# *Regolamento aziendale sulla sicurezza informatica*

*Linee guida per la sicurezza delle informazioni*
*e*
*norme di comportamento per l'utilizzo di strumenti informatici*

## Premessa

Il presente documento, che sostituisce le eventuali versioni precedentemente prodotte, definisce le regole per l'utilizzo di strumenti informatici e per prevenire i relativi problemi al fine di ottenere maggiore "sicurezza" nei suoi aspetti fondamentali, che si possono di seguito sintetizzare:

- **riservatezza**: prevenzione contro l'accesso non autorizzato alle informazioni
- **integrità**: le informazioni non devono essere alterabili da incidenti o abusi
- **disponibilità dei dati**: il sistema deve essere protetto da interruzioni impreviste

Più precisamente :

- salvaguardare la **riservatezza** dell'informazione significa ridurre a livelli accettabili il rischio che un'entità possa, volontariamente o involontariamente, accedere all'informazione stessa senza esserne autorizzata;
- salvaguardare l'**integrità** dell'informazione significa ridurre a livelli accettabili il rischio che possano avvenire cancellazioni o modifiche di informazioni a seguito di interventi di entità non autorizzate o del verificarsi di fenomeni non controllabili (come il deteriorarsi dei supporti di memorizzazione, la degradazione dei dati trasmessi su canali rumorosi, i guasti degli apparati, i problemi ai sistemi di distribuzione dell'energia, gli incendi, gli allagamenti) e prevedere adeguate procedure di recupero delle informazioni (ad esempio i piani di back-up);
- salvaguardare la **disponibilità** dell'informazione significa ridurre a livelli accettabili il rischio che possa essere impedito alle entità autorizzate l'accesso alle informazioni a seguito di interventi di altre entità non autorizzate o del verificarsi di fenomeni non controllabili del tipo già visto al punto precedente.

Il raggiungimento di questi obbiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici ma anche di opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto sofisticate, non saranno efficienti se non usate propriamente. A tal proposito si ricorda che le precauzioni di tipo tecnico cercano di proteggere le informazioni durante il loro transito tra i vari sistemi e, nel momento in cui esse raggiungono gli utenti finali, la loro protezione dipende esclusivamente da questi ultimi; nessuno strumento tecnologico può sostituirsi al senso di responsabilità ed al rispetto delle norme.

Si raccomanda pertanto, a tutti gli utenti, di attenersi alle presenti linee guida ed a fare tutto il possibile al fine di garantire la "sicurezza" dei dati ed evitare l'appropriazione indebita di informazioni da parte di terzi. L'assunto è "***NON C'E' PRIVACY SENZA SICUREZZA***"

Si riepilogano di seguito i riferimenti normativi a cui questo documento si è ispirato:

- decreto legislativo 12 febbraio 1993, n. 39, recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera *mm)*, della legge 23 ottobre 1992, n. 421;
- D.P.R 28 luglio 1999, n. 318 recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675.

- direttiva P.C.M. del 16 gennaio 2002 recante Sicurezza informatica e delle telecomunicazioni;
- decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali;
- D.Lgs. 1 agosto 2003, n. 259 – Codice delle comunicazioni elettroniche
- decreto legislativo 28 febbraio 2005, n. 42, recante istituzione del sistema pubblico di connettività e la rete internazionale della pubblica amministrazione, a norma dell'articolo 10 della legge 23 luglio 2003, n. 229;
- decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale
- decreto legislativo 4 aprile 2006, n. 159 recante disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82
- delibera n. 13 del 1° marzo 2007 del Garante recante le linee guida per posta elettronica e internet
- direttiva 02/09 del 26/05/2009 del Ministro Renato Brunetta

Per raggiungere gli obiettivi precedentemente elencati, è necessario istituire una serie di norme comportamentali a livello aziendale con lo scopo di sviluppare procedure e tecnologie atte al miglioramento dell'attenzione nei confronti della sicurezza ICT (Information and Communication Technology). Questi interventi devono tener conto dell'esigenza di una stretta collaborazione tra Servizio di Ingegneria di Supporto all'Informatica e gli operatori al fine di gestire in modo cooperativo e condiviso la sicurezza ICT e di evitare che la vulnerabilità di un anello della catena possa compromettere tutta l'infrastruttura.

A tale proposito vale la pena sottolineare che l'obiettivo finale di questo documento è quello di promuove azioni volte a gestire correttamente le informazioni di carattere pubblico ed a salvaguardare i diritti della personalità nel mondo virtuale.

La citata Direttiva del 16 gennaio 2002 dal titolo "Sicurezza informatica e delle telecomunicazioni" è stato il primo atto normativo che ha delineato un insieme coerente di interventi per attuare un livello minimo di sicurezza ICT nel settore pubblico.

L'adeguamento alla direttiva concerne soprattutto aspetti organizzativi. Infatti, un modello organizzativo coerente alla Direttiva citata, in molti casi richiede la formazione di personale specializzato e la definizione di nuovi ruoli nell'assetto organizzativo.

È quindi necessario predisporre dei piani di formazione e di informazione rivolti a tutte le fasce di impiegati, oltre che alle figure dirigenziali che devono approvare scelte e investimenti concernenti la gestione della sicurezza ICT. In particolare tutto il personale dell'Azienda deve essere consapevole, in misura adeguata alle mansioni svolte, dei rischi che comporta l'uso delle tecnologie ICT e deve essere dotato di un codice scritto che indichi i comportamenti corretti da adottare e le attività da svolgere in caso di mal funzionamento o guasto. Per le attività di formazione è auspicabile che venga mantenuto attivo permanentemente un apposito gruppo all'interno dell'Azienda, che eroghi con regolarità sia i corsi base sia i corsi di aggiornamento.

La società dell'informazione non conosce confini; proprio per questo motivo e per proteggerla da diverse tipologie di attacchi, deve essere prevista una struttura di difesa che operi anche a livello centrale.

La sempre maggiore disponibilità di servizi in rete fa accrescere il livello di rischi informatici. Va poi tenuto presente che la presenza crescente di tali rischi, causa la perdita di fiducia dei cittadini nei servizi elettronici ed in particolare in quelli pubblici: in ultima analisi potrebbe determinarsi un "rifiuto" dei processi innovativi su cui si fonda lo sviluppo della società dell'informazione. Pertanto, l'assenza di adeguati livelli di sicurezza nei sistemi può comportare l'insuccesso dei progetti con conseguenze negative in termini di sviluppo.

Inoltre, in sistemi totalmente interconnessi, quali sono le attuali strutture informatiche, è necessario che ciascun elemento del sistema abbia un adeguato livello di sicurezza, comprese le postazioni di lavoro degli utenti finali. Un difetto di sicurezza in un personal computer di un utente può infatti essere fonte di problemi per i sistemi ad esso collegati e propagarsi in modo incontrollato nelle strutture informatiche dell'Azienda.

La divulgazione della conoscenza dei rischi e delle relative precauzioni per evitarli, definita come "cultura della sicurezza", è un elemento essenziale dello sviluppo dei servizi ICT. Infatti, rispetto al passato, è cambiato il concetto stesso di sicurezza che non è più una responsabilità dei Servizi Informatici ma coinvolge significativamente anche gli utenti finali. Man mano che i servizi diventano più complessi e pervasivi, man mano che le strutture informatiche surrogano quelle tradizionali, diventa sempre più importante che tutti i soggetti interessati adoperino le nuove tecniche con la stessa familiarità e cura con cui utilizzano gli strumenti tradizionali.

È bene sottolineare che quando si parla di "cultura della sicurezza" non si intende solo la coscienza del fatto che esistono problemi di sicurezza ma anche il possesso delle nozioni che consentono di prevenire, affrontare e risolvere questi problemi. Naturalmente queste nozioni dipendono dai

contesti e dal ruolo delle parti interessate, ma in ogni caso, il bagaglio di conoscenze necessario per interagire con sistemi informatici deve comprendere i concetti essenziali della sicurezza.

Per raggiungere questo obiettivo, è necessaria una capillare azione di sensibilizzazione e responsabilizzazione.

Internet gioca un ruolo fondamentale nello sviluppo dei servizi, per le caratteristiche di capillarità della rete ed il suo basso costo. Per contro l'utilizzo di Internet comporta diversi problemi di sicurezza e, soprattutto, comporta la necessità di associare credenziali affidabili ai soggetti che ne sfruttano i servizi.

L'Azienda deve adeguare i processi alla strategia definita dal presente documento, in modo da assicurare un livello di sicurezza commisurato all'importanza dei servizi resi agli utenti.

È necessario garantire la riservatezza, l'integrità e la disponibilità dei dati presenti nel sistema informativo aziendale. Si devono quindi adottare adeguate misure tecnologiche e organizzative affinché:

- i dati riservati trattati siano protetti nei riguardi di ogni tipo di accesso e di consultazione illeciti. In questi casi, deve essere possibile risalire con certezza all'autore degli stessi;
- tutti i dati trattati siano protetti da modifiche non autorizzate. Nel caso in cui comunque questo evento dovesse verificarsi, è necessario che siano state prese misure preventive atte a ripristinare il dato al suo valore corretto, ed individuare inequivocabilmente l'autore delle modifiche;
- i dati siano disponibili a chi ne ha la facoltà di consultarli, con un livello di disponibilità non inferiore a quanto concordato con i rispettivi responsabili. In caso di guasti o malfunzionamenti devono essere messe in atto tutte le contromisure per garantire il ripristino tempestivo degli stessi.

Spesso il software è la principale fonte di incidenti informatici, che possono essere causati da errori involontari commessi in fase di programmazione o da "malware" come trojan horse o da altri programmi illeciti inseriti dolosamente.

Un programma illecito può consentire l'effettuazione di attacchi informatici che vanno dalla violazione della riservatezza e/o integrità dei dati sino al blocco del sistema.

Internet è una fonte incomparabile di informazione ed un potente mezzo di comunicazione. In questo senso ne va incoraggiato l'uso.

Per contro va evitato che i dipendenti dell'Azienda usino la rete per la diffusione di informazioni riservate, oppure dedichino il loro tempo lavorativo ad attività non attinenti alle loro mansioni, o addirittura ad attività penalmente illecite.

Non bisogna poi dimenticare che Internet può essere la sorgente più importante, dal punto di vista statistico, di attacchi remoti o della diffusione di virus che possono compromettere il corretto funzionamento dell'intero sistema.

Per far fronte a questi problemi, nella predisposizione e messa in opera di servizi di rete, è necessario tenere fermi i seguenti obiettivi:

- tutti i dipendenti dell'amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro secondo le direttive di seguito espresse, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato (file di log). Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet evitando eventi dannosi anche al fine di non ledere l'immagine dell'Azienda;
- vanno messe in atto tutte le necessarie precauzioni al fine di evitare che intrusi possano intromettersi nel sistema informatico o che attraverso Internet possano essere introdotti virus o altre forme di codice maligno. Deve anche essere richiamata l'attenzione dei dipendenti sulle possibili conseguenze dell'abbandono della propria postazione informatica, lasciando incautamente inserita la propria password;
- inoltre devono essere realizzate tutte le infrastrutture necessarie per far fronte all'evenienza di un attacco informatico di qualunque forma. E' quindi assolutamente necessario proteggere da possibili danneggiamenti o intrusioni tutte le risorse coinvolte ed adottare tutte le misure necessarie per poter consentire, oltre che il ripristino del sistema, anche l'individuazione dell'attaccante.

## Attività svolte a livello centrale

L'uscita verso la rete internet di tutti i collegamenti aziendali, è concentrata in un unico nodo principale. Questo punto, chiamato tecnicamente "centro stella", raccoglie tutte le apparecchiature hardware ed i sistemi di tracciamento atti a verificare la correttezza dei collegamenti secondo i principi espressi in premessa.

Il governo di un'infrastruttura complessa ed articolata come quella in oggetto per soddisfare le esigenze precedentemente espresse nonché l'adeguamento della rete alle norme in materia di trattamento dei dati personali, rende necessaria l'implementazione di una piattaforma di tipo "**protocollo AAA**". **È** un protocollo che realizza le tre funzioni di autenticazione (*authentication*), controllo degli accessi (*authorization*) e tracciamento del consumo delle risorse da parte degli utenti (*accounting*). L'espressione "*protocollo AAA"* non si riferisce dunque a *un particolare* protocollo ma a una famiglia di protocolli che offrono, anche in modi diversi, i servizi di autenticazione (***authentication***), controllo degli accessi (***authorization***) e tracciamento delle attività degli utenti relative all'infrastruttura ed ai servizi da essa veicolati (***accounting***). Tale infrastruttura, inoltre, fornisce all'Azienda diritti e strumenti di "*provisioning*" estese a tutte le risorse esistenti, ovvero utenti, PDL (Postazioni Di Lavoro), stampanti, servizi di rete, servizi applicativi, etc.

Lo strumento tecnologico adottato per la realizzazione dell'infrastruttura è l'implementazione del dominio di **Active Directory** basato su tecnologia Microsoft Windows 2003 Server.

Consistente in n. 4 server DC Active Directory presenti al centro stella di S. Maria La Grande + n. 2 server DC presenti al Poliambulatorio di Librino.

**Il Dominio presente è di tipo a struttura centralizzata** e dotato di un elevato livello di ridondanza delle componenti critiche. Tale soluzione ci ha consentito di ridurre i costi relativi all'acquisizione dell'hardware, all'implementazione della soluzione ed al suo controllo.

Tramite gli strumenti di amministrazione di Windows, si e' proceduto alla definizione ed applicazione delle *policy* di sicurezza all'interno del dominio ASPCT, relativamente ai privilegi operativi dell'utenza e alla gestione della configurazione delle postazioni di lavoro, integrandole con tutti gli aspetti di gestione della sicurezza aziendale.

L'attivazione e la gestione delle *policy* di domino *Active Directory*, ci permette di definire dei criteri di profilazione operativa di utenti e risorse e rende possibile tracciare, controllare e gestire l'intero ciclo di vita aziendale delle risorse secondo criteri conformi alle normative di riferimento.

L'utenza della rete ASPCT accede oggi ai servizi internet tramite un accesso centralizzato disponibile presso il centro stella di via S. Maria La Grande a Catania, attualmente quindi:

- Tutti gli utenti ASPCT possono accedere ad internet, se **autorizzati**, in modalità centralizzata tramite il centro stella;
- Il servizio di accesso **profila i diritti** di accesso verso internet del singolo utente o del gruppo di utenti ASPCT;

- Tutte le attività svolte dallo stesso, sono poste sotto ***log*** secondo legge, affinché su eventuale richiesta degli organi competenti, possa essere documentata l'attività del singolo utente per periodo temporale, per tipologia di servizio, o per destinazione internet raggiunta;
- L'accesso ad internet, oltre ad essere regolamentato, si può definire "**sicuro"** ovvero è stato **filtrato il traffico in ingresso** ed in uscita al fine di:
    - Impedire l'accesso a siti internet i cui contenuti non sono direttamente assimilabili all'attività istituzionale
    - Impedire il download o l'upload di contenuti non istituzionali;
    - Effettuare il filtraggio di contenuti potenzialmente pericolosi, es. Virus, spyware, malware, adware, etc;

Nel centro stella sono presenti 2 firewall in modalità ridondata, che attualmente controllano gli accessi da e verso internet.

Attraverso le stesse macchine è stata realizzata la possibilità di accesso dall'esterno alla rete aziendale, tramite VPN (rete privata virtuale) di tipo SSL, ovvero con crittografia elevata.

In particolare è stato implementato un servizio sui firewall di "content-filtering" verso internet, cioè il filtro dei contenuti che passano per la rete.

Questa modalità di filtro permette di "fermare" solo i contenuti e non i siti inteso come url. Questa soluzione permette di definire degli ambiti di contenuti di siti, potenzialmente pericolosi dal punto di vista della sicurezza (come siti di malware,ecc.), e per la particolare tipologia di ASP CT, dove le sedi sono dislocate sul territorio provinciale e sono collegate con il centro stella tramite HDSL, si e' reso necessario il filtraggio di siti con contenuti multimediale, al fine di limitare l'utilizzo di banda sulle varie sedi.

Di seguito si elencano le categorie di siti attualmente non permessi verso internet:

**Potenziali Consumatori di Banda**

- Condivisione File Peer-to-Peer
- Download Multimediali
- Radio e TV via Internet

**Potenziali violazioni alla sicurezza**

- Malware

- Spyware

**Potenzialmente Non Produttivi**

- Giochi

**Potenzialmente a Rischio**

- By-pass Proxy
- Phishing

**Controversi**

- Materiale per Adulti
- Scommesse
- Gruppi Estremisti
- Pornografia

Sulle singole macchine (PC) è inoltre installato un software antivirus, che è controllato centralmente da un server posto al Poliambulatorio di Librino. Purtroppo non sempre è possibile tale installazione a causa della vetustà della macchina

## Comportamenti e regole a cui bisogna attenersi

- *Chiudere a chiave cassetti ed uffici*

  *Per evitare che persone non autorizzate accedano ai dati, il primo livello di protezione è sicuramente quello fisico, ed un cassetto od una porta chiusi a chiave sono sicuramente ostacoli non banali per chi vuole accedere a dei dati. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e leggere i documenti posti su una scrivania o visibili su uno schermo. Si richiede pertanto, ove necessario, di chiudere a chiave cassetti e uffici in caso di assenza prolungata e prima di lasciare il posto di lavoro a fine giornata e per la pausa pranzo.*

- *Conservare supporti di memoria e stampe in luoghi sicuri.*

  *Alla conservazione dei supporti di memoria (DVD, CD, dischetti, etc.) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. Come il*

*personale ha l'accortezza di non lasciare importanti documenti alla portata di sguardi indiscreti, così deve comportarsi con dischetti e stampe contenenti dati riservati. Il personale deve riporre tali supporti sotto chiave non appena terminato il loro utilizzo.*

- *Stampe di documenti riservati*

  *Per stampe riservate deve essere evitato l'utilizzo di periferiche di rete, in quanto le informazioni potrebbero essere intercettate da altre persone si fisicamente che per mezzo di appositi programmi; se è indispensabile l'utilizzo di tali periferiche, usare almeno la modalità di stampa ritardata impostando un tempo sufficiente per raggiungere la stampante prima che inizi il suo lavoro. Le stampe devono essere ritirate appena prodotte e non devono essere lasciate sulle stampanti, soprattutto su quelle di rete.*

- *Non gettare nel cestino stampe di documenti che possono contenere informazioni confidenziali.*

  *Se si trattano dati di particolare riservatezza, si consideri la possibilità di dotarsi di una macchina distruggi-documenti (shredder) per l'eliminazione di stampe non più necessarie. In particolare è possibile che l'utente effettui varie copie di stampe prima di ottenerne una che lo soddisfi: soprattutto se il documento contiene dati riservati, distruggere personalmente le copie non utilizzate. In ogni caso non gettare mai documenti cartacei senza averli prima fatti a pezzi.*

- *Non lasciare lavori incompiuti sullo schermo.*

  *Si deve avere l'accortezza di non lasciare lavori incompiuti sullo schermo e chiudere le applicazioni quando si lascia il posto di lavoro; l'assenza potrebbe essere maggiore del previsto e bisogna considerare che un documento presente sullo schermo ha la caratteristica di attirare la curiosità delle persone.*

- *Spegnere il computer se ci si assenta per un periodo di tempo lungo.*

  *Lasciare un computer acceso non crea problemi al suo funzionamento e velocizza il successivo accesso. Tuttavia, un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza, maggiore è la probabilità che nel frattempo avvenga un'interruzione dell'energia elettrica che possa portare un danno all'elaboratore, alla sua configurazione o al documento stesso.*

- *Proteggere attentamente i dati.*

  *Bisogna prestare particolare attenzione ai dati importanti, di cui si è comunque personalmente responsabili. Poiché può risultare difficile distinguere tra dati normali e dati importanti, è buona norma trattare tutti i dati come se fossero importanti. Come minimo proteggerli con password e non dare a nessun altro utente il permesso di accesso (lettura o modifica).*

- *Manutenzione Hardware e Software*

  *In questa Azienda è stato installato un Dominio Active Directory che permette di gestire le credenziali degli utenti che si autenticano sulla rete. Ove possibile, tutti i PC sono stati dotati di una installazione di base che comprende vari software. Non è permesso modificare o rimuovere queste installazioni. Nel caso in cui sia necessaria la modifica di questo ambiente, tale intervento deve essere richiesto al Servizio Ingegneria Informatica ed eseguito solo dopo autorizzazione scritta.*

- *Impostare il salvaschermo*

  *E' importante impostare il salvaschermo con richiesta di password per poter riprendere il controllo della postazione; in tal modo se ci si assenta per alcuni minuti dal proprio posto di lavoro, il PC diviene inutilizzabile.*

- *Abilitare l'accesso tramite password, ove possibile.*

  *Gli applicativi come WORD ed EXCEL permettono di proteggere i propri dati tramite password. Imparare a utilizzare queste caratteristiche che offrono un buon livello di riservatezza.*

- *Cambio delle password e loro scelta*

  *Cambiare periodicamente le proprie password di accesso, anche nelle applicazioni dove non si è obbligati a farlo. Tutte le password devono essere scelte in modo tale da essere difficili da indovinare; evitare le solite date di nascita, numeri di telefono, nomi di familiari o del cane, etc.. E' sconsigliabile anche l'utilizzo di parole che sono contenute nei dizionari (italiano, inglese, etc.) in quanto con alcuni programmi è possibile "provare" tutte le password e, quelle contenute in dizionari, sono le prime ad essere tentate. In generale è preferibile una password non "debole", composta da una sigla non banale di almeno 8 caratteri, che comprenda lettere, numeri e simboli di interpunzione. Per evitare di scrivere la*

*password in giro e per evitare di essere troppo banali, è possibile ad esempio scegliere una frase, anche complessa ma che sicuramente non si dimentica e che contenga anche numeri, e poi utilizzare solo alcuni caratteri come, ad esempio, le lettere iniziali delle parole. Non utilizzare la stessa password per sistemi o programmi differenti, o password già utilizzate in precedenza in quanto, se viene scoperta una password di un'area, è facile che venga tentato il suo utilizzo per accedere anche ad altre aree e a distanza di tempo.*

- *Custodia delle password di accesso*

  *Anche se le password digitate non vengono solitamente ripetute in chiaro a video, quando se ne digita una, questa può essere carpita da altri guardando i tasti che vengono premuti; quindi l'inserimento di una password deve essere necessariamente fatto lontano da occhi indiscreti. Se le password di accesso impostate vengono scritte su fogli tenuti in evidenza o, ancor peggio, su parti del computer (ad es. il monitor), tutti gli sforzi fatti per proteggere i dati non servono a nulla. Anche i sistemi più avanzati di protezione non sono attualmente in grado di offrire rimedio alla sbadataggine di lasciare incustodita la propria password o la propria stazione di lavoro.*

- *Account di accesso*

  *L'accesso ai Server o in generale al dominio, come quello di ogni programma critico, richiede di identificarsi a mezzo di un nome utente ed una password. Le operazioni vengono registrate (file di LOG) tenendo traccia dell'utente che le ha eseguite e quindi in base all'account utilizzato. Ogni utente deve avere l'accortezza di non permettere ad altri di utilizzare le proprie chiavi di accesso, anche per non rendersi responsabile di operazioni non eseguite personalmente. Nel caso si stia utilizzando una stazione di lavoro e si intenda passare a lavorare su una differente, l'utente è tenuto a chiudere le applicazioni e le sessioni di lavoro aperte sul suo computer ed autenticarsi sull'altro sempre con le proprie credenziali. A tal fine è stata disabilitata, ove possibile, la funzionalità che permetta di utilizzare le stesse chiavi di accesso da più di un computer alla volta.*

- *Avvio dei computer, impostazioni di BIOS*

  *Ove possibile, sulle macchine (PC) è stata installata una password di BIOS a livello di amministratore. In questo caso le impostazioni prevedono l'avvio del computer da CD/DVD e successivamente da HD. Negli altri casi assicurarsi di non far partire accidentalmente il*

*computer da dischetto o CD e, se possibile, impostare il BIOS in modo da avere come "primary boot device" il disco rigido di avvio e proteggere l'accesso al BIOS tramite password. Infatti se il dischetto o il CD fossero infetti, il virus potrebbe trasferirsi nella memoria RAM ed infettare altri file. Impostando la partenza dal disco rigido si evitano anche errori o dimenticanze accidentali.*

- *Uso di computer ed account per personale esterno.*

  *La consultazione dei sistemi da parte di personale esterno in generale non deve essere permessa. Nel caso che personale esterno debba installare del nuovo software o hardware (schede o apparecchiature) sulla postazione di lavoro di un utente, l'operazione deve essere permessa solo in presenza dello stesso utente.*

- *Condivisioni*

  *Al fine di limitare la diffusione di virus, furti e danneggiamenti di documenti, problemi di funzionamento delle stazioni di lavoro, è fatto espressamente divieto di condividere il disco fisso del proprio computer o anche solo parte di esso. Nel caso vi siano delle esigenze di condividere documenti e/o dati, deve essere fatto presente al Responsabile che, con l'Amministratore di sistema, provvederà ad analizzare il problema e, qualora possibile e consentito dalle normative vigenti, verrà creata una apposita area di scambio con le opportune protezioni.*

- *Accesso remoto sulla macchina (PC) per teleassistenza*

  *Per ottimizzare i tempi di intervento e ridurre i relativi costi, è possibile che il Servizio di Ingegneria Informatica richieda all'utente il permesso di accedere al PC. Solo dopo avere ottenuto dall'utente l'autorizzazione, il personale del Servizio Ingegneria Informatica potrà connettersi in teleassistenza per svolgere le attività che il caso richiede.*

- *Usare il salvataggio automatico dei dati. Non dimenticare i salvataggi volontari*

  *Molti programmi applicativi, WORD ed EXCEL, consentono di salvare automaticamente il lavoro a intervalli fissi di tempo, in modo da minimizzare il rischio di perdita di dati in caso di guasti, mancanze di corrente, errori di programma. L'utente deve verificare se tale funzionalità sia possibile sui programmi utilizzati e, nel caso, verificare che sia attiva; comunque salvare manualmente il proprio lavoro frequentemente e prendere l'abitudine di gestire i propri dati senza fare esclusivo affidamento sul sistema.*

- *Effettuare salvataggi dei dati e conservare le copie in un luogo sicuro*

  *Nel caso si presentassero dei mal funzionamenti dell'elaboratore e fosse necessaria una sua nuova installazione o una sua sostituzione, oppure anche la sola sostituzione del suo disco fisso interno, il personale informatico riesce a ripristinare la funzionalità di tutti i programmi autorizzati procedendo con delle nuove installazioni: può accadere che non sia in grado di recuperare i dati e/o documenti che erano presenti prima del guasto, come pure le personalizzazioni effettuate dall'utente. E' fondamentale che ogni utente salvi i propri documenti critici anche su altri supporti fisici (CD, DVD, PenDrive); tali copie dovranno essere tenute chiuse a chiave in armadi possibilmente blindati e ignifughi collocati in un luogo differente rispetto a quello dove risiede l'elaboratore; quest'ultima accortezza è utile soprattutto in caso di incendio: più le copie di sicurezza sono distanti dall'elaboratore e meno è probabile che vengano distrutte con esso.*

- *Non riutilizzare dischetti per affidare dati a terzi*

  *L'utente deve avere l'accortezza di non far circolare dischetti che siano stati precedentemente utilizzati per contenere dati o documenti importanti, o anche solo delle loro copie di sicurezza, in quanto i vecchi dati, anche se i file sono stati cancellati dal dischetto, spesso possono essere letti a mezzo di appositi programmi di utilità. Neanche la formattazione assicura l'eliminazione dei dati dai dischi e, nel dubbio, è sempre meglio usare un dischetto nuovo.*

- *Utilizzo di Modem*

  *Il loro utilizzo è vietato qualunque sia il loro impiego in quanto, con tali apparecchi, si crea un punto di accesso non controllato e aperto al mondo esterno, che può rendere maggiormente vulnerabile non solo le postazioni di lavoro su cui sono collegate, ma l'intera rete. Nel caso fossero necessarie connessioni con l'esterno, si devono richiedere le necessarie abilitazioni. L'installazione di modem, ove indispensabile, deve essere eseguita a cura del personale tecnico, ed esclusivamente a seguito di autorizzazione espressamente approvata per iscritto dal Servizio Ingegneria Informatica, previa autorizzazione del Responsabile del Servizio Ingegneria Informatica che certifichi l'impossibilità di raggiungere i medesimi obiettivi in modi maggiormente sicuri. In caso venisse autorizzato l'utilizzo di modem, l'elaboratore deve essere comunque disconnesso dalla rete locale durante tutto il periodo di attivazione del modem, si deve controllare di avere l'installazione locale di un antivirus ag-*

*giornato, nonché installare un Personal Firewall con configurazione molto restrittiva definita dal Responsabile del Servizio Ingegneria Informatica: in ogni caso l'utente diventa responsabile di eventuali danni che possano derivare al sistema ed alla rete a causa dell'utilizzo del modem.*

- *Utilizzo di access point wireless*

  *Il loro utilizzo è generalmente vietato e autorizzabile solo in presenza di un adeguato livello di crittografia (chiave WEP). Con tali apparecchi, si può creare un punto di accesso non controllato e aperto al mondo esterno, che può rendere maggiormente vulnerabile non solo le postazioni di lavoro su cui sono collegate, ma l'intera rete. L'installazione, ove indispensabile, deve essere eseguita a cura del personale tecnico, ed esclusivamente a seguito di autorizzazione espressamente approvata per iscritto dal Servizio Ingegneria Informatica, previa autorizzazione del Responsabile del Servizio Ingegneria Informatica che certifichi l'impossibilità di raggiungere i medesimi obiettivi in modi maggiormente sicuri.*

- *Altre apparecchiature*

  *E' fatto divieto agli utenti di collegare, o permettere ad altri di farlo, qualsiasi tipo di apparecchiatura sulle porte seriali, parallele, USB, etc. di qualsiasi elaboratore o apparato di rete. E' permessa l'installazione solo dei kit per la firma digitale e di stampanti purché non siano collegate, in alcun modo, a linee telefoniche (ad es: stampanti multifunzioni, fax).*

- *Virus informatici*

  *Su ogni personal è utile l'installazione di un programma antivirus che deve comunque essere tenuto aggiornato. E' tuttavia compito dell'utente accertarsi che tale programma venga eseguito correttamente, che non siano prodotti messaggi di mal funzionamenti o di presenze di virus informatici, oltre ad accertarsi che avvengano realmente gli aggiornamenti e che il programma sia "attivo" per il controllo del sistema. Nel caso si vogliano modificare le configurazioni del software antivirus è necessario prima contattare il personale tecnico. Gli utenti sono invitati a lanciare periodicamente dei controlli su tutto il disco locale del proprio computer. Nel caso si riscontrino delle anomalie o dei virus, deve essere contattato il personale informatico per le opportune verifiche. Si ricordi che la prevenzione dalle infezioni da virus su un computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus. Inoltre, se non si hanno adeguate misure antivirus, si potrebbe incorrere in una perdita irreparabile di dati o in un blocco anche molto*

*prolungato della postazione di lavoro. Si raccomanda di proteggere, quando possibile, i dischetti da scrittura prima di leggerli da altri computer (a mezzo dell'apposita linguetta del dischetto); è uno dei mezzi di prevenzione che riduce i rischi di danneggiare i documenti, infatti i virus non possono rimuovere la protezione meccanica.*

- *Fonti di dati, uso di internet*

  *Gli utenti devono utilizzare i computer in dotazione per assolvere il proprio lavoro e devono pertanto utilizzarli per accedere ad informazioni inerenti le proprie mansioni. Non si devono quindi copiare o "scaricare" programmi, file musicali, immagini con contenuti pornografici, etc. dalla rete internet o da altre fonti. Non si debbono visitare siti illegali (ad esempio depositi di software pirata) che sono spesso usati come "specchietto per le allodole" per attirare visitatori su cui condurre attacchi informatici.*

- *Posta elettronica, diffidare di dati, programmi, messaggi*

  *Gli utenti non devono aderire, con la posta elettronica, a "catene di Sant'Antonio" nelle loro varie forme e versioni; solitamente dietro a messaggi di protesta, commoventi o contenenti promesse di premi, si nascondono società specializzate nella raccolta di indirizzi e-mail che poi provvedono a distribuirli per scopi pubblicitari . Iniziano quindi ad arrivare migliaia di messaggi di posta elettronica da fonti spesso non rintracciabili, che possono mettere in crisi i server e comunque generano inutile traffico di dati che abbassa le prestazioni della rete. I virus informatici più diffusi negli ultimi tempi, si diffondono a mezzo della posta elettronica; una volta che un virus ha infettato un computer, spesso si diffonde automaticamente verso tutti gli indirizzi contenuti nella rubrica e/o tutti i PC dell'intera rete aziendale. È pertanto necessario prestare attenzione ai messaggi ricevuti anche se sembrano provenire da persone conosciute. Non aprire gli allegati se non attesi, soprattutto se si tratta di programmi eseguibili e, in ogni caso, controllarli con antivirus aggiornati.*

- *Dati e programmi provenienti dall'esterno:*

  *Come per la posta elettronica, è buona norma diffidare di tutti i dati e programmi che si ricevono, anche se la fonte appare affidabile o il contenuto molto interessante; si applicano quindi le stesse precauzioni.*

- *Provenienza dei computer e linee telefoniche:*

  *Possono essere utilizzati solo computer da tavolo e portatili di proprietà dell'Azienda o avere autorizzazione del Dirigente; possono essere collegati alla rete locale solo i computer che sono stati opportunamente configurati dal personale informatico aziendale e, per tutto il tempo in cui sono connessi alla rete locale, devono essere utilizzati esclusivamente da dipendenti e non essere in alcun modo collegati alla linea telefonica.*

- *Utilizzo di computer portatili:*

  *I PC portatili sono un facile bersaglio per i ladri quindi, se si ha la necessità di gestire dati riservati su di essi, questi devono essere protetti con almeno le password di BIOS e programmi di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto); deve inoltre essere effettuato periodicamente il salvataggio dei dati.*

- *Uso di altri computer*

  *Il personale NON deve permettere, a persone non dipendenti, il collegamento dei propri computer, anche se portatili, o altri apparati elettronici di qualsiasi natura, sia alle reti fonia/dati che ai computer in dotazione presso questi uffici, nonostante ci sia un motivo apparentemente valido. In tale modo si cercano di limitare i rischi relativi a conflitti di configurazioni ed alle intercettazioni di comunicazione e dati.*

- *Installazioni di nuovi programmi*

  *E' fatto divieto agli utenti di installare qualsiasi tipo di software, in particolar modo giochi e programmi che permettano condivisioni di file (software di condivisione file Peer to Peer tipo Napster, Emule, etc): tutte le installazioni di programmi devono essere effettuate esclusivamente a cura o con l'ausilio del personale tecnico del Servizio di Ingegneria Informatica e comunque richieste ed autorizzate dall'Amministrazione, in quanto le licenze di utilizzo dei programmi devono essere conteggiate e, se necessario, acquistate.*

  *Il personale che dovesse trasgredire tali norme, si assume la responsabilità personalmente per i danni eventualmente arrecati sia per la non osservanza delle regole sul copyright che per i danni provocati sulla rete.*

  *I responsabili delle U.O. sono invitati a mettere in atto ogni misura di vigilanza e di controllo affinché gli operatori osservino le disposizioni sopra impartite allo scopo di evitare, oltre che l'applicazione delle sanzioni previste dalla normativa vigente, l'adozione delle correlate misure disciplinari.*

*Nel raccomandare la puntuale osservanza di quanto contenute nella presente disposizione, si rende noto che da parte del competente Servizio saranno effettuate ispezioni dirette all'accertamento dello stato di regolarità delle installazioni software. Vedi Ordine di Servizio n. 140 del 2008*

- *Correzioni su archivi*

  *Gli utenti sono tenuti a correggere personalmente i dati negli archivi, utilizzando le maschere degli applicativi rilasciati; nel caso questo non sia possibile e sia necessario un intervento di personale informatico, deve essere presentata apposita richiesta recante il problema e l'intervento proposto nei suoi dettagli; l'utente è tenuto a controllare personalmente il tecnico e l'esito del suo intervento.*

- *Stampa di riepiloghi e statistiche*

  *Gli utenti sono tenuti ad utilizzare solo i programmi Aziendali in dotazione, anche per produrre riepiloghi e stampe di qualsiasi natura, in quanto gli stessi sono stati testati. Nel caso si richieda ai tecnici di produrre altre stampe, si è tenuti ad affiancarli, controllandone l'operato.*

- *Non violare le leggi in materia di sicurezza informatica.*

  *Ricordarsi che anche solo un tentativo di ingresso non autorizzato in un sistema costituisce un reato. Se si è interessati a studiare la sicurezza della propria postazione di lavoro o della rete di cui fate parte, chiedere preventivamente l'autorizzazione al Responsabile dell'Ufficio ed eseguire tutte le operazioni affiancati da un tecnico informatico aziendale. Non utilizzate senza autorizzazione software che possa danneggiare la rete, creare problemi o allarmi di sicurezza, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.*

- *Segnalare tempestivamente qualsiasi variazione del comportamento della propria postazione di lavoro*

  *E' importante fare presenti tutti i problemi che si verificano perché possono essere il sintomo di un attacco in corso.*

- *Segnalare comportamenti che possano far pensare a tentativi di ridurre la sicurezza del sistema informativo.*

  *Devono essere segnalate al Responsabile del Servizio di Ingegneria Informatica, ad esempio, le richieste insistenti di altri utenti per avere accesso a postazioni di lavoro, dati o per conoscere password. Analogamente non devono essere presi in considerazione messaggi o telefonate che chiedono di compiere operazioni "strane" sul computer (ad esempio, cambiare subito la password con una data per telefono o nel corpo del messaggio).*

- *Utilizzo di supporto tecnico*

  *Il personale può rivolgersi solo ai supporti tecnici "ufficiali" secondo le modalità indicate nei relativi contratti in essere e quindi non rivolgersi a personale di altre ditte o strutture oltre quelle previste. Il personale è tenuto a non comunicare alcuna informazione relativa a funzionalità e configurazioni della rete o delle postazioni di lavoro. Gli utenti devono controllare le configurazioni che i tecnici effettuano e, nel caso debba essere comunicata una password, questa deve essere cambiata subito dopo l'intervento. Deve essere segnalato qualsiasi dubbio, anche sull'operato del personale tecnico, al Responsabile del Servizio di Ingegneria Informatica.*

- *Non dare informazioni di alcun genere*

  *Spesso, il vero hacker, non attacca il sistema per via informatica, ma utilizza tecniche di "ingegneria sociale", carpendo la fiducia dell'operatore che si trova ad essere il vero punto debole della catena di sicurezza. Non dare mai informazioni di alcun genere, specialmente per telefono, anche a persone apparentemente conosciute. Un hacker utilizza tecniche molto sofisticate per ingannare il malcapitato, simulando situazioni che portano l'operatore a dargli fiducia.*

- *Sicurezza e salute*

  *Il personale deve verificare che le postazioni di lavoro rispettino le normative vigenti, prestando particolare attenzione ai collegamenti elettrici, e segnalare al Rappresentante per la sicurezza qualsiasi dubbio o anomalia riscontrata (vedere anche D.L. 626/94).*

## Conclusioni

In questo quadro complesso e tecnicamente molto elaborato si inserisce la normativa sulla tutela dei dati personali.

L'esigenza di garantire la sicurezza dei sistemi di trattamento delle informazioni è obbligatoria e gli strumenti normativi che progressivamente vengono emessi, saranno necessariamente in stretta sintonia con i progressi tecnologici.

L'uso di sistemi informatici consente di riporre maggiore fiducia nella loro sicurezza e rende più facilmente perseguibili gli autori di eventuali frodi, costituendo quindi un ulteriore elemento di dissuasione.

Di seguito si riporta la disposizione dell'ordine di servizio n. 140 del 2008 attualmente in vigore, che recita:

> *E' fatto divieto agli utenti di installare qualsiasi tipo di software, in particolar modo giochi e programmi che permettano condivisioni di file (software Peer to Peer tipo Napster, Emule, etc).*
>
> *Tutte le installazioni di programmi devono essere effettuate esclusivamente a cura o con l'ausilio del personale tecnico del Servizio di Ingegneria Informatica e comunque autorizzate dall'Amministrazione, in quanto le licenze di utilizzo dei programmi devono essere acquistate e, se necessario, conteggiate.*
>
> *Il personale che dovesse trasgredire tali norme, si assume la responsabilità personalmente per i danni eventualmente arrecati sia per la non osservanza delle regole sul copyright che per i danni eventualmente provocati sulla rete.*
>
> *I responsabili delle U.O. sono invitati a mettere in atto ogni misura di vigilanza e di controllo affinché gli operatori osservino le disposizioni sopra impartite allo scopo di evitare, oltre che l'applicazione delle sanzioni previste dalla normativa vigente, l'adozione delle correlate misure disciplinari.*
>
> *Nel raccomandare la puntuale osservanza di quanto contenuto nella presente disposizione, si rende noto che da parte del competente Servizio saranno effettuate ispezioni dirette all'accertamento dello stato di regolarità delle installazioni software.*
>
> *I Responsabili di tutte le U.O. sono tenuti al controllo dell'attuazione delle disposizioni presenti in questo documento.*

*Eventuali criticità dovranno essere tempestivamente segnalate al Servizio Ingegneria di Supporto all'Informatica.*

## Applicazione del regolamento

Il personale che dovesse trasgredire le regole presenti in ogni parte di questo documento, si assume la responsabilità per i danni eventualmente arrecati all'Azienda.

I responsabili di tutte le U.O. sono tenuti a mettere in atto ogni misura di vigilanza e di controllo dell'attuazione delle disposizioni presenti in questo documento, affinché si osservino le regole descritte, allo scopo di evitare, oltre che l'applicazione delle sanzioni previste dalla normativa vigente, l'adozione delle correlate misure disciplinari.

Si raccomanda a tutti la puntuale osservanza di quanto contenuto nel presente documento.

---