



Soluzioni Informatiche - Articolo di approfondimento

Amministratori di Sistemi Informativi

La regolamentazione voluta dal Garante della Privacy

L'autore

Roberto Müller, laureato al Politecnico di Milano in Ingegneria Informatica, svolge attività di consulenza e progettazione di soluzioni ICT presso la Faticoni S.p.A. di Cagliari.

Recapiti: +39 070 5292 255 - 3291831581 - roberto.muller@faticoni.it

Il presente articolo è inoltre pubblicato sulla rivista trimestrale "**Informazione**", dell'Ordine degli Ingegneri di Cagliari e sul sito del medesimo ordine <http://www.ingegneri-ca.net/informazione/115/info115-f.pdf>.

Amministratori di Sistemi Informativi

La regolamentazione voluta dal Garante della Privacy

Il settore dell'informatica è senza dubbio uno tra i più giovani settori dell'ingegneria, a differenza di altri che possono vantare tradizioni secolari e qualcuno addirittura millenarie. Nonostante questa giovinezza, tuttavia l'informatica si distingue per diverse caratteristiche peculiari, quali la trasversalità in molteplici settori e l'estrema velocità evolutiva. A quest'ultima caratteristica, purtroppo, non fa eco il quadro normativo il quale lascia, di fatto, licenza poetica per improvvisazioni spesso a dir poco temerarie.

Il Garante della Privacy, che apparentemente non avrebbe nulla a che fare con l'Informatica, ha invece introdotto una serie di norme che iniziano a porre delle basi interessanti sulle quali occorre porre la giusta attenzione da molteplici punti di vista.

Nello specifico, in questo articolo, esamineremo due argomenti: il primo legato alle misure minime di sicurezza informatica ed il secondo legato al **tracciamento delle attività degli amministratori di sistemi informativi**.

Si precisa sin d'ora che scopo del presente articolo è fornire una informazione di massima e richiamare l'attenzione su argomenti di possibile interesse: esulano dallo scopo gli approfondimenti di natura giuridica perché non di competenza dello scrivente e quelli squisitamente tecnico/operativi, in quanto non consoni allo spirito informativo/divulgativo dell'articolo.

Misure minime di sicurezza

Il 30 Giugno del 2003, attraverso il Decreto Legislativo n. 196 chiamato "*Codice in materia di protezione dei dati personali*", veniva abrogata e superata la precedente legge 675/96, "*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*", introdotta per rispettare gli Accordi di Schengen ed entrata in vigore nel maggio 1997.

Grazie alla nuova normativa, mirata ad una maggiore e più completa tutela generale della Privacy all'interno delle aziende pubbliche e private, si è fornita anche una indicazione sul come trattare i dati personali attraverso l'utilizzo di sistemi di elaborazione elettronica dei dati, ossia i

sistemi informativi. Nello specifico, gli articoli 33 e 34 forniscono una serie completa di indicazioni che devono essere messe in atto sotto la responsabilità del Titolare del Trattamento dei dati:

Art. 33 (Misure minime)

1. *Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.*

Art. 34 (Trattamenti con strumenti elettronici)

1. *Il trattamento di dati personali effettuato con strumenti elettronici e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:*

- a) *autenticazione informatica*
- b) *adozione di procedure di gestione delle credenziali di autenticazione*
- c) *utilizzazione di un sistema di autorizzazione*
- d) *aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici*
- e) *protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici*
- f) *adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi*
- g) *tenuta di un aggiornato documento programmatico sulla sicurezza;*
- h) *adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.*

Da tali indicazioni si nota la necessità e obbligatorietà dell'utilizzo di soluzioni complete ed articolate ove vengano messi insieme le funzionalità di autenticazione ed autorizzazione presenti, per esempio, nel Dominio Windows ma non solo, le Group Policy di accesso ai dati, i sistemi di protezione perimetrale (firewall) abbinati a sistemi di protezioni interna e così via. Il tutto deve essere poi evidentemente armonizzato con un adeguato corso di formazione a tutto il personale aziendale, in quanto tutte le misure risultano perfettamente inutili se, abbandonando la sede di lavoro a fine giornata, si lasciano i pc accessi, con login effettuato, consentendo a chiunque di accedere ad informazioni riservate.

Tali indicazioni, spesso trascurate o sottovalutate sia nel pubblico che nel privato, celano in realtà un alto grado di responsabilità, da quanto emerge dalle sanzioni previste:

Art. 169. Misure di sicurezza

1. *Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.*

All'interno dell'*Allegato B DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA* della 196/2003, sono previste altresì una serie di attività con cadenza periodica, atte a tenere costantemente aggiornati sia la documentazione (DPS, Documento Programmatico per la Sicurezza) che i sistemi:

Entro il 31 marzo di ogni anno:

- aggiornare le lettere di incarico e predisporre quelle per i nuovi incaricati;
- verifica delle autorizzazioni di accesso ai dati;
- programma per interventi di formazione agli incaricati;
- aggiornamento del DPS (il Documento Programmatico della Sicurezza rappresenta il documento ufficiale che ogni azienda, pubblica e privata, deve redigere / aggiornare entro il 31 marzo di ogni anno. In tale documento sono riportate tutte le indicazioni riguardanti l'organizzazione messa in atto per la salvaguardia dei dati, in conformità alle disposizioni della 196/2003)

Almeno ogni 12 mesi

- verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione (all. B, comma 14)
- aggiornamento sistemi operativi per prevenire vulnerabilità (all. B, comma 17)

Almeno ogni 6 mesi

- disattivazione credenziali di autenticazione non usate nei sei mesi precedenti (all. B, comma 7)
- aggiornamento sistemi operativi per prevenire vulnerabilità, in caso di trattamento di dati sensibili o giudiziari (all. B, comma 17)
- aggiornamento antivirus e di protezione in generale (all. B, comma 16);

Almeno ogni settimana

- salvataggio dati (backup) (all. B, comma 18).

Ulteriori dettagli operativi sono specificati sempre all'interno dell'allegato B.



Figura 1 - Datacenter

Tracciamento delle attività degli amministratori di sistemi informativi

Con disposizione del Garante per la Privacy del 27 Novembre 2008,, è stato stabilito che entro il 28 Febbraio 2009 (prorogato al 15 Dicembre 2009) le aziende - private e pubbliche - dovevano organizzarsi per registrare e conservare i dati relativi agli accessi degli Amministratori di Sistema sui sistemi da loro gestiti, al fine di agevolare la "verifica sulla loro attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici" (Gazzetta Ufficiale n. 300, 24 Dicembre 2008). Nella pratica, ogni azienda, dopo aver individuato i sistemi (dispositivi di rete, database, apparati di sicurezza e sistemi software complessi) che contengono i dati più critici ed averne nominato gli amministratori, dovrà dotarsi di un sistema di gestione dei file di log in grado di tracciare gli accessi degli operatori ai dispositivi ed alle applicazioni che gestiscono. Questo sistema deve conservare i dati in maniera sicura per un periodo minimo di sei mesi e deve essere consultabile dall'azienda e dalle autorità.

Con il provvedimento del 27 Novembre 2008, modificato il 25 giugno 2009, il Garante pone l'accento sulla significativa quanto trascurata importanza dell'Amministratore di Sistema, vitale per la tutela dei dati. Il provvedimento, dotato di contenuti estremamente chiari, sottolinea in particolare:

... omissis

“Con la **definizione di "amministratore di sistema"** si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.”

... omissis

“Nel loro complesso, le norme predette (675/96 e 196/2003 ndr) mettono in rilievo la particolare **capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni**, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre **attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta**, a oggi non contemplati per lo svolgimento di uno dei ruoli più delicati della "Società dell'informazione".

... omissis

“In altri casi, non soltanto in organizzazioni di piccole dimensioni, **si è invece riscontrata, anche a elevati livelli di responsabilità, una carente consapevolezza delle criticità insite nello svolgimento delle predette mansioni, con preoccupante sottovalutazione dei rischi** derivanti dall'azione incontrollata di chi dovrebbe essere preposto anche a compiti di vigilanza e controllo del corretto utilizzo di un sistema informatico.”

Da quanto sopra e da molte altre interessanti considerazioni che si tralasciano per brevità, è scaturita la necessità di porre indicazioni chiare sulle caratteristiche dell'Amministratore di Sistema:

4.1 Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema **deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato**, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.” ... omissis ...

Visto il ruolo strategico dell'Amministratore di Sistema, emerge la necessità di monitorarne adeguatamente le attività, in quanto l'incarico non può basarsi unicamente sulla fiducia:

4.4 Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

4.5 Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Analogamente a quanto avvenuto per le Misure Minime di Sicurezza, anche in questo caso per rispondere in modo conforme alla normativa, occorre porre in essere principalmente due attività:

- 1) adottare una serie di strumenti informatici in grado di tenere traccia degli accessi a tutti i dispositivi da parte dell'Amministratore. In commercio esistono numerosi sistemi, in grado di soddisfare pienamente quanto richiesto, fornendo inoltre preziose funzionalità ausiliarie.
- 2) affidare l'incarico di Amministratore di Sistema a personale dotato di adeguate competenze oggettivamente certificate

Come ogni altro incarico e come giustamente riportato nella norma, anche quello dell'Amministratore di Sistema dovrebbe essere affidato **previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato.**

Purtroppo capita assai di frequente invece che, sia per carenza legislativa che per superficiale conoscenza della materia, l'incarico venga affidato a chi "muove più velocemente il mouse" tra i diversi possibili candidati.

Ma vista la carenza legislativa, il Titolare del trattamento può comunque ricercare elementi oggettivi nella valutazione del candidato?

L'analisi dei requisiti parte ovviamente dal CV professionale, che deve essere trattato con attenzione in quanto spesso si tende a considerare sotto l'unico cappello dell'Informatica qualunque attività legata al mondo dei computer mentre così ovviamente non è: deve essere evidente il possesso di esperienze legate all'amministrazione di sistemi, database, sistemi di networking etc. Come contro esempio, esperienze nella programmazione o nell'assistenza tecnica hardware non sono particolarmente indicative, anche se ovviamente prese insieme ad altre esperienze possono concorrere a definire un profilo professionale particolarmente ampio.

Altri requisiti da ricercare nel CV, oltre ai percorsi scolastici ed accademici, sono le certificazioni tecniche, spesso rilasciate direttamente dai produttori di sistemi hardware e software. A puro titolo indicativo ma non certo esaustivo, si pensi alla gestione del network, per la quale un valido ed universalmente riconosciuto titolo è rappresentato dalla certificazione CCNA (Cisco Certified Network Associate) rilasciata da CISCO Systems. Analogamente risulta preziosa una certificazione Microsoft sui sistemi Windows Server (2000, 2003, 2008) piuttosto che sul database SQL, che ha come concorrente l'universale certificazione Oracle Database Administrator. Particolarmente moderna risulta anche la certificazione tecnica VMware sugli ambienti virtuali, chiamata VMware Certified Professional – VCP. Sono altresì senz'altro valide certificazioni quelle di System Administrator rilasciate da SUN Microsystems e da altri produttori di sistemi UNIX / Linux quali HP e Red Hat.

In generale, solitamente tutte le grandi case mondiali dell'informatica (chi per l'hardware e chi per il software) prevedono il rilascio di certificazioni e l'erogazione di corsi che attestano l'acquisizione di capacità tecniche.



Faticoni S.p.A. è Certificata UNI EN ISO 9001:2008 per la
"Progettazione, Realizzazione, Manutenzione di soluzioni Hardware e Software"

Bibliografia

**Garante della Privacy: Decreto legislativo 30 giugno 2003, n. 196
CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248>

Garante della Privacy: Allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza" <http://www.garanteprivacy.it/garante/doc.jsp?ID=1557184>

Obblighi di sicurezza e documento programmatico: al 30 giugno la redazione del "dps"
<http://www.garanteprivacy.it/garante/doc.jsp?ID=771307>

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499>