Microsoft®

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

Data di pubblicazione: Aprile 2004

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Il presente documento è stato redatto con la preziosa collaborazione della Business Unit Sicurezza e Controlli di

INDICE

EXECUTIVE SUMMARY

*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"[1]. 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

[1] Emanato con decreto legislativo del 30 giugno 2003 n.196,

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, SANZIONI PENALI E AMMINISTRATIVE PER IL RESPONSABILE DELL'AZIENDA

Le misure di sicurezza richieste dal Codice sono articolate in due gruppi:

- quelle "minime", la cui mancata adozione comporta sanzioni penali per il responsabile legale dell'azienda e/o se designato per il responsabile del trattamento (solitamente l'amministratore delegato o una figura di alto livello), ma anche per chiunque essendovi tenuto omette di adottarle;
- quelle più ampie, o "idonee", decise in autonomia dal titolare in relazione alle proprie specificità che, se non adottate, in caso di danno dovuto a trattamenti di dati non protetti adeguatamente concorreranno all'individuazione delle responsabilità e del conseguente risarcimento economico.

Sono previste, inoltre, misure per titolari particolari quali i fornitori di un servizio di comunicazione elettronica accessibile al pubblico o gli organismi e gli esercenti le professioni sanitarie.

1.5 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.

1.5.1 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.

1.5.2 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[2] - 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.

1.5.3 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.

[2] Per una definizione di dato sensibile o giudiziario si veda il glossario riportato in allegato

1.5.4 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[3] 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 .

1.5.5 La certificazione delle misure minime di sicurezza

Le misure da adottare sono molte e potrebbe accadere che in azienda si preferisca avvalersi di installatori esterni, soprattutto nei casi in cui non si abbiano tutte le competenze necessarie. In tali circostanze, i titolari hanno il diritto di farsi rilasciare dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del decreto legislativo.
Il Codice, infatti, prevede questa circostanza e prescrive che chi adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Disciplinare tecnico allegato al Codice.

1.5.6 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

[3] Solo per il 2004 è previsto che il DPS venga redatto entro il 30 giugno

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.

1.6 ALTRE IMPORTANTI SCADENZE

L'adozione delle misure minime di sicurezza e di quelle più ampie per gli strumenti elettronici deve essere dichiarata nella "notificazione[4]" al Garante da compilare, per chi vi è tenuto, entro il 30 aprile 2004. Di seguito sono riepilogate le altre scadenze.

1.6.1 Documento programmatico sulla sicurezza e Relazione accompagnatoria al bilancio d'esercizio

Misure	Soggetti già tenuti a redigere o aggiornare il DPS[5]	Soggetti non obbligati a redigere o aggiornare il DPS in base alla previgente disciplina
DPS 2004	Aggiornamento DPS entro **il 30 giugno 2004.**	Redazione DPS entro il **30 giugno 2004**.
Relazione accompagnatoria del bilancio esercizio 2003	Riferimento al DPS redatto o aggiornato nel 2003 (con facoltà di indicazione aggiuntiva dell'aggiornamento 2004 in itinere), oppure menzione dell'aggiornamento eventualmente già effettuato nel 2004.	Nessun riferimento se il DPS 2003 o il DPS 2004 non sono stati adottati, oppure riferimento al DPS eventualmente già adottato nel 2004. Facoltà di indicazione del DPS eventualmente predisposto nel 2003 e facoltà di indicazione dell'aggiornamento 2004 *in itinere*.

[4] La 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.

[5] Titolari di un trattamento di dati sensibili o relativi a provvedimenti giudiziari di cui agli artt. 22 e 24 della legge n. 675/1996, effettuato mediante elaboratori accessibili mediante una rete di telecomunicazione disponibili al pubblico

1.6.2 Disposizioni transitorie

Termini	Adempimenti
30 giugno 2004	Adozione per il 2004 di tutte le "misure minime" non previste dalla precedente disciplina. Termine ultimo per predisporre il documento a data certa per descrivere le obiettive ragioni tecniche che non consentono di applicare entro giugno alcune nuove misure minime (documento utilizzabile unicamente nel caso del tutto particolare previsto dall'art. 180, comma 2, del Codice per i soli strumenti elettronici).
1° gennaio 2005	Adozione nuove misure minime su strumenti elettronici non previste in base alla precedente disciplina (solo per i soggetti legittimati a predisporre il predetto documento a data certa).

1.7 PER SAPERNE DI PIÙ

Il testo integrale del Codice è disponibile sul sito del Garante per la protezione dei dati personali, in: http://www.garanteprivacy.it In particolare le misure minime di sicurezza sono riportate nell'allegato B, ottenibile sempre dallo stesso sito.

2 LE SOLUZIONI MICROSOFT

2.1 PREMESSA

Come descritto all'inizio di questo documento, le tecnologie, i prodotti e i Partner Microsoft possono offrire una soluzione ideale per i responsabili delle aziende che si trovano a dover adempiere agli obblighi di legge imposti dal Codice. Microsoft vuole così rendere più semplice il lavoro che gli Amministratori Delegati, i Responsabili Finanziari e i Responsabili dei Sistemi Informativi devono svolgere ai sensi del DLG 196/03.

In questa sezione vengono descritti i prodotti e le tecnologie che servono per realizzare una infrastruttura di rete sicura e affidabile in grado di rispondere nel miglior modo possibile ai requisiti di legge. Al termine di questa sezione viene riportata una tabella riepilogativa delle tecnologie più adatte a rispondere al singolo requisito di legge.

2.2 SOLUZIONI MICROSOFT PER LE AZIENDE CON SERVER DI RETE

In questa sezione sono illustrate le soluzioni Microsoft per le imprese dotate di almeno un server di rete. Questo tipo di configurazione è da considerarsi di riferimento per la maggior parte delle imprese che utilizzano più di un solo personal computer per la gestione dei dati. La presenza di un server di rete permette infatti di centralizzare una serie di operazioni (dalla verifica degli accessi al backup dei dati all'installazione degli aggiornamenti), semplificando il lavoro e riducendo i tempi di amministrazione.

2.2.1 Credenziali di autenticazione e controllo accessi

Il Codice prescrive che siano assegnate (o associate) e gestite credenziali di autenticazione e profili di autorizzazione per ciascun incaricato al trattamento dei dati personali. La gestione dell'autenticazione utente e del controllo di accesso si rivela spesso un'operazione onerosa e nel corso della quale è facile commettere errori che possono esporre alle sanzioni previste dalla legge.
Microsoft Active Directory, incluso in Windows Server 2003, centralizza la gestione dei profili degli utenti, e gestisce sistemi di autenticazione standard, quali Kerberos, certificati X.509 e smart card, permettendo inoltre il controllo degli accessi sulla base dei ruoli svolti in azienda.
Gli strumenti messi a disposizione sono:

- protezione e gestione delle password (lunghezza minima, scadenza, rinnovo, ecc.) grazie ad un'unica procedura di accesso alle risorse di rete;
- profilazione utente grazie all'impostazione di privilegi per il controllo dell'accesso agli oggetti della directory e ai singoli elementi dati che li costituiscono;
- gestione della sicurezza anche dei sistemi client collegati;
- sicurezza nell'accesso ad Internet attraverso il supporto per i protocolli sicuri standard di Internet e i meccanismi di autenticazione degli utenti quali Kerberos, PKI (*Public Key Infrastructure*) e LDAP (*Lightweight Directory Access Protocol*);

- gestione della lista degli incaricati al trattamento dei dati in relazione al profilo di autorizzazione ed al conseguente ambito di trattamento consentito.

La crittografia dei dati è stata potenziata e semplificata in Windows Server 2003 ed è inoltre possibile utilizzare criteri di restrizione per il software onde evitare i danni e le altre azioni provocati da virus o da altro codice pericoloso (programmi maligni).

Infine va menzionato *Windows Rights Management Services* (RMS), una funzionalità di sicurezza integrata in Windows Server 2003 che opera congiuntamente con le applicazioni client per salvaguardare le informazioni confidenziali e i dati sensibili dell'azienda in qualsiasi circostanza, permettendo all'utente di definire quali documenti possono essere letti, modificati, inoltrati o stampati. Microsoft Office 2003 sfrutta appieno questa funzionalità offerta da Windows Server 2003: per garantire la massima sicurezza di documenti e dati condivisi negli ambienti di collaborazione, Office 2003 integra la nuova funzionalità IRM (Information Rights Management), una tecnologia di protezione a livello di file che impedisce l'utilizzo non autorizzato di informazioni e documenti, estendendo Windows® Rights Management Services alle applicazioni di Microsoft Office 2003 e a Microsoft® Internet Explorer.

Ulteriori informazioni sono reperibili sul sito
http://www.microsoft.com/italy/windowsserver2003/default.mspx

2.2.2 Protezione da programmi maligni e prevenzione delle vulnerabilità

Per la protezione da virus, worm e altri programmi maligni, Microsoft propone Internet & Security Accelerator Server 2000 (ISA Server 2000), un firewall multilivello di classe Enterprise, che alle classiche funzioni di difesa perimetrale aggiunge, se usato insieme a Microsoft Exchange Server e Internet Information Services, caratteristiche di protezione evolute. ISA Server consente anche il controllo della navigazione Internet degli utenti della rete aziendale.

Per la gestione degli aggiornamenti che consentono di eliminare le vulnerabilità sono disponibile due soluzioni di tipo centralizzato:

- SUS, *Software Update Services*, un servizio gratuitamente scaricabile dal sito web di Microsoft che permette il deployment degli aggiornamenti di sicurezza del sistema operativo client e server;
- SMS, *System Management Server 2003*, che oltre alle funzionalità di SUS offre altre caratteristiche quali la gestione dell'inventario del software installato in azienda e la gestione degli asset informatici.

Per aiutare nella scelta della migliore soluzione per la gestione degli aggiornamenti Microsoft ha predisposto un documento reperibile sul sito
http://www.microsoft.com/windowsserversystem/sus/suschoosing.mspx . Ulteriori informazioni sono a disposizione sul sito http://www.microsoft.com/italy/windowsserversystem/default.mspx

2.2.3 Affidabilità, copie di sicurezza e ripristino dei dati

La soluzione Microsoft per garantire affidabilità e sicurezza delle basi di dati è Microsoft SQL Server 2000, un database relazionale affidabile, sicuro e scalabile che supporta diverse tecnologie hardware e software per la gestione dell'alta affidabilità.

Microsoft SQL Server ha ottenuto la certificazione di sicurezza "C2" TCSEC (*Trusted Computer System Evaluation Criteria*) da parte della National Security Agency statunitense.

In particolare, per gli aspetti di sicurezza SQL Server garantisce il pieno supporto dei requisiti di legge per il trattamento dei dati. Tra le funzionalità presenti vanno segnalate:

- crittografia a livello di rete: SQL Server 2000 supporta automaticamente la crittografia dei dati e del traffico di rete tra i sistemi client e server di una rete; questo consente di proteggere i dati che fluiscono dagli application server verso Microsoft SQL Server;
- crittografia del file system: SQL Server 2000 protegge i file di dati utilizzando in modo appropriato il supporto per la crittografia del file system integrata in Windows Server 2003; ciò consente di proteggere anche i dati sensibili, per i quali, in alcuni casi, è prevista, appunto, la cifratura delle informazioni.

Microsoft Exchange 2003 è la soluzione per le problematiche legate all'antispamming ed alla gestione in sicurezza della posta elettronica. In particolare mediante l'utilizzo di questo prodotto è possibile ottenere:

- accesso sicuro via Internet da Outlook;
- controllo della junk mail con supporto in tempo reale per blacklists ed anti spamming;
- scollegamento automatico dopo un periodo di inattività;
- filtro sulla connessione;
- supporto per il clustering a 4 e 8 nodi;
- centralizzazione dei servizi di ripristino delle caselle postali;
- centralizzazione dei servizi di ripristino dello storage.

Ulteriori informazioni sono reperibili sul sito
http://www.microsoft.com/italy/windowsserversystem/default.mspx

2.3 SOLUZIONI MICROSOFT PER IL SOLO CLIENT

In questa sezione sono illustrate le tecnologie Microsoft per i PC client che aiutano il rispetto della normativa per la protezione dei dati.

2.3.1 Credenziali di autenticazione e controllo accessi

I sistemi operativi della famiglia Windows 9X[6] 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[7].

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.

[6] Comprende i SO: Windows 95, Windows 98, Windows 98 SE, Windows ME
[7] Per Windows NT 4.0 l'uso di strumenti biometrici è possibile grazie all'utilizzo di software aggiuntivi di terze parti

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

Microsoft Windows XP fornisce, insieme al sistema operativo, un personal firewall[8] 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

2.3.3 Salvataggio dei dati

Windows 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.

2.3.4 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.

2.3.5 Ulteriori informazioni

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

2.4 SICUREZZA DI MICROSOFT OFFICE

Office 2003 offre i seguenti strumenti per la sicurezza:

- back-up e ripristino automatico dei file in uso in occasione di crash di sistema; autoriparazione dei file in uso se danneggiati o in caso di impossibilità a riparare estrazione dei dati recuperati; ripristino automatico delle applicazioni in caso di malfunzionamenti;
- protezione dall'accesso indesiderato ad e-mail e documenti o parti di essi mediante password, con crittografia fino a 128 bit;
- protezione dei documenti e e-mail da manomissioni rispetto all'originale, attraverso firma digitale;
- protezione contro virus negli script: diversi livelli di protezione da macro con possibilità di riconoscere le macro firmate digitalmente che si vogliono eseguire;

[8] Il firewall viene installato automaticamente dalla versione XP SP2 in poi

- Authenticode per add-ins e macro: meccanismo di firma digitale che assicura che questi componenti software non siano stati manomessi;
- protezione contro i virus che si propagano attraverso le agende (address book) degli utilizzatori, tramite il blocco degli accessi automatici all'agenda indirizzi;
- blocco degli allegati alla posta elettronica (Outlook) eseguibili che potrebbero trasportare virus;
- API antivirus, che permette l'installazione di antivirus di terze parti per ulteriore protezione da virus che possano oltrepassare tutte le citate misure di sicurezza;
- protezione della privacy circa il riferimento agli autori dei documenti consentendo di rimuoverne i meta-dati;
- Sicurezza dell'XML Expansion Pack: impedisce che Expansion Pack (utilizzati in soluzioni Smart Document) non autorizzati vengano scaricati.

Office 2003, se utilizzato insieme a Windows 2003, offre anche i servizi di *Information Rights Management* (IRM) che aiutano a proteggere i contenuti digitali e la proprietà intellettuale, offrendo la possibilità ad un utente di impedire l'inoltro, la stampa, il salvataggio in altro file, la modifica e/o la copia di un documento Word o un messaggio e-mail o un foglio Excel.

Per quanto riguarda, infine, le problematiche legate allo spamming ed alla gestione in sicurezza della posta elettronica, Microsoft Outlook 2003 include funzionalità concepite appositamente per bloccare i messaggi indesiderati che molti utenti ricevono ogni giorno, con la possibilità di controllare i tipi di messaggi ricevuti e specificare i mittenti da cui si desidera ricevere messaggi.
Outlook 2003 integra diverse caratteristiche per la protezione dai messaggi non richiesti:

- **Filtro per i messaggi indesiderati.** Outlook utilizza un'innovativa tecnologia sviluppata da Microsoft Research per stabilire se un messaggio deve essere considerato indesiderato, in base a una serie di parametri come l'ora di invio e il contenuto. Il filtro non esclude specifici mittenti o particolari tipi di e-mail, ma esamina il contenuto nel complesso, utilizzando un'avanzata funzione di analisi della struttura del messaggio per determinare la probabilità con cui potrebbe essere considerato indesiderato dall'utente.

  Per impostazione predefinita il filtro applica un livello di controllo basso, progettato per individuare i più comuni messaggi indesiderati. Tutti i messaggi intercettati dal filtro vengono spostati in una speciale cartella "Posta Indesiderata", da dove l'utente potrà eventualmente recuperarli in un secondo tempo. È possibile aumentare il livello di controllo del filtro (incrementando il rischio di bloccare alcuni messaggi regolari) oppure impostare Outlook in modo che i messaggi indesiderati vengano definitivamente eliminati all'arrivo.
- **Elenco di mittenti affidabili.** Se un messaggio di posta elettronica viene erroneamente contrassegnato come indesiderato dal filtro, è possibile aggiungere il mittente all'elenco dei mittenti affidabili. Gli indirizzi di posta elettronica e i nomi di dominio inclusi in questo elenco non vengono mai considerati indesiderati, indipendentemente dal contenuto del messaggio.
  I contatti corrispondenti vengono contrassegnati come attendibili per impostazione predefinita e la posta inviata da questi ultimi non viene mai scartata. Con Microsoft Exchange Server i messaggi provenienti dall'interno dell'organizzazione vengono sempre considerati attendibili, indipendentemente dal contenuto. Gli utenti possono configurare

Outlook in modo da accettare solo messaggi provenienti dagli indirizzi contenuti nell'elenco dei mittenti affidabili, per avere un completo controllo sulla posta in arrivo.

- **Elenco di mittenti indesiderati.** I messaggi provenienti da determinati indirizzi o nomi di dominio possono essere facilmente bloccati aggiungendo il mittente all'elenco dei mittenti indesiderati. I messaggi ricevuti dalle persone o dai domini specificati in questo elenco verranno sempre considerati indesiderati, indipendentemente dal contenuto.
- **Elenco di destinatari affidabili.** È anche possibile definire una lista di distribuzione da inserire nell'elenco dei destinatari affidabili. Tutti i messaggi inviati agli indirizzi di posta elettronica o ai domini inclusi in questo elenco non verranno mai trattati come posta indesiderata, indipendentemente dal contenuto.
- **Aggiornamento automatico.** Microsoft fornirà aggiornamenti periodici per assicurare l'efficienza del filtro per i messaggi indesiderati. La funzionalità di aggiornamento automatico non è tuttavia inclusa nella versione beta 2.

Il filtro per i messaggi indesiderati è attivato per impostazione predefinita. La prima volta che un messaggio viene spostato nella cartella Junk E-mail, l'operazione viene segnalata da una finestra di dialogo.
Per modificare le impostazioni relative alla posta indesiderata, scegliere Opzioni dal menu Sturmenti e fare clic su Posta Indesiderata. Per aggiungere nomi agli elenchi Mittenti Atendibili, Destinatari Attendbili o Mittenti Bloccati, è sufficiente fare clic con il pulsante destro del mouse su un messaggio e scegliere Posta Indesiderata dal menu visualizzato oppure scegliere Posta Indesiderata dal menu Azioni.

Ulteriori informazioni sulla sicurezza di Office sono reperibili sui siti
http://www.microsoft.com/italy/office/default.mspx
http://www.microsoft.com/italy/informationworker/

2.5 CERTIFICAZIONE DI SICUREZZA E PARTNER MICROSOFT

La rete dei Partner di Microsoft è in grado di offrire il necessario supporto affinché possano essere recepite le misure minime di sicurezza prescritte dalla legge. In particolare la partnership con Oasi – Business Unit Sicurezza e Controlli - permette di proporre a tute le aziende una offerta di alta qualità composta da tecnologie e servizi di consulenza integrati.
Per sapere dove è possibile trovare un partner Microsoft di suo gradimento, specializzato nell'offrire servizi di consulenza relativi ad aspetti di sicurezza e privacy, può consultare il sito http://directory.microsoft.com/ResourceDirectory/Services.aspx e selezionare la voce "Servizi di protezione" alla voce "Servizi richiesti"

2.6 LINEE GUIDA PER LA REALIZZAZIONE DI PROGETTI DI SICUREZZA DELLA RETE

Microsoft mette a disposizione dei propri clienti un insieme di "best practice" su come gestire la sicurezza dei propri sistemi e dei propri dati. Tale documentazione è disponibile gratuitamente online sul sito http://www.microsoft.com/italy/sicurezza all'interno del Security Guidance Centre. Su questo sito è possibile accedere a incontri di formazione tecnica in aula, webcast e avere accesso

alla documentazione per la messa in sicurezza dei server e dei client, oltre che per la gestione degli aggiornamenti.

Dallo stesso sito è possibile abbonarsi, sempre in maniera completamente gratuita, al servizio di alerting sulle problematiche di sicurezza attraverso il quale si viene automaticamente informati via e-mail dei nuovi problemi di sicurezza riscontrati da Microsoft e degli aggiornamenti messi a disposizione.

2.7 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.

2.7.1 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.

2.7.2 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.

2.7.3 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.

2.7.4 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

3 SCHEDA DI RIEPILOGO DEGLI ADEMPIMENTI E DELLE SOLUZIONI MICROSOFT

Le piccole e medie imprese che necessitano di una soluzione semplice ed integrata possono trovare in Microsoft Small Business Server 2003 (SBS 2003) e Office 2003 Small Business Edition la soluzione ideale per risolvere i problemi legati al rispetto del Codice in materia di protezione dei dati personali.SBS 2003 è infatti un prodotto che include al suo interno Windows Server 2003, Exchange 2003, SQL Server 2000, ISA Server 2000 e molti altri servizi. Tutte le tecnologie elencate in questo documento sono presenti in SBS 2003, il quale, se usato congiuntamente con Windows XP e Office 2003 sui dispositivi PC client, offre tutto quanto serve per adempiere al Codice.

Le grandi aziende possono invece affidarsi a soluzioni più articolate, basate sempre sui prodotti elencati nella tabella sottostante e implementati attraverso la rete di Partner Microsoft specializzati.

Per entrambe le tipologie di azienda è invece da analizzare la soluzione di gestione delle licenze software più opportuna per rimanere sempre aggiornati e proteggere al meglio i propri dati.

Di seguito viene riportata la tabella riassuntiva delle tecnologie Microsoft che aiutano le aziende a soddisfare i requisiti previsti dal Codice in materia di protezione dei dati personali.

	Misura richiesta	***Soluzione Microsoft***
1.	Censimento e aggiornamento dei trattamenti	• Active Directory; • SMS 2003 (per gli aspetti di Software Inventory e Asset management)
2.	Lista degli incaricati	• Active Directory
3.	Gestione delle credenziali di autenticazione	• Active Directory per la parte server; • sistema di autenticazione da Windows 2000 in poi per la parte client;
4.	Password, token o dispositivi biometrici	• Active Directory per la parte server; • sistema di autenticazione da Windows 2000 in poi per la parte client;
5.	Protezione della sessione di lavoro	• Active Directory per la parte server; • sistema di autenticazione da Windows 2000 in poi per la parte client;
6.	Profilazione dei privilegi per l'accesso	• Active Directory per la parte server; • sistema di autenticazione da Windows 2000 in poi per la parte client;
7.	Aggiornamento programmi per prevenire vulnerabilità e correggere difetti del software	• SUS (Software Update Services) e SMS (System Management Server 2003) per la parte server; • Microsoft Update per la parte client;
8.	Adozione di misure idonee per	• Windows Server 2003, SQL Server 2000,

	assicurare l'integrità e disponibilità dei dati	Exchange Server 2003, Office 2003
9.	Salvataggio e ripristino dati	• Windows Server 2003, SQL Server 2000, Exchange Server 2003 per la parte server; • personal firewall di Windows XP e Office 2003 per la parte client;
10.	Ripristino dei dati e sistemi salvati	• Task periodici da Windows 2000 in poi e Office 2003
11.	Difesa dagli accessi abusivi	• Windows Server 2003, SQL Server 2000, Exchange Server 2003 per la parte server; • personal firewall di Windows XP e Office 2003 per la parte client; • Enterprise firewall Microsoft Internet & Acceleration Server (ISA) •
12.	Protezione supporti rimovibili	• Windows Server 2003 per la parte server; • Windows XP per la parte client
14.	Analisi dei rischi informatici	• Servizi professionali Microsoft o dei Partner
14.	Relazione di conformità dell'installatore per adozione misure minime	• Servizi professionali Microsoft o dei Partner
15.	Formazione specifica degli incaricati	• Servizi professionali Microsoft o dei Partner

4 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