

PROVVEDIMENTO A CARATTERE GENERALE DEL 27 NOVEMBRE 2008 (COME MODIFICATO IN BASE AL PROVVEDIMENTO DEL 25 GIUGNO 2009)

MISURE E ACCORGIMENTI PRESCRITTI AI TITOLARI DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA

In molti casi, non soltanto in organizzazioni di piccole dimensioni, si è riscontrata una carente consapevolezza delle criticità insite nello svolgimento delle mansioni di amministratore di sistema, con preoccupante sottovalutazione dei rischi. Ecco perché il Garante ha ritenuto opportuno emanare un provvedimento di carattere generale nel quale si delineano alcune misure di carattere organizzativo che favoriscano un più agevole controllo del rischio.

Essere consapevoli che:

Definizione

- La definizione di "amministratore di sistema" individua generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento vengono ad esse equiparate altre figure quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Responsabilità

- Il legislatore ha considerato la qualità di "operatore del sistema" (qualità che a tutti gli effetti è propria di un amministratore di sistema) come una circostanza aggravante nella commissione di molti reati, tra cui: accesso abusivo a sistema informatico o telematico (art. 615 ter), frode informatica (art. 640 ter), danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter), danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinquies).

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.
- Anche qualora l'amministratore sia un semplice incaricato, il titolare e il responsabile devono attenersi a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29 del Codice.

Designazioni individuali

- La designazione deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Elenco degli amministratori di sistema

- Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
- Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni tramite: 1) l'informativa ex art. 13 del Codice nell'ambito del rapporto di lavoro; oppure 2) il disciplinare tecnico la cui adozione è

prevista dal provvedimento del Garante n. 13 del 1° marzo 2007; oppure 3) strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

Servizi affidati in outsourcing

- Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

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.

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.