# D.Lgs. 196/2003

# Note Tecniche

*a cura di*

*Ing. Andrea Guido Sommaruga*

retro della copertina

# Indice

# 1 Introduzione

Il D.Lgs. 196/2003 in materia di protezione dei dati personali prevede una serie di adempimenti per la messa in sicurezza delle informazioni raccolte sia dai privati che dalle società.

Tra le misure di sicurezza imposte ci sono delle misure sia fisiche sui locali che logiche a difesa delle attrezzature e dei documenti.

Il D.Lgs. 196/2003 sostituisce completamente la precedente Legge 675/1996.

**La principale novità introdotta dal D.Lgs. 196/2003 è l'introduzione del Documento Programmatico sulla Sicurezza tra le misure minime obbligatorie** e questo estende il numero di soggetti obbligati alla compilazione del DPS.

## 1.1 Premessa

Il contenuto di questo documento può essere utilizzato come guida all'interpretazione del D.Lgs. 196/2003 ma è una semplice raccolta di considerazioni o consigli a cura dell'Autore. L'autore non si assume nessuna responsabilità in merito a danni che possono essere causati dall'implementazione dei sistemi di protezione descritti ed in merito ad eventuali interpretazioni errate o non sufficientemente aderenti al testo del D.Lgs. 196/2003.

Queste brevi note non vogliono assolutamente sostituire la documentazione di eventuali apparati o programmi usati a difesa delle reti. Per la configurazione dei Router, Firewall, Antivirus e Server si rimanda sempre ai manuali forniti con le applicazioni.

## 1.2 Proroghe

Nella G.U. del 2 marzo 2005 n.50 pubblica la Legge 1° marzo 2005, n.26 di conversione del Decreto Legge n.314 del 30 dicembre 2004, (milleproroghe) con cui si spostani i temini di applicazione del D.Lgs. 196/2003 come segue:

- al 31 dicembre 2005 (invece del 30 giugno 2005) il termine per l'adozione delle nuove misure minime di sicurezza e del DPS.
- al 31 marzo 2006 (anzichè il 30 settembre 2005) il termine per l'adeguamento tecnologico ad opera dei titolari che dispongono di strumenti che per ragioni tecniche, non consentono l'immediata applicazione delle misure minime di sicurezza (sistemi obsoleti).

# 2 Commenti al testo del D.Lgs. 196/2003

Definizione di **Dato** e di **Trattamento**.

Il codice sulla tutela dei dati personali definisce due diverse tipologie di dati, i **Dati Personali** ed i **Dati Sensibili**. Viene inoltre definito **Trattamento** qualsiasi operazione svolta sui dati raccolti sia in forma manuale che in forma automatizzata mediante elaboratori elettronici.

A seconda della tipologia di dato trattato sono stabilite diverse misure di sicurezza da adottare per la tutela dei dati.

Normalmente i dati sono raccolti come archivi cartacei ad esempio schedari o in database memorizzati su calcolatori.

Definizione di database

...prese da internet...

- *Database: Termine che indica un insieme di dati riguardanti uno stesso argomento, o più argomenti correlati tra loro. La base di dati, oltre ai dati veri e propri, deve contenere anche gli elementi necessari alla loro rappresentazione, quali ad esempio le informazioni sulla loro struttura e sulle relazioni che li legano.*
- *Database o, base dati o banca dati: Archivio (gestito per mezzo di elaboratori elettronici) di informazioni omogenee e relative ad un campo concettuale ben identificato, le quali siano state classificate, codificate, organizzate e registrate in apposite memorie in modo da facilitare il loro reperimento da parte di categorie più o meno vaste di utenti.*
- *Database: Per database (base dati, banca dati o archivio) si intende un insieme di informazioni di diverso tipo. Questi dati sono organizzati secondo criteri ben precisi che permettono una rapida consultazione. Database geografico - Database dedicato a informazioni di tipo territoriale. Dati spaziali - Dati geometrici caratterizzati da un riferimento geografico.*
- *Database: È una raccolta di informazioni organizzata in modo che un programma può selezionare velocemente i dati desiderati, è una specie di archivio elettronico. I tradizionali database sono organizzati per field, record e file (campi, righe e tabelle). Un field è una singola informazione, un record è un set completo di field ed un file è una raccolta di record.*
- *Videoscrittura: Programma che consente di scrivere documenti di testo. Ogni documento può avere formati diversi (dimensioni della pagina, impostazione dei paragrafi, caratteristiche del testo come font e stile...) ed essere in ogni momento modificato o stampato. La videoscrittura è stata una delle primissime applicazioni a passare su personal computer. Il metodo di scrittura del documento varia a seconda del tipo di applicazione utilizzata per la videoscrittura.*

...dal vocabolario della lingua Italiana TRECCANI...

- *Dato: ...con un uso più specifico in informatica, dati: elementi di un'informazione costituiti da simboli (numeri e lettere) che devono essere elaborati, per lo più elettronicamente, secondo un determinato programma; il termine compare in locuzioni che per lo più traducono le corrispondenti inglesi quali, banca di dati, memorizzazione di dati, trattamento dei dati, verifica dei dati....*

Un Database è semplicemente una **collezione di dati organizzati**.

Nel mondo cartaceo esistono tantissimi esempi di comunissimi database, basti pensare ad un dizionario o al classico elenco telefonico, sono entrambi esempi di database in cui le singole voci sono organizzate in modo di facilitarne la ricerca: nel caso degli elenchi tipicamente in ordine alfabetico.

Esistono dei programmi chiamati DBMS (Database Management System), che consentono la gestione dei dati mediante l'ausilio di strumenti informatici. Rispetto ai database cartacei, gli archivi elettronici offrono molta più flessibilità e consentono ricerche mediante chiavi multiple: cosa molto difficile con gli archivi cartacei.

Dal punto di vista informatico viene quindi definito **database relazionale** una **collezione di dati organizzata in tabelle tra loro collegate mediante chiavi di ricerca e indici**.

Esempi di programmi che gestiscono un database e quindi dei dati, sono i classici programmi di contabilità. In questo caso i programmi gestiscono degli archivi anagrafici e contabili organizzati in tabelle tra di loro correlate con indici.

I database contengono quindi "**dati**" in forma facilmente **elaborabile** con strumenti elettronici secondo procedure per lo più automatizzabili.

Questi archivi devono quindi essere protetti con tutti gli strumenti previsti dal D.Lgs. 196/2003 per le elaborazioni con strumenti elettronici.

Gli eventuali documenti prodotti con i programmi di videoscrittura o i disegni prodotti con i programmi di CAD non sono dati in senso stretto, ma possono essere considerati delle semplici copie in formato digitale dei documenti cartacei. Ai sensi del D.Lgs. 196/2003 devono sicuramente essere protetti con tutti gli strumenti per il trattamento manuale dei documenti cartacei.

*Ndr. Questa è un'interpretazione personale del testo del D.Lgs. 196/2003 motivata dalla considerazione che i documenti della videoscrittura ed i disegni non contengono "dati" nel vero senso del termine ovvero informazioni elaborabili automaticamente.*

# 3 Misure minime di sicurezza

**La principale novità introdotta dal D.Lgs. 193/2003 è il fatto di avere inserito il Documento Programmatico sulla Sicurezza (DPS) tra le misure minime di sicurezza obbligatorie.** Tutti si trovano quindi a dovere compilare il DPS.

DPS: Documento Programmatico sulla Sicurezza

Il DPS è un documento che deve descrivere le procedure adottate per garantire la sicurezza delle informazioni. Deve dettagliare i compiti e le responsabilità, deve contenere un'analisi dei dati e le misure prese per la loro protezione.

**Come prima considerazione occorre premettere che il D.Lgs. non distingue tra piccole organizzazioni come gli studi professionali e le grandi organizzazioni aziendali.**

Ovviamente le due realtà sono profondamente diverse. Nelle grandi organizzazioni l'applicazione del D.Lgs. 196/2003 segue fedelmente l'organigramma aziendale; in base alle funzioni le persone saranno dotate di differente accesso ai database aziendali.

Nel caso di piccole realtà come gli studi professionali l'attività è organizzata in modo diverso e questo prevede anche un differente approccio all'applicazione del D.Lgs. 196/2003.

La prima grande differenza è che nelle grandi organizzazioni il singolo ha una visibilità ridotta sulle informazioni aziendali mentre negli studi professionali in linea di massima tutti possono accedere a tutte le informazioni.

E' infatti abbastanza raro che ci siano differenti accessi alle informazioni secondo il ruolo delle persone. Al limite in alcuni casi ci sono limitazioni, dettate più da criteri di competenza che di reale segretezza, all'accesso a quelli che costituiscono i dati contabili della fatturazione.

Per un piccolo studio spesso è il professionista che si occupa direttamente dell'emissione delle parcelle lasciando poi all'eventuale segretaria la gestione dell'iter operativo. Gli eventuali collaboratori sono a volte lasciati esterni alla gestione della fatturazione.

La contabilità dei piccoli studi professionali comunque in genere è tenuta all'esterno dai commercialisti, le uniche cose svolte all'interno sono la fatturazione clienti il più delle volte gestita con i fogli di calcolo. La protezione delle fatture clienti comunque è solo di interesse del professionista, per quanto riguarda il D.Lgs. 196/2003 si tratta di documenti necessari per adempiere ad un obbligo di Legge.

Per quanto riguarda i progetti veri e propri svolti dagli studi professionali in genere sono accessibili a tutti i dipendenti e/o collaboratori.

Per il D.Lgs. 196/2003 è quindi necessario identificare una sola figura. Le lettere di incarico come addetto al trattamento dati saranno quindi tutte impostate alla stessa matrice, ovviamente indirizzate nominalmente alle singole persone.

## 3.1 Distribuzione dei Compiti

La fase di distribuzione dei compiti è fondamentale al fine di una corretta gestione del sistema informativo aziendale.

Per le grosse organizzazioni i compiti delle varie unità sono gestiti dai singoli capi area. Nelle realtà di una certa dimensione inoltre esiste un ufficio di Organizzazione e Metodi che stabilisce a priori i ruoli aziendali.

Nel caso di piccolissime realtà come gli studi professionali la distribuzione dei compiti è molto semplificata. In linea di massima tutte le persone dello studio devono essere al corrente dei vari progetti in modo di potere tutti collaborare, in base alle proprie competenze, allo svolgimento del progetto stesso.

Chiaramente il personale amministrativo avrà compiti orientati alla gestione amministrativa dello studio e dei progetti mente il personale tecnico avrà un ruolo più attivo per quanto riguarda le fasi del progetto vero e proprio delegando la gestione amministrativa.

Dal punto di vista delle lettere di incarico previste dal D.Lgs. 196/2003 in linea di massima tutte le persone dello studio hanno libero accesso ai documenti relativi ai progetti ed alla loro gestione amministrativa. Dovranno quindi essere redatte le singole “lettere di Incarico al trattamento” per ogni dipendente e collaboratore in cui si illustreranno i compiti ed i documenti a cui i singoli avranno accesso.

La contabilità e le procedure di gestione di paghe e stipendi sono di norma fatte gestire da studi esterni. In questo caso il Titolare dello studio deve provvedere a formalizzare le lettere di “Incarico al trattamento” anche per gli studi esterni. (Contabilità, paghe e stipendi)

## 3.2 Analisi dei rischi

La fase di analisi dei rischi serve per identificare quali sono i trattamenti dei dati che possono per loro natura esporre i dati a possibili fughe o a possibili trattamenti illeciti.

Occorre premettere che le violazioni al D.Lgs. 196/2003 possono essere fondamentalmente di due tipi:

- mancata adozione di tutte o in parte delle misure minime
- trattamento illecito dei dati raccolti

Per quanto riguarda la prima categoria di violazioni non occorrono commenti: si spiega da sola. Il discorso è leggermente più complicato per quanto riguarda il trattamento illecito.

Premesso che la Legge nasce pensando di “**proteggere**” il trattamento dei dati e non di “**vietarlo**”. La protezione consiste principalmente nell'adozione di misure passive a protezione dei dati e la definizione rigorosa delle modalità di trattamento lecite dei dati.

**I dati possono quindi essere raccolti e trattati solo per le finalità per cui sono stati raccolti**: ogni trattamento per finalità diverse è considerato illecito.

Una fase fondamentale per l'analisi dei rischi consiste nell'identificare con esattezza il tipo di dati raccolto ed analizzarne i possibili trattamenti illeciti.

Al solito per le grosse organizzazioni, in cui il sistema informativo aziendale è prevalentemente basato su database, ci possono essere molte forme di trattamento illecito dei dati inseriti ad esempio estrapolando i dati mediante funzioni di esportazione per riutilizzarli per altri fini commerciali (esempio rivendita degli stessi).

Nel caso degli studi professionali l'assenza di un vero database, con i dati inseriti in tabelle organizzate, rende minimo il rischio di trattamenti illeciti dei dati raccolti.

Ipotizzando di avere memorizzato sul server di rete solo documenti di video scrittura e disegni fatti al CAD, l'unico trattamento illecito dei dati prevedibile può essere l'estrapolazione manuale ad esempio degli indirizzi partendo dalle lettere scritte o dalle fatture emesse. Sarebbe comunque un'operazione completamente manuale che richiede molto tempo e non presenta particolari vantaggi. Si può quindi ipotizzare che il rischio di trattamento illecito dei dati inseriti, estrapolati da documenti o disegni, sia minimo.

Sempre per gli studi professionali è anche minimo il rischio di perdita dei dati sui calcolatori.

Le tipiche applicazioni di videoscrittura e di CAD sono utilizzate solo come ausilio alla produzione di materiale cartaceo quindi il sistema informatico si riduce ad essere una semplice memoria in forma digitale dei documenti archiviati nello studio in forma cartacea.

Nel caso di distruzione o perdita del sistema informatico si può sempre sapere quali dati o documenti erano inseriti basandosi sugli originali cartacei archiviati.

Chiaramente il sistema informatico è anche un ottimo ausilio per la produzione di documenti e disegni e quindi "**perderne il contenuto**" non sarebbe una cosa piacevole. Dal punto di vista pratico praticamente bloccherebbe l'attività dello studio quindi è sempre meglio non lesinare sulle copie di sicurezza (backup) indipendentemente dal fatto che queste sono richieste anche dal D.Lgs. 196/2003.

*Dal punto di vista della stesura del DPS si tratta di specificare che nello studio il sistema informatico viene utilizzato solo come ausilio alla gestione di progetti (videoscrittura) e disegni (CAD) e che l'archivio degli originali è conservato in studio in forma cartacea. Il sistema informatico ricopre quindi il ruolo marginale di copia in forma digitale degli originali cartacei conservati in studio. Non essendoci data base veri e propri bensì documenti e disegni, i dati personali sono inseriti sotto forma di indirizzi o di dati fiscali nei singoli documenti e questo ne preclude qualsiasi forma di trattamento informatico automatizzabile. Il rischio di trattamenti illeciti dei dati è quindi minimo.*

*Ndr. Dal mio punto di vista i documenti relativi ai programmi di videoscrittura ed i disegni con i CAD sono da considerarsi copie degli originali cartacei e quindi da trattare con le stesse procedure valide per gli archivi cartacei. Non sono riconducibili a dati trattati elettronicamente.*

# 4 Misure minime di sicurezza per la parte informatica

Il D.Lgs. 196/2003 prevede una serie di misure minime relative all'accesso ai sistemi informatici. Sintetizzando introduce alcuni obblighi:

A) Autenticazione per l'accesso ai sistemi informatici

B) Adozione di procedure di gestione delle Credenziali di Autenticazione

C) Utilizzazione di un sistema di autorizzazione

D) Aggiornamento periodico delle autorizzazioni di accesso

E) Protezione degli strumenti informatici

F) Adozione di procedure per effettuare copie di sicurezza e piano di disaster recovery

G) Redazione ed aggiornamento annuale del Documento Programmatico sulla Sicurezza

Anche in questo caso le modalità di adeguamento al D.Lgs. 196/2003 variano molto a seconda della dimensione dell'organizzazione.

## Autenticazione: punti A) B) C) D)

Sicuramente il punto comune, indipendentemente dalla dimensione dell'organizzazione, è che il D.Lgs. 196/2003 prevede l'identificazione degli utenti mediante autenticazione che può essere realizzata sia con una semplice procedura che chiede nome utente e password che con identificazioni biometriche delle persone. Ovviamente la prima modalità è quella più utilizzata. L'identificazione biometrica, ad esempio mediante impronte digitali, delle persone allo stato attuale presenta costi molto alti e quindi gli svantaggi superano quasi sempre i vantaggi.

Per una grossa società, in cui il sistema informatico è composto da una o più reti, da più server di rete e da vari programmi gestionali basati su database, i punti A) B) C) e D) sono di complessa gestione ed implementazione.

In questo caso occorre utilizzare sistemi di autenticazione, ovvero programmi caricati sui server, che consentano di collegare i singoli utenti con una sola autenticazione (login) a tutti i servizi di loro competenza.

Le procedure di verifica periodica delle autorizzazioni delle persone, che devono essere svolte dall'amministratore di sistema in collaborazione con i responsabili dei dati, prevedono la revoca delle autorizzazioni delle persone che hanno lasciato l'organizzazione e l'inserimento delle nuove assunzioni.

Al punto B) il D.Lgs. 196/2003 intende adottare un sistema di gestione delle autenticazioni che ad esempio obblighi tutti gli utenti ad associare una password al loro identificativo utente (user-id). La password deve soddisfare i criteri di sicurezza imposti e deve essere cambiata obbligatoriamente dopo un certo periodo di tempo variabile a seconda del tipo di dati raccolto.

Dal punto di vista del Legislatore non è possibile basarsi sulla fiducia che l'utente rispetti il cambio della password di sua spontanea volontà: se non la cambia entro una certa data il sistema informatico gli deve inibire l'accesso.

**L'autenticazione informatica e la gestione dei criteri di autenticazione è il punto più critico per le piccole realtà in particolare modo per gli studi professionali**.

Non è una cosa semplicissima da realizzare e soprattuto da mantenere. Richiede inoltre anche una buona conoscenza informatica. In molte realtà professionali è necessario l'intervento di personale esterno per la realizzazione del sistema di autenticazione.

Negli studi piccoli comunque c'è anche un altro problema: spesso ci sono delle stazioni di lavoro dedicate a compiti specifici con ad esempio la stazione di lavoro dedicata alla posta elettronica ed internet oppure la stazione di lavoro dedicata allo scanner per l'acquisizione dei documenti o disegni cartacei.

Tra le stazioni condivise tra più persone è facile anche trovare delle stazioni di lavoro dedicate al CAD ovvero dei calcolatori con monitor grande e con il programma di CAD installato. In certi studi professionali il CAD non è molto utilizzato e non viene quindi fornito a tutti gli utenti, anche per ovvie questioni di costo della licenza e della macchina per supportarlo.

Queste postazioni sono in genere condivise tra tutti gli utenti dello studio, sono quindi postazioni sempre accese e disponibili per chiunque abbia la necessità di usare internet o di acquisire i documenti.

Raramente queste macchine sono dotate di password per il loro accesso ed in qualsiasi caso sono password note a tutti, sono macchine condivise tra tutti!

L'adozione obbligatoria di password personali per l'accesso al sistema informatico vieta questa pratica: non è possibile avere stazioni di lavoro usate da tutti indistintamente con la stessa password. **Si deve sempre utilizzare il proprio codice di accesso personale al sistema informatico e questo codice non deve assolutamente essere divulgato a terzi**.

In molti piccoli studi professionali non si è dotato i sistemi informatici di password personali per ogni singolo utente perché in genere non vengono fatte distinzioni nella visibilità dei documenti: tutti gli utenti hanno accesso a tutti i documenti salvati sul server.

Il server di rete è un calcolatore che condivide il suo spazio disco tra tutti gli utenti di una rete, che prevede un suo meccanismo di autenticazione e che deve essere utilizzato come unità centrale di salvataggio dei dati.

In tanti casi di piccole o piccolissime reti oltre tutto non esiste nemmeno un server di rete. Spesso si trovano degli studi professionali con i calcolatori non collegati tra loro in rete, sono semplicissimi calcolatori su cui il singolo utente lavora e non usano nulla di condiviso, al limite la stampante collegata con il deviatore. In alcuni casi i calcolatori sono stati collegati in rete perché è stata installata internet, con il router e la connessione ADSL, ma le macchine sono rimaste a tutti gli effetti isolate tra loro. In questo caso le stampanti sono condivise mediante la rete ma nulla di più.

In queste piccole realtà l'adozione delle password di accesso personali per ogni singolo utente avrà un impatto notevole sull'organizzazione. Comunque il D.Lgs. 196/2003 indica chiaramente la necessità di utilizzare un sistema di autenticazione e quindi di dotarsi di User-id personali e password.

## Protezione dei sistemi informatici: punto E)

Il punto E), la protezione dei sistemi informatici, non presenta grosse differenze tra piccole e grandi organizzazioni. La differenza principale è solo nel tipo di tecnologia utilizzato. Per le grosse organizzazioni il firewall deve essere una macchina molto veloce altrimenti rallenta la consultazione su internet. Nelle piccole organizzazioni invece è necessario che gli strumenti utilizzati richiedano la minima manutenzione da parte dell'utente che, il più delle volte, non ha sufficienti strumenti informatici per gestirli.

- adozione di software antivirus
- adozione firewall a protezione dell'accesso ad internet

Nel caso del software antivirus è richiesto un periodico aggiornamento delle definizioni dei virus. Il D.Lgs. 196/2003 richiede l'aggiornamento con una frequenza al massimo semestrale.

L'obbligo di dotare i sistemi di antivirus aggiornati, oltre ad una norma di Legge, è anche adottata dal buon senso: non è possibile avere un sistema funzionante in modo affidabile senza un antivirus. Basta un nulla per trovarsi il sistema infettato dai virus.

Per le grandi organizzazioni i servizi di antivirus e di firewall vengono gestiti completamente dal personale del centro elaborazione dati che provvede in modo centralizzato all'aggiornamento quotidiano degli antivirus ed all'aggiornamento delle regole sui firewall. Dal punto di vista dell'utente le operazioni sono comunque tutte trasparenti.

Nelle piccole organizzazioni e negli studi professionali è più difficile incontrare servizi di antivirus centralizzati. In linea di massima l'antivirus è installato manualmente su tutti i calcolatori degli utenti e viene mantenuto aggiornato mediante semplici automatismi che verificano automaticamente se esistono aggiornamenti e li installano.

Per quanto riguarda i firewall in genere le piccole organizzazioni non sono dotate di veri e propri firewall ma adottano dei piccoli router per la connessione ad internet della rete che realizzano il firewall a livello di nat ovvero dall'esterno è in genere possibile accedere solo all'indirizzo pubblico del router ma non alle singole macchine della rete.

Questi dispositivi non sono in genere caratterizzati da un altissimo livello di sicurezza, soprattutto viste le scarse informazioni che danno i fornitori di telefonia in fase di installazione, ma nelle piccole organizzazioni e negli studi professionali dove spesso manca una figura con conoscenze informatiche approfondite, non ha senso usare tecnologie più sofisticate perché potrebbero per assurdo essere usate peggio.

## Salvataggio dati: Punto F)

Il D.Lgs. 196/2003 prevede anche al punto F) la definizione di un piano di salvataggio dei dati. Per capirne lo scopo è necessario ricordare che il **Legislatore vuole imporre degli standard minimi di sicurezza per garantire la conservazione dei dati e la loro accessibilità nel tempo**. Si deve infatti essere sempre in grado di rispondere entro 7 giorni all'eventuale richiesta da parte di una persona o del Garante di sapere se vengono trattati i dati personali del soggetto in questione e se si quali. Non è quindi ipotizzabile la risposta del tipo non posso sapere che dati ho raccolto perché non funziona il sistema informatico oppure perché a causa di un guasto ho perso tutti i dati.

Per adeguarsi al D.Lgs. 196/2003 è quindi necessario predisporre un piano di salvataggio periodico dei dati, prevedendo anche le procedure per l'archiviazione dei supporti di salvataggio e le procedure per la loro eventuale distruzione qualora non servano più allo scopo. **La procedura per il salvataggio deve essere dettagliata nel DPS. Analogamente in fase di distribuzione dei compiti al personale deve essere identificata la persona che si deve occupare di fare ed archiviare le copie di sicurezza e questo compito deve essere specificato nella lettera di incarico**.

Nel caso degli studi professionali, come ho già più volte sottolineato in questo documento, non si utilizzano quasi mai dei database ma si ha quasi sempre a che fare con documenti prodotti da videoscrittura e da programmi di CAD.

**Anche nel caso degli studi professionali le copie di sicurezza sono essenziali, oltre che per adempiere ad un obbligo di Legge, per garantire il salvataggio del lavoro svolto e di non perdere documenti in caso di guasti al sistema o di problemi con virus.**

Le copie di sicurezza possono comunque essere effettuate anche salvando i direttori in cui sono contenuti i documenti su dei normalissimi CD-R o DVD-R a seconda della mole di documenti da salvare. E' comunque necessario documentare la procedura adottata nel DPS ed incaricare esplicitamente un addetto al salvataggio dati.

## 4.1 Misure minime a protezione dei locali

La protezione dei locali, nel caso di grosse realtà aziendali, assume una notevole importanza. Sono necessari sistemi di allarme antifurto e antincendio ed in alcuni casi anche il controllo ai cancelli per evitare che il personale possa trafugare materiali o documenti.

Negli studi professionali in genere le cose sono molto più semplici. Il personale molte volte ha le chiavi per l'accesso ai locali e lo studio si basa su un rapporto di reciproca fiducia.

Come misure minime a protezione dei locali in genere è adottata una porta blindata, un impianto di allarme e possibilmente l'impianto antincendio.

## 4.2 Modalità di ripristino del sistema informativo

Il D.Lgs. 196/2003, come più volte illustrato in questo documento, non distingue grandi realtà e piccole organizzazioni.

Oltre alle procedure di salvataggio dei dati / documenti vere e proprie il **D.Lgs. 196/2003 impone anche l'adozione di un piano di ripristino del sistema in caso di evento catastrofico: il piano di disaster recovery che deve ovviamente essere dettagliato nel DPS e deve contenere tutte le informazioni per il ripristino del sistema in caso di evento grave** come ad esempio la distruzione totale delle macchine.

Per le grosse società il sistema informativo è di una certa complessità, c'è la sala macchine che contiene i server aziendali ed il personale del CED (Centro Elaborazione Dati) che li gestisce. In questo caso il personale del CED si preoccupa sia dei salvataggi quotidiani del sistema che di pianificare la gestione dell'eventuale ripristino della disponibilità dei sistemi (disaster recovery) in caso di evento che danneggi seriamente la struttura.

I sistemi informativi delle grosse aziende sono impostati su database, per potere disporre dei dati è necessario avere perfettamente funzionanti i sistemi su cui girano i programmi per la gestione dei database. In caso di eventi disastrosi è si deve come prima cosa ripristinare la funzionalità di tutti i server quindi ricaricare i salvataggi dei database dalle copie di sicurezza. Queste procedure non sono molto semplici e richiedono un piano dettagliato di disaster recovery.

Per gli studi professionali la situazione è profondamente diversa.

Come già accennato in precedenza in genere negli studi professionali non ci sono data base quindi il ripristino del sistema a seguito di eventi disastrosi è molto semplice.

I salvataggi dei documenti (videoscrittura e disegni) vengono fatti generalmente su dispositivi rimovibili, come dischi fissi esterni o CD-R, e per ripristinare il sistema è in genere sufficiente disporre di un nuovo calcolatore funzionante, caricare i programmi utilizzati (videoscrittura e CAD) e ripristinare i dati dai backup.

Il piano di disaster recovery per uno studio professionale in cui non si utilizza nessun particolare database (Microsoft Access non conta!) si riduce ad un semplice elenco dei programmi da installare su ogni singolo calcolatore con le eventuali chiavi di licenza dei programmi utilizzati: deve comunque essere dettagliato nel DPS.

Per il ripristino delle funzionalità del sistema è sufficiente disporre di un calcolatore, con caratteristiche simili a quelli distrutti, sul quale ricaricare i documenti.

*Ndr. Ribadisco il concetto che per gli studi professionali non è essenziale avere la disponibilità del sistema informatico per sapere quali dati personali si trattano: salvo casi particolari sono solo dati fiscali relativi ai vari lavori svolti.*

## 4.3 Piano di formazione

**Il D.Lgs. 196/2003 considera la sicurezza un fatto dinamico**. Non è possibile fare una fotografia statica del piano di sicurezza perché, soprattutto per la parte informatica, è soggetto a continui piccoli ritocchi in funzione del cambio della tecnologia utilizzata.

Nelle grandi organizzazioni questi cambi sono pianificati con interventi formativi in aula illustrando le modifiche ai singoli responsabili di area che saranno poi portavoce per illustrare le variazioni alle persone del loro gruppo. Con molti dipendenti la formazione richiede una pianificazione a priori: non è possibile introdurre nessun cambiamento se prima non si è previsto l'opportuno piano di formazione per comunicare il cambiamento al personale altrimenti si rischiano delle disfunzioni.

Nei piccoli studi le cose sono decisamente diverse, l'introduzione di una qualsiasi novità è in genere immediatamente comunicata a tutti. Dato il numero ridotto di persone da avvisare è ipotizzabile anche una normalissima comunicazione a voce delle novità introdotte.

Dal punto di vista del DPS previsto dal D.Lgs. 192/2003 questo si riduce in una semplice annotazione alla voce “pianificazione interventi formativi” inserendo una frase di questo tipo: “*Le eventuali modifiche introdotte al piano di sicurezza saranno immediatamente comunicate a tutto il personale dipendente ed ai collaboratori mediante comunicazione orale o, ove necessario per motivi di complessità, anche con comunicazione scritta che riepiloghi le principali novità introdotte”*.

## 4.4 Aggiornamenti del DPS

La sicurezza non è un fatto statico, soprattutto per le parti legate all'informatica la tecnologia continua a correre e si devono adeguare le procedure relative alla sicurezza in base ai cambi della tecnologia disponibile.

Anche il Documento Programmatico della Sicurezza deve riportare queste eventuali variazioni. Allo scopo il legislatore ha previsto che il DPS debba obbligatoriamente essere riesaminato entro il 31 marzo di ogni anno solare.

Ovviamente “riesaminato” non significa che deve per forza essere modificato: è anche possibile constatare che non ci sono stati cambi significativi rispetto all'edizione precedente e quindi convalidare l'edizione precedente anche per un altro anno.

*Ndr. nel D.Lgs 196/2003 non ho trovato un esplicito riferimento alla necessità di dotare il DPS e le sue successive versioni di “Data Certa” però si fa cenno a delle date entro le quali tali documenti devono essere prodotti. Personalmente ritengo di interpretare questi vincoli temporali come la necessità di dotare il DPS e le successive revisioni di “Data Certa”.*

# 5 Riepilogo delle misure minime

Misure minime di sicurezza:

- Stesura del Documento Programmatico sulla Sicurezza (DPS)
  E' considerata una misura minima di sicurezza obbligatoria.
- Definizione compiti e responsabilità
  E' una fase preparatoria in cui si delineano i compiti delle varie persone
- Lettere di Incarico Trattamento dati
  Incarico nominale per tutti i dipendenti ed i collaboratori: si tratta di predisporre le lettere di incarico a durata illimitata e revocabile in qualsiasi momento, consegnalre agli interessati e farsi firmare una copia per ricevuta.
- Adozione sistema di Autenticazione sul sistema informatico
  Si tratta di attivare il meccanismo delle password del sistema operativo.
  Puo' essere un lavoro complesso che richiede l'intervento di personale competente.
- Adozione di politiche per il cambio password periodico
  Si tratta di attivare le funzioni di cambio password obbligatorie del sistema operativo.
  Puo' essere un lavoro complesso che richiede l'intervento di personale competente.
- Adozione di una procedura di salvataggio periodico dati
  Definire che cosa si deve salvare, con che frequenza e come (ad esempio tutti i documenti su CD-R una volta alla settimana). Si deve anche definire dove archiviare i supporti usati per il salvataggio.
- Adozione di un dispositivo di sicurezza, firewall, a protezione da internet
  **Richiede l'intervento di persone competenti**. E' comunque fondamentale per la sicurezza del sistema
- Adozione di un programma antivirus da mantenere aggiornato periodicamente.
  Installare su tutti i calcolatori e sul server un programma antivirus ed attivare le funzioni di aggiornamento automatico se la rete è collegata ad internet oppure procedere all'aggiornamento manuale se la rete non è collegata ad internet.
  E' una misura essenziale per l'integrità dei dati.
- Istruzione al personale
  Ricordarsi di illustrare sempre a tutti gli utenti del sistema informativo le eventuali variazioni alle procedure di sicurezza. Queste variazioni devono comunque essere annotate anche sul DPS.
- Aggiornamento annuale del DPS
  Provvedere alla revisione almeno annuale del DPS per verificare che sia sempre attuale e che non si basi su sistemi di protezione superati.

# 6 La sicurezza in 13 punti

1. **UTILIZZATE LE CHIAVI!**
   Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.

1. **CONSERVATE I DISCHETTI IN UN LUOGO SICURO**
   Per i dischetti si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato.Riponeteli sotto chiave non appena avete finito di usarli.

1. **UTILIZZATE LE PASSWORD**
   Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:
   La password di accesso al computer (BIOS) impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
   La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato ai Vostri dati sui server.
   La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.
   Imparate a utilizzare questi tre tipi fondamentali di password. Scegliete una password facile da ricordare na difficile da indovinare!

1. **ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI**
   Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete le stampe quando non servono più.

1. **NON LASCIATE TRACCIA DEI DATI RISERVATI**
   Quando riutilizzate un dischetto, prima riformattatelo sempre. Per evitare problemi non riutilizzate mai i CD-R non completamente scritti.. Nel dubbio, è sempre meglio usare un supporto nuovo.

1. **PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI**
   I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, utilizzate una procedura di backup periodico e proteggete il portatile con le password di accensione.

1. **NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD**
   Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

1. **CUSTODITE LE PASSWORD IN UN LUOGO SICURO**
   Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

1. **NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ**
   Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

1. **NON UTILIZZATE APPARECCHI NON AUTORIZZATI**
   L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la Rete, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con l'Amministratore di rete.

1. **NON INSTALLATE PROGRAMMI NON AUTORIZZATI**
   Utilizzate solo i programmi autorizzati dall'Amministratore di rete. Non fidatevi assolutamente dei programmi trovati su CD o scaricati da Internet.

1. **APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS**
   La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

1. **CONTROLLATE LA POLITICA LOCALE RELATIVA AI BACKUP**
   Verificate personalmente che i Vostri dati siano regolarmente salvati dal Responsabile dei Backup.

# 7 A proposito dell'impaginazione

In questo modello sono stati introdotti 5 stili di paragrafo personalizzati :

- Text body 1,2 e 3 rispettivamente per il corpo del testo seguente le intestazioni Heading 1,2 e 3 (Intestazione 1,2,3 nella versione localizzata). L'impostazione di questi stili avviene automaticamente ogni volta che si va a capo dopo una delle intestazioni citate. Utilizzano il carattere Times.

. Titolo Copertina, Già Esplicativo Nel Nome. Utilizza Il Carattere Times.

- Testo riportato. E' utile per riportare brevi testi contenenti codice di programmazione per macro, StarBasic, etc. Utilizza il carattere Courier.

Nel caso non vengano automaticamente attivati, questi stili si possono applicare manualmente, selezionandoli tra gli stili personalizzati (Modelli Utente) contenuti nello Stilista (premere il tasto F11 per visualizzarlo/nasconderlo)

Sono stati modificati anche 3 degli stili standard e cioè Heading 1,2,3 (Intestazione 1,2,3 nella versione localizzata), con uno sfondo giallo, ombreggiato con riquadro grigio-azzurro, esattamente come i titoli riportati in queste pagine.

Nelle righe d'intestazione sono riportati automaticamente i titoli dei capitoli modificati con lo stile Heading 1 (Intestazione 1) più il numero di versione che deve essere modificato manualmente.

Ne piè di pagina è indicata la data corrente e il numero di pagina. Dal momento che questo documento è stato pensato per la stampa, i due campi sono alternativamente posizionati a destra e a sinistra, utilizzando due stili di pagina diversi, in modo da rispecchiare l'andamento delle pagine stampate. Per lo stesso motivo è stata introdotta una pagina di retro-copertina.

L'indice è modificabile in automatico a patto che si siano utilizzati gli stili contenuti nello Stilista. E' sufficiente posizionare il cursore lampeggiante al suo interno (1 click sinistro) e poi cliccare col tasto destro su di esso, scegliendo Update Index (Aggiorna Indice).

La sezione World Wide Web può essere tolta se non si desidera pubblicare il proprio lavoro per OpenOffice.org o, eventualmente, la si può modificare a propria discrezione.

La sezione licenza dovrebbe essere opportunamente compilata con i propri dati e le disposizioni di licenza che si desiderano. Si consiglia, inoltre, di adottare la GNU Free Documentation License seguendo così la tradizione del Software Libero che permette la libera distribuzione e modifica dei documenti prodotti, nel rispetto delle condizioni della licenza citata.

# 8 Crediti, Ringraziamenti, Licenza

## 8.1 Crediti

Autore dell'impaginazione grafica del modello : Mirto Silvio Busico <m.busico@ieee.org>

Autore del testo introduttivo al modello : Gianluca Turconi <luctur@openoffice.org>

## 8.2 Ringraziamenti

A tutti i volontari che ogni giorno dedicano parte del loro tempo per realizzare le migliaia di applicazioni Open Source e a tutti gli utenti che accettano di impegnarsi nella migrazione dalle applicazioni commerciali a cui sono abituati, alle nuove applicazioni Open Source.

In particolare per gli spunti sull'impaginazione grafica del modello ringrazio Mirto Silvio Busico e Gianluca Turconi.

## 8.3 Licenza