Pubblica Amministrazione locale: adempimenti per gli Amministratori di Sistema

Il Provvedimento del Garante Privacy del 27 novembre 2008

Paolo Giardini
Direttore Osservatorio Privacy e Sicurezza delle Informazioni

paolo.giardini@solution.it

Agenda:

- Il provvedimento del Garante
- Perché questo provvedimento
- Chi è l'amministratore di sistema (AdS)
- Quali requisiti deve avere l'AdS
- Come valutare l'AdS
- La lettera di nomina
- La valutazione periodica
- La questione dei log
- La gestione dei sistemi informativi
- Domande ricorrenti

Il perché del provvedimento

Dareste le chiavi di casa al primo venuto?

Il provvedimento sugli AdS

"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"
27 novembre 2008
(G.U. n. 300 del 24 dicembre 2008)

- Adottato il 27 novembre 2008
- Prima scadenza prevista 30 marzo 2009
- Proroga al 30 giugno 2009
- Avvio consultazione pubblica 21 aprile
- Seconda proroga al 15 dicembre 2009

Abbiamo avuto un anno di tempo

Adesso il provvedimento è operativo:

siete in regola?

a

CHI

avete dato

le chiavi di casa?

Destinatari del provvedimento

.

Tutti i titolari di trattamenti di dati personali effettuati sia in **ambito pubblico** che **privato.**

Sono esenti: I Titolari che effettuano trattamenti con strumenti elettronici soltanto a fini amministrativi e contabili. (art. 29 legge 133/2008 – provv. 27/11/2008)

Cosa prevede il provvedimento

In breve:

- Individuazione degli AdS
- Valutazione delle caratteristiche soggettive
- Nomina degli AdS ed individuazione ambito
- Registrazione dei log di accesso
- Valutazione periodica dell'operato

Chi è l'Amministratore di Sistema

"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."

(punto 1 del provvedimento 27/11/2008)

Definiamo meglio l'Amministratore di sistema

Con questo termine il Garante intende non solo "*il tecnico incaricato della gestione del sistema informatico*" ma in senso molto più ampio anche tutti coloro che per le loro funzioni possono od hanno la possibilità di accedere "**anche in modo fortuito**" ai dati personali.

.

In pratica?

Si va quindi dal tecnico che accede al pc per cambiare il mouse, al gestore di database, all'addetto al backup, al webmaster, al programmatore che gestisce il programma dell'anagrafe o quello per la gestione delle buste paga.

Nomina dell'Amministratore di sistema

Il Titolare (o il responsabile) deve effettuare la nomina ad amministratore di sistema "*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 della sicurezza*".

La nomina è **individuale**.

Cosa intendere per "valutazione"

Si parla di capacità tecniche, professionali, e di condotta, non di requisiti morali: **Esperienza**, **Capacità**, **Affidabilità.**
In questo senso, l'AdS deve avere caratteristiche equiparabili a quelle richieste ai Responsabili del trattamento.
*"il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla **sicurezza**."* *(art. 29 D.lgs 196/2003)*

Come effettuare la valutazione

La valutazione di un candidato AdS si può basare su curriculum lavorativo, curriculum studiorum, certificazioni, corsi di qualificazione.

Meglio ancora, farsi supportare da una entità esterna che sia in grado di effettuare una corretta valutazione.

In ogni caso...

Documentare !!!

Al limite, fare compilare un atto di notorietà (autocertificazione) per curriculum, certificati di servizio, seminari di aggiornamento,...

Un suggerimento?

La **certificazione EUCIP** (European Certification of Informatics Professionals) è lo standard richiesto presso molte Pubbliche Amministrazioni come indicato da Digit-PA (ex CNIPA) nel Manuale operativo - Dizionario dei profili di competenza per le professioni ICT (ottobre 2009)

Casi particolari

Non sono ”Amministratori di Sistema” nella accezione data dal Garante quei soggetti che solo **occasionalmente** intervengono sui sistemi, ad esempio a seguito di guasti, manutenzioni, installazioni.
Nel caso particolare in cui il Titolare, avendo una struttura informatica ridotta, può fare a meno di una figura professionale **specificamente dedicata** alla amministrazione dei sistemi o comunque abbia ritenuto di non farvi ricorso, il provvedimento non si applica.

La nomina

- Deve essere **individuale**
- Deve essere riferita alla **valutazione effettuata**
- Deve contenere l'elencazione analitica degli ambiti di operatività in base al profilo di autorizzazione, ovvero, **elencare i compiti attribuiti**
- Deve essere firmata dal **titolare** o dal **responsabile** (attività da prevedere fra le mansioni)
- E' bene che sia controfirmata per **presa visione**
- E' valida fino a **revoca**

L'elenco degli Amministratori di Sistema

- Il Titolare deve redigere un elenco nominativo degli amministratori e dei rispettivi compiti.
- L'elenco deve comprendere i nominativi di eventuali AdS esterni (outsourcing)

Ho l'elenco. Cosa ne faccio?

- L'elenco degli AdS deve essere riportato in un documento da mantenere aggiornato e conservare per eventuali ispezioni.
- Il Titolare deve rendere noti o conoscibili i nominativi degli AdS che gestiscono sistemi informatici con i quali si trattino dati personali dei lavoratori (regolamento, informativa, intranet, bacheca, circolare,...)

Il caso degli outsourcer

Vi sono due possibilità.

- Se il soggetto esterno è nominato “responsabile”, allora come tale redigerà l'elenco degli AdS e controllerà il loro operato

- Se il soggetto esterno non viene nominato “responsabile”, allora dovranno essere previste specifiche **clausole contrattuali** che prevedano quanto richiesto dal provvedimento

E la verifica periodica?

- L'operato degli AdS deve essere oggetto almeno annualmente di una **verifica** da parte del Titolare o Responsabili del trattamento
- Dovrà essere **verificata la rispondenza** alle misure organizzative, tecniche e di sicurezza indicate dalla normativa per i trattamenti di dati personali
- Dovrà essere quindi prevista una **specifica procedura per la valutazione**, della quale deve essere informato l'AdS
- Si deve fare attenzione al problema del divieto di **controllo sull'attività dei lavoratori** (statuto dei lavoratori)

Ma cosa significa in pratica?

La verifica dell'operato degli AdS verterà su:

- **Audit** sull'applicazione dei quanto disposto nell'allegato B del Codice
- **Analisi dei Log** di accesso ai sistemi da parte degli AdS
- Dovranno essere esaminati gli eventuali **incidenti di sicurezza** verificatisi
- Può essere utile una **checklist**, ma soprattutto sarà necessario implementare un **sistema di gestione** dei sistemi informativi

Documentare la verifica

Il risultato della verifica sarà un documento nel quale il titolare o il responsabile descriveranno l'avvenuta valutazione, i metodi utilizzati, le risultanze e le eventuali misure per migliorare l'operato degli AdS e la sicurezza dei sistemi. Questo documento andrà allegato alla documentazione conservata dal titolare.

I log di sistema

Ogni sistema informatico registra in speciali file gli eventi di sistema: accensione, chiusura, logon utenti, errori, ecc.
Un buon sistemista controlla periodicamente questi log per individuare errori e verificare il buon funzionamento dei sistemi

La registrazione degli accessi

- Il provvedimento richiede che vengano registrati gli **accessi** (login) ai sistemi di elaborazione ed agli archivi elettronici effettuati dagli amministratori di sistema
- Le registrazioni devono avere "*caratteristiche di **completezza**, **inalterabilità** e possibilità di **verifica** della loro **integrità***".
- Le registrazioni debbono comprendere data e ora e la descrizione dell'evento che le ha generate.
- La registrazione deve essere conservata per almeno 6 mesi.

Scendiamo in dettaglio

- Devono essere registrati **solo gli accessi degli AdS** (login)
- Non devono essere registrate le **attività svolte** dagli AdS
- Non devono essere registrati gli accessi e le attività degli **utenti**
- La registrazione deve comprendere anche gli accessi degli AdS ai **sistemi client** e **workstation**, non solo ai server

Completezza, inalterabilità, possibilità di verifica dell'integrità

- **Completezza**: i log devono comprendere tutti gli eventi di accesso, uscita, errore di accesso
- **Inalterabilità**: non sono richiesti specifici livelli di sicurezza. Ogni titolare potrà decidere autonomamente in base al contesto operativo
- Verifica **dell'integrità**: una volta registrati i log non devono essere modificabili
- Salta all'occhio che sussistono evidenti discrasie in questi enunciati.

A cosa deve servire il log?

La raccolta dei log serve per verificare **anomalie** nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso...). L'analisi dei log può essere compresa tra i criteri di **valutazione** dell'operato degli amministratori di sistema. (FAQ 16)

Tecnicamente parlando

- **Non è obbligatoria** l'adozione di apparati hardware e/o software aggiuntivi
- In **casi semplici** possono bastare le funzionalità disponibili nei sistemi operativi
- Possono essere utilizzati **software open source** o soluzioni reperibili in rete (comunicato 10/01/2010)
- Nel caso sia necessario, è **possibile filtrare** i dati raccolti dai log e mantenere solo quelli relativi agli accessi degli AdS

Il che non vuol dire che la soluzione sia semplice!

- Deve essere garantita l'**integrità dei log**
- Non devono essere raccolti **dati non pertinenti**
- Sarà comunque il **titolare** che deve **valutare** l'**idoneità** degli strumenti disponibili oppure l'**adozione di strumenti più sofisticati**
- L'**analisi dei rischi** aiuta a **valutare** le misure tecniche da applicare per garantire i log

La gestione dei sistemi informativi

- Inventario HW e SW
- Brogliaccio di sistema
- Registro degli interventi tecnici
- Modulo incidenti di sicurezza
- Applicazione del provvedimento su Internet e posta elettronica del 13 marzo 2007

In altre parole è necessaria una **gestione** dei sistemi informatici precisa, puntuale, coordinata. Meglio ancora, **certificata**.

Sanzioni

La **mancata applicazione** delle **misure di sicurezza** viene punita con l'arresto fino a 2 anni e fino a 120.000 euro di multa

Reati legati all'attività di AdS

- 615 *ter* c.p. - accesso abusivo a sistema informatico
- 640 *ter* c.p. - frode informatica
- 635 *bis* e *ter* c.p. – danneggiamento informazioni, dati e programmi informatici
- 635 *quater* e *quinques* c.p. – danneggiamento sistemi informatici e telematici

Domande ricorrenti

- L'elenco degli AdS va inserito nel DPS?
- Deve essere registrata ogni attività effettuata?
- Devono essere apposte firme digitali ai log?
- Posso rifiutare la nomina?
- La nomina dell'Ads è obbligatoria?
- Quali responsabilità e rischi per l'Ads?

- Altre domande?

Grazie per la vostra attenzione

http://blog.solution.it
paolo.giardini@solution.it

Link Utili

http://www.cnipa.gov.it/site/it-IT/Attività/Qualità_delle_forniture_ICT/Manuali/Dizionario_dei_profili_di_competenza_per_le_professioni_ICT/
http://www.garanteprivacy.it/garante/doc.jsp?ID=1676654
http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499
http://blog.solution.it
http://www.fabiodiresta.com/?p=375