LINEE GUIDA SULLA SICUREZZA DEI DATI
DECRETO LEGISLATIVO 30 GIUGNO 2003, N.196
CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

febbraio 2008

INTRODUZIONE

Questo documento fornisce le linee guida sulle prescrizioni e sulle procedure per la gestione e lo sviluppo della sicurezza dei dati agli operatori di ACTAGEST o ACTAPRIVACY, incaricati del trattamento dati, ed agli incaricati degli altri trattamenti dati della nostra organizzazione.

Per **dato personale** si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Per **trattamento** si intende qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
Per **sicurezza** si intende il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti.

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;
Integrità: Le informazioni non devono essere alterabili da incidenti o abusi;
Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.
In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

LINEE GUIDA PER LA SICUREZZA

1. Utilizzare le chiavi!

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio e riponete i documenti negli appositi contenitori alla fine di ogni giornata di lavoro.
La conservazione e la cura delle chiavi degli uffici, degli armadi e dei luoghi sicuri e il loro utilizzo deve essere registrata e controllata.
Qualsiasi criterio di sicurezza attiva o passiva che viene adottato come grate, porte blindate, antifurti, videosorveglianza, controllo accessi, luoghi sicuri, e quanto altro aumenta il livello di sicurezza dei vostri dati.
Il livello di sicurezza dovrà essere proporzionato al proprio trattamento dei dati e adatto al luogo ma un primo livello di sicurezza deve sempre essere comunque garantito.

2 Conservare i documenti in luoghi sicuri

Tutti i documenti cartacei devono essere posti in contenitori con etichette che devono riportare un Identificativo, ma mai i nominativi di clienti, fornitori o contatti o qualsiasi altra informazione immediatamente riconducibile a persone fisiche o giuridiche. Tutti i contenitori con i documenti devono essere posti in scaffalature a giorno, se poste in luoghi controllati, o in armadi con serratura o ripostigli con porte con serratura se posti in luoghi non controllati o aperti al pubblico.
I dati per cui viene richiesto il blocco o la cancellazione, ma che devono essere mantenuti per un obbligo di legge o a propria tutela in quanto relativi ad adempimenti contrattuali svolti, dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serratura.
I dati sensibili o giudiziari dovranno sempre essere posti in armadi con serratura o ripostigli con porte con serrature e sono consegnati agli incaricati sotto la loro responsabilità e, al di fuori dell'orario di lavoro, solo previa registrazione.
I dati estremamente riservati dovranno essere posti in armadi blindati, casseforti o luoghi sicuri (locali in muratura con porta blindata).
Non lasciate documenti con dati personali sui tavoli, dopo averli utilizzati riponeteli sempre nei loro contenitori.

3. Conservare i CD in un luogo sicuro

Per i CD, DVD, dischetti, pen drive e per qualsiasi altro tipo di supporto removibile di dati, si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave in armadi o archivi non appena avete finito di usarli.

4. Ancorare i computer con dati

Ancorare tutti i computer che contengono dati e gli hard disk esterni con supporti o cavi di sicurezza è un primo significativo ostacolo al furto dei dati oltre che delle vostre attrezzature.

5. Utilizzate le password

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

- la password di accesso al computer che impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio;
- la password di accesso alla rete che impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio;
- la password di ACTAGEST o ACTAPRIVACY che impedisce l'accesso al sistema di gestione della propria organizzazione;
- la password dei programmi specifici che impedisce l'accesso ai documenti realizzati con quelle applicazioni.
- la password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

L'utilizzo di questi tipi fondamentali di password è obbligatorio. Imparatene l'utilizzo, e nel caso dobbiate comunicare, almeno temporaneamente, ai tecnici incaricati dell'assistenza, la vostra password registrate l'ora di comunicazione e di rinnovo della vostra password. Scegliete le password secondo le indicazioni della sezione successiva.

Potete registrare in ACTAGEST o ACTAPRIVACY le vostre password per l'accesso a computer o siti Internet in quanto l'accesso alle password è consentito solo agli operatori che le hanno create, nemmeno il gestore può leggere le vostre password che sono memorizzate criptate.

Se archiviate dati sensibili o giudiziari sui vostri computer criptate sempre i dati.

6. Attenzione alle stampe e ai fax di documenti riservati

Non lasciate accedere alle stampe o ai fax persone non autorizzate; se la stampante o il fax non si trovano sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Posizionate le stampanti e i fax in luoghi controllati e non accessibile al pubblico ed a visitatori. Distruggete personalmente le stampe quando non servono più. E' opportuno l'utilizzo di una macchina distruggi documenti, indispensabile nel caso di documenti sensibili o giudiziari.

7. Non utilizzate le email per dati riservati

Non inviate MAI dati sensibili o riservati via email come numeri di carta di credito, password, numeri di conti bancari.

8. Prestate attenzione all'utilizzo dei computer portatili

I computer portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di

backup periodico. Se durante la giornata vi spostate molto dalla vostra postazione o addirittura la notte lasciate il vostro portatile in ufficio, ancorate il computer portatile con cavi di sicurezza o riponetelo in armadi blindati.

9. Non fatevi spiare quando state digitando le password

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di digitazione.

10. Custodite le password in un luogo sicuro

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

11. Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identità

Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro computer.

12. Non utilizzate apparecchi non autorizzati

L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutti i dati dell'organizzazione. Per l'utilizzo consultatevi con il responsabile del trattamento dati.

13. Non installate programmi non autorizzati

Solo i programmi acquistati dalla vostra organizzazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il responsabile del trattamento dati.

14. Applicate con cura le linee guida per la prevenzione da infezioni di virus

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

15. Controllate la politica locale relativa ai backup

I vostri dati potrebbero essere gestiti su un server, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup.
Chiedete al responsabile del trattamento dati quali sono le operazioni di back up che dovete eseguire, con quali modalità e con quali tempi.
Il responsabile del trattamento dati curerà con estrema cura ed attenzione i backup periodici di tutti i dati.

16. Utilizzate gruppi di continuità

Utilizzare almeno un gruppo di continuità per il computer server e per il computer su cui risiede il vostro sistema di gestione ACTAGEST o ACTAPRIVACY.

17. Segnalate le anomalie

Segnalate sempre, al più presto, al responsabile del trattamento dati, qualsiasi tipo di anomalia si verifichi, sia nelle funzionalità del computer su cui operate, sia sia sulla rete di computer su cui operate, sia sul sistema di gestione ACTAGEST o ACTAPRIVACY che state utilizzando, sia su qualsiasi altra applicazione che state utilizzando.

Segnalare in tempo le anomalie e circostanziare gli eventi è fondamentale per prevenire problemi ben più consistenti.

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Come si trasmette un virus:

- attraverso programmi provenienti da fonti non ufficiali;
- attraverso le macro di alcuni programmi;
- attraverso le email ricevute;
- attraverso il download da Internet.

Come *NON* si trasmette un virus:

- attraverso file di dati non in grado di contenere macro (file di testo, pdf, jpg, ecc.);
- attraverso email non contenenti allegati.

Quando il rischio da virus si fa serio:

- quando si installano programmi;
- quando si copiano dati da dischetti;
- quando si scaricano dati o programmi da Internet.

Quali effetti ha un virus?

- effetti sonori e messaggi sconosciuti appaiono sul video;
- nei menù appaiono funzioni extra finora non disponibili;
- lo spazio sul disco si riduce inspiegabilmente;
- le funzionalità dei computer rallentano repentinamente.

Come prevenire i virus:

1. Usate soltanto programmi provenienti da fonti fidate

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati dal responsabile del trattamento dati.

2. Assicuratevi di non far partire accidentalmente il Vostro computer da dischetto, CD o DVD

Infatti se il dischetto fosse infettato, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.

3. Assicuratevi che il vostro software antivirus sia aggiornato

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è

vitale che il programma antivirus sia aggiornato periodicamente (non oltre sei mesi). Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informatevi con il responsabile del trattamento dati per maggiori dettagli.

4. Assicuratevi che sul vostro computer sia attivato il Firewall

Verificate dalle preferenze del vostro computer, o chiedete al responsabile del trattamento dati, che sul vostro computer sia attivato il Firewall e solo i privilegi di rete minimi necessari per le vostre esigenze d'accesso ai dati, oltretutto se sul vostro computer non vi collegate ad Internet o non inviate fax staccate il cavo telefonico per evitare possibili accessi.

5. Non diffondete messaggi di provenienza dubbia

Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: le email di questo tipo sono dette con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da vostra sorella o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli *hoax* più diffusi).

6. Non partecipate a "catene di S. Antonio" e simili

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

7. Non aprite allegati alle email inviate da sconosciuti

Non aprite allegati alle email con file di tipo exe, zip, sit, doc contenete macro, e qualsiasi altro formato a voi sconosciuto se non siete certissimi della provenienza. Potete aprire solamente allegati di tipo pdf, jpg e file di testo che non contengono macro.

SCELTA DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "poco sicura". La scelta di password "sicure" è, quindi, parte essenziale della sicurezza informatica.

Le password di ogni operatore di ACTAGEST o ACTAPRIVACY sono conosciute solo dall'operatore, nemmeno il gestore di ACTAGEST o ACTAPRIVACY può accedere al vostro posto.

Le password esterne conservate in ACTAGEST o ACTAPRIVACY sono visualizzabili solo dall'operatore che le ha create, nemmeno il gestore di ACTAGEST o ACTAPRIVACY può visualizzarle.

Cosa NON fare

NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.
NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
NON scegliete password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
NON usate il Vostro nome utente. È la password più semplice da indovinare
NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono ecc.

Cosa Fare

Cambiare la password a intervalli regolari. La normativa sulla privacy prevede che se sono trattati dati sensibili o giudiziari la password deve essere cambiata ogni tre mesi altrimenti ogni sei mesi. ACTAGEST o ACTAPRIVACY vi chiederà automaticamente quando cambiare la vostra password.
La password deve essere lunga almeno otto caratteri, meglio se con un misto di lettere, numeri e segni di interpunzione.
Nelle password utilizzare esclusivamente i caratteri ASCII, come a-z, A-Z, 0-9 e caratteri di punteggiatura come "!" e " %." Si può verificare che le password che contengono alcuni caratteri accentati o caratteri non romani, come il cirillico o il giapponese, non funzionino, soprattutto in soluzioni database e file tra piattaforme diverse.
Le password di ACTAGEST o ACTAPRIVACY e quelle di molti altri sistemi sono sensibili all'uso delle maiuscole e delle minuscole.
Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi la password viaggiano

in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata per ACTAGEST o ACTAPRIVACY e per sistemi “sicuri”.

Come scegliere una password

Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe. La frase “Tanto và la gatta al lardo che ci lascia lo zampino” può ad esempio fornire, tra le tante possibilità, “Tvlgalcclz”, oppure “Quarantaquattro gatti in file per sei col resto di due” che può fornire “44Gifp6Crd2”.

ACTA Area Software

ACTA ARCHITETTURA srl

www.actaareasoftware.com

info@actaareasoftware.com