

Documento programmatico sulla sicurezza (rev. 0)**Legge sulla privacy nr. 675/96 e D.P.R. n. 318/99 sulle misure di sicurezza per la protezione dei dati personali**

Varese, lì 15/04/2004

GENERALITÀ

Il presente documento intende fornire una prima valutazione sui criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati a misure di sicurezza nonché sui criteri adottati per assicurare l'integrità dei dati.

Il presente documento scaturisce dalla analisi di valutazione dei rischi e si dovrà provvedere all'aggiornamento del presente documento nel caso di sostituzione di attrezzature o di cambiamenti nella disposizione degli spazi di lavoro.

Gli incaricati del trattamento sono stati debitamente informati circa il contenuto del presente documento e sono obbligati ad uniformarsi allo stesso mentre il responsabile del trattamento è obbligato a vigilare sull'osservanza delle disposizioni stesse da parte degli incaricati.

Il presente documento è stato ulteriormente illustrato nel corso di una riunione, tenutasi in orario di lavoro, alla quale hanno partecipato il titolare, i responsabili e gli incaricati del trattamento, nel rispetto delle disposizioni di cui al [DPR 31/99, art. 6 che prevede l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni](#), nonostante la predetta norma riguardi esclusivamente gli elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico che non sono in possesso della società.

PROTEZIONE DELLE AREE E DEI LOCALI

Contro i rischi di intrusione i locali sono dotati di impianto di allarme a sensori infrarossi, attivabile mediante digitazione di un codice in possesso del personale dipendente. Si raccomanda pertanto, l'attivazione di detto sistema di allarme al termine dell'orario di lavoro.

Oltre a tale sistema, nelle ore di chiusura, la ditta usufruisce del servizio svolto da società che opera nel campo della vigilanza privata che segnalerà al titolare ed al responsabile del trattamento, tramite comunicazione telefonica, eventuali situazioni anomale riscontrate durante il servizio di vigilanza. A tal fine i recapiti telefonici del titolare e del responsabile del trattamento sono stati comunicati alla predetta società di vigilanza. Relativamente ai locali, essendo le finestre protette da grate in ferro, non si ritiene di dover fornire ulteriori indicazioni. Circa la protezione delle aree, stante introduzione di password di Bios e password di rete si ritiene che non debba sussistere ulteriore protezione delle aree adibite a posti di lavoro.

Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione contabili dei clienti dello studio) sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.

L'ubicazione di stampanti ed apparecchi telefax tradizionali non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

CRITERI E PROCEDURE PER ASSICURARE L'INTEGRITÀ DEI DATI

Di seguito si illustrano le norme applicate per garantire la sicurezza e l'integrità dei dati per:

COMPUTER E SUPPORTI INFORMATICI:

in primo luogo occorre osservare che i computer, esclusi i server, risultano tutti sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti, ecc.; in secondo luogo si evidenzia come siano collegati a gruppi di continuità che consentono di escludere la perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica. I servers si trovano al piano primo della sede e sono collegati ad apposito ed esclusivo gruppo di continuità.

L'integrità dei dati è inoltre garantita mediante idonee procedure di salvataggio periodico (backup) che consistono nell'utilizzo di tre serie distinte (A – B – C) di 5 cassette da utilizzarsi giornalmente al termine dell'orario lavorativo. Ogni settimana la prima cassetta di ogni serie viene archiviata definitivamente facendo scorrere l'utilizzo delle altre cassette di una posizione.

ISI s.r.l. ha acquisito apposito armadio ignifugo e stagno per la conservazione e archiviazione dei supporti di salvataggio.

L'introduzione di password di Bios all'accensione dei personal computer, di password dello screen-saver e di password per l'accesso in rete determina un livello di sicurezza, circa i dati contenuti nei PC, ritenuto più che soddisfacente.

L'introduzione di dette password ha inibito ad estranei l'uso dei personal computer, attraverso i quali si accede alla posta elettronica ed all'archivio dei messaggi telefax inviati.

I floppy disk e/o i CD/DVD Riscrivibili contenenti file (copie di lettere, ecc.) che a loro volta contengono dati dei clienti possono essere riutilizzati esclusivamente previa formattazione del floppy stesso, in modo da impedire la lettura dei dati precedenti, così come stabilito dalla Legge. I floppy disk e/o i CD/DVD Riscrivibili contenenti dati, prima della formattazione, sono custoditi dalla persona che li ha creati e che quindi è autorizzata al trattamento dei dati in essi contenuti. La conservazione avviene in cassettiere con serratura la cui chiave è in possesso della persona incaricata del trattamento.

Per quanto riguarda infine l'obbligo previsto dall'art. 4, c. 1, let. c) del Regolamento di cui al DPR 318/99, gli elaboratori sono dotati di programma antivirus che viene aggiornato sotto la responsabilità del titolare del trattamento a cadenza almeno semestrale, programma che consente di rilevare immediatamente all'apertura di un file la presenza di virus.

Per le modalità operative si faccia riferimento alla procedura PQ06c – Gestione dei sistemi informatici e privacy

SUPPORTI CARTACEI:

relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nei seguenti:

- ❖ qualsiasi documento che i Clienti consegnino alla società va inserito, quando personale, in apposite cartelline non trasparenti;
- ❖ qualsiasi documento che la società consegni ai Clienti va inserito in apposite buste o cartelline non trasparenti.

Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non contiene alcun dato (praticamente il primo foglio funge da copertina).

SI RAMMENTA CHE IL CONSENSO/INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI, FATTO SOTTOSCRIVERE A CIASCUN CLIENTE, PREVEDE CHE COPIE ED ORIGINALI DELLA DOCUMENTAZIONE DELL'INTERESSATO POSSANO ESSERE CONSEGNATE A PERSONALE DIPENDENTE DEL CLIENTE E CHE DETTA AUTORIZZAZIONE DA PARTE DEL CLIENTE AVRÀ VALIDITÀ SINO A REVOCA DA EFFETTUARSI CON LETTERA RACCOMANDATA A.R. DA INVIARE ALLA SOCIETÀ E CHE TALE REVOCA AVRÀ EFFETTO DAL GIORNO SUCCESSIVO A QUELLO DEL RICEVIMENTO.

Le copie dei telefax inviati mediante apparecchio tradizionale sono riconsegnate a colui che ha eseguito o fatto eseguire la trasmissione, avendo cura di porre quale primo foglio il rapporto di trasmissione formato A4 che viene stampato dal fax, con di seguito i fogli contenenti il messaggio. Per ciò che concerne le trasmissioni del telefax, nella copertina del messaggio è inserita la seguente dicitura:

“QUALORA QUESTO MESSAGGIO FOSSE DA VOI RICEVUTO PER ERRORE VOGLIATE CORTESAMENTE DARCENE NOTIZIA A MEZZO TELEFAX OD E-MAIL E DISTRUGGERE IL MESSAGGIO RICEVUTO ERRONEAMENTE. QUANTO PRECEDE AI FINI DEL RISPETTO DELLE LEGGE 675/96 SULLA TUTELA DEI DATI PERSONALI.”

GESTIONE DEI DATI ESTERNAMENTE DALL'AZIENDA:

relativamente all'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare...

Allegati:

1. Analisi preliminare dei dati
2. Analisi dei rischi
3. PQ06c – Gestione dei sistemi informatici e privacy
4. Modulo comunicativa clienti e fornitori
5. Modulo lettere di incarico

Il Titolare del trattamento