DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi di quanto previsto dall'Art. 34 comma 1. g) del decreto legislativo 30 giugno 2003 n. 196)

CONSORZIO A.T.O. BRENTA

Il Titolare del Trattamento

IL PRESIDENTE
Lino Ravazzolo

1. Sommario

2. Riferimenti del documento

Titolo	**D.P.S del Consorzio A.T.O. Brenta**
Data prima redazione	03.06.2004
Versione	3.0
Data ultimo aggiornamento	Marzo 2011
Redatto da	Provincia di Padova per il Consorzio A.T.O. Brenta

3. Riferimenti normativi

Visto il D.L.vo 196/2003, in particolare gli art. dal 31 al 36:

Titolo V
SICUREZZA DEI DATI E DEI SISTEMI

CAPO I
MISURE DI SICUREZZA

Art. 31
(Obblighi di sicurezza)

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 32
(Particolari titolari)

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.
2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.
3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

CAPO II
MISURE MINIME DI SICUREZZA

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 è 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.

Art. 35
(Trattamenti senza l'ausilio di strumenti elettronici)

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

Art. 36
(Adeguamento)

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.
1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Visto inoltre l'allegato tecnico B "Disciplinare Tecnico in materia di misure minime di sicurezza" del D.L.vo 196/2003, con particolare riguardo al punto 19:

ALLEGATO B
DISCIPLINARE TECNICO
IN MATERIA DI MISURE MINIME DI SICUREZZA
(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla

diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati
personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati

dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro
trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone

ammesse, a qualunque titolo, dopo l’orario di chiusura, sono identificate e registrate.
Quando gli archivi non sono dotati di strumenti elettronici per il
controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Richiamato il documento predisposto dall'AIPA (ora CNIPA) "Linee guida per la definizione di un piano per la sicurezza" dell'ottobre 1999;

Richiamato il documento redatto dal CNIPA "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" di marzo 2004;

Richiamato il documento "Guida operativa per redigere il Documento Programmatico sulla sicurezza" predisposto dal Garante per la Protezione dei dati personali;

Il Consorzio A.T.O. Brenta ha ritenuto di provvedere alla stesura del presente "Piano Programmatico per la sicurezza"

4. Oggetto e scopo del documento

Oltre alla citata obbligatorietà del presente documento, il Consorzio A.T.O. Brenta, intende affrontare il problema "Sicurezza" in un contesto più ampio.

In particolare è maturata la convinzione che la sicurezza non dipenda solo dagli strumenti tecnici, ma anche e soprattutto dall'organizzazione e dal coinvolgimento della struttura a tutti i livelli.

In tale contesto, cogliendo l'occasione dell'adempimento imposto dal D.L.vo 196/2003, questo Ente adotterà il documento programmatico come utile strumento per formalizzare, razionalizzare ed ottimizzare le strategie in materia di sicurezza, oltre che a definire strategie per la formazione ed informazione degli utenti sulla sicurezza.

5. Elenco dei trattamenti di dati personali (Regola 19.1 dell'allegato B del D.L.vo 196/2003)

In questa sezione viene inserito l'elenco dei trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati trattati e della struttura (o reparto, funzione, ufficio, ...) interna od esterna che operativamente effettua il trattamento. Nella redazione della lista può essere utile fare riferimento anche alle informazioni contenute nelle notificazioni eventualmente inviate al Garante anche in passato.

Informazioni essenziali.

Per ciascun trattamento sono riportate le seguenti informazioni:

Identificativo del trattamento: consiste in un codice, facoltativo, ma utile per il titolare, in quanto consente un'identificazione univoca e più rapida di ciascun trattamento nella compilazione delle altre tabelle

Descrizione sintetica: descrive il trattamento in modo da consentire una comprensione immediata della tabella.

Natura dei dati trattati: dovrà essere indicato se, tra i dati oggetto del singolo trattamento elencato, sono presenti dati sensibili o giudiziari, oltre ad altri dati personali.

Struttura di riferimento: indica la struttura (o reparto, funzione, ufficio, ecc.) all'interno della quale viene realizzato il trattamento. Il livello di sintesi utilizzato è stabilito dal titolare. Ad esempio, in caso di strutture complesse, è possibile indicare la macro-struttura (direzione del personale) oppure uffici specifici (uff. paghe, ufficio sviluppo risorse, ufficio controversie sindacali, ecc.)

Altre funzioni che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporti l'attività di diverse strutture è opportuno indicare oltre quella che primariamente detiene la responsabilità dell'attività, anche quelle che concorrono, siano esse interne od esterne all'organizzazione del titolare.

Banca dati: il nome o l'identificativo dell'eventuale banca dati (ovvero del data base o dell'archivio informatico) in cui sono contenuti i dati che sono trattati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso elencare le banche.

Ubicazione fisica dei supporti di memorizzazione: contiene l'indicazione del luogo in cui risiedono fisicamente i dati, cioè dove si trova (in quale sede, centrale o periferica, presso quale fornitore di servizi, etc.) l'elaboratore sui cui dischi sono memorizzati, i luoghi di

conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, Cd, ecc.). Il livello di dettaglio deve essere funzionale alla esigenze della politica della sicurezza da definire.

Tipologia di dispositivi di accesso: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.

Tipologia di interconnessione: descrizione sintetica e qualitativa della rete informatica che collega i dispositivi d'accesso utilizzati dagli incaricati ai dati: rete locale, Extranet,Internet, ecc.

Tali informazioni sono contenute nelle allegate tabelle 01−A e 01−B.

6. Distribuzione dei compiti e delle responsabilità (Regola 19.2 dell'allegato B del D.L.vo 196/2003)

In questa sezione è costruita una mappa che associa ad ogni struttura (o reparto, dipartimento, ufficio) i trattamenti da questa effettuati, descrivendo sinteticamente l'organizzazione della struttura medesima e le relative responsabilità.

Informazioni essenziali.

Struttura aziendale: contiene lo stesso identificativo utilizzato nella sezione precedente.

Responsabile della struttura: indica il ruolo o la qualifica del dirigente o del responsabile della struttura (non deve essere confuso il responsabile del trattamento ai sensi dell'art. 29).

Trattamenti operati dalla struttura: contiene, se necessario su più righe per ciascuna struttura, i trattamenti per i quali la struttura ha la primaria responsabilità.

Compiti della struttura: contiene una descrizione sintetica dei compiti assegnati alla struttura in ciascuno dei trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.).

Tali informazioni sono contenute nelle allegate tabelle 01–A e 01–B.

7. Valutazione dei rischi (Regola 19.3 dell'allegato B del D.L.vo 196/2003)

7.1. Analisi dei rischi

L'analisi del rischio sta alla base di ogni percorso di sicurezza, dato che solo conoscendo il tipo di rischio, posso definirne il grado l'accettabilità e le eventuali contromisure da adottare.

Specifichiamo comunque che il rischio, per tutte le misure minime di sicurezza obbligatorie per legge, non è calcolabile in quanto va rispettato nei termini previsti. Per tutti gli aspetti in cui l'adozione delle misure minime non sia sufficiente, si provvederà a definire una gradazione delle misure adottabili.

In tali contesti, cioè qualora sia necessaria una graduazione delle misure adottabili, si dovrà adottare una valutazione del rischio basata sui seguenti criteri :

1. si considerano gravi le minacce che possono limitare e/o rendere difficoltosa l'erogazione delle attività di gestione e/o rese al pubblico;
2. si considerano gravi le minacce che portano alla divulgazione/modifica/produzione illegittima di dati personali o sensibili o che comportino un danno patrimoniale per l'azienda;
3. si considerano gravi le minacce che possono limitare la disponibilità di servizi informatici a supporto delle attività di gestione o delle attività rese al pubblico;
4. si considerano gravi le minacce che portano alla modifica illecita di messaggi - e quindi di informazioni gestite dall'azienda - qualora tali messaggi abbiano come contenuto dati sensibili o personali o la loro modifica comporti un danno patrimoniale per l'azienda;
5. si considerano gravi le minacce di fraudolenta impersonificazione - masquerade qualora ciò porti alla produzione di falsi atti contenenti dati sensibili o personali o che comportino un danno patrimoniale per l'azienda;
6. si considerano gravi le minacce di fraudolenta impersonificazione - masquerade - qualora ciò porti alla modifica fraudolenta di dati sensibili o personali originariamente legittimi, o qualora ciò porti ad un danno patrimoniale per l'azienda;
7. si considerano gravi le minacce di intercettazione qualora i dati intercettabili riguardino dati personali di natura sensibile ai sensi della legge sulla tutela dei dati personali;

8. si considerano gravi le minacce di perdita parziale o totale di dati, siano essi sensibili, personali o comuni;

7.2. Rischi di maggiore rilevanza e soglie di accettabilità

Per una corretta definizione dei rischi, si ritiene opportuno definire il "dominio di sicurezza" del Sistema Informatico, con il quale si definisce il confine tra l'interno e l'esterno. Il dominio di sicurezza è definito dall'insieme di strutture ed attrezzature fisiche, procedure organizzative, risorse umane, che fanno riferimento ad una medesima autorità in grado di definire, determinare e controllare le politiche e gli strumenti di sicurezza adeguati allo scopo e rispondenti alla normativa vigente.

7.2.1. Minacce alla disponibilità di servizio

I criteri adottati per definire la frequenza della minaccia sono i seguenti:

- Interruzioni alla continuità di servizio dovute a guasti fisici;

Tipo di sistema	Probabilità di interruzione di servizio
Sistema completamente ridondato	Poco probabile
Sistema parzialmente ridondato	Mediamente probabile
Sistema non ridondato	Altamente probabile

- Interruzioni alla continuità di servizio dovute ad attacchi al sistema;

Tipo di sistema	Probabilità di interruzione di servizio
Sistema all'interno del confine aziendale	Poco probabile
Sistema posto all'esterno del confine aziendale o sul confine aziendale, o nella DMZ, o accessibile da utenti posti al di fuori del confine aziendale	Altamente probabile

7.2.2. Minacce di modifica illecita, minacce di fraudolenta impersonificazione

Per tali minacce, la discriminante è rappresentata dalla collocazione del sistema all'interno o all'esterno del confine aziendale.

Tipo di sistema	Probabilità di interruzione di servizio
Sistema all'interno del confine aziendale	Poco probabile
Sistema posto all'esterno del confine aziendale o sul confine aziendale, o nella	Altamente probabile

DMZ, o accessibile da utenti posti al di fuori del confine aziendale	

7.2.3. Minacce di intercettazione

Tipo di sistema	Probabilità di interruzione di servizio
Funzionalità applicative utilizzate da utenti posti all'interno del confine aziendale e che utilizzano sistemi posti all'interno del confine aziendale	Poco probabile
Funzionalità applicative fornite da sistemi posti al di fuori del confine aziendale o sul confine aziendale, o nella DMZ, o accessibili da utenti posti all'esterno del confine aziendale e che utilizzano sistemi posti all'interno del confine aziendale	Altamente probabile
Funzionalità ed attività di gestione sistemistica e di concessione/revoca/modifica funzionalità applicative	Altamente probabile

Le informazioni relative ai rischi specifici degli apparati critici sono elencate e riassunte nell'allegata TABELLA 11

Le informazioni relative ai rischi specifici sono elencate e riassunte nell'allegata TABELLA 03

8. Politiche di sicurezza e gestione del rischio (Regola 19.4 dell'allegato B del D.L.vo 196/2003)

Gli obiettivi di sicurezza che l'Ente si pone con la redazione del seguente plano e con l'attuazione delle misure di sicurezza previste sono:

1. per tutti i dati assoggettati al Decreto Legislativo 196 del 2003, dare attuazione a quanto previsto dall'art. 31 laddove dice che "1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.";
2. Dare attuazione a quanto previsto dall' allegato B del D.L. 196/2003;
3. dare attuazione a misure di sicurezza ulteriori - rispetto a quelle previste dal D.L. 196/2003 - che l'Ente ritenga opportune e necessarie nell'ottica del perseguimento degli obiettivi istituzionalmente attribuiti;
4. ridurre a livelli ritenuti accettabili i principali rischi di sicurezza a cui il sistema informativo aziendale è sottoposto;
5. mantenere, compatibilmente con i vincoli di sicurezza sopra enunciati, il massimo livello di usabilità del sistema.

Misure per il perseguimento degli obiettivi di sicurezza individuati.

Si ritiene che gli obiettivi di sicurezza siano raggiungibili mediante la predisposizione delle seguenti misure:

- nomina dei responsabili dei trattamenti e degli incaricati dei trattamenti;
- attuazione delle misure di tutela fisica degli apparati;
- attuazione delle misure di sicurezza logica degli apparati;
- definizione delle procedure di continuità ed emergenza;
- definizione delle misure di recupero da disastro;
- definizione di regole di buon uso del sistema informativo aziendale;
- attuazione delle misure di contenimento dei virus informatici;
- attuazione delle misure di informazione e formazione del personale aziendale sugli aspetti di sicurezza informatica;

- misure di sicurezza relative alla salvaguardia delle informazioni detenute su supporto cartaceo.

8.1. Nomina dei responsabili dei trattamenti e degli incaricati del trattamento

8.1.1. Nomina dei responsabili

L'Art. 4 del D.L.vo 196/2003 definisce:

f) "**titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) "**responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) "**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

Al Titolare e ai responsabili, qualora nominati, compete la definizione del profilo di sicurezza del Sistema Informativo aziendale e la messa in atto delle idonee misure di attuazione.

Si richiamano di seguito gli atti che il titolare ha adottato per la nomina formale dei responsabili del trattamento:

Prima approvazione DPS con D.G. n. 47 del 27.03.2006

Regolamento per la tutela della riservatezza dei dati personali approvato con D.G. n. 114 del 27.12.2000

8.1.2. Definizione dei profili

Secondo quanto prescritto dall'allegato B del D.L. 196/2003

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati. necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Allo scopo di dare attuazione a quanto sopra richiamato occorre che i responsabili dei trattamenti (per tutti quei trattamenti per i quali sia stato individuato un responsabile) o il titolare (per tutti quei trattamenti per i quali non sia stato nominato un responsabile), diano comunicazione scritta all'unità Sistemi Informativi della avvenuta assegnazione di autorizzazioni di accesso, affinché questi possano attuare le dovute configurazioni tecniche sui sistemi, tali da dare attuazione alle disposizioni.
Per rendere possibile ciò:

- Si predispone un elenco dei profili assegnabili agli utenti, specificati nell'allegata TABELLA 10B. A ciascun utente è già stato attribuito il relativo profilo di accesso, così come indicato nell'allegata TABELLA 10A;
- Si individua un modulo così detto di CONCESSIONE/REVOCA/MODIFICA abilitazioni applicative che i responsabili utilizzeranno per le comunicazioni del caso al Servizio Informativo Aziendale. Sarà compito del Servizio Informativo Aziendale conservare con la dovuta cura tali dichiarazioni. In ogni momento dovrà essere possibile dimostrare la corrispondenza fra le abilitazioni applicative realmente concesse e le autorizzazioni al trattamento conservate in detto archivio.

Almeno due volte all'anno dovrà essere formalizzato un verbale in cui il responsabile del trattamento attesti la sussistenza delle condizioni che determinano la concessione delle abilitazioni applicative vigenti. A tale scopo il Servizio Informativo Aziendale dovrà produrre l'elenco aggiornato delle abilitazioni applicative assegnate e vigenti che i responsabili del trattamento certificheranno come corrispondenti alle necessità operative delle rispettive mansioni e minime a tal fine.

8.2. Tutela fisica degli apparati

Al fine di predisporre le adeguate misure di tutela fisica degli apparati è necessario poter disporre degli inventari delle attrezzature.
Si dispone pertanto la compilazione e l'aggiornamento, ogni volta che si renda

necessario, dell'elenco degli apparati informatici critici, contenente l'elenco dei server, degli apparati di rete e di tutte le infrastrutture considerate critiche. Tale elenco è contenuto nell'allagata TABELLA 11.
E' inoltre previsto che le prese di rete, se non utilizzate, vengono mantenute scollegate dagli apparati, evitando di collegare con il cavo di raccordo la presa dal patch panel all'apparato.

8.2.1. Collocazione dei server e degli apparati di rete

Tutti gli apparati di categoria server dovranno essere collocati in locali che presentino almeno le seguenti caratteristiche:

- **locali chiusi ad accesso controllato**: l'accesso ai locali nei quali siano ospitati i sistemi di elaborazione o i sistemi di comunicazione dovrà essere interdetto a chiunque, fatta eccezione per il personale autorizzato. Se eventualmente si rendesse necessario l'accesso a detti locali da parte di personale non autorizzato - per es. da parte di tecnici della manutenzione di ditte fornitrici, ecc..., i visitatori andranno opportunamente identificati e accompagnati durante tutta la loro permanenza in detti locali da personale autorizzato. Deroghe a tale regola potranno essere concesse solo dietro precisa motivazione e andranno comunque segnalate ai responsabili della gestione dei server.
- **locali dotati di alimentazione elettrica tutelata**: dovrà essere garantita presenza di gruppo di continuità in grado di fungere da backup per brevi interruzioni di energia elettrica. Nel caso non sia possibile porre sotto gruppo di continuità l'alimentazione dell'intero locale, potranno essere utilizzati gruppi di continuità singoli per singole macchine;
- **locali dotati di opportuno condizionamento**: i locali dovranno possedere condizioni idonee di microclima - in termini di temperatura, polverosità, umidità - e nel caso questo non sia garantibile attraverso misure passive, andranno predisposte le adeguate misure attive di condizionamento;
- **locali dotati di impianto antincendio**: i locali dovranno essere dotati di un adeguato impianto antincendio e possibilmente dovranno essere monitorati in continuo attraverso sensori per la rilevazione precoce degli aumenti di temperatura e di fumo;

Tutti gli apparati attivi di rete andranno collocati in armadi chiusi a chiave che

garantiscano le seguenti caratteristiche:

- valori corretti di temperatura;
- valori corretti di polverosità
- valori corretti di umidità;
- gruppo di continuità/stabilizzatore

E' responsabile della messa in atto e della gestione delle opportune tutele hardware dei server l'unità Sistemi Informativi. Qualora non esista tale servizio e non si sia provveduto ad individuare un responsabile addetto, sarà responsabile della corretta collocazione il titolare, o i responsabili del trattamento, qualora individuati.

8.2.2. Caratteristiche hardware dei server

Tutti i sistemi di elaborazione di categoria server in uso in azienda - non importa se di proprietà, o a qualsiasi altro titolo detenuti e di cui si abbia la responsabilità - devono avere almeno le seguenti caratteristiche:

- per quanto possibile andranno privilegiate configurazioni hardware dei server ridondanti che garantiscano la continuità di servizio - per es. doppio alimentatore in configurazione ridondante, configurazione di server in cluster con funzionalità di "MutuaI Take Over" o similari, doppia scheda di rete al fine di creare macchine "Multi Homed" in grado di poter resistere a guasti singoli sulla scheda di rete, ecc...
- tutte le aree di memoria su disco magnetico destinate a contenere i dati dovranno essere tutelate da misure di ridondanza - con tecniche almeno di mirroring, preferibilmente RAID;
- ogni server dovrà possedere un dispositivo di backup di adeguate dimensioni e velocità unità di backup -, nel caso l'azienda disponga di sistemi di backup centralizzato, tale informazione andrà dettagliata nella scheda che accompagna i server aziendali
- ogni server dovrà riportare affissa una scheda individuale nella quale dovrà essere obbligatoriamente indicato dove è possibile trovare copia delle informazioni per l'accesso USERID e PASSWORD del super utente - per manovre di emergenza sull'elaboratore. Tali informazioni andranno conservate in luogo presidiato e sotto chiave e dovranno essere conservate in busta sigillata e firmata dal locale responsabile della gestione del server. Andrà tenuto registro di chi ha accesso a tali informazioni e andrà indicato succintamente il motivo.

È responsabile della messa in atto e della gestione delle opportune tutele hardware dei server l'unità Sistemi Informativi. Qualora non esista un tale servizio e non si sia provveduto ad individuare un servizio competente in materia sarà responsabile della corretta collocazione il titolare, o i responsabili del trattamento qualora nominati.

8.2.3. Politiche di gestione dei Backup

Al fine di tutelare adeguatamente i dati gestiti nei vari sistemi di elaborazione è necessario predisporre un adeguato piano di backup.

A tal fine si dispone quanto segue:

- la programmazione dei salvataggi dovrà essere conservata per iscritto nella scheda individuale del server, e su ogni server dovrà essere affissa la programmazione dei salvataggi e l'elenco degli ultimi 3 salvataggi effettuati, comprensivi di data e ora di inizio salvataggio, firma leggibile dell' operatore che ha operato il salvataggio, e luogo dove vengono conservati i supporti magnetici contenenti i salvataggi. Nel caso il salvataggio avvenga in maniera non presidiata - per es. nottetempo con procedura schedulata -, andranno registrati i controlli sul buon esito del backup messi in atto dall'operatore preposto - per es. mediante salvataggio di opportuni log. Tali informazioni possono essere conservate e gestite anche in maniera informatizzata, purchè siano gestite su un diverso sistema e ne sia sempre garantita l'accessibilità da parte del personale di manutenzione e gestione.
- i supporti fisici contenenti i backup andranno conservati in luogo sicuro e diverso da quello dove ha sede il server corrispondente, in maniera tale da minimizzare la probabilità di distruzione contestuale di server e dati di salvataggio. Tali supporti andranno conservati in armadi ignifughi chiusi a chiave, o comunque in luoghi che abbiano un ragionevole grado di resistenza agli incendi.
- dovrà essere adottato un set minimo di supporti per i salvataggi a rotazione - per es. un supporto diverso per ogni giorno della settimana - e l'effettuazione di un backup non sovrascrivibile almeno una volta al mese.
- Sono responsabili della attuazione dei passi previsti dalle politiche di backup i vari incaricati di tali mansioni.

È responsabile della formulazione di adeguate politiche di backup l'unità Sistemi Informativi. [Qualora non esista un tale servizio e non si sia provveduto ad individuare un servizio competente in materia sarà responsabile delle formulazione di adeguate politiche di backup il titolare, o i responsabili del trattamento qualora nominati.].

Le informazioni specifiche relative ai backup e ai ripristini sono contenute nelle allegate TABELLA 05A e TABELLA 05B

8.3. Sicurezza Logica

8.3.1. Misure minime di sicurezza

Misure minime di sicurezza relative a trattamenti che vengono messi a disposizione come servizi di elaboratori connessi in rete pubblica:

1. Il trattamento di dati personali è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo [oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.]

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. (D.L. 196/2003 Allegato B, punti 1, 2, 3 ,4).

5. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Pertanto si dispone che ogni utente definito, non venga più cancellato, ma disabilitato nel caso cessi di essere in uso, in maniera tale da evitarne il riutilizzo (D.L. 196/2003 Allegato B, punti 6)

6. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. Qualora il sistema operativo dell' elaboratore su cui risiede l' applicativo lo consenta, è abilitato il cambio password, che l'incaricato potrà autonomamente effettuare in un qualsiasi momento successivo al primo accesso, e in ogni altro momento successivo; per quei sistemi operativi per i quali non sia

disponibile tale modalità di cambio password, o non sia comunque abilitabile per ragioni tecniche, è individuata una procedura organizzativa opportuna per il cambio password mediante l'ausilio del personale tecnico dell'unità Sistemi Informativi (D.L. 196/2003 Allegato B, punti 5);

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l' autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato. (D.L. 196/2003 Allegato B, punti 7,8,9,10)

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. NOTA BENE: per dettagli al riguardo si veda la Sezione: dedicata alla individuazione degli incaricati del trattamento;

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione. (D.L. 196/2003 Allegato B, punti 12, 13, 14) Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell' ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere

redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell' azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. (D.L. 196/2003 Allegato B, punti 15, 16,20, 17, 18)

Il reimpiego dei supporti di memorizzazione è vietato qualora siano serviti per la memorizzazione di dati personali o sensibili si veda a questo proposito la Sezione: relativa al buon uso del sistema informativo e di comunicazione. È inoltre genericamente vietato l'utilizzo di supporti di memorizzazione rimovibili per lo scambio di dati sensibili (D.L. 196/2003 Allegato B, punti 21 e 22).

È responsabile della formulazione di opportune politiche di gestione dei sistemi di elaborazione che garantiscano il rispetto delle misure minime di sicurezza e della attuazione delle misure attuative, per la parte di competenza, l'unità Sistemi Informativi. [Qualora non esista un tale servizio e non si sia provveduto ad individuare un servizio competente in materia sarà responsabile di tali aspetti il titolare, o i responsabili del trattamento qualora nominati.].

9. Regole di buon uso del sistema informatico

Vengono qui richiamate alcune proibizioni e obblighi che il dipendente ha nell'uso della infrastruttura informatica aziendale e più in generale nella fruizione del sistema informativo dell'Ente.

9.1. Crimine informatico e tutela del diritto d'autore

Vista la legge 248 del 18/08/2000 relativa alla tutela del diritto d'autore si vietata la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi, si ricorda infatti che anche i manuali sono coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del titolare dei diritti esclusivi. Il Servizio Informativo Aziendale [o altra struttura tecnica preposta], qualora tecnicamente possibile deve predisporre copie di riserva dei programmi dotati di regolare licenza allo scopo di prevenire accidentali perdite dell'originale e quindi danni patrimoniali all'azienda. Tale copia di riserva potrà essere usata soltanto per ripristinare le funzionalità del programma, quando non sia possibile utilizzare il programma originale.

E' fatto specifico divieto a tutti gli utenti di installare qualunque tipo di software (anche se freeware, shareware,…) che non sia preventivamente autorizzato dall'unità Sistemi Informativi

9.2. Tutela dei dati memorizzati sulle stazioni di lavoro personali e reimpiego dei supporti di memorizzazione

L'azienda persegue una politica di centralizzazione nella gestione dei dati aziendali, per cui progressivamente le gestioni locali di dati scompariranno sostituite da gestioni centralizzate su server. Fino a che questo processo non sarà stato portato a compimento potranno esistere gestioni locali di dati su stazioni di lavoro personali, personal computer non connessi in rete o connessi in rete, ma con la possibilità di gestire localmente documenti e/o dati la cui tutela è demandata a all'utente finale. L'effettuazione dei salvataggi con frequenza opportuna (almeno comunque settimanale) su supporti magnetici e la conservazione degli stessi in luogo idoneo (possibilmente sotto chiave e in contenitori ignifughi) è compito del singolo dipendente che usa la stazione nel caso di stazioni di lavoro usate da un solo utilizzatore, da un incaricato opportunamente individuato dal

responsabile del trattamento nel caso di stazioni di lavoro condivise.

È vietato l'uso di supporti di memorizzazione removibili per la memorizzazione di dati personali o sensibili. Deroghe a tale regola sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione ai sensi del D.L. 196/2003 Allegato B, punti 21 e 22:

1. è possibile il reimpiego del supporto solo nel caso non siano più recuperabili le informazioni precedentemente memorizzate;
2. nel caso non sia garantibile il requisito di cui al punto (1), il supporto removibile dopo l'uso andrà distrutto. In generale i supporti di memorizzazione - anche non removibili - che contengono dati personali o sensibili, nel caso non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dimessi - per es. per obsolescenza o per guasto -, dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.

9.3. Buon uso della rete di comunicazione

La rete di trasmissione dati e fonia è un prezioso bene aziendale condiviso e pertanto va gestita nel rispetto delle esigenze complessive di azienda. In funzione di ciò viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione dell'unità Sistemi Informativi. È altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro o di altri dispositivi direttamente connessi alla rete dati o fonia per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati. In particolare tali divieti si possono tradurre, anche se non esaurire, nelle seguenti esplicite proibizioni:

- divieto di condividere cartelle in rete (né dotate di password, né sprovviste di password);
- divieto di alterare la configurazione delle configurazioni di rete di stazioni di lavoro e altri dispositivi in rete (stampanti condivise, ecc...), comprendendo in ciò anche il divieto di aggiungere protocolli di retè o servizi in rete (per es. condivisione di stampanti in rete, browsing di risorse di rete, ecc...);
- divieto di monitorare ciò che transita in rete.

È inoltre vietata l'installazione non autorizzata di Modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne all'azienda.

È vietata l'installazione di hardware o software di qualsiasi tipo che consenta o faciliti il *by pass* delle misure di presidio del confine aziendale - per es. software di comunicazione che garantiscano accessi che non passino dai Firewall Aziendali o dagli altri accessi autorizzati e presidiati.

9.4. Doveri connessi alla corretta conservazione delle parole chiave di accesso e dei dispositivi di accesso

L'utente è tenuto a conservare nella massima segretezza la parola di accesso ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.

Inoltre l'utente è tenuto a scollegarsi dal sistema ogni qual volta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (per es. perché impegnato in compiti che richiedono totalmente la sua attenzione). Occorre prestare anche particolare attenzione alle stampe prodotte con sistemi informatizzati: la produzione dei documenti deve essere presidiata o collocata in locali ad accesso controllato.

L'utente è inoltre tenuto a conservare con la massima cura eventuali dispositivi per l'accesso ai sistemi aziendali e ad usarli conformemente alle specifiche indicazioni d'uso. La perdita o danneggiamento degli stessi sarà sanzionata.

È bene porre l'accento sulla necessità che i responsabili delle unità organizzative operino un costante e meticoloso controllo volto ad evitare pratiche che la normativa identifica come veri e propri crimini, ma che nella pratica comune risultano assai diffuse e a vari livelli tollerate.

Ciò risulta tanto più importante se si pensa che senza la collaborazione attiva di tutte le articolazione organizzative aziendali non sarà possibile arginare i costi sempre crescenti indotti da un cattivo uso delle attrezzature informatiche (si pensi a titolo esemplificativo al proliferare dei virus informatici che potrebbe essere arginato adottando semplici regole di controllo delle informazioni provenienti dall' esterno dell' azienda, ecc..).

Si dispone quindi che i responsabili delle varie macro articolazioni organizzative, di concerto con l'unità Sistemi Informativi adottino gli atti e le misure necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione dell'azienda.

10. I Virus informatici – malicious code

Al fine di prevenire le infezioni virali si adottano le seguenti misure:

- si dotano tutte le attrezzature e tutti i Server in dotazione all'Ente di un adeguato software antivirale e si stabilisce l'aggiornamento delle firme almeno in ragione giornaliera. Le attrezzature da mantenere aggiornate, oltre a tutti i pc collegati in rete, sono riportate nell'allegata TABELLA 11;
- si dota di software antivirale e si predispongono adeguati meccanismi per mantenere tale software aggiornato su tutti i PC collegati alla rete in modo automatico. Per i PC non collegati alla rete ma correntemente utilizzati, l'aggiornamento dovrà avvenire a cura dell'unità Sistemi Informativi con cadenza almeno semestrale;
- Nel caso non sia possibile predisporre adeguati meccanismi per mantenere il software antivirale aggiornato sarà cura del consegnatario della stazione di lavoro aggiornare il software almeno in ragione settimanale seguendo l'opportuna procedura tecnica di aggiornamento.
- per quanto possibile sono stati configurati i profili abilitativi di tutti gli utenti aziendali con privilegi che non consentano l'installazione o l'esecuzione di programmi non autorizzati sia sulle macchine client che sui server

Si invitano inoltre

gli utenti:

- alla massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione (dischetto removibile, nastro magnetico, disco magneto-ottico e ogni altro supporto di memorizzazione removibile) sia stato utilizzato su un computer diverso dal proprio occorrerà verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato non sarà possibile utilizzare il supporto di memorizzazione in quanto potenzialmente infetto;
- in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;
- è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure; nel caso

pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri. Nel caso si abbia notizia di un nuovo tipo di virus, comunicare tale informazione all'unità Sistemi Informativi e non inviare indiscriminati messaggi a tutti i propri conoscenti dato che ciò evita l'ingenerarsi di falsi allarmi e di inutili catene di Sant' Antonio.

11. Criteri e modalità di ripristino dei dati (Regola 19.5 dell'allegato B del D.L.vo 196/2003)

In questa sezione sono descritti i criteri e le procedure adotti per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati.

L'importanza di queste attività deriva direttamente dalla eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che quando sono necessarie le copie dei dati siano disponibili e le procedure di reinstallazione siano efficaci. Pertanto è opportuno descrivere sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino

Informazioni essenziali.

Data base: contiene l'identificativo del data base o dell'archivio interessato.

Dati sensibili o giudiziari contenuti: contiene l'elenco dei dati sensibili o giudiziari contenuti nel database o archivio.

Criteri individuati per il salvataggio (procedure operative in essere): contiene una descrizione della tipologia di salvataggio e della frequenza con cui viene effettuato.

Ubicazione di conservazione delle copie: contiene l'indicazione del luogo fisico in cui sono custodite le copie dei dati salvate.

Struttura operativa o persona incaricata del salvataggio: contiene il nominativo della persona incaricata di effettuare il salvataggio e/o di controllarne l'esito o del coordinatore del gruppo preposto.

Per quanto riguarda il ripristino, le informazioni essenziali sono le seguenti:

Data base/archivio: contiene l'identificativo del *data base* o dell'archivio interessato.

Scheda operativa: contiene il riferimento alla scheda operativa che descrive la procedura di ripristino

Pianificazione delle prove di ripristino: contiene l'indicazione delle date in cui si prevede di effettuare dei *test* di efficacia delle procedure i salvataggio/ripristino dei dati adottate.

Delle politiche aziendali sulle procedure di backup di sì è già trattato nel Paragrafo 8.2.3. Il dettaglio dei salvataggi delle Banche Dati è specificato nell'allegata TABELLA 05.

12. Pianificazione degli interventi formativi (Regola 19.6 dell'allegato B del D.L.vo 196/2003)

In questa sezione sono riportate le informazioni necessarie per disporre di un quadro sintetico dell'impegno formativo che si prevede di sostenere in attuazione della normativa.

Informazioni essenziali.

Corso di formazione: riporta l'identificativo del corso di formazione.

Descrizione sintetica: contiene la descrizione sintetica degli obiettivi del corso.

Classi di incarico interessate: contiene l'elenco delle classi omogenee di incarico a cui il corso è destinati e/o le tipologie di incaricati interessati.

Numero di incaricati interessati: contiene il numero di addetti interessati dal corso.

Numero di incaricati già formati/da formare nell'anno: contiene l'indicazione del numero di addetti già formati negli anni precedenti e quelli di cui si prevede la formazione nell'anno in corso.

Le informazioni relative alla pianificazione dei corsi di formazione sono contenute nell'allegata TABELLA 06.

13. Trattamenti affidati all'esterno (Regola 19.7 dell'allegato B del D.L.vo 196/2003)

Obiettivo di questa sezione è redigere un quadro sintetico delle attività trasferite a terzi che comportano il trattamento di dati personali con l'indicazione sintetica del quadro contrattuale in cui tale trasferimento si inserisce, in riferimento alla protezione dei dati personali.

Informazioni essenziali

Attività delegata: contiene l'identificativo dell'attività che è stata oggetto di delega a terzi.

Descrizione sintetica: contiene una descrizione sintetica dell'attività.

Dati personali, sensibili o giudiziari interessati: contiene l'elenco dei dati personali, sensibili o giudiziari oggetto di trattamento per la realizzazione dell'attività delegata.

*Soggetto delegat*o: riporta l'identificativo della società o del consulente a cui è stato affidato l'incarico.

Descrizione dei criteri per garantire l'adozione delle misure: perché sia garantito un adeguato trattamento dei dati è necessario che il soggetto esterno a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento a:

1. Trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
2. Adempimento degli obblighi previsti dal codice per la protezione dei dati personali;
3. Rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
4. Impegno a relazionare periodicamente sulle misure di sicurezza adottate (anche mediante eventuali questionari e liste di controllo) e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

In questa casella sono riportati gli impegni contrattualmente assunti nel caso specifico.

Date delle verifiche: contiene l'indicazione del numero e delle date delle verifiche previste.

Gli elenchi relativi alle attività esternalizzate si trovano nell'allegata TABELLA 07.

14. Amministratore di Sistema (Provvedimento a carattere generale del Garante – 27 novembre 2008 doc. web 1577499)

1. 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. 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.

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" 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.

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinques) di recente modifica1.

La disciplina di protezione dei dati previgente al Codice del 2003 definiva l'amministratore di sistema, individuandolo quale "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c) d.P.R. 318/1999).

Il Codice non ha invece incluso questa figura tra le proprie definizioni normative. Tuttavia le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, 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.

Nel loro complesso, le norme predette 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"2.

Nel corso delle attività ispettive disposte negli ultimi anni dal Garante è stato possibile rilevare quale importanza annettano ai ruoli di system administrator (e di network administrator o database administrator) la gran parte di aziende e di grandi organizzazioni pubbliche e private, al di là delle definizioni giuridiche, individuando tali figure nell'ambito di piani di sicurezza o di documenti programmatici e designandoli a volte quali responsabili.

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.

Con il presente provvedimento il Garante intende pertanto richiamare tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema.

L'Autorità ravvisa inoltre l'esigenza di individuare in questa sede alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito di organizzazioni ed enti pubblici e privati, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

2. Quadro di riferimento normativo

Nell'ambito del Codice il presente provvedimento 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.

3. Segnalazione ai titolari di trattamenti relativa alle funzioni di amministratore di sistema

Ai sensi del menzionato art. 154, comma 1, lett. h) il Garante, nel segnalare a tutti i titolari di trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sulla necessità di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema; richiama inoltre l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare in caso di incauta o inidonea designazione.

4. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici

Di seguito sono indicati gli accorgimenti e le misure che vengono prescritti ai sensi dell'art. 154, comma 1, lett. c) del Codice, a tutti i titolari dei trattamenti di dati personali effettuati con strumenti elettronici, esclusi, allo stato, quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008).

I seguenti accorgimenti e misure lasciano impregiudicata l'adozione di altre specifiche cautele imposte da discipline di settore per particolari trattamenti o che verranno eventualmente prescritte dal Garante ai sensi dell'art. 17 del Codice.

Per effetto del presente provvedimento:

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. Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

4.2 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.

4.3 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 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 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 pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare 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.

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 quali amministratori di sistema.

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 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.

5. Tempi di adozione delle misure e degli accorgimenti

Per tutti i titolari dei trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, le misure e gli accorgimenti di cui al punto 4 dovranno essere introdotti al più presto e comunque entro, e non oltre, il termine che è congruo stabilire, in centoventi giorni dalla medesima data.

Per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.

TUTTO CIÒ PREMESSO IL GARANTE:

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, nel segnalare a tutti i titolari di trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sull'esigenza di valutare con particolare attenzione l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (system administrator), amministratore di base di dati (database administrator) o amministratore di rete (network administrator), laddove tali

funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato;

2. ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive l'adozione delle seguenti misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice), salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte di recente per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008):

a. Valutazione delle caratteristiche soggettive.

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e 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 quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

b. Designazioni individuali.

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

c. 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 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 l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle

proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

d. 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 quali amministratori di sistema.

e. 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 riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f. 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 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;

3. dispone che le misure e gli accorgimenti di cui al punto 2 del presente dispositivo siano introdotti, per ttti i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, al più presto e comunque entro, e non oltre, il termine che è congruo stabilire in centoventi giorni dalla medesima data; per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.