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)

CONSIDERAZIONI PRELIMINARI

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 ed 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: *system administrator (amministratore di sistema), network administrator (amministratore di rete), database administrator (amministratore di data base).*

Gli amministratori di sistema così ampiamente individuati, anche se la loro principale attività riguarda altri settori, sono concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (*backup/recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione *hardware* comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

Le funzioni tipiche dell'amministrazione di un sistema sono richiamate nell'Allegato B del D.lgs 196/2003 e ss.mm.ii, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di *backup* e *recovery* dei dati) alla custodia delle credenziali, alla gestione dei sistemi di autenticazione e di autorizzazione.

Quadro di riferimento normativo

Nell'ambito del Codice il provvedimento sopra citato si richiama, in particolare, all'art. 154, comma 1, lett. h), rientrando tra i compiti dell'Autorità quello di promuovere la *"conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati".*

La lett. c) del medesimo comma 1 prevede poi la possibilità, da parte del Garante, di prescrivere misure e accorgimenti, specifici o di carattere generale, che i titolari di trattamento sono tenuti ad adottare.

La Circolare 18 aprile 2017 , n. 2/2017 "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)", ha come obiettivo "*indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi".* In tale

contesto risulta evidente l'aumento di importanza delle misure relative agli amministratori di sistema.

MISURE E ACCORGIMENTI ADOTTATE DAL TITOLARE DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI (ai sensi dell'art. 154, comma 1, lett. c) del Codice)

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. Per tale motivo gli "amministratori" sono stati individuati tra il personale della S.C. ICT & Sistemi Informativi con più anni di esperienza nello specifico settore di attività.

2. Designazioni individuali

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. A tale scopo il titolare ha inviato ad ogni Amministratore elencato nel documento allegato, atto di nomina con una lettera di incarico in cui sono indicate le rispettive mansioni e gli ambiti di intervento.

Funzioni attribuite:

a. *Amministratori di sistema:*
   - Accesso a tutti i server in lettura/scrittura
   - Backup/restore degli archivi
   - Predisposizione delle procedure di disaster recovery
   - Creazione di nuovi utenti di rete e/o loro modifica
   - Attribuzione nuovi nome computer del dominio
   - Attribuzione dei permessi di accesso agli utenti di rete
   - Creazione o modifica di aree condivise in rete
   - Monitoraggio degli eventi e dei servizi offerti dai servers
   - Installazione e configurazione del sistema operativo
   - Manutenzione ed aggiornamento dei sistemi operativi ed antivirus dei servers
   - Installazione di software applicativo

b. *Amministratori di rete:*
   - Attribuzione nuovi indirizzi IP
   - Backup/restore delle configurazioni firmware degli apparati (switch) di rete attiva
   - Aggiornamenti firmware degli apparati (switch) di rete attiva
   - Monitoraggio degli eventi di intrusione nella rete
   - Modifica delle regole di sicurezza del firewall per rispondere a nuove esigenze oppure per migliorare la funzionalità del firewall a bloccare eventi di intrusione nella rete
   - Aggiornamento costante della mappa di rete e del censimento PDL

c.*Amministratori di database:*
   - Backup/restore dei database
   - Modifica della struttura fisica delle tabelle del database
   - Attribuzione dei permessi di accesso utenti alle tabelle del database

- Manutenzione applicativi, test funzionalità, reportistica
- Gestione sicurezza

Il titolare, nella qualità di datore di lavoro, è tenuto a rendere nota l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, in relazione ai diversi servizi informatici cui questi sono preposti. A tal fine è predisposto opportuno atto deliberativo di approvazione e tutta la documentazione è resa disponibile sul sito Intranet dell'A.O. Mauriziano alla sezione Privacy e nel sito Internet sotto Amministrazione Trasparente.

Nel seguito si intende come "Amministratore di Sistema" la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati e i software applicativi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali (inglobando pertanto la dicitura Amministratore di database e Amministratore di rete)

3. Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in ***caso di accertamenti anche da parte del Garante.***

4. Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in *outsourcing o all'esterno,* il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

A tal fine il Titolare ha predisposto opportune richieste protocollate alle Società che gestiscono data base esterni con dati relativi all'AO Mauriziano al fine di conoscere e registrare il nominativo degli Amministratori, richiedendo per ogni tipologia di dati trattata, il nominativo degli Amministratori, le funzioni attribuite ed il profilo di autorizzazione assegnato.

Si richiede che le Società rispettino la normativa in termini di registrazione degli accessi e conservazione dei log per almeno sei mesi.

5. 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 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.

Operativamente, con cadenza annuale viene controllata la rispondenza delle attività degli amministratori alle:

- misure <u>organizzative</u> controllando che le funzioni attribuite a ciascun amministratore siano effettivamente congrue a ciò che l'individuo è capace di fare; azioni possibili da intraprendere per migliorare eventuali deficienze → fare ricorso a corsi di formazione specifici e/o sostituzione o cambio di ruoli tra personale dipendente
- misure <u>tecniche</u> controllando che le funzioni attribuite a ciascun amministratore siano state svolte dal punto di vista tecnico secondo normativa vigente; azioni possibili da intraprendere per migliorare eventuali deficienze tecniche → aggiornare i sistemi hardware e/o software utilizzati

- misure di sicurezza controllando che:
  - non siano stati segnalati abusi/intrusioni o perdita di dati riconducibili ad amministratori di sistema; azioni da intraprendere nel caso in cui ci fossero state segnalazioni → controllare gli access log relativi al periodo segnalato;
  - non sia necessario attuare modifiche per migliorare la rispondenza di quanto implementato alle normative vigenti e per diminuire i possibili eventi di intrusione nella rete; azioni da intraprendere → verificare che le raccomandazioni segnalate nei VulnerabilityReports trimestrali siano state attuate o se no motivate in verbali scritti

6. 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

- all'analisi centralizzata dei log di accesso prodotti da tutti i servers ed apparati attivi

- alla conservazione dei log di accesso per almeno 6 mesi

La S.C. ICT & Sistemi Informativi ha attivato un contratto con la Società T-Consulting per la raccolta e messa in sicurezza dei logs di sistema di alcuni servers predefiniti, su un loro portale Web, con le caratteristiche richieste da normativa. L'accesso è consentito ad un incaricato, che conserverà, oltre alle credenziali di accesso al portale, anche una chiave di cifratura dei dati.

Il responsabile della Privacy aziendale è stato incaricato alla conservazione della chiave di cifratura dei dati.