D.Lgs. 196/2003
DPS

versione 1.0

Dicembre 2005

a cura di

andrea guido sommaruga

Revisioni

v. 0.3 – Modificato lettere Nomina Incaricati

v. 1.0 – Estratto le lettere ed inserite in un documento a parte

viale tunisia, 25 - 20124 - Milano

retro della copertina

(inserito per la gestione delle stampe in fronte retro)

Indice

1 D.Lgs. 196/2003

Con il D.Lgs. 196/2003 è stata inserita tra le misure minime obbligatorie di sicurezza anche la stesura del Documento Programmatico della Sicurezza (DPS) che deve descrivere le misure prese a tutela dei dati raccolti.

1.1 Premessa

[..il presente DPS è stato redatto pensando ad uno studio tecnico di Geometra/Ingegnere/Architetto che fa attività principalmente di progettazione/direzione lavori. Per attività di tipo diverso deve essere riadattato..]

Il presente documento, in ottemperanza alle prescrizioni del D.Lgs. n. 196/2003 ("Codice della Privacy"), individua le linee guida generali, le azioni e le misure per il trattamento dei dati personali in condizione di sicurezza con la finalità di ridurre al minimo, con riferimento alla tipologia dei dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

Il sistema informatico descritto nel presente documento deve ritenersi sicuro in quanto intende garantire la disponibilità, l'integrità e l'autenticità, nonché la riservatezza dell'informazione e dei servizi per il trattamento, attraverso l'attribuzione di specifici incarichi, la certificazione delle fonti di provenienza dei dati e le istruzioni per le persone autorizzate ad effettuare i trattamenti.

La stesura del presente documento si ispira a:

1. identificazione e distinzione delle responsabilità delle figure coinvolte nel trattamento; l'identificazione, l'inventario e l'analisi dell'hardware, del software e delle banche dati
2. valutazione del rischio
3. esposizione delle misure di sicurezza preventive e correttive
4. piano di formazione agli incaricati ed elenco adempimenti periodici

Questo documento non vuole essere un manuale di utilizzo dei vari programmi e dei vari sistemi operativi. Nel documento viene detto "*che cosa fare*" e non "*come farlo*".

Per istruzioni dettagliate sul "*come fare*" occorre fare riferimento ai manuali dei vari programmi utilizzati.

1.2 Altri documenti correlati

2 Organigramma

2.1 Definizione dei Soggetti

Ai sensi del D.Lgs. 196/2003 il Titolare del Trattamento dei dati viene identificato nel titolare dello studio [completare nome cognome]

Il Titolare del Trattamento dei dati, data l'organizzazione dello studio professionale, ricopre anche la funzione di Responsabile del Trattamento dei dati. Procede quindi alla nomina degli Incaricati al trattamento e di un Amministratore di sistema.

L'Amministratore di Sistema ha il compito di affiancare il Responsabile al trattamento dei dati per quanto riguarda le parti tecniche di configurazione delle attrezzature informatiche e l'implementazione del meccanismo di autenticazione. [..completare o modificare, può essere una persona esterna..]

Vengono nominati, mediante lettera controfirmata per accettazione, i seguenti soggetti:

Nomina	Persona nominata
Responsabile del trattamento	Non viene fatta nomina, il Titolare del trattamento è automaticamente anche il Responsabile del trattamento.
Amministratore di Sistema	[..nome, cognome, ruolo..]
Personale Dipendente	
Incaricato al trattamento	[..nome, cognome, ruolo..]
	[..nome, cognome, ruolo..]
	[..nome, cognome, ruolo..]
	[..nome, cognome, ruolo..]
	[..nome, cognome, ruolo..]
Collaboratori Esterni	
	[..nome, cognome, ruolo..]
	[..nome, cognome, ruolo..]
	[..nome, cognome, ruolo..]
Società di servizi Esterne	
Commercialista	[..ragione sociale ruolo..]
Studio Legale	[..ragione sociale ruolo..]
Impresa di pulizie	[..ragione sociale ruolo..]

3 Inventario

3.1 Elenco dei calcolatori utilizzati

La seguente tabella riepiloga i calcolatori in dotazione dello Studio. Ogni calcolatore viene identificato mediante un numero progressivo di inventario per le attrezzature informatiche. Il numero di inventario viene attribuito alle sole unità centrali e viene utilizzato per identificare univocamente ogni singola postazione di lavoro ai fini del D.Lgs. 196/2003 e per la gestione delle Licenze del software installato.

Per ogni calcolatore è riportato il numero identificativo, la marca ed il modello, la data di acquisto, il principale utente del calcolatore, la funzione del calcolatore ed il sistema operativo utilizzato.

La data di acquisto serve per avere un'idea dell'affidabilità della macchina. Oltre una certa età i calcolatori non sono più in grado di sostenere compiti critici.

Tabella calcolatori

nr	Marca/modello	Data Acq.	Utilizzatore	Tipo	S.Operat.
srv-1				Server	Win2000 server
pc-1				Stazione lavoro	win 98
pc-2				Stazione lavoro	win 98
pc-3				Stazione lavoro	XP pro
pc-4				Stazione lavoro	XP pro
pc-5				Stazione lavoro	XP pro

[..adeguare alla realtà..]

3.2 Elenco dei programmi utilizzati

La seguente tabella riepiloga i principali programmi in uso presso lo studio. Per ogni singolo programma viene identificato il campo di utilizzo ed il tipo di informazioni trattate.

Come ulteriore documentazione, indipendentemente dal D.Lgs. 196/2003 conviene inoltre conservare un elenco di tutte le licenze del software in uso. Le licenze devono essere archiviate in raccoglitori e mantenute rigorosamente in ordine: può essere necessario esibire alla Guardia di Finanza le licenze dei programmi acquistati.

Nel caso di utilizzo di programmi gratuiti o open source si consiglia di archiviare tra le licenze la copia stampata da internet del sito web da cui sono stati scaricati. Si ricorda comunque che anche i programmi gratuiti sono sempre forniti con una licenza (in genere scritta in qualche file associato al programma). E' sempre meglio verificare di persona che la licenza consenta l'utilizzo anche in ambito lavorativo dei programmi in questione. Ci sono molti programmi gratuiti solo per uso personale.

Tabella programmi utilizzati

Programma	Tipo di trattamento	Contiene Dati
Videoscrittura / fogli calcolo	Elaborazione testi e fogli di calcolo	NON CONTENGONO DATI
CAD	Disegno	NON CONTENGONO DATI
Programma posta elettronica	Posta elettronica	Contiene le rubriche indirizzi email ed i messaggi di posta elettronica

Programma di Contabilità	Dati amministrativi fatture clienti / fornitori	Database clienti fornitori

[..adeguare l'elenco in base ai programmi realmente utilizzati..]

3.3 Elenco delle banche dati su calcolatore

Con il temine banca dati si intende un'insieme di tabelle tra di loro collegate in cui i dati sono organizzati in record e campi. La banca dati contiene quindi “dati trattabili con sistemi informatici”.

La successiva tabella riepiloga le banche dati memorizzate sui calcolatori dello studio.

tabella banche dati su sistema informatico

Banca Dati	Tipo di trattamento	Tipo Dati	Archiviati su
Contabilità	Gestione amministrativa fatturazione clienti e fornitori	GENERICI	server
Rubrica indirizzi email	Elenco indirizzi posta elettronica	PERSONALI	server

[..adeguare in base ai programmi usati, verificare se si utilizza un programma di contabilità..]

3.4 Elenco delle banche dati su carta

La presente tabella riepiloga le banche dati su supporto cartaceo utilizzate per lo svolgimento delle normali attività dello studio

I documenti in questione non contengono dati sensibili.

La parte amministrativa contiene soli i dati fiscali necessari per le scritture contabili. L'elenco del telefono contiene solo gli indirizzi dei Clienti / Fornitori / Collaboratori ed i rispettivi numeri di telefono.

La gestione del personale (paghe e stipendi) è affidata ad uno studio esterno.

La tenuta della contabilità è affidata ad uno studio esterno.

tabella banche dati su carta

Banca Dati	Tipo di trattamento	Tipo Dati	custoditi
Prima nota	Elenco cartaceo movimenti contabili entrata uscita	FISCALI	Amministrazione
Fatture clienti	Copia su carta fatture clienti	FISCALI	Amministrazione
Fatture fornitori	Originali fatture fornitori	FISCALI	Amministrazione
Elenco telefonico dello Studio	Elenco numeri di telefono dei clienti e fornitori dello studio	GENERICI	Disponibile a tutti

[..Adeguare in base agli elenchi che si tengono in studio..]

3.5 Elenco delle sedi

Ai fini del D.Lgs. 196/2003 si elencano le sedi dove possono essere contenuti dati o documenti dello studio.

I documenti in forma cartacea vengono conservati in appositi armadi dotati di serratura, siti nei locali dello studio. Eventuali progetti archiviati sono conservati negli archivi in cantina.

Le copie di salvataggio dei dischi del server sono conservate nell'armadio preposto nel locale dello studio. Le copie storiche mensili sono invece conservate in altra sede presso l'abitazione del titolare.

Tabella elenco sedi

Descrizione	Tipo di documenti contenuti
Locali dello studio	Documenti di videoscrittura e disegni del CAD Elenchi cartacei telefono e prima nota Originali cartacei dei documenti prodotti con la videoscrittura Originali cartacei dei disegni prodotti con il CAD I locali dello studio non sono accessibili al pubblico e sono protetti da impianto di allarme e porta blindata
Cantina (locale chiuso a chiave)	Documenti e disegni storici L'archivio in cantina contiene esclusivamente disegni, progetti e l'archivio storico della contabilità. NON sono conservati in cantina DATI PERSONALI
Abitazione del Titolare	Presso l'abitazione del Titolare sono conservate le copie storiche mensili di salvataggio dei dischi del server.

4 Prospetto di valutazione dei rischi

La seguente tabella è utilizzata per evidenziare la valutazione dei rischi in base agli eventi che possono verificarsi.

Il rischio che si deve valutare è la possibile perdita dei dati trattati o il possibile trattamento illecito.

Si premette che l'attività dello studio è un'attività prevalentemente di progettazione, allo scopo vengono quindi prodotti documenti con la videoscrittura o con i fogli di calcolo per la stesura di capitolati, computi metrici, preventivi e quanto altro serve per la progettazione.

Con i programmi di CAD vengono inoltre disegnate piante, prospetti e planimetrie.

Sia la videoscrittura che i programmi di CAD vengono utilizzati solo come strumenti per la produzione dei documenti o dei disegni che sono conservati in originale in forma cartacea presso l'archivio dello studio.

```
Un qualsiasi malfunzionamento del sistema informatico, ivi
compresa perdita di documenti o danneggiamento dei dischi, non
costituisce un problema: si è sempre in grado di dire che tipi
di documenti ed eventualmente che dati erano contenuti dagli
originali in forma cartacea.
```

Il rischio viene espresso a seconda la seguente scala di valori:

- **A** = **Alto**
- **M** = **Medio**
- **B** = **Basso**
- **N** = **Nullo**

Ci sono alcuni elementi di rischio a cui, data la ridotta dimensione dello studio, viene attribuito un rischio nullo. Ad esempio la “non conoscenza delle regole” ha un rischio nullo in quanto le regole sono semplici, le persone sono poche e tutti sono al corrente di tutto.

Tabella analisi dei rischi

Risorsa	Fattore di rischio	Rischio	Contromisura
Risorse umane	1.1. Errori umani	Basso	Personale motivato
	1.2. Non conoscenza delle regole	Nullo	Poche regole semplici
Hardware	2.1. Furto delle attrezzature	Basso	Impianto di allarme
	2.2. Incendio / Allagamento	Basso	Impianto di allarme
	2.3. Fulmini	Basso	Protezioni elettriche
	2.4. Danneggiamento volontario attrezzature	Nullo	Personale di fiducia
	2.5. Obsolescenza tecnologica	Nullo	
	2.6. Non disponibilità del sistema informativo	Nullo	Disponibile tutto su carta
Software	3.1. Danni causati da malfunzionamenti software	Basso	
	3.2. Danni causati da virus	Basso	Protetto da antivirus
	3.3. Danni causati da software spyware	Basso	Protetto da antispyware
	3.4. Obsolescenza software	Nullo	
	3.5. Problemi alle password ed al sistema di autenticazione	Nullo	
Dati, Documenti e Disegni	4.1. Integrità logica database	Basso	
	4.2. Integrità fisica database	Basso	
	4.3. Accessi ai dati non autorizzati	Nullo	
	4.4. Furto dati	Basso	Solo dati fiscali
	4.5. Distruzione dati	Nullo	Disponibile tutto su carta
	4.6. Furto documenti e disegni	Basso	
	4.7. Distruzione documenti e disegni	Basso	
Internet	5.1. Mancanza connessione internet	Nullo	Usata solo per email
	5.2. Malfunzionamento connessione internet	Nullo	Usata solo per email
	5.3. Intrusione dall'esterno	Basso	Protezione da firewall

5 Elenco delle misure di sicurezza

5.1 Misure minime

Il Disciplinare tecnico di cui all'Allegato B, art. 36 D.Lgs. 196/2003 prevede delle misure minime di sicurezza che, nel caso dello studio professionale possono essere riepilogate secondo il seguente schema.

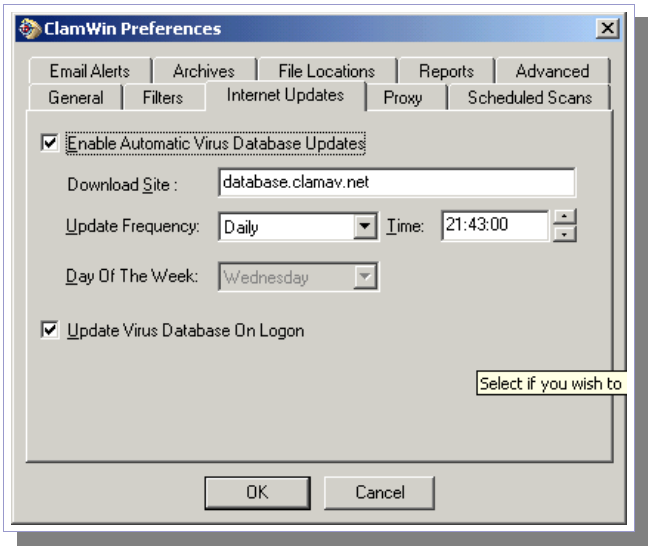
Sistema di autenticazione

Il sistema informatico deve essere dotato obbligatoriamente di un sistema di autenticazione (user-id e password) che deve rispettare i seguenti requisiti:

- Assegnazione User-id personali per ogni utente con password personale da non divulgare)
- Obbligo di custodia delle password
- Modifica periodica delle password
- Disattivazione User-id obsoleti

Antivirus

Il sistema informatico deve essere dotato obbligatoriamente di un programma antivirus aggiornato con cadenza almeno semestrale (questo secondo il D.Lgs 196/2003). Per garantire una sicurezza accettabile, nel caso di connessione della rete locale o dei singoli calcolatori, ad internet l'aggiornamento deve essere impostato in modo automatico dal programma antivirus.



Nell'esempio è riportata la schermata delle opzioni di ClamWin antivirus, un antivirus Open Source distribuito gratuitamente, in cui si evidenzia la modalità di aggiornamento sia all'accensione della macchina che alle 21:43 di ogni giorno. [..aggiornare l'esempio con il programma in uso..]

Sui calcolatori è installato l'antivirus di:

[..dettagliare il programma antivirus usato, nome, produttore, metodo di aggiornamento, frequenza di aggiornamento ..]

Copie di sicurezza

Il D.Lgs. 196/2003 impone di pianificare le copie di sicurezza dei dati nell'ottica di evitare le possibili perdite di dati per potere sempre essere in grado di accedere ai dati per eventuali verifiche, modifiche o revoche dei dati trattati. Non è ipotizzabile il fatto di non potere modificare i dati personali di una persona che ne faccia richiesta per il solo fatto che il sistema non funziona o che si sono persi i dati.

- Definire la modalità e la frequenza delle copie di sicurezza (almeno settimanale)
- Incaricare una o più persone ad effettuare le copie di sicurezza
- Prevedere un armadio idoneo per contenere i supporti usati per le copie di sicurezza
- Prevedere un piano di disaster recovery per ripristinare il sistema in caso di danni gravi.

[.. inizio parte da adeguare al caso specifico ..]

Tutti i dati ed i documenti dello studio sono memorizzati sui dischi del server di rete. Sui singoli calcolatori degli utenti non ci sono dati o documenti da salvare. Il piano di copie di sicurezza prevede quindi solo la copia dei dischi del server.

Il server è dotato di masterizzatore di DVD e le copie di sicurezza vengono effettuate periodicamente su DVD.

E' assegnato il compito alla [...persona...] che provvederà con frequenza settimanale ad effettuare le copie di sicurezza.

Le copie vengono effettuate utilizzando 4 diverse serie di dischi riscrivibili che vengono utilizzati ciclicamente per avere sempre disponibili le copie delle ultime quattro settimane. L'ultima settimana del mese le copie vengono effettuate su DVD-R e vengono mantenute a tempo indeterminato.

I DVD utilizzati per le copie di sicurezza sono archiviati in apposito armadio dotato di serratura.

Le copie di salvataggio mensile vengono portate in altra sede a cura del Titolare dello studio.

Il sistema informatico dello studio è usato per compiti di videoscrittura e disegno con il CAD. Non utilizza nessun tipo di data base. In caso di danneggiamento totale delle attrezzature informatiche è sufficiente dotarsi di un calcolatore con installati i programmi di CAD e di videoscrittura utilizzati e ripristinare le copie effettuate.

Il sistema informatico contiene solo immagini digitali degli originali riprodotti e conservati su carta. Anche in assenza del sistema informatico è quindi possibile in qualsiasi momento accedere ai dati e documenti dall'archivio degli originali.

Non esistono documenti o dati salvati su calcolatore dei quali non sia stata effettuata una copia cartacea.

[..fine parte da adeguare al caso specifico ..]

Formazione del personale

Il D.Lgs. 196/2003 prevede l'obbligo di introdurre nel DPS anche il piano di formazione permanente del personale in base ad una visione dinamica della sicurezza: si evolvono le tecniche e gli strumenti quindi il personale deve essere costantemente aggiornato.

Data la dimensione assai contenuta dello studio professionale sia in termini di persone che di tipi di lavoro svolti, si ritiene di potere avvertire tempestivamente tutto il personale ed i collaboratori qualora ci sia qualsiasi variazione alle procedure adottate.

Se queste variazioni sono di tale entità da richiede menzione nel DPS, si provvederà all'immediato aggiornamento ed alla relativa distribuzione facendo cenno delle novità introdotte nella apposita sezione “aggiornamenti” inserita in calce al presente documento.

Aggiornamenti periodici

Il D.Lgs. 196/2003 prevede alcune operazioni da fare ad intervalli di tempo regolari tra cui:

- Revisione annuale del DPS (entro il 31 marzo di ogni anno solare)
- Revisione annuale della lista degli Incaricati al trattamento
- Revisione annuale delle attrezzature sia come hardware che come software
- Rinnovo licenze antivirus

[.. inizio parte da adeguare al caso specifico ..]

Il DPS viene costantemente mantenuto aggiornato in caso di modifiche. In qualsiasi caso entro il 31 marzo di ogni anno viene rivisto il DPS per garantirne l'attualità.

Se non ci sono modifiche da apportare nella sezione revisioni viene evidenziata la revisione annuale segnando che: ...alla data gg.mm.aaaa il DPS risulta ancora conforme alle modalità di lavoro e viene mantenuto invariato.

Per quanto riguarda la Revisione della lista degli incaricati la struttura dello studio professionale è molto piccola e quindi se ci sono cambi tra i dipendenti ed i collaboratori si provvede immediatamente a disabilitare le vecchie user-id ed a revocare le lettere di Incarico.

La revisione annuale delle attrezzature viene svolta in collaborazione con il personale che fa assistenza alla rete di calcolatori dello studio e, se vengono riscontrati calcolatori non più affidabili dal punto di vista hardware si procede alla loro sostituzione con relativo aggiornamento degli elenchi contenuti nel presente DPS.

Il sistema informativo è prevalentemente utilizzato per la videoscrittura e quindi è assai improbabile riscontrare macchine con software obsoleto.

Annualmente è previsto anche il rinnovo delle licenze del software antivirus.

[..fine parte da adeguare al caso specifico ..]

6 Elenco delle Misure idonee

L'atricolo 31 del D.Lgs. 196/2003 prevede una serie di misure che devono essere adottate; nel caso dello studio professionale possono essere riepilogate secondo il seguente schema.

6.1 Misure Organizzative

Le misure organizzative sono una serie di norme documentate che illustrano come comportarsi nelle varie situazioni. Sono assimilabili ad una specie di regolamento sull'uso delle attrezzature dello studio.

[..le seguenti istruzioni possono essere soggette a modifiche a seconda della struttura..]

Istruzioni in merito alle password

Le password sono personali e segrete. E' fatto divieto di accedere al sistema mediante user-id e password di altri. E' cura dei singoli incaricati custodire la propria password evitando che non venga divulgata.

- Cambiare la password periodicamente (al massimo ogni tre mesi).
- Non utilizzare password facili da indovinare (come nome, data di nascita, nome del cane o dei figli ecc.)
- Non scrivere la password su monitor, tastiera o altri punti in cui risulta accessibile a tutti.
- Non comunicare mai a terzi la propria pasword.

Istruzioni sulla conservazione dei supporti di backup

I supporti utilizzati per i backup contengono documenti di proprietà dello studio e come tali devono essere custoditi con la massima cura. Data la tipologia di lavoro dello studio sui supporti di backup si trovano documenti di videoscrittura e disegni del CAD. Non ci sono applicazioni che fanno uso di un database quindi non esistono dati conservati in forma di tabelle facilmente rielaborabili per altri fini.

I documenti sono comunque da proteggere con la massima cura perchè sono il patrimonio dello studio.

I supporti di backup (DVD-R e DVD-RW) sono custoditi a cura del responsabile dei backup nell'apposito armadio dotato di serratura.

Eventuali DVD-R obsoleti che contengono documenti devono essere distrutti prima del loro smaltimento tra i rifiuti.

```
Attenzione non tentare di spezzare i DVD o i CD; date le
loro doti di resistenza meccanica c'è un'alta probabilità
di ferirsi alle mani ed agli occhi per le schegge.
```

I CD ed i DVD possono essere distrutti semplicemente graffiando la superficie dalla parte dell'etichetta con qualche cosa di duro ed appuntito come la punta di una forbice.

Istruzioni sulla conservazione dei programmi

I programmi utilizzati presso lo studio sono patrimonio dello studio. I supporti originali devono essere conservati con cura nell'apposito armadio dotato di serratura.

```
Si ricorda che i programmi sono dotati di licenza d'uso e
che tali licenze devono essere sempre mantenute in ordine
in modo di poterle esibire nel caso di eventuali
richieste da parte della Guardia di Finanza.
```

E' vietato installare abusivamente qualsiasi tipo di software senza l'autorizzazione del Responsabile del Trattamento dei dati o dell'Amministratore di sistema.

Criteri per trattamenti affidati a strutture esterne.

Nel caso di dati o documenti da trasmettere a strutture esterne occorre preventivamente verificare che tali strutture dispongano di idonee misure di sicurezza per garantire la corretta gestione dei dati trasferiti.

Nel caso di strutture esterne è sempre necessario nominare un incaricato al trattamento per conto dello studio presso la struttura esterna. L'incarico può essere dato a seconda dei casi alla struttura esterna o nominalmente ad una persona della struttura esterna.

Ove è possibile è sempre meglio dare l'incarico alla struttura esterna come società. La lettera di incarico è fatta con la stessa impostazione delle lettere per i dipendenti ed i collaboratori, deve essere consegnata al destinatario con ricevuta per accettazione.

Nella lettera di incarico deve essere dettagliata la finalità di trattamento dei dati che gli vengono affidati e questo cambia caso per caso.

Tra le strutture esterne utilizzate dallo studio troviamo:

- Studio commercialista
- Studio legale
- Studio consulente del lavoro (paghe e stipendi)
- Impresa di pulizie

Anche l'impresa di pulizie fa parte dei soggetti da incaricare. Devono essere nominati con lettera per avere la possibilità di accedere ai locali.

6.2 Misure Fisiche

[..da adeguare al caso specifico ..]

La sicurezza dei locali è garantita da una certa serie di misure di protezione. I locali in cui si svolge l'attività dello studio professionale non sono aperti al pubblico. Gli eventuali ospiti esterni sono sempre accompagnati da personale dello studio.

Date le ridotte dimensioni della struttura non sono necessarie procedure di registrazione degli accessi e di vigilanza.

I locali sono protetti contro i tentativi di furto da impianto di allarme e da porta blindata. L'impianto di allarme è inoltre dotato di sensore fumi per prevenire gli incendi.

I locali sono dotati di appositi armadi dotati di serratura per la custodia dei documenti cartacei e dei supporti usati per il salvataggio dei dati.

La rete elettrica è protetta da rischio fulmini mediante protezioni da sovracorrenti e da sovratensioni installate nel quadro elettrico. Per la parte informatica inoltre il server e gli appartati di rete sono tenuti sotto gruppo di continuità.

6.3 Misure Logiche

[..da adeguare al caso specifico ..]

Dal punto di vista logico vengono adottate delle verifiche per garantire la massima protezione dei dati e dei documenti.

Data la tipologia dei documenti memorizzati sul server di rete, ovvero l'assenza di dati organizzati in database, non ci sono rischi di trattamenti illeciti automatizzati.

I pochi dati generali che si possono trovare riguardano principalmente la gestione della fatturazione clienti e fornitori e le agende del telefono.

In particolare vengono costantemente monitorate le seguenti attività:

Verifica del funzionamento dei programmi antivirus e degli aggiornamenti automatici

Verifica del funzionamento dei dischi del server verificando lo stato del RAID

Controlli sull'operato di eventuali persone esterne chiamate per la manutenzione dei sistemi

Verifica del corretto funzionamento del firewall a protezione di internet

Verifica dello stato delle batterie del gruppo di continuità

Verifica periodica del corretto funzionamento dei dispositivi di salvataggio provando a recuperare qualche documento dalle copie di sicurezza.

7 Allegati

Il allegato al presente Documento Programmatico della Sicurezza si allegano i modelli per la principale tipologia di documenti richiesti dal D.Lgs. 196/2003.

[..questi documenti sono redatti pensando al tipico caso di uno studio tecnico di Geometra/Ingegnere o Architetto, devono essere quindi adattati alla realtà dello studio professionale..]

- Nomina come Incaricato al Trattamento dei dati personali
- Nomina come Amministratore di Sistema (*)
- Lettera all'impresa di pulizie (**)
- Informativa ai Fornitori
- Informativa ai Clienti
- Informativa ai Dipendenti
- Istruzioni agli incaricati (da allegare alle lettere di nomina)
- Modulo di comunicazione della Password (***)

(*) La figura dell'amministratore di sistema è facoltativa: serve una nomina solo nel caso in cui non ci siano conoscenze tecniche all'interno dello studio per configurare ed amministrare i sistemi informatici.

(**) Ovviamente solo se esiste un'impresa di pulizie o se l'incarico è dato al custode.

(***) Le credenziali (User-Id e password) vengono assegnate dall'amministratore di sistema e vengono comunicate agli interessati mediante modulo in busta chiusa. Ad ogni cambio delle password gli interessati provvederanno a darne copia in busta chiusa al Titolare del Trattamento che le custodirà in cassaforte.

Oltre ai documenti richiesti dal D.Lgs. 196/2003 si consiglia anche di richiedere una specie di consenso al trattamento dei dati in cui vengono anche forniti dal committente, sotto la sua responsabilità, i dati fiscali necessari per la fatturazione. Si ricorda che, non avendo un documento del committente in cui Vi comunica ufficialmente i suoi dati fiscali, l'eventuale emissione di fatture a partite iva false o inesistenti è un reato imputabile allo studio. In caso contrario è una richiesta del committente.

L'informativa per i liberi professionisti può essere semplicemente affissa nei locali in punto visibile al pubblico (interpretazione del Garante).

8 Istruzioni agli incaricati

Le presenti istruzioni devono essere allegate alle lettere di incarico al trattamento dati consegnate per formalizzare gli incarichi. Sono essenziali per comunicare a tutti quali sono le finalità del trattamento e le procedure di sicurezza adottate.

Gli incaricati dei trattamenti di dati personali devono scrupolosamente attenersi alle seguenti istruzioni che devono essere considerate ordine di servizio.

8.1 Principi generali

Tutte i dati, progetti e disegni devono essere sempre trattati in modo lecito e secondo le norme che disciplinano l'etica professionale. Essi devono essere trattati solo per le finalità per cui sono stati raccolti: nel caso dello studio per lo svolgimento dei progetti su incarico dei committenti.

```
E' vietato qualsiasi utilizzo dei dati, documenti,
progetti per fini diversi rispetto l'attività dello
studio.
```

8.2 Definizioni

- **Trattamento**: sono quelle operazioni o complesso di operazioni, effettuate con o senza strumenti elettronici, concernenti raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, comunicazione, diffusione, cancellazione o distruzione di dati;
- **Dato personale**: è qualunque informazione relativa a persona fisica, giuridica, ente, impresa o associazione che ne consentano l'identificazione, diretta o indiretta;
- **Dato sensibile**: è il dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose o filosofiche, 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;
- **Incaricato**: il soggetto autorizzato dal titolare a compiere operazioni di trattamento dei dati.
- **Amministratore di Sistema**: la persona (o le persone) che configurano la rete di calcolatori ed i router.

8.3 Riservatezza

Il personale dello studio deve sempre usare la massima cautela nel trattare dati, documenti e disegni: il materiale è tutto di proprietà dello studio.

E’ vietata ogni cessione all'esterno di dati o documenti fatto salvo il caso in cui ciò sia necessario per lo svolgimento degli incarichi affidati.

Utilizzo attrezzature

Tutto il materiale messo a disposizione del personale dallo studio è destinato solo per lo svolgimento delle normali attività lavorative.

```
Qualsiasi utilizzo a fini personali delle attrezzature
messe a disposizione dallo studio è espressamente
vietato.
```

In particolare modo è vietato utilizzare a fini personali la connessione ad internet ivi compresa la posta elettronica.

E' vietato utilizzare o installare programmi non forniti dallo studio anche qualora questi programmi siano gratuiti e liberamente reperiti su internet.

Gli unici programmi leciti sono quelli forniti dallo studio, per i quali si possiedono regolare licenza

Il Personale dello studio è tenuto ad utilizzare esclusivamente strumenti e programmi forniti o autorizzati dall’azienda, e soltanto per svolgere le mansioni d’ufficio. E’ vietato l’utilizzo di floppy, di altri supporti o di programmi non autorizzati. I dispositivi (terminali e PC) devono essere disattivati durante le assenze (comprese le pause) dell’utente. Alla sera tutti i calcolatori, ad esclusione del server, devono essere spenti.

Si ricorda che il software è protetto da licenza d'uso e dai diritti di autore e come tale non può essere liberamente duplicato ed utilizzato.

Si ricorda che anche tutto il materiale disponibile su internet, siano foto, documenti, programmi o musica, è protetto dai diritti di autore e come tale non può essere utilizzato liberamente.

User-Id e password personale

Ad ogni dipendente è assegnata una chiave di autenticazione al sistema informatico composta da un identificativo utente (User-Id) ed una password personale. Questa chiave di accesso è strettamente personale e non deve essere ceduta a terzi.

E' vietato scrivere la password su biglietti o etichette esposti in modo visibile su scrivania, mobili, tastiera, monitor ed in ogni altro punto visibile da terzi.

E' cura dell'utente sostituire la password ogni tre mesi ed ogni qual volta vi sia anche il semplice sospetto che ne sia venuta meno la segretezza verso chiunque.

E’ vietato l’utilizzo del medesimo User-Id per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

L'amministratore di sistema può in qualsiasi momento, su richiesta del responsabile del trattamento, revocare la User-Id di un utente ed inibire quindi l'accesso al sistema.

Archivio documenti e disegni cartacei

Lo scopo principale dello studio tecnico è lo sviluppo di progetti per conto dei committenti. Per lo svolgimento della normale attività non sono necessarie particolari

raccolte di dati, fatto salvo i dati fiscali e pochi altri dati tecnici (catastali, autorizzazioni ecc.) che comunque sono dati di pubblico dominio.

Tutti i documenti cartacei devono essere gestiti in modo di ridurre al minimo la possibilità di perdita o danneggiamento degli stessi. Quando non utilizzati i documenti, i progetti ed i disegni devono essere archiviati negli appositi armati.

L'accesso agli archivi dei documenti, progetti e disegni è consentito a tutto il personale dello studio. L'archivio amministrativo delle fatture clienti e fornitori è di norma utilizzato dal personale che si occupa dell'amministrazione ma può essere visionato in qualsiasi momento anche dal personale dell'area tecnica.

Gli unici elenchi in forma cartacea gestiti nello studio sono gli elenchi dei clienti e fornitori utilizzati come rubrica telefonica oltre alla prima nota che riprende tutte le scritture contabili.

L'elenco telefonico, che deve essere custodito nei cassetti delle scrivanie delle singole persone, contiene comunque solo "**dati comuni"** ovvero indirizzo e numero di telefono dei clienti e dei fornitori.

Non è consentito effettuare fotocopie degli archivi cartacei e portarle all'esterno dei locali dello studio salvo esplicita autorizzazione da parte del titolare del trattamento.

Accesso alla rete di calcolatori

L'accesso ai calcolatori dello studio ed alla rete, ivi compresa la semplice connessione ad internet, è consentita solo ai dipendenti o collaboratori dello studio. L'eventuale accesso di terzi è consentito solo se previamente autorizzato: l'amministratore di sistema dovrà provvedere alla creazione di una User-Id ed una password per gli ospiti.

Sanzioni

Il mancato rispetto alle norme contenute nel presente documento può determinare l'insorgere di responsabilità di tipo disciplinare, civile o anche penale, con l'applicazione – ove ne ricorrano i presupposti – delle relative sanzioni, oltre all'eventuale risarcimento del danno cagionato.

9 Crediti, Ringraziamenti, Licenza

9.1 Crediti

9.2 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.

9.3 Licenza

10 Impaginazione di questo documento

In questo modello sono stati introdotti vari 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 1,2,3,4 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, Times 32pt.

```
Testo riportato. E'utile per riportare brevi testi contenenti
esempi ecc. Utilizza il carattere Courier 12pt.
```

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 della pagina 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 nella pagina di copertina.

Nel 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 Aggiorna Indice.

Il grassetto è ottenuto con lo stile **Enfasi Forte.**

Lo stile *Enfasi* serve invece per *evidenziare il testo con il corsivo*.

C'è inoltre lo stile per le cornici delle immagini.