

**Mi adeguo alla legge.  
E mi sento inadeguato.**

*Alessio L.R. Pennasilico*  
*mayhem@recursiva.org*  
*<http://www.aipsi.org>*



- ✓ **Socio ed attivista di AIPSI, AIP, ILS, LUGVR, Metro Olografix, OpenGeeks/OpenBeer, recursiva.org, Sikurezza.org, no1984, Spippolatori, CLUSIT e VoIPSA.**
- ✓ **Svolge attività di consulenza presso diverse aziende, principalmente in merito a tecnologie legate ad Internet, al networking ed alla sicurezza.**
- ✓ **Security Evangelist @ [www.alba.st](http://www.alba.st)**



**ISSA®**, con l'attiva partecipazione dei singoli soci, e dei relativi capitoli in tutto il mondo, è la più grande associazione no-profit di professionisti della sicurezza.

**Contribuiscono ad incrementare la conoscenza e la crescita professionale: l'organizzazione di forum educativi, la redazione di documenti e pubblicazioni, oltre all'interazione fra i vari professionisti della sicurezza.**

**I soci sono professionisti nel campo della sicurezza a tutti i livelli, e vari settori: telecomunicazioni, formazione, sanità, finanza, industria e government.**

- ◆ Organizzazione di forum educativi
- ◆ Redazione di documenti e pubblicazioni specializzate
- ◆ Interscambio di esperienze fra i professionisti del settore (nazionali e internazionali)
- ◆ Riferimento per la ricerca di professionisti di sicurezza IT
- ◆ Interazione con altre organizzazioni professionali
- ◆ Rilascio di attestati e certificazioni specifiche



## ***Introduzione***

### ***DPS - Documento Programmatico sulla Sicurezza***

#### ***Misure minime previste***

***Gestione delle password***

***Utilizzo di antivirus***

***Applicazione delle correzioni***

***Utilizzo di firewall***

***Gestione dei salvataggi***

## ***Conclusioni***

# Introduzione

Dal 31.03.2006 è finalmente entrato in vigore il D.LGS. 196/2003.

Viene imposto come **obbligatorio per legge** un **corretto trattamento delle informazioni** che riguardano terzi da parte delle aziende e dei professionisti.

La legge impartisce indicazioni tanto operative quanto tecniche.

Quelli che vengono indicati come requisiti minimi spesso non sono rispettati in molti contesti, quindi è positivo che la legge li richieda.

Tuttavia **le misure minime sono inadeguate**, nella maggior parte dei casi.

Per questa ragione spesso vengono **richieste misure “adeguate”**.

Questa legge viene percepita come una “imposizione”, come un “costo aggiuntivo” e le aziende sono spesso restie ad adeguarsi.

Pensiamo tuttavia al nostro avvocato, al nostro medico, al nostro videonoleggio, etc etc.

Noi **pretendiamo** che i nostri dati vengano gestiti in modo adeguato.

# Documento Programmatico sulla Sicurezza

Se la privacy era “il diritto di essere lasciati soli” (Warren & Brandeis, 1890) oggi è diventato “**il diritto a chiedere di se stessi**” (Lisi, 2005).

*Vogliamo e dobbiamo sapere chi ha quali dati che ci riguardano, come e per quali fini li utilizza.*

Il trattamento elettronico inoltre può esporre informazioni che ci riguardano a **rischi forse non previsti.**

**Pretendiamo che chi possiede informazioni che ci riguardano le protegga in modo adeguato.**

*Pretendiamo che i nostri dati vengano gestiti secondo modalità analizzate a priori, e continuamente riviste, al fine di migliorarle.*

Per questa ragione viene richiesto di redarre un documento che spieghi quali dati vengono trattati ed in che modo.

Mettere per iscritto le procedure “dovrebbe”  
costringere a prendere coscienza del trattamento,  
di certo aiuta ad essere informati su quali nostri  
dati vengono trattati da chi ed in che modo.

“La 626/1994 veniva inizialmente percepita allo  
stesso modo: imposizione, intralcio, costo.

I primi risultati, non solo nelle procedure, ma  
soprattutto nell'atteggiamento si iniziano a  
vedere solo oggi, dopo 10 anni” (Bortolani, 2006).

# Misure minime previste

La legge prevede password di almeno 8 caratteri alfanumerici, che vengano cambiate ogni 3 o 6 mesi e che non siano riconducibili all'utente.

Vengono consigliate strategie di autenticazione semplici, che non spingano l'utente a comportamenti a rischio.

La biometria viene accettata ma non consigliata.

Se le password salvate sono particolarmente a rischio, le altre non sono di certo al sicuro.

Password sniffer, password cracker et similia sono programmi diffusissimi ed utilizzabili da chiunque, che permettono di ottenere credenziali in pochi giorni, se non in poche ore.

L'utilizzo di rainbow table, inoltre, rende tutte queste operazioni ancora più veloci.

La legge prevede l'utilizzo di un antivirus che deve essere aggiornato ogni 6 mesi.

Risulta evidente come un semplice antivirus non protegga da tutte le minacce.

La frequenza di 6 mesi è del tutto inadeguata a qualsiasi tipo di realtà, persino per un privato.

Le misure minime prevedono l'utilizzo di software aggiornati e l'applicazione delle correzioni almeno ogni 6 mesi.

Risulta del tutto inopportuno lasciare trascorre tutto questo tempo per correggere una vulnerabilità.

Non è necessario essere un target interessante, esistono programmi che ricercano in automatico computer vulnerabili.

Viene finalmente resa obbligatoria l'adozione di un firewall per proteggere la rete e la sua verifica semestrale.

Tuttavia il firewall non è una misteriosa e magica scatola nera che “collego e mi protegge”.

Come ogni strumento diventa utile se frutto di una analisi a priori e se gestito nel modo corretto, con continuità nel tempo.

Abbiamo bisogno che sia una legge ad imporre di fare delle copie di sicurezza dei dati?

Un backup settimanale è comunque insufficiente nella maggior parte dei casi.

Dolo, errori e guasti sono un rischio giornaliero.

Poiché il backup contiene tutti i dati aziendali va protetto adeguatamente (crittografia?).

# Conclusioni

## **La sicurezza non è un prodotto, ma un processo.**

Essere consapevoli è il primo passo:

Le organizzazioni devono proteggere le  
informazioni che ci riguardano.

Noi dobbiamo pretendere che siano adeguatamente  
protette.

Le mie esigenze e le tecnologie cambiano rapidamente. Voglio sapere e verificare periodicamente **chi possiede dati** che mi riguardano, a che titolo e per che fine; ma soprattutto **come li conserva**.

*Prendo che i miei dati, indipendentemente dalla loro presunta “segretezza”, vengano comunque gestiti con metodi che ne garantiscano l'effettiva e necessaria riservatezza.*

<http://www.garanteprivacy.it> - documenti vari

<http://www.aipnet.it> - mailing list

<http://www.sikurezza.org> - lex mailing list

[http://www.recursiva.org/documenti/sicurezza\\_e\\_privacy.pdf](http://www.recursiva.org/documenti/sicurezza_e_privacy.pdf)

<http://punto-informatico.it/p.asp?i=52086&r=PI>

Queste slide sono state realizzate da Alessio L.R. Pennasilico, mayhem, per AIPSI e sono soggette alla licenza Creative Commons nella versione Attribution-ShareAlike 2.0; possono pertanto essere distribuite liberamente ed altrettanto liberamente modificate, a patto che se ne citi l'autore e la provenienza.



**Domande**

# Grazie per l'attenzione!

*Alessio L.R. Pennasilico*  
*mayhem@recursiva.org*  
*<http://www.aippsi.org>*

