda la tipologia di dati trattati, si precisa che il Comune di Sesto Fiorentino è ***titolare*** del trattamento dei dati, strutturati in banche dati elencate all'allegato B del presente documento (censimento degli *asset* informativi).

1.4 Termini e definizioni

Di seguito vengono riportate alcune definizioni, riprese dal D.Lgs. 30/06/2003 n. 196 e altre dal documento AIPA dell'ottobre 1999 dettante Linee Guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella Pubblica Amministrazione, che verranno utilizzate nel presente documento:

- "**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- "**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "**dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;
- "**dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- "**dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- "**titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- "**responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- "**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- "**comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

- "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- "**banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- **sicurezza fisica** il ruolo della sicurezza fisica è quello di proteggere le persone che operano sui sistemi, le aree e le componenti del sistema informativo; può essere ricondotta alla sicurezza di area (per prevenire accessi fisici non autorizzati) e sicurezza delle apparecchiature (protezione da danneggiamenti accidentali o intenzionali e sicurezza degli impianti di alimentazione e condizionamento);
- **sicurezza logica:** protezione dell'informazione e conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. Sono da intendersi come l'insieme di misure di sicurezza di carattere tecnologico e di natura procedurale ed organizzativa che concorrono nella realizzazione del livello di sicurezza da raggiungere;
- **sicurezza organizzativa:** gli aspetti organizzativi della sicurezza riguardano principalmente:

• la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo Sicurezza

• l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate (es. procedure per la gestione degli incidenti, procedure per il controllo del ciclo di vita del software; procedure per la continuità operative, procedura per la gestione della sicurezza della rete

- **monitoraggio delle misure di sicurezza**: attività di verifica continua dell'efficacia delle misure di sicurezza adottate; il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di "log" (log file), cioè i file in cui i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono tutte le principali operazioni svolte dagli utenti per loro tramite.
- **audit di sicurezza:** attività di verifica, svolte da personale che non abbia responsabilità di gestione del sistema informatico oggetto della verifica, anche non annunciate, volte a stabilire che le misure di sicurezza implementate ed il loro effettivo dispiegamento svolgano correttamente le funzionalità per cui sono state adottate.

1.5 Responsabilità in materia di sicurezza

Per la dettagliata definizione delle responsabilità in materia di sicurezza per i singoli trattamenti, si rimanda all'allegato "*matrice delle responsabilità in materia di sicurezza*". Tale documento fa parte integrante del Documento programmatico sulla sicurezza (allegato A al presente documento).

La matrice delle responsabilità contiene, fra l'altro, le seguenti informazioni:

1. IDENTIFICAZIONE DEL TRATTAMENTO
2. IDENTIFICAZIONE DEI DATI TRATTATI
3. TITOLARE DEL TRATTAMENTO
4. RESPONSABILE/I DEL TRATTAMENTO

1.6 Il sistema informatico comunale: breve descrizione

Il sistema informatico del Comune di Sesto Fiorentino è basato su una architettura di rete Fast Ethernet, che si estende dal Palazzo Comunale alle principali sedi distaccate, collegate mediante fibre ottiche di proprietà. Le sedi attualmente connesse con il centro stella (Palazzo Comunale, Piazza V.Veneto) sono:

- via Garibaldi (Polizia Municipale)
- via Gramsci (Istituzione Servizi Culturali Educativi e Sportivi)
- via Dante (Settore Assetto del Territorio)
- via delle Robinie (biblioteca di Doccia)
- via Cavallotti (Lavori pubblici)

Sono inoltre connessi mediante collegamenti in fibra i due varchi con telecamere a controllo della Zona a Traffico Limitato.

Presso tutte le sedi esiste una rete locale in cat. 5 o 6. Il numero complessivo dei client di rete nelle varie sedi citate ammonta a 336 (al 17/12/2010). Il sistema operativo client di riferimento è Windows XP Professional SP2; esiste tuttora un certo numero di macchine dotate di sistema Windows 2000 Professional SP4, destinate alla progressiva sostituzione, mentre è stata completata a fine 2006 l'eliminazione dei sistemi client Windows 95/98.

Il sistema firewall è basato su Linux (distribuzione Ubuntu) con software di packet filtering iptables. gestito dal software di configurazione OpenSource "FWBuilder" Sullo stesso firewall è inoltre implementato un sistema di content filtering per il web OpenSource "DansGuardian". La connessione ad internet avviene mediante la rete di Consiagnet accreditata presso la Rete Telematica Regionale Toscana RTRT; il collegamento è di tipo HDSL a 4 Mbit/s.

Il sistema operativo server di riferimento è Windows 2003 Server e Linux Ubuntu Server 8.04 LTS, il DBMS principale è SQL Server 2000.

Per i dettagli implementativi si rimanda al censimento asset (allegato B).

SEZIONE 2: IDENTIFICAZIONE E VALUTAZIONE DEI BENI E DEI RISCHI

2.1 Oggetto e finalità

La presente sezione definisce i criteri e le modalità operative adottate per individuare i beni da proteggere e i rischi per la sicurezza delle aree, dei dati e delle trasmissioni dei dati.

Le misure di sicurezza adottate al Comune di Sesto Fiorentino e descritte nel presente documento hanno origine da una attenta analisi dei rischi.

Tale analisi comporta una stima del rischio al fine di stabilire il livello di rischio accettabile, gli interventi per eliminare o ridurre al minimo il rischio e per minimizzare le probabilità di accadimento.

2.2 Campo di applicazione

Le indicazioni e le prescrizioni contenute nella presente sezione sono applicabili a tutte le attività connesse all'uso dei Sistemi Informativi Automatizzati.

2.3 Riferimenti normativi

art. 19.3 – Allegato B – D.Lgs. 30/06/2003 n. 196

2.4 Responsabilità

2.4.1 Titolare del trattamento

Il titolare, in quanto tale, è il soggetto che esercita poteri di indirizzo, coordinamento e controllo in materia di sicurezza. Il titolare è responsabile dell'analisi e della valutazione dei rischi che sono azioni strumentali all'adozione del documento programmatico sulla sicurezza. Nella presente sezione vengono descritte le modalità per lo svolgimento delle dette operazioni.

Il titolare può delegare ad un *Gruppo costituito ad hoc per la privacy* la effettuazione delle operazioni descritte in questa sezione. Il Gruppo può essere incaricato dal titolare di svolgere le operazioni di analisi e valutazione dei rischi secondo le disposizioni contenute nella presente sezione. Provvede a segnalare al titolare eventuali correzioni e non conformità e procede annualmente alla revisione del documento programmatico, a fronte di una nuova analisi e valutazione dei rischi.

2.5 Criteri per l'individuazione delle risorse e dei rischi

Le risorse da tutelare, al fine di adottare le misure di sicurezza, sono le seguenti:

- hardware
- software
- risorse professionali
- reti di telecomunicazione
- ambiente di lavoro/locali
- dati (personali e/o sensibili; giudiziari)
- supporti di memorizzazione

Per l'elenco di tali risorse e la loro classificazione si rimanda al documento di inventario dei beni denominato "Censimento asset sistema informativo" (allegato B al presente documento).

Esso include:

- L'identificazione e classificazione dei beni informativi (banche dati)
- L'identificazione e classificazione dei beni fisici (server, workstations, dispositivi di rete)
- Identificazione della locazione fisica
- Identificazione e classificazione del software applicativo

Compiuto il monitoraggio del sistema informativo, si è proceduto all'analisi dei rischi, che si è concretizzata nell'individuazione dei fattori di rischio e nella successiva loro valutazione.

E' da notare come il censimento, anche in base agli orientamenti del Garante, è stato condotto con un livello di dettaglio non inutilmente alto: *in particolare non rientrano nel censimento tutte le basi dati residenti sui singoli PC affidati ai dipendenti*, che sono protette in base ai criteri di buona gestione della stazione di lavoro e alle policy di sicurezza generali. Dall'allegato A (rilevazione trattamenti) è comunque possibile rilevare tutte le informazioni relative a questi trattamenti.

2.6 Criteri per la valutazione dei rischi

La metodologia adottata per l'analisi dei rischi prevede lo svolgimento delle seguenti attività:

- **Identificazione dei beni** oggetto del campo di applicazione (dati, software, hardware) e valutazione dell'impatto, in termini di perdite in cui si incorrerebbe qualora tali beni fossero, deliberatamente o accidentalmente, scoperti (perdita di riservatezza), o modificati (perdita di integrità) o fossero resi indisponibili o venissero distrutti (perdita di disponibilità).

- Analisi del rischio di tipo "qualitativa", che include l'identificazione delle **minacce** (per gruppi di beni) e stima delle connesse probabilità di manifestarsi

- Identificazione delle **vulnerabilità** (per gruppi di beni) e valutazione dei livelli di tali vulnerabilità ovvero della loro gravità intesa come probabilità che una minaccia possa essere portata a termine con successo sfruttando quella vulnerabilità

- Calcolo dei **livelli del rischio**, in base al valore dei beni ed in base ai livelli stimati delle minacce e delle vulnerabilità

- Gestione del rischio (vedi Sezione 3)

L'analisi del rischio è contenuta nella tabella allegato C al presente documento. Si è utilizzato il seguente metodo:

- per ogni *asset* rilevato nel censimento del sistema informativo si sono individuate le possibili minacce, che non sono ovviamente le stesse per le varie categorie di *asset;*

- per ogni minaccia si è stimato l'impatto sull'asset in questione, utilizzando una scala empirica da 1 a 5 (1: danno lieve; 5: danno gravissimo); l'analisi è stata effettuata in riferimento ai tre parametri di impatto (integrità, disponibilità, riservatezza: vedi anche paragrafo 1.2) ed alle possibili conseguenze in termini di valore del bene, costi di riparazione, danno all'immagine, eventuale interruzione di servizio pubblico;
- la somma delle tre tipologie di minaccia è stata quindi moltiplicata per la probabilità del verificarsi dell'evento dannoso (anche in questo caso si è utilizzata una scala da 1 a 5: livello 1 = evento improbabile; livello 5 = evento altamente probabile);
- il risultato finale (compreso fra 0 e 75, viste le scale adottate) dà un'idea del rischio complessivo per il determinato *asset.*

Le misure di sicurezza adottate o da adottare prendono spunto da questa valutazione.

Si segnala altresì che una corretta analisi del rischio dovrebbe procedere per analisi dei trattamenti, piuttosto che degli asset. Vista la complessità e la numerosità dei trattamenti, ed il fatto che la grande maggioranza di essi è di tipo "mono-asset", ovvero insiste su di un solo database, si può ritenere l'analisi *asset-based* come una buona approssimazione dell'analisi dei rischi basata sull'esame dei trattamenti dati.

2.7 La situazione rilevata

Dall'analisi così condotta, per quanto riguarda le basi dati, emerge un livello di rischio complessivamente non elevato, con picchi in corrispondenza degli accessi indesiderati in sola lettura ad un certo numero di banche dati, questo in virtù della molteplicità degli accessi richiesti per doveri d'ufficio a tali banche dati. La presenza di un numero elevato di entry point costituisce di per sé un *vulnus*, mitigabile solo con una corretta gestione della stazione di lavoro.

Per quanto riguarda gli asset fisici (server) si nota un grado di rischio leggermente più elevato per quei server in funzione da diversi anni che hanno probabilità di avaria maggiore. In questo caso si provvederà a limitare il rischio mediante l'esecuzione costante dei backup, la pronta disponibilità degli interventi di manutenzione e la progressiva eliminazione dei server obsoleti secondo un piano di rinnovamento hardware.

SEZIONE 3: LA GESTIONE DEI RISCHI: LE MISURE DI SICUREZZA PER IL TRATTAMENTO DEL RISCHIO ED IL PIANO OPERATIVO

3.1 Oggetto e finalità

Scopo della presente sezione è definire le **misure adottate e le eventuali ulteriori misure da adottare** nonché il piano operativo per la loro messa in funzione. In particolare, le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:

- **prevenzione**: attività che permette di ridurre/impedire gli incidenti di sicurezza, agendo direttamente sulla diminuzione delle probabilità di manifestazione reale di tali incidenti;
- **protezione**: attività che permette di ridurre/eliminare la gravità degli effetti nocivi dell'accadimento negativo.

Il Comune di Sesto Fiorentino programma specifiche attività di prevenzione e protezione per ognuno degli agenti di minaccia identificati.

3.2 Applicabilità

Le indicazioni e le prescrizioni contenute nella presente sezione si applicano a tutte le attività svolte dal Comune di Sesto Fiorentino, aventi influenza sul livello di sicurezza del Sistema informativo.

3.3 Riferimenti

D.lgs. 30/06/2003 n. 196
Ordinanza sindacale Comune di Sesto Fiorentino n.365/2004

3.4 Responsabilità

3.4.1 Titolare del trattamento

Il Comune di Sesto Fiorentino è titolare del trattamento dei dati contenuti nelle banche dati di cui all'allegato A del presente documento.

In qualità di titolare, il Comune di Sesto Fiorentino è il primo responsabile delle misure di sicurezza, ai sensi dell'art. 4 del D.lgs. 30/06/2003 n. 196.

La omessa adozione di misure di sicurezza è sanzionata penalmente ai sensi dell'art. 169 dello stesso decreto.

Oltre alle misure minime, il Comune di Sesto Fiorentino adotta misure ulteriori ritenute idonee alla salvaguardia dell'integrità, riservatezza e disponibilità dei dati e delle trasmissioni.

3.4.2 Responsabili del trattamento

Il titolare del trattamento ha nominato, ai sensi dell'art. 29 del D.lgs. 196/2003 più responsabili che per esperienza, capacità e affidabilità fornisce idonea garanzia del pieno rispetto delle disposizioni in materia di privacy, incluso il profilo della sicurezza. I compiti affidati ai responsabili sono analiticamente specificati per iscritto dal titolare. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle istruzioni impartite.

Il responsabile del trattamento:

- **gestisce e coordina** le attività legate alla sicurezza, sia dei soggetti interni, sia degli eventuali soggetti esterni, in base alle istruzione impartite dal titolare
- **individua e aggiorna periodicamente** le misure preventive e protettive atte alla eliminazione/riduzione dei rischi individuati
- **sottopone al titolare l'elenco delle misure preventive e protettive** e, in base alle sue indicazioni, predispone il programma di attuazione particolareggiato di tali misure.

Con ordinanze sindacali n.365/2004 e n.29/2005 e successive presso il Comune di Sesto Fiorentino sono stati individuati quali responsabili del trattamento dati i Dirigenti di Settore, limitatamente ai trattamenti effettuati nel loro settore di competenza.

Tipi di trattamento dati particolari sono stati oggetto di ordinanze ad hoc.

I Responsabili, con proprio atto, individuano gli Incaricati del trattamento fra i dipendenti appartenenti al proprio Settore.

3.5 Misure di prevenzione e protezione

Dopo aver individuato e valutato i fattori di rischio connessi alle risorse e ai beni da proteggere, vengono identificate le misure di prevenzione e protezione più idonee ad eliminare o ridurre il rischio al livello ritenuto accettabile.

Il programma di attuazione delle misure è stabilito dal responsabile del trattamento; le misure strettamente legate alla pianificazione del sistema informatico (scelte hardware-software, sistemi di networking, policy di accesso ai sistemi) sono invece di competenza del Servizio Sistemi Informativi.

3.5.1 Sicurezza fisica

Misure di sicurezza in atto

I server di rete sono posizionati in ambienti chiusi al pubblico, dotati di sistemi antincendio e di climatizzazione (tranne che per il server SV22). Tutte le sedi comunali sono dotate di sistemi di allarme antiintrusione.

I server sono alimentati tramite prese elettriche protette da gruppo di continuità per quanto riguarda il Palazzo Comunale; tutti i server situati al di fuori del Palazzo sono dotati di un gruppo di continuità elettrica a servizio del singolo asset.

Tutti i server sono dotati di sistemi di *fault-tolerance* (RAID 1 o RAID 5, alimentatori ridondati); il server firewall (SV14) è dotato di RAID 1, ed è inoltre presente un "clone" dello stesso, pronto per l'immediata attivazione in caso di guasto.

Gli hard disk dei PC destinati a rottame o comunque destinati all'alienazione, vengono resi inservibili prima della consegna agli incaricati dello smaltimento.

L'accesso al palazzo comunale è controllato durante il giorno da personale addetto, che procede all'identificazione dei visitatori non abituali. Dal 2005 è attivo un sistema di controllo interno basato su telecamere IP. Le telecamere sono dotate di rilevatore di movimento in modo da attivare la registrazione di un filmato di lunghezza impostabile.

Sono state inoltre attivate nel 2005 cinque postazioni di controllo accessi con lettore di badge e telecamera presso le cinque principali sedi comunali (Palazzo Comunale e sedi di Via Dante, Via Gramsci, Via Garibaldi, Via Barducci). Gli accessi a tali sedi sono consentiti, fuori dall'orario di apertura al pubblico, soltanto ai possessori di badge abilitato o previa identificazione da parte dell'usciere in servizio.

Presso la sede di Via Garibaldi l'ingresso per i dipendenti è separato da quello per i cittadini, che possono liberamente accedere ai soli sportelli al pubblico.

Misure di sicurezza fisica da adottare

E' prevista la climatizzazione del locale che ospita il server SV22 e la contestuale ristrutturazione della sala apparati nel Palazzo Comunale, sfruttando server di tipo rack e riorganizzando la distribuzione dei sistemi.

3.5.2 Sicurezza logica

Misure in atto: server

I server dotati di Windows Server sono dotati del più recente Service Pack di **aggiornamento** e vengono settimanalmente sottoposti ad update automatico mediante la funzione "Windows Update". Su tutti i server è installato il software antivirus (F-Secure) con aggiornamenti automatici centralizzati.

Stesso vale per i server dotati di LINUX Ubuntu 8.04 LTS server i quali sono aggiornati con cadenza almeno settimanale delle patch di sicurezza rilasciate dal mantainer "Canonical"

L'accesso alle *console* di sistema è riservato ai soli utenti amministratori – identificati nominalmente da account personali del tipo: adm.nomeproprio - ed esiste meccanismo di lock in caso di inutilizzo della console medesima oltre i 10 minuti.

E' stato messo in servizio nel 2009 un server dedicato mail/agenda/antispam/antivirus, che intercetta le mail dirette dominio *comune.sesto-fiorentino.fi.it* e pone in un'area di quarantena le email indesiderate.

Tutti i server dipartimentali vengono sottoposti a **backup** quotidiano dei dati (su nastro o su dispositivo di storage) ed esiste un'immagine dei dischi ("Ghost") che viene semestralmente rinnovata. Le cassette di salvataggio vengono utilizzate ciclicamente a gruppi di tre e custodite in stanze diverse da quelle del server sottoposto a backup.

Misure in atto: stazioni di lavoro

L'accesso alle stazioni di lavoro avviene esclusivamente tramite digitazione di nome utente e **password personale** (autenticazione su dominio Windows 2000). E' possibile effettuare un "logon" locale alla macchina solo disponendo della password di amministrazione PC, nota ai soli addetti del Servizio Sistemi Informativi.

Tutte le stazioni di lavoro sono dotate di **screen saver** protetto da password, ad attivazione automatica dopo 10 minuti di inattività da parte dell'utente; questo settaggio avviene di *default* per tutti gli utenti al momento del logon.

Tutti gli utenti, ad esclusione del gruppo di amministratori di dominio, non hanno **privilegi di amministrazione** sui singoli PC, e non possono quindi installare liberamente software né modificare le impostazioni di rete del computer.

Su tutti i PC collegati alla rete interna è installato un sistema di **antivirus** (F-Secure) con aggiornamenti centralizzati che vengono distribuiti ai client in tempo reale. Anche i PC portatili in possesso di alcuni dirigenti e funzionari sono stati installati con lo stesso criterio di mancata concessione delle credenziali di amministrazione e la stessa impostazione di antivirus; ovviamente in questo caso l'aggiornamento avviene solo al momento della riconnessione del PC alla rete comunale.

I dipendenti sono stati invitati ad adottare politiche di **clear desk** e **clear screen**: nessun documento contenente dati riservati – a partire dalle password di rete - deve essere lasciato in vista sulla scrivania, e deve essere mantenuta la massima cura nell'accesso alle applicazioni, accertandosi della chiusura delle stesse al momento di abbandono temporaneo della postazione di lavoro.

A cura del responsabile amministrazione rete è mantenuto aggiornato un archivio hardware che viene utilizzato per indirizzare le politiche di rinnovamento del parco macchine.

Misure in atto: sistema di rete

E' attualmente dislocato nelle principali sedi di lavoro almeno un server di dominio dotato di servizi DNS. Ciò consente di garantire l'**autenticazione** degli utenti anche in caso di *failure* delle connessioni in fibra ottica fra le sedi.

Misure da adottare nel breve-medio periodo: server di rete

Fino alla fine degli anni Novanta il Comune di Sesto Fiorentino ha adottato un approccio all'Information Technology di tipo "dipartimentale": ogni Settore comunale ed in pratica ogni applicativo client/server doveva in linea di principio avere a disposizione un hardware dedicato. Questa soluzione, se da un lato ha garantito la massima flessibilità nell'implementazione dei sistemi, dall'altro ha provocato una proliferazione di server di rete che ha causato un notevole dispendio di energie per la corretta gestione; è già in atto dal 2002, e proseguirà negli anni a venire, una strategia di *server consolidation,* rivolta alla riduzione del numero di server di rete ed al consolidamento degli applicativi su un numero minore di hardware con potenze di calcolo e capacità maggiori.

E' stata istituito uno strumento automatizzati di *log analysis*, che permetteranno una più efficiente gestione delle condizioni di allarme e di anomalia in rete. Il sistema raccoglie tutti i log di sistema di tutti i server – ivi compresi gli eventi di login/logoff degli utenti e degli amministratori di sistema – in modo da recepire la direttiva di disponibilità dei log in merito alle attività degli amministratori di sistema.

Misure da adottare nel breve-medio periodo: stazioni di lavoro

Il processo di ammodernamento delle stazioni di lavoro è in atto costantemente da alcuni anni, con l'obiettivo di dotare ogni dipendente di un PC che consenta di interagire al meglio con la rete, sia in termini di prestazioni della macchina che di affidabilità della stessa. E' da notare inoltre come l'adozione di Windows XP Professional o Windows 7 con l'installazione di antivirus e delle comuni applicazioni di ufficio non può essere efficientemente realizzata su hardware di livello troppo basso.

Misure da adottare nel breve-medio periodo: sistema di rete

Oltre al costante aggiornamento dei dispositivi di rete (comunque meno pressante rispetto alla condizione server-pc, data la relativa minore velocità evolutiva di tali dispositivi) è previsto entro l'anno 2011 la realizzazione di un sistema di **ridondanza** fisica delle connessioni in fibra fra sedi comunali, realizzando connessioni wireless tra il palazzo Comunale e le sedi distaccate mediante antenne direzionali ad alto guadagno da lasciare normalmente in condizione di *stand-by*. Ciò per consentire un rapido ripristino in caso di tranciatura della fibra di esercizio.

3.5.3. Politica di controllo accessi alla rete

La password personale viene assegnata dal responsabile amministrazione rete ed è soggetta a cambiamento al primo *logon* dell'utente.

Gli account di rete sono assegnati **ad personam** e non sono legati al ruolo ricoperto (non esistono utenti del tipo "ufficioX", "servizioY"). Unica eccezione è costituita dal servizio di portineria per il quale è stato creato un account ad hoc, in virtù della rapida turnazione degli addetti.

Il sistema consente un massimo di **tre tentativi di *logon*** falliti, dopo i quali si ha il blocco dell'account. Il cambio delle password è obbligatorio ogni due mesi (ferma restando la possibilità per l'utente di effettuarlo più frequentemente) e non è consentito riutilizzare le password usate nei mesi precedenti. Le password devono contenere almeno 8 caratteri.

Per gli utenti a tempo determinato si ha il *lock* automatico dell'account alla data di scadenza del contratto di lavoro; si ha l'eliminazione immediata dell'account in caso di dimissioni.

La necessità della riservatezza del proprio account di rete è stata più volte raccomandata a tutti i dipendenti.

3.5.4. Politica di controllo accessi agli applicativi e ad Internet

L'utente di rete viene abilitato di *default* al solo servizio di posta elettronica (a ogni dipendente è assegnato un indirizzo email e all'accesso al sito intranet aziendale (ospitato sul server indicato con SV01 dal censimento asset). Le altre *permissions* vengono assegnate in base alla mansione del dipendente ed alle funzioni che è destinato a svolgere.

Nel rispetto di quanto previsto dal Codice dell'Amministrazione Digitale tutti i dipendenti tecnici ed amministrativi sono dotati di casella di posta elettronica internet.

L'accesso ad Internet avviene esclusivamente attraverso proxy server (attualmente tale servizio è svolto dal server identificato con codice SV29), ed è consentito per i soli utenti autorizzati, previa domanda da parte del dirigente responsabile. I log dell'accesso ai siti vengono periodicamente controllati ad evitare abusi.

Gli applicativi in uso possiedono tutti un meccanismo proprietario di accesso (username e password). Gli account utente sono definiti dal responsabile di Settore, che identifica i dipendenti che devono accedere ad ogni singola procedura.

Sono definiti opportunamente gli utenti sui database SQL Server, con la eliminazione delle eventuali utenze di default impostate come prima installazione.

L'accesso alle procedure web esterne di servizio (ad es. SIATEL, SISTER, sistema Infocamere) avviene esclusivamente tramite digitazione di utente e password personali.

3.5.5 Sicurezza delle trasmissioni dei dati

La rete di trasmissione dati costituisce il mezzo attraverso cui è possibile l'accesso ai dati personali/sensibili ospitati sui sistemi di produzione.

L'accesso agli apparati di rete è ristretto mediante password e opportuna configurazione degli apparati stessi, in modo da impedire accessi non autorizzati e negazioni del servizio.

Il collegamento ad Internet e l'accesso ai server in DMZ avviene attraverso un firewall (identificato con SV14 nel censimento asset) ed un router (identificato con NE16 nel censimento asset) gestito direttamente da Telecom Italia nell'ambito dei rapporti con la Rete Telematica Regionale Toscana alla quale il Comune di Sesto Fiorentino aderisce. La connessione al web è di tipo HDSL 2 Mbit/s, con collegamento di backup ISDN 128 kbit/s in caso di *failure* del collegamento principale.

La configurazione del firewall impedisce connessioni dall'esterno verso la rete interna comunale, mentre sono concesse connessioni verso i server esposti nella DMZ (server SV23 e SV24).

Le connessioni verso l'esterno sono consentite a tutti gli utenti limitatamente alla porta TCP legate al servizio email (POP3 - 110). L'accesso al web avviene esclusivamente attraverso il server proxy (SV29).

Viene inoltre svolto un servizio di monitoraggio in grado di rilevare anomalie nei flussi di traffico di rete, attivando strumenti manuali di controllo del traffico dati (tipo *tcpdump*) in caso di necessità.

Su alcuni server (SV04, SV10, SV11) sono installati modem analogici per consentire l'assistenza a distanza da parte delle ditte fornitrici del software applicativo. Le connessioni avvengono mediante software dedicati (PcAnywhere, LapLink) solo su iniziativa dei dipendenti comunali autorizzati e solo verso numerazioni telefoniche predefinite: non esistono RAS attivi a disposizione sulla rete telefonica. Al termine dell'operazione di assistenza la connessione viene immediatamente disattivata.

Sono inoltre configurate alcune rotte sul firewall a servizio di selezionati server di rete (SV08, SV26, SV31) che consentono l'accesso in Terminal Server da un singolo IP specifico. Questi accessi vengono utilizzati per la teleassistenza da parte delle ditte fornitrici di software. Le imprese hanno a disposizione un account di rete per il logon ai server, normalmente disabilitato, che viene attivato solo in occasione di interventi da remoto.

Sono presenti in rete locale due access point (WiFi 802.11 g) che consentono l'accesso in LAN ai soli dispositivi individuati puntualmente tramite indirizzo MAC. E' inoltre attivata su entrambi i dispositivi la protezione crittografica WPA.

3.5.6 Sicurezza organizzativa

Gli incaricati al trattamento di dati personali e sensibili devono adottare comportamenti idonei a ridurre al minimo la possibilità di distribuzione accidentale dei dati ed in particolare:

-le stampe contenenti dati sensibili devono immediatamente essere ritirate e custodite in appositi armadi muniti di serratura;

-eventuali stampe parziali, non andate a buon fine, devono essere distrutte e non gettate in contenitori a cui tutti possono accedere;

-i PC non devono essere lasciati incustoditi una volta entrati in applicativi in grado di gestire i dati sensibili e personali (anche se il meccanismo di screen saver protetto – vedi paragrafo 3.5.2 – contribuisce ad evitare accessi indebiti);

-l'eventuale condivisione di cartelle sulla propria stazione di lavoro deve avvenire seguendo criteri di assegnazione di *permission* ed evitando la condivisione senza password.

Le procedure comportamentali per la gestione della propria postazione di lavoro, la sicurezza nella posta elettronica e le linee guida per l'utilizzo della posta elettronica costituiscono parte fondamentale del piano di formazione di cui alla sezione 4 del presente documento. E' prevista entro la fine del 2007 la redazione di un breve vademecum sulle problematiche di sicurezza e sui comportamenti da adottare, e la sua diffusione a tutti i dipendenti.

In caso di necessità di accesso al sistema temporaneo da parte di terzi, si procede alla creazione di account di rete provvisori, dotati delle *permission* minimali per lo svolgimento dell'attività.

Il personale è a conoscenza delle procedure per segnalare prontamente gli incidenti di sicurezza o eventuali minacce o debolezze (attacchi virali, comportamenti anomali della stazione di lavoro); sono state inoltre stabilite procedure per segnalare malfunzionamenti hardware e software. Dall'inizio del 2007 è operativa una procedura intranet per la segnalazione di problemi sulla propria stazione di lavoro e la conseguente richiesta di interventi tecnici.

Sono attivi contratti di manutenzione per tutte le componenti hardware del sistema (server, stampanti, PC e apparati di rete) con tempistiche di intervento prestabilite, e per ogni software applicativo gestionale. A partire dal 2003 sono stati inoltre attivati due contratti di consulenza sistemistica per interventi di emergenza e di riconfigurazione dei sistemi, rispettivamente per ambienti Windows e Linux. Il contratto di assistenza Windows è affidato all'impresa Tecnolink di Firenze, mentre l'assistenza Linux è affidata al Dr. Leandro Dardini, funzionario presso la Direzione Sistemi informativi del Comune di Montecatini Terme.

3.6 Piano di ripristino

In caso di eventi di media gravità, comportanti il danneggiamento non irreparabile di uno degli *asset* informativi, si procede con la massima celerità alla valutazione puntuale del danno, e vengono poste in atto contestualmente le misure per la riparazione dell'eventuale guasto hardware (allertando i partner del caso, i cui riferimenti vengono mantenuti aggiornati) e per il ripristino della disponibilità dei dati, sfruttando le copie di backup. Vengono inoltre avvisati i settori comunali della temporanea inaccessibilità del sistema, comunicando i tempi previsti di ripristino.

Nel caso di eventi di gravità elevata (distruzione fisica di asset, eventi calamitosi) si procede al ripristino delle funzionalità seguendo un criterio di priorità legato all'impatto della mancata disponibilità del sistema sulla cittadinanza. Il tutto ovviamente a valle della messa in sicurezza degli ambienti di lavoro ed al ripristino delle condizioni minime di funzionalità, valutando un eventuale ripristino dei dati in sedi diverse da quelle originali.

3.7 Responsabilità operative

Oltre alle attività previste per i responsabili del trattamento dati, descritte al paragrafo 3.4, si ritiene opportuno descrivere nel seguito le competenze degli addetti ai sistemi

informativi, ai quali è necessario fare riferimento sia per la gestione quotidiana del sistema sia per la gestione delle emergenze.

- *Ing. Nicola Mersi* **nome utente amministratore: adm.nicola** (Analista di Organizzazione, attuale titolare della posizione organizzativa Servizi Informativi): coordinamento delle attività di gestione ordinaria del sistema informatico; gestione dei sistemi di connessione ad internet e del web server/mail server in attuazione delle policy di sicurezza; redazione ed aggiornamento del presente DPS;

- *Gabriele Batignani* **nome utente amministratore: adm.gabriele** (gestore banche dati): gestione delle banche dati su SQL Server e delle applicazioni client/server dell'Ente; gestione del sistema antivirus centralizzato; applicazione delle policy di salvataggio dati dei server;

- Ing. Sandro Tolaini **nome utente amministratore: adm.sandro** (Analista di sistema – IT engeneering): Gestione dei sistemi operativi; Implementazione politiche di sicurezza, Gestione e manutenzione dei repository documentali

- *Sig. Maurizio Lazzeretti* **nome utente amministratore: adm.maurizio** (Analista Programmatore – responsabile rete): gestione ordinaria dei sistemi hardware (server, client) e della rete locale; responsabile della manutenzione del parco macchine; amministratore della rete (gestione utenti, group policies);

- *Sig. Federico Buci* **nome utente amministratore: adm.federico** (Collaboratore Informatico): assistenza agli utenti, collaborazione per gli interventi di ordinaria manutenzione.

I dipendenti sopraindicati compongono il gruppo "Amministratori di Sistema", con i più ampi poteri sulla gestione delle risorse informatiche.

E' presente inoltre il collaboratore coordinato e continuativo Leonardo Borgheresi che coadiuva Maurizio Lazzeretti e Federico Buci nelle attività di configurazione hw/sw e assistenza agli utenti finali.

Il gruppo lavora in sinergia, con frequenti scambi informativi, e vengono pianificate riunioni di coordinamento mensili per la programmazione delle attività.

Le attività di routine (installazione di particolari software client, configurazione di base dei PC) sono riportate in apposite schede operative che sono a disposizione dei soli amministratori sul sito intranet comunale. Questo permette di evitare errori di configurazione e di ottimizzare i tempi di esecuzione di tali operazioni.

SEZIONE 4: PIANO DI FORMAZIONE

4.1 Oggetto e obiettivi

L'introduzione di un sistema di sicurezza delle informazioni impatta certamente sulle modalità operative e sull'organizzazione del lavoro. Per questo il Comune di Sesto Fiorentino pianifica gli interventi formativi rivolti sia agli incaricati del trattamento, che ai dirigenti.

Gli incaricati al trattamento dei dati, che eseguono operazioni di trattamento su indicazione scritta del titolare o del responsabile, devono essere in possesso di competenze tecniche volte a valutare e 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.

4.2 Campo di applicazione

Le seguenti norme si applicano a tutti i dipendenti e collaboratori del Comune di Sesto Fiorentino che si trovino ad interagire con il sistema informatico dell'ente.

4.3 La pianificazione della formazione

Al fine di consolidare l'efficacia delle contromisure di sicurezza di carattere fisico, logico ed organizzativo, il Comune di Sesto Fiorentino elabora un piano di formazione del personale, che include gli aspetti concernenti la sicurezza delle informazioni.

4.4 La formazione per gli incaricati

La formazione rivolta agli incaricati del trattamento persegue i seguenti obiettivi:

- formarli sui rischi che incombono sui dati
- fornire istruzioni per il trattamento e sulle misure disponibili per prevenire incidenti di sicurezza
- fornire informazioni sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività
- fornire informazioni sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure di sicurezza adottate
- fornire le informazioni di base per un corretto uso della stazione di lavoro, delle applicazioni di ufficio, della posta elettronica e del web
- fornire le informazioni di base per l'utilizzo dei prodotti open-source per la protezione dei dati personali (tipo PGP, pretty good privacy).

4.5 La formazione dei dirigenti

La formazione rivolta ai dirigenti-responsabili trattamento, persegue i seguenti obiettivi:

- fornire le conoscenze per la corretta applicazione delle norme sulle misure minime di sicurezza dei dati personali e sulla normativa di riferimento
- fornire le conoscenze per una corretta impostazione ed aggiornamento delle politiche di sicurezza ed analisi dei rischi.

4.6 La formazione degli amministratori di sistema

Vengono organizzate, su iniziativa degli amministratori stessi, partecipazioni a convegni e corsi di formazione su tematiche riguardanti principalmente la sicurezza informatica e le nuove tecnologie. La formazione viene attuata anche con modalità a distanza (e-learning) e con momenti di applicazione "in laboratorio", ovvero in porzioni di rete protette, delle tecniche apprese.

SEZIONE 5: MONITORAGGIO DELLE MISURE ADOTTATE

5.1 Oggetto e obiettivi

L'efficacia e la validità nel tempo delle misure di sicurezza adottate è oggetto di costante monitoraggio da parte del Comune di Sesto Fiorentino

5.2 Modalità operative per il monitoraggio

Il monitoraggio continuo delle misure di sicurezza è insito nella natura stessa delle tecnologie adottate a garanzia della sicurezza dei dati trattati presso le strutture del Comune di Sesto Fiorentino.

L'attività di monitoraggio, effettuata principalmente attraverso la raccolta ed analisi dei *log file*, consente di intercettare quanto prima eventuali attacchi al sistema, tentativi riusciti o meno di accesso al sistema e l'esecuzione di operazioni sospette.

Vengono effettuate le analisi dei "*log*" dei server di rete interna e dei server presenti in DMZ.

Vengono monitorati accessi ed attività: (log eventi (user id, data, ora, log on, log off, tentativi di log on falliti, identificazione stazione di lavoro); l'attività di controllo dei log viene attualmente effettuata ad intervalli non regolari; è in programma una pianificazione più puntuale, insieme con la dotazione di strumenti automatizzati di *log analysis*.

I clock dei PC in rete sono sincronizzati con un server master che fornisce il tempo di riferimento.

Vengono periodicamente effettuati dei TCP-scan della rete interna per verificare l'eventuale presenza di servizi in ascolto su determinate porte, indizio della presenza di trojan o altri malware sulle stazioni di lavoro.

In caso di rilevazione di un incidente di sicurezza viene convocata una riunione informale degli addetti ai Sistemi Informativi, durante la quale vengono messe a punto le strategie da adottare per limitare l'eventuale danno e per evitare il ripetersi dell'incidente. Al contempo viene stabilito se estendere le misure individuate a tutte le macchine in rete, se modificare le *group policy* in atto, e viene - qualora ritenuto opportuno - comunicata formalmente ai dipendenti la presenza del rischio ed i comportamenti da adottare in merito.

INDICE

ALLEGATI

Allegato A: **elenco trattamenti dati**/matrice delle responsabilità - integrato con elenco trattamenti dati sensibili, ex Delibera Giunta n. 96 del 15/5/2006

Allegato B: **censimento degli asset informativi**

Allegato C: **documento di analisi del rischio**

Gli allegati completi sono a disposizione presso il Servizio Sistemi Informativi del Comune di Sesto Fiorentino