

# Sicurezza Legislativa dei Dati Aziendali

Massimiliano Campita  
IT Architect CISA Certified  
(Certified Information Systems Auditor)

Consulente tecnico giuridico Forze Armate

**Forum IBM Italia**  
**Segrate 8 settembre 2009**



# Sicurezza Legislativa (per la Conformità) (ambito nazionale)

- D Lgs 196/2003 (Privacy)                      Sanzioni civili e penali (carcere)
  - Testo unico, di seguito denominato "Codice" che garantisce il trattamento dei dati personali nel rispetto dei diritti e delle libertà fondamentali; in particolare:
  - Disciplinare Tecnico per trattamenti elettronici:
    - Sistemi di Autenticazione ed Autorizzazione
    - Misure di Sicurezza generale, aggiornate almeno annualmente, contro i rischi di intrusione e frode
- Comunicato Stampa del 22 marzo 2004
  - Obblighi misure minime di sicurezza:
    - Introduzione del DPS Aziendale (Documento Programmatico Sicurezza)
    - Presentazione del DPS aggiornato nella relazione sul bilancio di esercizio dell'azienda, a partire dal 2003
- Provvedimento del 27 novembre 2008
  - Registrazione Accessi
  - Elenco del Amministratori di sistema e valutazione caratteristiche
  - Verifica delle attività di garanzia della sicurezza informatica aziendale
  - Servizi in Outsourcing

# Sicurezza Legislativa

(Normativa del 27 novembre 2008)



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

- **Registrazione degli accessi**
- **Elenco degli amministratori di sistema e loro caratteristiche**
- **Verifica della attività**
- **Servizi in outsourcing**

# Premesse Generali

La composizione della Normativa ha analizzato la reale possibilità per cui un Amministratore di Sistema ha la concreta capacità, per atto intenzionale come per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati per i quali non è legittimato ad accedere secondo il profilo di autorizzazione attribuito.

Pertanto si è reso necessario promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure, tecniche organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare (due diligence) nell'ambito della Sicurezza Aziendale in riferimento alla gestione di banche dati o reti informatiche, sistemi di elaborazione utilizzati da una molteplicità di incaricati con diverse funzioni, applicative o sistemistiche

I titolari dei trattamenti sono tenuti, ai sensi dell'art. 31 del Codice, ad adottare misure di sicurezza «idonee e preventive» in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile (articoli 15 e 169 del Codice);

# Definizione di 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.

## **Chi sono gli Amministratori di Sistema, nelle Aziende?**

Application Administrator

Amministratore di un particolare tipo di applicazione.

Amministratore di Sistema Operativo

Network Administrator

Security Administrator

Database Administrator

L'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti.

# Registrazione degli Accessi

E' richiesta l'adozione di sistemi di controllo che consentano la registrazione degli accessi effettuate dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici.

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 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;

# Elenco degli AdS e relative caratteristiche

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante

Qualora ritenga facoltativamente di designare uno o più responsabili del trattamento, il titolare è tenuto a individuare solo 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, comma 2, del Codice)

Gli AdS DEVONO essere nominati mediante formale lettera di incarico. In mancanza di tale documento, la Società è passibile di una sanzione che varia dai 30.000 ai 180.000 euro mentre la persona (AdS) di fatto è passibile di un reato penale.

# Verifica delle Attività

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente «responsabili» ed «abilitati» ad espletare specifiche fasi lavorative che possono comportare elevate criticità rispetto alla Protezione ed alla Sicurezza dei dati.

Viene pertanto richiesta una verifica (almeno annuale) da parte dei titolari del trattamento sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati.

# Servizi in Outsourcing

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte della società esterna, quali amministratori di sistema, riportando competenze ed attività nel Documento Programmatico di Sicurezza, alla pari di un AdS interno.

# Le Responsabilità Giuridiche

**Nei reati informatici ci si riferisce alle seguenti responsabilità giuridiche**

**Reati previsti dal Codice Penale, anche come aggravanti:**

Abuso della qualità di Operatore di Sistema per le fattispecie di:

- \* Accesso abusivo a sistema informatico o telematico (art. 615-ter)
- \* Frode informatica (art. 640-ter)
- \* Concorso nei reati di accesso illecito e trattamento illecito dei dati personali
- \* Danneggiamento di informazioni, dati e programmi informatici (articoli 635-bis e ter)
- \* Danneggiamento di sistemi informatici e telematici (articoli 635-quater e quinquies)

**Reati previsti dal Codice Civile:**

- \* Danni per omesso controllo (2050 c.c.)
- \* Danni per omesso aggiornamento del sistema (2043 c.c.)

# Sicurezza Legislativa dei Dati Aziendali

Massimiliano Campita  
IT Architect CISA Certified  
(Certified Information Systems Auditor)

Consulente tecnico Giuridico Forze Armate

**Grazie per la Vostra  
Attenzione**

**Forum IBM Italia  
Segrate 8 settembre 2009**

