GUIDA AZIENDALE ALLA SICUREZZA INFORMATICA

Introduzione

Il presente documento costituisce una prima regolamentazione della materia ed è suscettibile di modifiche e/o integrazioni sulla base dell'evoluzione del processo di realizzazione del Sistema Informativo dell'Ente, della tecnologia e delle osservazioni ed esperienza dell'utenza, oltre che dalle norme vigenti.

Contesto Normativo di Riferimento

- D.lgs. n° 518 del 1992 *"Attuazione della Direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore"* che modifica il regio decreto n° 633 del 1941, relativo al diritto d'autore, integrandolo con norme relative alla tutela giuridica dei programmi per elaboratore
- L. n° 547 del 1993 *"Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"* che modifica il codice penale italiano introducendo i cosiddetti "computer crimes"
- L. n° 675 del 1996 *"Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"*
- D.lgs. 11/5/99, n. 135, "Disposizioni integrative della legge 31/12/96, n. 675, sul trattamento di dati sensibili da parte di soggetti pubblici"
- D.P.R. 28 luglio 1999 n. 318, *"Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo* 15, *comma* 2, *della legge* 31 *dicembre* 1996, *n.* 675"
- L. 7 agosto 1990 n° 241- Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
- L. 15 marzo 1997, n° 59 -Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa
- L. 15 maggio 1997, n° 127 -Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e controllo
- .L. 16 giugno 1998 n° 191 -Modifiche ed integrazioni alle leggi: n° 59 del 15/3/1997 e n° 127 del 15/5/1997, nonche norme in materia di formazione del personale dipendente e di lavoro a distanza nelle pubbliche amministrazioni
- C.P. art. 615-ter -*Accesso abusivo a un sistema informatico o telematico,* art. 615- quater: *Detenzione e diffusione abusive di codici di accesso a sistemi informatici o telematici,* art. 615-quinquies -*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*

REGOLE BASE

1. Proteggete il PC da furti e/o uso illecito.
2. Maneggiate con cura i dati contenuti nel Vs. PC.
3. Trattate confidenzialmente le Password che vi saranno rilasciate.
4. Accertatevi che i dati provenienti da fonti esterne non sono infetti da virus.
5. Utilizzate esclusivamente software per i quali l'Azienda possiede una regolare licenza.
6. Fate attenzione ai rischi connessi allo scambio di dati elettronici (dischetti o CD duplicati senza autorizzazione) con terzi esterni all'Azienda.
7. Accertatevi che le apparecchiature che intendete allacciare alla rete aziendale. siano autorizzate (inventariate e/o assistite dall'Azienda).
8. Attenetevi alle disposizioni di volta in volta emanate.
9. Segnalate immediatamente i casi d'utilizzo non corretto o potenzialmente pericoloso delle attrezzature informatiche al Sistema Informativo o al personale preposto

PRINCIPALI ACCORGIMENTI

1. Proteggere il PC da furti e uso illecito

Assicuratevi che nessuno possa accedere al Vs. PC quando non siete presenti e conservate sotto chiave i dischetti o i nastri di backup di vostra pertinenza.
Spegnete il PC quando vi assentate o andate a casa, e se deve restare accesso prendete misure di sicurezza (password sullo screen saver). Utilizzate lo screen saver più semplice possibile tra quelli già in dotazione alla macchina (es.: schermo nero).
Non consentite a personale non espressamente autorizzato dal Vs. Responsabile e/o dal Sistema Informativo di utilizzare il Vs. PC.
Se avete in dotazione un PC portatile, non lasciatelo mai incustodito.

2. Maneggiate con cura i dati del Vs. PC

2.1. Informazioni confidenziali
Tutte le informazioni devono essere trattate con cura. Le informazioni confidenziali/sensibili (dati aziendali, contatti istituzionali e relativi nominativi) devono inoltre essere protette da visioni illecita.
Salvate sempre le informazioni confidenziali su HardDisk e non su supporti mobili.

(soprattutto dischetti/CDROM) che possono essere facilmente trafugati, e sono inoltre molto deteriorabili. Se dovete fare una copia di riserva utilizzate il server aziendale, se disponibile, oppure un altro PC "sicuro".
Ritirate subito dalle stampanti i documenti che contengono informazioni confidenziali, relativi agli Enti con i quali intercorrono rapporti istituzionali.

2.2. Salvataggio e ripristino
Il salvataggio è l'unico sistema che garantisce il ritrovamento dei dati in caso di perdita o altro problema sul computer.
Decidete e rispettate una "strategia di salvataggio" (giornaliera, settimanale, mensile) in base all'importanza e alla variabilità dei vs. dati.
Salvate i vostri dati preferibilmente sul server aziendale, se esiste, oppure su un altro PC. Se effettuate salvataggi su dischetto/CDROM assicuratevi di effettuare una rotazione e una sostituzione abbastanza frequente dei supporti. Conservateli in luogo sicuro e non accessibile ad altri se contengono dati riservati.

2.3. Smaltimento dei supporti di dati
Tutti i supporti (computer, dischetti/CDROM, stampe) contenenti dati confidenziali devono essere smaltiti nel modo corretto per evitare che vengano divulgate involontariamente informazioni che riguardano l'Azienda o Enti ad essa correlati.
Accertatevi quindi che vengano resi inutilizzabili i supporti magnetici e i documenti contenenti dati riservati.
Non gettare i dischetti senza averli formattati o comunque aver reso irrecuperabili le informazioni relative a dati confidenziali.
Se richiedete lo smaltimento di un PC provvedete prima personalmente, o richiedete al Sistema Informativo di farlo, alla rimozione di tutti i dati in esso contenuti.

3. Trattate confidenzialmente le password

3.1. Cura delle password
La password costituisce una misura di sicurezza efficace se usata correttamente.
Le password sono utilizzate a vari livelli all'interno di un PC. In linea di massima evitate di assegnare password all'accensione, a meno che abbiate l'uso esclusivo della macchina (es. portatili), per consentire in ogni caso l'accesso in emergenza e manutenzione. Potete e dovete invece assegnare una password riservata per :
- accedere all'elaboratore e alle risorse di rete via S.O. Windows;
- gestire il Vs. accesso alle procedura aziendali;

• gestire il Vs. accesso alla posta elettronica
In linea di principio, ogni password è personale e non va comunicata ad altri.

Le password "sicure" sono costituite da almeno sei caratteri di cui almeno una deve essere una cifra o un carattere speciale. Non usate strutture riconoscibili come nomi o date di nascita. Se temete di dimenticarla, un metodo utile consiste nell'utilizzare le iniziali di una frase o di una filastrocca.
Evitate di memorizzare le Vs. password di accesso in procedure automatiche (es: nelle informazioni di collegamento di cartelle condivise di Vs. colleghi)
Conservate in luogo sicuro tutti i numeri telefonici, i codici PIN e le informazioni necessarie per accedere alla rete aziendale.

4. Accertatevi che i dati provenienti da fonti esterne non siano infetti da virus

4.1. Pericolosità dei virus
I virus possono alterare o distruggere i dati e i programmi che utilizzano i sistemi operativi di Microsoft (Windows, anche nelle più recenti versioni ed ora anche altri quali Linux).Sono sempre più diffusi su Internet, spesso in forma di programmi "utili" o di "intrattenimento".
I PC aziendali sono di norma provvisti di un programma antivirus: se non ne disponete o ne avete una versione non aggiornata rivolgetevi al Sistema Informativo.
Non caricate, comunque, sul Vs. PC programmi di qualsiasi origine che non siano stati forniti dall'Azienda per l'esecuzione della normale attività.
Se dovete utilizzare dischetti o scaricare file da Internet, prima dell'utilizzo eseguite una scansione per accertarvi che non siano infetti da virus.

5. Utilizzate esclusivamente i software per i quali la società possiede una regolare licenza

5.1. Copyright
Sul vostro PC è autorizzato l'uso del solo software con licenza. In particolare, non eseguite di vostra iniziativa modifiche o upgrade di sistemi operativi o di programmi applicativi: le macchine che vi sono state date in dotazione sono configurate in modo adeguato per le loro caratteristiche hardware e per le vostre esigenze, e dispongono delle relative licenze d'uso solo per i programmi installati dal Sistema Informativo.

Ogni manomissione espone il responsabile aziendale a violazioni di norme aziendali, civili e penali (se realizzate a fini di lucro o comunque illeciti).
Se avete bisogno di tools specifici (soprattutto di Internet downloads) informatevi presso il Sistema Informativo per essere certi di eseguire una procedura sicura.
Se avete in dotazione un masterizzatore per l'effettuazione di copie di sicurezza o per l'archiviazione di dati, ricordate che è assolutamente vietato effettuare duplicazioni di software commerciale o di qualsiasi prodotto coperto da copyright utilizzando gli strumenti aziendali.

6. Fate attenzione ai rischi connessi allo scambio di dati elettronici con terzi

6.1. La posta elettronica

La sicurezza in ambito e-mail costituisce un grave problema, anche considerando il fatto che i messaggi possono essere intercettati.
Usare la dovuta cautela quando si inviano messaggi e-mail. Il loro contenuto può essere considerato come presa di posizione ufficiale dell'Azienda. Seguite i regolamenti vigenti per i comunicati stampa.
Usate cautela nella gestione dei destinatari. Possibilmente tenete separati i destinatari interni da quelli esterni. Non utilizzate liste prestabilite se non conoscete i destinatari.
Non inviate informazioni che possano violare, per il loro contenuto o per il destinatario, disposizioni di legge o linee guida aziendali, o che possano compromettere l'immagine dell'azienda. Ciò soprattutto nel caso si tratti di informazioni che possono compromettere o danneggiare una o più persone.
Non inviate messaggi sotto un altro nome, eccetto quando abbiate ricevuto appropriata delega. La responsabilità personale continua a sussistere anche in caso di delega.
Non inviate catene telematiche di "Sant'Antonio". Se ricevete un messaggio di tal genere comunicatelo subito al Sistema Informativo. Non attivate in nessun caso gli allegati.
I messaggi e-mail devono essere brevi e concisi: fate un uso limitato di immagini e allegati non necessari. Comprimete tutti gli attachment con un opportuno programma.
Non usate nei messaggi di posta i caratteri accentati della tastiera italiana, che non sono supportati dai normali protocolli di e-mail.

6.2. Furto di informazioni

Malintenzionati di vario genere possono essere interessati ad accedere ai sistemi

sito "sicuro", verificando la corrispondenza tra le informazioni di identificazione presenti sulla pagina e quelle presenti nell'indirizzo di collegamento (URL) (es.: se la home page di un sito fa riferimento al Ministero dell'Ambiente, ma la URL è del tipo *"www.pincopalla.it"*, è probabile che le informazioni ivi contenute e gli eventuali collegamenti ad altri siti non siano sicuri).
A volte può capitare che vi venga proposto un "download" a cui è associato un "certificato" di tipo Verisign di una parte terza. E' questa una misura di sicurezza in via di estensione. Naturalmente potete procedete con fiducia al download solo se vi fidate sia del certificato che del certificante.

8.Attenetevi alle disposizioni contrattuali e giuridiche

8.1. Osservanza delle disposizioni contrattuali e giuridiche
Attenetevi alle disposizioni circa la tutela dei dati e dei diritti d'autore (brevetti, copyright, tutela dei marchi). Queste disposizioni valgono anche per il software aziendale, che non va assolutamente intaccato o manomesso.
Accertatevi che l'uso delle risorse informatiche rispetti l'immagine professionale dell'Azienda, perché le autorità giudiziarie possono imporre di rendere pubbliche le informazioni, i backup e altri dati che si trovano nei nostri sistemi.

8.2. Non osservanza delle disposizioni contrattuali e giuridiche
La non osservanza delle regole contenute nella presente guida può esporre a sanzioni e nei casi gravi, può portare a procedimenti penali o civili.

9.Segnalate immediatamente i casi sospetti

9.1. Il vostro aiuto è indispensabile
Il vostro aiuto concreto nello scoprire e comunicare le violazioni delle misure di sicurezza è importante per garantire una protezione adeguata.
Siete perciò pregati di segnalare ogni anomalia (smarrimento o furto di informazioni, virus, violazioni di sicurezza constatate o presunte) ai vostri superiori o al Sistema Informativo, in modo che possano essere prese le misure necessarie.