Il presente Manuale è stato realizzato da

XP CONSULTING
gianni buccoliero

Il Codice in materia di protezione dei dati personali (DLG 196/03) e le ricadute sui sistemi informatici delle aziende e delle Pubbliche Amministrazioni

*D*al 1 Gennaio 2004 è in vigore, in Italia, il "Codice in materia di protezione dei dati personali" (Decreto legislativo n. 196 del 30/6/2003) che riforma interamente la disciplina sulla privacy. Il

Codice abroga e sostituisce tutte le precedenti leggi, decreti e regolamenti in materia, riunendo in un unico organico contesto l'intera normativa sulla privacy.
Tutte le aziende sono tenute a rispettare la nuova normativa, la cui corretta applicazione consente, non solo di adempiere agli obblighi di legge, ma anche di migliorare l'organizzazione aziendale, i processi di lavoro e la qualità dei risultati. Il Codice richiede l'adozione di diverse misure di sicurezza per garantire che i dati trattati siano custoditi e controllati secondo alcune misure minime di sicurezza: a titolo di esempio possiamo citare il fatto che ogni persona che accede alla banca dati (dall'anagrafica dei clienti ad archivi contenenti dati sensibili) deve essere preventivamente incaricata e riconosciuta dal sistema attraverso un identificativo associato ad una password che deve essere lunga almeno otto caratteri, modificata all'atto del primo collegamento e non deve essere agevolmente riconducibile al proprietario. Altre misure minime prevedono l'aggiornamento costante del software con le ultime "patch" rilasciate dal produttore e il backup settimanale dei dati. Oltre alle misure minime il Codice prevede altre misure di sicurezza più ampie "idonee" a garantire ulteriormente la protezione dei dati e dei sistemi.
In generale il Codice prescrive di fatto la realizzazione di un vero e proprio sistema di sicurezza che protegga i dati custoditi all'interno dell'azienda.

Le misure di sicurezza adottate devono essere riportate in un Documento Programmatico annuale sulla Sicurezza (DPS) la cui redazione o aggiornamento deve essere riportata nella relazione accompagnatoria al bilancio aziendale. Il DPS deve essere redatto entro il 31 Marzo di ogni anno. Tutte le misure di sicurezza previste devono essere attive entro il 30 giugno 2004. La mancata adozione delle misure minime di sicurezza rende penalmente perseguibili gli inadempienti (ovvero chiunque essendovi tenuto omette di adottarle), salvo l'adozione di un ravvedimento operoso. La mancata adozione delle misure minime o di quelle idonee può portare il soggetto cui si riferiscono i dati e che è stato danneggiato a chiedere un risarcimento dei danni.

Microsoft, attraverso le proprie tecnologie, i propri prodotti e i suoi migliori Partner, può fornire una soluzione rivolta ai responsabili delle aziende che si trovano a dover agire in fretta per adempiere agli obblighi di legge ed evitare quindi le sanzioni penali e amministrative che gravano sugli inadempienti. In particolare le ultime versioni dei sistemi operativi Microsoft (Windows XP per il sistema client e Windows Server 2003 per il sistema server), congiuntamente con Microsoft Office 2003, offrono una serie di funzionalità per la sicurezza dei sistemi che permettono di adempiere semplicemente agli obblighi previsti dal Codice, sia per quanto riguarda le misure minime che per quanto concerne le misure idonee. Inoltre Microsoft mette a disposizione tecnologie per la gestione automatica degli aggiornamenti di sicurezza in grado di mantenere sempre allineate le vostre tecnologie Microsoft con le ultime versioni rilasciate. Microsoft, infine, offre ai propri clienti un modo semplice e immediato per avere sempre la versione più aggiornata del proprio software attraverso la licenza denominata "Software Assurance", che oltre a questo vantaggio permette la possibilità di installare il software sui PC di casa o la possibilità di avere della formazione online sui prodotti acquistati.
Attraverso la propria rete di Partner qualificati, Microsoft è in grado di aiutare le aziende che dovessero adeguare la sicurezza dei propri sistemi, attraverso competenze specifiche e "best practice" nate dalla pluriennale esperienza maturata.

1 IL NUOVO CODICE SULLA PRIVACY

1.1 ADEMPIMENTI ED OPPORTUNITÀ

Chiunque tratta dati personali è tenuto a rispettare gli obblighi prescritti dal "Codice in materia di protezione dei dati personali. Aziende, imprese, ditte, studi professionali, banche, assicurazioni, organizzazioni ed esercenti le professioni sanitarie, ed ogni altra categoria, privata e pubblica, indipendentemente dalle loro dimensioni, sono tenute ad operare nel rispetto di precise regole che riguardano la sicurezza dei dati e dei sistemi al fine di ridurre al minimo le fonti di rischio e garantire correttezza, integrità ed aggiornamento delle informazioni.

Tra gli interventi richiesti per la sicurezza dei dati e dei sistemi, a secondo dei casi è necessario organizzare e disciplinare l'uso di:

- sistemi di autenticazione informatica;
- credenziali di autenticazione (password, codici identificativi, carte a microprocessore, certificati digitali, rilevatori di caratteristiche biometriche);
- sistema di autorizzazione informatica;
- protezione dei dati e sistemi dalle intrusioni di virus, internet worm, programmi maligni;
- aggiornamenti delle vulnerabilità individuate con *patch, hot fix, service pack*;
- protezione da intrusioni nei sistemi informatici;
- back up dei dati e organizzazione del ripristino;
- redazione di un aggiornato documento programmatico sulla sicurezza;
- tecniche di cifratura.

E' necessario anche che i sistemi di rilevazione biometria, di videosorveglianza, di localizzatori di persone, di lavoro a distanza, siano organizzati in conformità al Codice.

1.2 LA SICUREZZA COME VANTAGGIO COMPETITIVO

La corretta applicazione delle misure di sicurezza consente non solo di adempiere agli obblighi di legge, ma anche di migliorare l'organizzazione aziendale ottimizzando i processi di lavoro ed operare nella consapevolezza che i dati trattati siano corretti, integri, aggiornati – *come richiesto dal Codice all'art.11* - e costituiscano, perciò, vere informazioni d'impresa. La stessa impresa avrà quindi la garanzia di operare in sicurezza e in ottemperanza della legge e potrà godere della piena fiducia della propria clientela. In tal modo la sicurezza si trasforma da costo a investimento e vantaggio competitivo.

1.3 È NATO IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

Il Codice, all'art.1, introduce un nuovo e fondamentale diritto: *"chiunque ha diritto alla protezione dei dati personali che lo riguardano"*. I dati che devono essere protetti riguardano sia le persone fisiche (tutti noi), sia le persone giuridiche (i dati riferiti ad aziende, imprese, ditte, ecc.). La protezione dei dati personali è garantita da idonee e preventive misure di sicurezza obbligatorie per chi tratta i dati personali.

1.4 MISURE DI SICUREZZA MINIME

Le misure minime di sicurezza richieste dalla legge sono tecniche, informatiche, organizzative, logistiche e procedurali e sono tutte orientate a ridurre i rischi che incombono sui dati personali trattati. Le misure da adottare per la protezione dei trattamenti elettronici dei dati sono sinteticamente elencate di seguito.

1.4.1 Credenziali, autenticazione, autorizzazione

Alla base delle nuove misure minime sono poste le modalità per l'accesso ai dati che devono avvenire solo da parte delle persone autorizzate ed esplicitamente incaricate; ad esse dovranno essere assegnate o associate "credenziali di autenticazione", cioè parole chiave, codici identificativi, carte a microprocessore, token, certificati digitali, o dispositivi che riconoscono le caratteristiche biometriche. Tali credenziali dovranno consentire "l'autenticazione informatica" delle persone incaricate del trattamento di dati. Inoltre, quando più persone incaricate accedono ai dati, è necessario associare ad ogni soggetto uno specifico profilo per l'accesso. Il profilo identifica dei trattamenti di dati che possono essere svolti e costituisce "l'ambito del trattamento consentito"; l'intero processo è definito "sistema di autorizzazione" per l'accesso ai trattamenti consentiti e preventivamente individuati.
La legge definisce anche i criteri con cui le credenziali devono essere scelte; ad esempio la parola chiave usata in un sistema di autenticazione deve essere 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 deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere 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 dovrà essere modificata almeno ogni tre mesi.

1.4.2 Protezione da programmi maligni, prevenzione dalle vulnerabilità, salvataggio dei dati

Alcune misure previste dal codice sono rivolte a tutelare la sicurezza di tutte le tipologie di dati personali dalle nuove emergenti criticità:

- i dati personali devono essere protetti contro il rischio di intrusione e dell'azione di virus, internet worm, programmi maligni, ecc., mediante l'attivazione di idonei strumenti elettronici, (ad esempio antivirus, firewall, ed altri adeguati sistemi) da tenere aggiornati;
- gli strumenti elettronici – nel caso di trattamenti di dati sensibili e giudiziari - devono essere aggiornati periodicamente con programmi che consentono di eliminare le vulnerabilità individuate e correggere i difetti del software individuati (*patch*, *hot fix*, *service pack*);
- i dati devono essere salvati su copie di riserva almeno settimanalmente nel rispetto di apposite disposizioni tecniche e organizzative.

1.4.3 Backup, supporti rimovibili, ripristino

Se si trattano i cosiddetti dati sensibili o giudiziari questi dati dovranno essere protetti da ulteriori misure di sicurezza, quali:

- strumenti elettronici che evitano gli accessi abusivi (intrusioni);
- procedure per la generazione e la custodia di copie di sicurezza dei dati (back up);

- 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;
- disposizioni per riutilizzare o distruggere i supporti rimovibili sui quali sono registrati tali dati;
- strumenti per il ripristino della disponibilità dei dati e dei sistemi entro tempi certi e compatibili con i diritti degli interessati, non superiori a sette giorni.

1.4.4 Documento programmatico annuo sulla sicurezza

Rilevante l'importanza assunta dal Documento Programmatico annuo per la Sicurezza (DPS), che deve essere compilato o aggiornato entro il 31 marzo di ogni anno e contenere, tra l'altro:
- l'analisi dei rischi che incombono sui dati
- le misure da adottare per garantire l'integrità e la disponibilità dei dati
- la previsione di idonei interventi formativi degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati
- la descrizione dei criteri da seguire per garantire l'adozione delle misure minime di sicurezza in caso di outsourcing dei trattamenti.

Inoltre, solo per i dati personali idonei a rivelare lo stato di salute e la vita sessuale trattati da organismi sanitari e gli esercenti di professioni sanitarie, devono essere indicati i criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato, ad esempio attraverso la disgiunzione dei dati anagrafici da quelli riferiti alla salute.
Infine, ed è forse l'aspetto più innovativo che eleva il documento all'attenzione dei vertici aziendali rendendoli consapevoli delle scelte necessarie per garantire la sicurezza, vi è l'obbligo per il titolare di riferire nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza .

1.4.5 Misure di sicurezza idonee e responsabilità civile del titolare del trattamento

Le misure di sicurezza "minime" sono solo una parte degli accorgimenti obbligatori in materia di sicurezza (art. 33 del Codice). Infatti, come già previsto dalla legge n. 675/1996, esiste un obbligo più generale di ridurre al minimo determinati rischi, per cui occorre custodire e controllare i dati personali oggetto di trattamento per contenere le probabilità che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito.
Ciò va fatto adottando misure idonee anche in base al progresso tecnico, alla natura dei dati ed alla caratteristiche del trattamento.
L'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati; viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice), ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice).

Tali misure di sicurezza "idonee" sono individuate dal Titolare sulla base di una analisi specifica delle proprie caratteristiche tecnologiche, organizzative e di processo, tenuto conto delle "innovazioni tecnologiche" e delle soluzioni di sicurezza offerte dal mercato.

1.4.6 Credenziali di autenticazione e controllo accessi

I sistemi operativi della famiglia Windows 9X[1] non prevedono sistemi di autenticazione "nativi"; viceversa i SO successivi (Windows NT, Windows 2000, Windows XP, Windows Server 2003) sono dotati di sistemi di autenticazione ed autorizzazione completi che permettono non solo l'utilizzo di *user-id* e *password*, ma anche credenziali di autenticazioni "forti" quali *token* o *device* di riconoscimento biometrico[2].

Ovviamente, per la verifica delle credenziali di accesso al sistema, possono esser ancora utilizzati sistemi della famiglia 9X se utilizzati come client di reti con sistemi operativi server Microsoft, sistemi dai quali i client "ereditano" le funzionalità di sicurezza per il controllo degli accessi. Nel caso fosse necessario utilizzare un PC stand-alone con sistema operativo Windows 9X è infine possibile sviluppare applicativamente un sistema di autenticazione *ad hoc*, ma va posta estrema attenzione nel valutare i costi di tale sviluppo, soprattutto se paragonati al costo dell'aggiornamento del solo Sistema Operativo.

I requisiti di sicurezza richiesti dal Codice per le *user-id* e *password* possono essere completamente rispettati mediante l'utilizzo dei sistemi operativi di ultima generazione quali Windows XP e Windows Server 2003; in particolare si evidenzia che attraverso queste tecnologie è possibile rispettare le prescrizioni del codice in materia di protezione dei dati:

- avere *user-id* univoche;
- impedire all'amministratore di sistema di conoscere le password degli utenti;
- pre-impostare una lunghezza minima della password;
- pre-impostare l'obbligo di sostituzione della password al primo uso;
- pre-impostare la modifica periodica delle password;
- pre-impostare la "disattivazione automatica" delle user-id dopo sei mesi di inattività;
- pre-impostare la protezione mediante screen-saver, anche in modalità centralizzata.

Con Windows Server 2003 è possibile l'amministrazione centralizzata ed il controllo accessi anche di client mobili (wireless) e *device* basati su tecnologia Windows Mobile. L'amministrazione centralizzata permette di valutare non solo le credenziali di autenticazione ed il profilo di autorizzazione del client (desktop, portatile o palmare) che si vuole collegare alla rete, ma anche la corretta configurazione dello stesso, ad esempio per quanto riguarda la versione del SO, le patch installate o la versione di sistema antivirus presente.

1.4.7 Difesa da virus, Internet worm, programmi maligni ed intrusioni informatiche

Microsoft Windows 2000/XP fornisce, insieme al sistema operativo, un personal firewall[3] in grado di proteggere il sistema dagli attacchi più comuni. Il Sistema Operativo è in grado di sfruttare la tecnologia di Windows Update, in grado di aggiornare automaticamente il sistema con tutte le patch che sono state rese disponibili. Microsoft mette inoltre a disposizione gratuitamente un Bollettino sulla Sicurezza in grado di avvisare tutti gli utenti del rilascio di nuovi aggiornamenti e di situazioni critiche: http://www.microsoft.com/italy/sicurezza

[1] Comprende i SO: Windows 95, Windows 98, Windows 98 SE, Windows ME
[2] Per Windows NT 4.0 l'uso di strumenti biometrici è possibile grazie all'utilizzo di software aggiuntivi di terze parti
[3] Il firewall viene installato automaticamente dalla versione XP SP2 in poi

1.4.8 Salvataggio dei dati

Windows 2000/XP permette di pianificare attività periodiche in automatico per realizzare le copie di sicurezza dei dati. Una volta impostate le scadenze, il sistema automaticamente copia i dati su un dispositivo di backup.

1.4.9 Cifratura dei dati

Dalla versione Windows 2000 in poi, i sistemi operativi sono dotati di funzionalità di cifratura dei dati a livello anche di singolo file o cartella. Con Windows 2003 è possibile condividere documenti crittati anche tra diversi utilizzatori se autorizzati dal proprietario del documento.

1.4.10 Ulteriori informazioni

Ulteriori informazioni sulla sicurezza di Windows XP sono reperibili sul sito http://www.microsoft.com/italy/windowsxp/pro/default.mspx

1.5 MECCANISMI DI LICENZA DEL SOFTWARE

Microsoft propone una serie di possibilità di licenza del software, adatti alla piccola impresa o alla grande azienda o Pubblica Amministrazione, supportati dalle modalità di pagamento più diverse che meglio di adattano alle esigenze delle aziende. La scelta del migliore modello di licenza del software posseduto e da acquistare può aiutare in modo significativo a rimanere sempre aggiornati con il proprio software, elemento essenziale per garantire la massima sicurezza alla propria rete e per adempiere quindi agli obblighi di legge.

Ad esempio con Software Assurance, le aziende hanno accesso alla tecnologia più recente, distribuendo i pagamenti su base annuale. I dipendenti inoltre, possono usare il software a casa e hanno diritto a sconti sui prodotti Microsoft per uso personale.

1.5.1 Accesso automatico alle nuove versioni del software

L'accesso automatico alle nuove versioni del software rilasciate durante il periodo di validità del contratto rappresenta un elemento di vantaggio competitivo e protegge gli investimenti dell'azienda in tecnologia Microsoft. Questo diritto semplifica il processo di acquisizione del software e ottimizza il ciclo di rinnovo dell'infrastruttura IT aziendale garantendo una maggior efficienza operativa e una più elevata sicurezza dei sistemi grazie agli strumenti di produttività più avanzati e all'infrastruttura più innovativa.

1.5.2 Pagamenti dilazionati

Software Assurance consente di distribuire il costo del software con un pagamento dilazionato su un arco temporale di tre anni permettendo una più semplice pianificazione e gestione del budget.

1.5.3 A casa come in ufficio

I dipendenti di un'azienda che ha sottoscritto un contratto Microsoft Volume Licensing comprensivo di Software Assurance, possono ottenere una copia dei prodotti inclusi nel nuovo Microsoft Office System per installarli liberamente sul computer di casa e farne un uso personale o professionale.

1.5.4 Sconti per i dipendenti

Microsoft Employee Purchase Program offre ai dipendenti la possibilità di acquistare prodotti Microsoft (software, hardware e titoli Microsoft Press) con sconti vantaggiosi sui prezzi al dettaglio. I prodotti possono essere ordinati direttamente a Microsoft, tramite un sito Web di e-commerce protetto.
Per maggiori informazioni sulle modalità di licenza del software Microsoft potete consultare il sito http://www.microsoft.com/italy/licenze

2 ALLEGATO: GLOSSARIO PRIVACY

- **Trattamento:** "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 dati, anche se non registrati in una banca di dati"

- **Dato personale:** "qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"

- **Dato anonimo: "**il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile"

- **Dati identificativi:** "i dati personali che permettono l'identificazione diretta dell'interessato

- **Dati sensibili:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"

- **Dati giudiziari:** "i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale"

- **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 ed alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"

- **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"

- **Incaricati:** "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile"

- **Interessato:** "la persona fisica, la persona giuridica,l'ente o l'associazione cui si riferiscono i dati personali"

- **Strumenti elettronici:** “gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento”

- **Notificazione:** è una dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante per la protezione dei dati personali l’esistenza di un’attività di raccolta e di utilizzazione dei dati personali, svolta quale autonomo titolare del trattamento. La notificazione riguarda l’attività di trattamento di dati personali (a volte solo se registrati in banche dati o archivi indicati dalla legge o dal Garante), ma non una banca dati o un archivio in quanto tale. Può aversi, infatti, un trattamento anche se materialmente i dati non sono organizzati in una banca dati. Per le attività di trattamento dei dati che non esistevano prima del 1° gennaio 2004, la notificazione va effettuata prima che inizi il trattamento medesimo. Per le attività che erano già in essere prima del 1° gennaio 2004, la notificazione si può effettuare entro il 30 aprile 2004. La notificazione deve essere fatta solo nei casi previsti dal Codice (Art.37). Per maggiori informazioni sui soggetti tenuti e quelli esonerati si consulti il sito del Garante all’indirizzo: www.garanteprivacy.it

SOLUZIONI PER IL SINGOLO UTENTE

Ecco alcune precauzioni che il singolo utente può prendere per la sicurezza del proprio PC.

Installare un firewall di tipo software sul proprio computer che protegga il proprio PC da eventuali intrusioni;

Se si dispone di un sistema operativo che supporta più utenti, come tutti i sistemi operativi Windows basati su tecnologia NT (Windows NT, Windows 2000, Windows XP e Windows Server 2003), fare in modo che soltanto il proprio profilo appartenga al gruppo degli amministratori. Negare, inoltre, almeno la scrittura su disco a tutti coloro che non fanno parte del gruppo degli amministratori. In questo modo, se un malintenzionato riesce a penetrare nel proprio PC, non appartenendo al gruppo degli amministratori di sistema e, non conoscendo la password per accedere a tale gruppo, non potrà nella maggior parte dei casi apportare modifiche al proprio hard disk, ma potrà comunque leggere i dati. Eventualmente, quindi, negare anche la lettura dei dati a coloro che non fanno parte del gruppo amministratori. Attenzione: i sistemi operativi non basati su tecnologia NT, come Windows 95, Windows 98 e Windows ME sono monoutente, pertanto non consentono di operare sui gruppi come spiegato prima. In questo caso prestare più attenzione ed, eventualmente, eseguire un upgrade del proprio sistema operativo.

Proteggere il proprio profilo con password di accesso difficili da indovinare e di adeguata lunghezza.

Bloccare la diffusione di informazioni da parte del proprio browser Internet e negare l'accesso ai cookies (piccoli file che parecchi siti installano nel proprio computer per far funzionare alcuni servizi) e la lettura da parte dei siti di quelli già esistenti. In Internet Explorer, cliccare su Strumenti, Opzioni Internet. Cliccare su Protezione in alto nella finestra che sarà apparsa e scegliere almeno Media come livello di protezione. Cliccare su Privacy in alto e scegliere almeno Alta come livello di Privacy.

Installare un Antivirus efficiente sul proprio computer e aggiornarlo periodicamente.

Se si dispone di sistemi operativi obsoleti, aggiornarli con altri più nuovi.

INFORMAZIONI GENERALI RIVOLTE A TUTTI

Ultimamente si stanno diffondendo in Rete virus che attaccano sistemi operativi Microsoft. L'ultimo, il virus Blaster, attacca proprio i sistemi operativi Microsoft che dovrebbero essere più sicuri, come Windows NT, Windows 2000, Windows XP e Windows Server 2003. Per questo è importante installare un antivirus su tutti i computer ed eseguire sempre gli aggiornamenti consigliati, l'installazione delle patch per il proprio sistema operativo. La maggior parte di questi virus, tuttavia, si nasconde in allegati di posta elettronica. Se non si è sicuri, pertanto, del messaggio ricevuto, eliminarlo subito. Per molti virus che si diffondono tramite e-mail c'è un semplice trucco per scoprirli: in genere questi allegati si presentano con nomi tipo Readme.txt o Leggimi.doc. Come si può notare l'estensione del file presente fa pensare a file di testo o di Word. In verità, l'estensione dei file si deve vedere SOLO se è abilitata nel sistema operativo. Per esempio, se aprendo una propria cartella sull'hard disk si nota che tutti i file in quella cartella mostrano soltanto il nome e non l'estensione, significa che il nome Readme.txt non è il nome completo di estensione del file, ma solo il suo nome. Il nome completo sarà Readme.txt.xxx. L'estensione vera, pertanto non è .txt o .doc, ma un'altra. In questo caso, pertanto, il file non è assolutamente di testo o di Word, ma può essere uno script di Visual Basic o di linguaggio C. Non eseguire per nessun motivo tale file, ma eliminarlo subito. Se invece, la visualizzazione delle estensioni è abilitata sul proprio computer ed il file si presenta sempre come Readme.txt o .doc e basta, si può essere sicuri che il file è sicuro. Pertanto ciò che si deve ricordare è che le estensioni dei file devono vedersi in Windows SOLO se sono state esplicitamente abilitate dall'utente. Se tutti i file non mostrano la loro estensione e solo l'allegato e-mail scaricato la mostra, si capisce subito che c'è qualcosa che non va. In quel caso quella che sembra l'estensione fa parte, in verità, del nome del file, mentre l'estensione nascosta è un'altra. Se invece, tutti i file mostrano la propria estensione ed anche l'allegato e-mail appare con il nome più l'estensione che si è vista prima e basta, allora il file è sicuro. Comunque, per sicurezza, non aprire MAI i file sulla cui provenienza non si è certi.

Criteri e procedure per assicurare l’integrità dei dati

Di seguito si illustrano le norme applicate per garantire la sicurezza e l’integrità dei dati per:

· computer e supporti informatici: in primo luogo occorre osservare che i computer, incluso il server, risultano tutti sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti, ecc.; in secondo luogo si evidenzia che il server è collegato a gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica.

L’integrità dei dati è inoltre garantita mediante idonee procedure di salvataggio periodico (backup) che consistono nell’utilizzo di tre serie distinte (A – B – C) di 5 cassette da utilizzarsi giornalmente al termine dell’orario lavorativo. Ogni tre settimane la prima cassetta della serie A viene archiviata definitivamente facendo scorrere l’utilizzo delle altre cassette di una posizione.

La Società ha acquisito apposito armadio ignifugo e stagno per la conservazione e archiviazione dei supporti di salvataggio.

L’introduzione di password di Bios all’accensione dei personal computer, di password dello screen-saver e di password per l’accesso in rete determina un livello di sicurezza, circa i dati contenuti nei PC, ritenuto più che soddisfacente.

L’introduzione di dette password ha inibito ad estranei l’uso dei personal computer, attraverso i quali, tramite Proxy, si accede alla posta elettronica ed all’archivio dei messaggi telefax inviati; in merito a messaggi e-mail inviati a più destinatari, quale destinatario dovrà essere indicata la nostra

società con il nostro indirizzo e-mail, ed in CCN i destinatari (che in tal modo non possono individuare gli indirizzi e-mail degli altri destinatari, attraverso la funzione di proprietà).
Le cassette delle copie degli archivi sono custodite in contenitori di plastica e inserite in armadi che vanno, a fine orario di lavoro, chiusi a chiave, con custodia della chiave da parte della persona che effettua il primo turno di lavoro successivo.
I floppy disk contenenti file (copie di lettere, ecc.) che a loro volta contengono dati dei clienti possono essere riutilizzati esclusivamente previa formattazione del floppy stesso, in moda da impedire la letture dei dati precedenti, così come stabilito dalla Legge. I floppy disk contenenti dati, prima della formattazione, sono custoditi nello stesso modo delle cassette dei salvataggi.
Per quanto riguarda infine l'obbligo previsto dalle misure minime sulla sicurezza di cui all'allegato B del Codice della Privacy, gli elaboratori sono dotati di programma antivirus che viene aggiornato sotto la responsabilità del titolare del trattamento a cadenza almeno semestrale, programma che consente di rilevare immediatamente all'apertura di un file la presenza di virus.

E' compito degli "Amministratori di Sistema":

prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up secondo i criteri stabiliti dal "Responsabile del trattamento per la sicurezza dei dati";
assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
fare in modo che sia prevista la disattivazione dei "codici identificati personali" (User-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei "codici identificativi personali" (User-ID) per oltre 6 mesi;
proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

DISPOSIZIONI IN ORDINE ALL'ADOZIONE DELLE MISURE MINIME DI SICUREZZA NELL'AMBITO DELL'UFFICIO

QUALI SONO I DATI PERSONALI?

A titolo esemplificativo, citiamo:

a. il nome, il cognome, l'indirizzo, il numero di telefono, il codice fiscale, la partita I.V.A., dati bancari...
b. informazioni circa la composizione del nucleo familiare, la professione esercitata da un determinato soggetto, sia fisico che giuridico, la sua formazione...
c. fotografie, radiografie, video, registrazioni, impronte...
d. informazioni relative al profilo creditizio, alla retribuzione...
e. informazioni relative alla salute di un soggetto, alla vita sessuale, alla partecipazione ad associazioni di categoria, a partiti, trattenute sindacali, cartelle cliniche, rilevazioni di presenze...

Ci sono adempimenti diversi a seconda del soggetto che tratta i dati?

Si, ovviamente una ditta individuale che non si avvale di nessun collaboratore, sarà gravata da pochi adempimenti rispetto ad una struttura societaria.

A seconda della dimensione e della tipologia di struttura che effettua il trattamento dei dati, dal tipo di dati trattati (solo comuni? anche sensibili o semi-sensibili? giudiziari?) delle modalità di trattamento, dell'esistenza o meno di una struttura informatica collegata ad internet, gli adempimenti sono differenti.

Ai fini del rispetto delle misure minime di sicurezza di cui al D.P.R. 28 luglio 1999, n. 318 si adottano le seguenti misure:

- Svolgere materialmente le operazioni necessarie a garantire il funzionamento del sistema informatico, sotto la direzione del responsabile del trattamento.
- Attivare le nuove utenze e, contestualmente alla comunicazione di nome utente e password, consegnare ai nuovi utenti il Manuale per la Sicurezza.
- Verificare almeno una volta al mese l'elenco delle persone autorizzate ad accedere agli archivi.

- Mettere in atto tutte le indicazioni del *Documento programmatico sulla sicurezza dei dati* relative alla gestione delle parole chiave.