Istruzione privacy	*Codice*
Prescrizioni per gli incaricati del trattamento dati	**IP06**

*Il sottoscritto assicura che il presente documento è copia conforme dell'originale disponibile nella bacheca elettronica della **BTP SPA** alla data di consegna.* *L'eventuale revisione aggiornata è disponibile nell'area riservata di www.btpspa.it.*	*Distribuito a scopo informativo e non soggetto ad aggiornamento:*
Data consegna: / *Destinatario:*	*Distribuito in copia controllata:*

Rev.	Data	Descrizione modifiche	Redatto	Verificato	Approvato
01.01	*15/11/02*	*Revisione ISO 9001:2000*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*
02.01	*11/03/04*	*Adeguamento alla Legge sulla Privacy*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*
02.02	*20/08/05*	*Cambio ragione sociale*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*
03.a	*30/10/06*	*Aggiornamento alle modifiche del SI aziendale con collegamento diretto in alcuni Cantieri. Modifiche alla codifica dei documenti*	*Lilli (UQ)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*
04.a	*30/03/07*	*Aggiornamento in conformità con LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA ED INTERNET*	*Lilli (UQ)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*
04.b	*10/05/07*	*Modifica alla gestione delle cartelle sul Server Aziendale*	*Lilli (UQ)*	*Marullo (Resp. SI)*	*Marullo (Resp. SI)*
05.a	*09/06/07*	*Revisione per Sistema di Gestione Integrato*	*Lilli (UQ)*	*Marullo (Resp. SI)*	*Marullo (RDSGI)*
05.b	*09/12/08*	*Aggiornamento annuale*	*Lilli (UQ)*	*Marullo (Resp. SI)*	*Marullo (RDSGI)*

Indice

1 Oggetto

La presente Istruzione Operativa definisce le prescrizioni alle quali si deve attenere ogni incaricato del trattamento di dati personali e comunque ogni utente dei Sistemi Informatici della BTP SPA.

2 Generalità

L'Ufficio Qualità e Sistemi Informativi ha posto in atto alcuni sistemi per garantire la sicurezza dei Sistemi Informativi.

La scelta aziendale è stata comunque quella di porre poche limitazioni agli utenti per favorire il massimo utilizzo delle potenzialità che la tecnologia pone a disposizione.

Diventa quindi fondamentale la collaborazione degli utenti per mantenere un elevato grado di sicurezza dell'intero sistema informatico (vedi le note successive).

2.1.1 Dati personali

Per individuare eventuali attacchi ai quali è sottoposto il sistema è necessario effettuare periodicamente controlli che hanno lo scopo di individuare situazioni anomale come indicato nella Policy per l'utilizzo delle risorse informatiche[1].

2.1.2 Dati esclusivi

Ad ogni utente sono assegnati una casella di posta elettronica ed un'area di lavoro "esclusive", utilizzabili unicamente dall'utente stesso (ma sempre leggibili dai Sistemi Informativi) ed un PC in genere anch'esso di uso "esclusivo". **Non deve essere confuso l'uso "esclusivo" con la possibilità di uso "personale".**

3 Accesso alla rete locale

La rete locale (aziendale o dei cantieri nei quali è predisposta) offre la possibilità di accesso veloce ad Internet e la possibilità di utilizzare tutte le periferiche (stampanti, plotter, scanner, ecc).

Solo i PC appositamente configurati possono però essere collegati alla rete. In particolare non possono essere connessi alla rete i PC configurati per altri Cantieri o PC personali senza l'autorizzazione dell'Ufficio Qualità e Sistemi Informativi o del Responsabile dei Sistemi Informatici di Cantiere.

4 Continuità del lavoro

Quasi tutti i posti di lavoro sono alimentati tramite dei piccoli gruppi di continuità.

Lo scopo di questi apparati è quello di evitare la perdita del lavoro in corso in caso di interruzione momentanea della alimentazione. Non è scopo di questi gruppi permettere l'attività dell'utente in assenza di alimentazione (la capacità delle batterie di sostituire l'alimentazione è ovviamente molto limitata nel tempo).

In caso di interruzione di alimentazione è quindi necessario che ogni utente provveda immediatamente al salvataggio del proprio lavoro. Il salvataggio del lavoro in corso è inoltre consigliato periodicamente e comunque prima di abbandonare il proprio posto di lavoro per qualunque motivo.

5 Cartelle esclusive e di gruppo

E' opportuno che nessuna informazione sia memorizzata sul disco C della macchina.

Ogni utente ha a disposizione cartelle esclusive nelle quali memorizzare tutti i dati necessari per il proprio lavoro. Sono poi presenti cartelle di gruppo per memorizzare i dati condivisi.

Le cartelle hanno una affidabilità ed un costo aziendale differente in funzione della sicurezza del supporto, della periodicità delle operazioni di copia e della stratificazione dell'archiviazione delle copie.

Le Cartelle sono infatti memorizzate su supporti più o meno "sicuri" (in base all'affidabilità del supporto e del livello di ridondanza applicato).

Ovviamente la sicurezza fisica del supporto non garantisce rispetto ad eventi catastrofici (furti, incendi, ecc.) o da errori operativi (es. cancellazione o modifica errata di un dato); in questo caso è necessario ricorrere alle copie effettuate su supporti "removibili" e conservate in altri luoghi.

Alcune Cartelle vengono copiate automaticamente ogni notte, altre settimanalmente, altre non vengono mai copiate.

Dei supporti su cui sono state effettuate le copie vengono conservate più versioni in modo da poter recuperare anche errori operativi di cui ci si accorge dopo un certo tempo.

Lo spazio di archiviazione viene suddiviso per Livelli Qualitativi che partono da Aree di memorizzazione di alta qualità (molto costose perchè garantiscono al massimo sia la sicurezza del dato che la possibilità di un recupero a fronte di errori operativi anche rilavati dopo molto tempo) fino ad aree di bassa qualità (sulle quali non è garantita la sicurezza del dato a fronte di problemi fisici o operativi). Il livello qualitativamente più basso è la copia del dato su supporti non sempre in linea (es. CD o DVD) che deve essere utilizzato per liberare lo spazio in linea che è comunque limitato (ATTENZIONE: la rileggibilità dei dati da questi supporti non è garantita per tempo indefinito quindi, per dati da conservare per tempi molto lunghi, è opportuno effettuare più copie e verificare periodicamente la leggibilità dei supporti).

Per le aree di maggiore qualità sono state definite delle "quote" per una distribuzione dello spazio disponibile fra i vari utenti e/o uffici.

In generale è necessario che le aree più "costose" siano riservate a informazioni soggette a modifiche frequenti mentre su quelle di qualità inferiore dovranno essere memorizzati i dati che possono essere comunque recuperati in qualche modo (es. CD dei progetti di Gara, Informazioni su Progetti vecchi sulle quali non si lavora da tempo e che quindi sono già presenti in qualche copia di backup, ecc.).

Tutti gli utenti devono prestare attenzione alla corretta gestione della memorizzazione dei dati per evitare di saturare le aree di memorizzazione più costose spostando le informazioni "storiche" fra le aree ma mano che diminuiscono di "importanza" fino a provvedere alla loro cancellazione quando si esaurisce la necessità della disponibilità immediata del dato.

[1] *BTP ha scelto, per adesso, di non bloccare l'accesso a determinati siti per evitare che errori nella catalogazione automatica limitino le possibilità di utilizzo della rete. La responsabilità dell'uso della rete è quindi lasciata al singolo utente.*

Poiché è normale che si tenda ad accumulare dati si consiglia di creare (sia all'interno delle cartelle Esclusive che in quelle di Gruppo) una cartella denominata "Storico" (con sotto tutte le cartelle che si desidera) nella quale memorizzare dati che non subiscono variazioni (es. Documenti ricevuti da conservare, Documenti relativi a Cantieri chiusi, ecc.). Periodicamente sarà possibile effettuare copie su CD per liberare questo spazio pur avendo la disponibilità dei dati di interesse.

5.1 Cartelle sul Server della sede di Calenzano

Ogni utente ha a disposizione una Cartella personale sul Server identificata come unità di rete **V:** (**T:** per gli utenti non appartenenti alla BTP) ed ha accesso all'unità di rete **U:** limitatamente alle cartelle di Gruppo di interesse.

Le informazioni memorizzate su queste unità di rete utilizzano dischi del server ad altissima affidabilità e vengono copiate ogni notte su un dispositivo situato nella Colonica. Settimanalmente sono salvate su cassette per recuperi anche in caso di errori operativi.

Lo spazio totale delle cartelle **U:** e **V:** e dei dispositivi di memorizzazione storica è limitato e quindi ad ogni utente e ad ogni gruppo sono state assegnate delle "quote". Il sistema invierà automaticamente delle segnalazioni per posta al superamento del 90% e del 95% dello spazio autorizzato. Impedirà la memorizzazione dei files in caso di superamento della quota assegnata. In caso di messaggi di posta relativi al superamento dello spazio è fondamentale che l'utente cancelli informazioni non più necessarie o le sposti sull'unità K:.

Ogni utente ha anche a disposizione l'unità di rete **K: (Definita NO BACKUP)** all'interno della quale può gestire le cartelle dei Gruppi di suo interesse e una propria cartella Personale.

Queste cartelle sono memorizzate su supporti fisici con la normale affidabilità ma molto capienti. Anche queste cartelle vengono copiate ogni notte sul dispositivo in Colonica per garantire il recupero delle informazioni (al giorno prima) in caso di rottura del supporto fisico.

Di queste cartelle però non viene effettuata la copia su cassetta e quindi non esistono versioni "storiche".

Lo spazio a disposizione sull'unità di rete **K:** è molto grande e quindi, per adesso, non sono state definite delle quote ma è comunque responsabilità di ogni utente evitare di occuparlo inutilmente.

Ogni informazione soggetta a variazione deve essere memorizzata nelle unità di rete **U:** e **V:** mentre le informazioni statiche (es. copie di disegni di gara) o storiche (relative ad esempio a cantieri chiusi) dovranno essere memorizzate o spostate nell'unità di rete **K:**.

N.B: E' vietato memorizzare files musicali, immagini o video non strettamente legati al lavoro aziendale.

6 Configurazione esclusiva

A fronte di un guasto del PC esclusivo è necessario che ogni utente sia in grado di fornire le informazioni necessarie per permetterne la rapida sostituzione.

In particolare:

- programmi che utilizza;
- eventuali archivi salvati sul disco "C" invece che sulle cartelle del server (es. per i portatili);
- configurazione del proprio Desktop (collegamenti e richiami abituali);
- stampanti collegate;
- configurazione della posta;
- indirizzi memorizzati fra i "preferiti" su internet.

Una volta conclusa la sostituzione sarà responsabilità dell'utente validarla o segnalare problemi direttamente all'Ufficio "Qualità e Sistemi Informativi".

7 Stampanti

Le stampanti utilizzano varie tecnologie; in generale esiste una correlazione inversa fra costo d'acquisto e costo per copia.

Le stampanti legate alle singole postazioni hanno quindi un costo per copia decisamente superiore alle stampanti di area che hanno, in genere, anche una qualità migliore. E' quindi consigliabile utilizzare le stampanti di area qualora si dovessero inviare stampe composte di molte pagine.

In generale la stampa a colori è molto più costosa della stampa in bianco e nero. Quando non è necessario avere una stampa a colori è possibile personalizzare la stampa affinché utilizzi unicamente i livelli di grigio riservando il colore prevalentemente per stampe definitive e riservate all'esterno.

Per le multifunzioni Infotec vengono installati 2 profili della stessa: uno solo BN e uno solo Colore. Queste impostazioni esclusive definite dall'Amministratore di rete rendono più veloce e più efficace la stampa in BN o a Colori da parte dell'utente, riducendo lo spreco di stampe inviate per errore

Ogni utente è configurato per poter stampare su alcune stampanti. Esistono tre tipi di collegamenti possibili:

- collegamento diretto con la stampante collegata al PC;
- collegamento con una stampante collegata alla rete;
- collegamento con una stampante collegata ad un altro PC.

Nell'ultimo caso sarà possibile stampare solo se è acceso il PC al quale è connessa la stampante (anche senza inserire la password dell'utente).

8 Sicurezza da accessi indesiderati

8.1 Password

La password è lo strumento che consente di limitare l'accesso ai dati da parte di persone diverse da quelle espressamente autorizzate. E' quindi indispensabile che sia elemento certo di identificazione per proteggersi contro accessi indesiderati.

E' responsabilità di ogni utente provvedere a modificare la password fornita al momento dell'assegnazione di un PC. La password dovrà quindi essere modificata periodicamente (possibilmente una volta al mese e comunque ogni sei mesi) senza mai riutilizzare le vecchie per evitare che attraverso tentativi possa essere identificata da elementi esterni malintenzionati.

La scelta della password dovrà tener conto che questa non sia troppo facilmente individuabile (non deve contenere riferimenti personali quali data di nascita, luogo di nascita, ecc.) ne troppo difficile da ricordarsi tale da doverla scrivere. La password dovrà essere di almeno 8 caratteri alfanumerici

Sarà responsabilità dell'utente mantenere la massima riservatezza sulla propria password (non andrà comunicata ad altri o scritta in chiaro).

I Sistemi Informativi della BTP sono in grado di annullare la password di tutti gli utenti per poter accedere alle informazioni dell'impresa in caso di assenza dell'utente (il quale si accorgerà della modifica e potrà chiederne spiegazione). E' facoltà di ogni utente comunicare ai Sistemi Informativi il nominativo di un altro utente "fiduciario" al quale, se presente, i Sistemi Informativi dovranno comunicare la nuova password che a sua volta dovrà nuovamente cambiare potendo così accedere in modo "esclusivo" ai dati dell'utente assente.

Solo gli utenti operanti in cantieri non collegati direttamente al server di Calenzano dovranno scrivere la propria password in una busta chiusa che dovrà essere consegnata al Responsabile dei Sistemi Informatici di Cantiere che potrà, in casi di emergenza, utilizzarla analogamente a quanto visto prima e quindi provvederà a comunicalo, appena possibile, all'utente stesso.

8.2 Screen Saver

E' responsabilità di ogni utente non lasciare in alcun modo ed in nessuna occasione incustodito ed accessibile il computer in uso durante una sessione di trattamento dati. A tal fine è necessario utilizzare lo Screen Saver abilitando la richiesta della propria password dopo una inattività di alcuni minuti.

8.3 Riservatezza

L'accesso ai dati da parte di terzi può avvenire solo in caso di prolungata assenza o impedimento che renda indispensabile e indifferibile intervenire sul sistema per esclusive necessità di operatività e di sicurezza. In questo caso l'operazione deve essere concordata con il Responsabile del trattamento dei dati in modo da garantire la massima riservatezza.

In caso di affidamento di documenti contenenti dati riservati o critici, sarà cura dell'utente controllarli e custodirli fino alla restituzione, in modo che ad essi non accedano soggetti privi di autorizzazione, e restituirli al termine delle operazioni affidate.

9 Criteri per la posta elettronica

9.1 Generalità

Data l'importanza dell'e-mail per la normale conduzione del lavoro (consente comunicazioni asincrone e multiple ed inoltre lascia una traccia scritta), è essenziale un corretto utilizzo di questa risorsa, per ridurre eventuali rischi di carattere intenzionale o involontario e per assicurare la corretta gestione delle registrazioni ufficiali.

Inviare una mail da un indirizzo con dominio BTPSPA.IT corrisponde a scrivere sulla carta intestata aziendale. E' quindi proibito un uso a fini privati anche delle caselle con indirizzo nome.cognome@btpspa.it che non devono essere confuse con le caselle personali del tipo nome.cognome@libero.it .

9.2 Organizzazione delle proprie cartelle

E' necessario che ogni utente provveda alla manutenzione periodica delle proprie cartelle di posta per la catalogazione in apposite sottocartelle dei messaggi o la loro cancellazione.

Quando si ELIMINA un messaggio di posta questo viene spostato nella cartella POSTA ELIMINATA. E' necessario svuotare periodicamente la cartella di POSTA ELIMINATA per cancellare fisicamente il messaggio (soprattutto per quelli con grossi allegati) e liberare spazio.

9.3 Regole per la posta (FUORI SEDE)

Il programma di posta consente di definire il testo che si desidera venga inviato in risposta ad ogni messaggio che verrà inviato quando si è FUORI SEDE. Chiunque invierà una e-mail riceverà automaticamente il messaggio che lo informerà della impossibilità di leggere la posta in tempi brevi (nel messaggio "FUORI SEDE" è opportuno indicare la data di rientro prevista) e quindi potrà comportarsi di conseguenza.

Ovviamente la funzione è particolarmente utile per il periodo di ferie o di assenza prolungata.

E' quindi necessario attivarsi in tal senso per evitare che possa arrivare una comunicazione esterna urgente senza che nessuno la possa leggere ed attivarsi di conseguenza.

Per impostare la regola “FUORI SEDE” procedere come segue:

- Entrare in Outlook: Strumenti – Regole Fuori sede
- Selezionare l’opzione “Fuori sede”
- Inserire in “Testo per la risposta automatica ad ogni mittente” il messaggio che verrà inoltrato come risposta ad ogni mail ricevuto. E’ importante che sia specificata la data di rientro in sede.
- Confermare (senza indicare, nella finestra in basso, ulteriori regole).

Dopo aver settato il flag FUORI SEDE, ogni volta che verrà aperta la posta, per evitare di dimenticarsi di eliminare la funzione al rientro, viene posta la domanda: “Fuori Sede attivato: Disattivarlo?”.

9.4 Costo della posta su internet

Anche se il costo della posta su internet è molto basso va tenuto conto che in realtà non è nullo. La posta occupa, infatti, spazio sui server della posta e rappresenta comunque uno spreco di banda di trasmissione o una spesa viva per l'utente Internet con collegamenti "a consumo".

Anche se nel singolo caso queste spese assommano a pochi centesimi di euro, nell'aggregato le somme coinvolte possono essere rilevanti. Va soprattutto tenuto conto che i costi della posta elettronica sono asimmetrici, nel senso che gravano maggiormente sul destinatario che sul mittente.

9.5 Usi impropri della posta su internet

9.5.1 Spam

Sempre più spesso su internet circolano e-mail indesiderate (spam).

E' stato calcolato che le e-mail indesiderate rappresentano il 97% di tutte le e-mail che circolano su internet e solo per i server che la devono gestire viene consumata l'energia elettrica utilizzata da 2,5

milioni di abitazioni con una emissione di CO_2 pari a quella di 3,1 milioni di automobili.

La BTPSPA è dotata di sistemi Antispam che riducono il numero di questi messaggi ma non possono annullarli per non rischiare di eliminare messaggi validi.

Quando si ricevono tali e-mail indesiderate, che oltretutto costituiscono una violazione della privacy ed un reato per la legge italiana, le cose da evitare sono le seguenti:

- non rispondere al messaggio;
- non seguire le istruzioni contenute nel messaggio, anche quando queste indicano come farsi rimuovere dalla lista o, ancora meno, quando danno dei link ipertestuali a siti di qualunque genere.

E' comunque importante evitare di lasciare indirizzi in giro per la rete, soprattutto su siti che non si conoscono.

9.5.2 Gli hoax

Gli hoax (termine inglese che significa "imbroglio", "truffa", "bidone") sono messaggi diffusi in rete col metodo della catena di S. Antonio recanti contenuti falsi riconducibili sostanzialmente a due categorie:

- **falsi allarmi** relativi a virus informatici;
- false **catene di solidarietà** a beneficio di individui bisognosi (nella configurazione tipica si tratta di bambini affetti da gravissime malattie).

Gli hoax sono uno spreco di risorse e di tempo.

In caso di dubbio è necessario inviare il messaggio all'Ufficio Qualità e Sistemi Informativi che provvederà a controllarlo anche utilizzando le apposite liste presenti su internet.

9.5.3 Phishing

PHISHING [termine coniato dalla storpiatura del vocabolo inglese "fishing" (pescare)] è una tecnica fraudolenta che punta ad ottenere i dati personali (codici, password, dati della carta di credito, ecc) convincendo l'utente a fornirli con falsi pretesti.

Un servizio di home banking, e-commerce, ecc. non chiederà mai i codici di accesso, numeri di carta di credito, codici bancomat o password inviando e-mail o lettere o telefonicamente e quindi è necessario NON rispondere a tali richieste di informazioni personali eventualmente pervenute.

Per "non abboccare" non accedere mai al sito di un servizio di home banking, e-commerce, ecc. che chiede di autenticarsi da un link inserito in un messaggio (e-mail, istant messaging,...). Anche se il link nella e-mail o la barra degli indirizzi Web risulta (apparentemente) corretto, esistono delle tecniche per mascherare l'indirizzo fasullo con uno corretto. Entrare nella pagina digitando l'indirizzo direttamente nel browser (Explorer) o comunque controllare sempre l'indirizzo sulla barra.

9.6 Protezione da attacchi esterni

Dalla posta internet giungono ormai i maggiori “attacchi” alle imprese.

L'antivirus che protegge in sistema informatico aziendale provvede a controllare tutti gli allegati ripulendo o eliminando quelli ritenuti sospetti (all'utente arriva come allegato, al posto dell'allegato originale, un messaggio dell'antivirus che segnala la rimozione dell'allegato precedente).

In ogni caso è opportuno:

- non aprire messaggi di posta di cui non si conosce il mittente;
- non aprire messaggi di posta che, pur provenendo da mittenti noti, contengono un oggetto non chiaro, specialmente se in inglese (alcuni virus infatti si propagano utilizzando le agende dei PC infettati per rinviare messaggi infetti).

9.7 Tutela della privacy

Il garante per la privacy ha affermato che gli indirizzi e-mail non sono "pubblici" come possono essere quelli presenti sugli elenchi telefonici.

La vasta conoscibilità degli indirizzi e-mail che Internet consente, non rende lecito l’uso di questi dati personali per scopi diversi da quelli per i quali sono presenti on line. L’eventuale disponibilità in Internet di indirizzi di posta elettronica va "rapportata alle finalità per cui essi sono pubblicati sulla rete".

Per poter inviare e-mail senza violare la privacy degli utenti web è obbligatorio, dunque, ottenere prima il loro consenso.

9.8 Modalità di invio dei messaggi

Un messaggio può essere inviato ad uno o più destinatari indicati nel campo: "A".

Lo stesso messaggio potrà essere inviato sempre ad uno o più destinatari, con significato, "Per conoscenze" usando il campo "Cc".

E' importante usare il campo "A" per indicare l'effettivo destinatario (chi deve prendere decisioni od eseguire le indicazioni presenti nel messaggio) distinguendo attraverso l'apposito campo, i destinatari solo per conoscenza (che non sono tenuti a compiere nessuna azione diretta in relazione al messaggio).

Tutti i proprietari delle caselle postali indicate sia nel campo "A" che nel campo "Cc" vedranno a chi è stata inviato lo stesso messaggio.

Se si desidera è possibile utilizzare il campo "Ccn" (per conoscenza nascosto) che consente di far giungere il messaggio anche ad altre persone senza che nessun altro lo possa sapere.

Il campo "Ccn" viene utilizzato anche per la difesa della privacy in quanto, in questo modo, non si diffondono gli indirizzi quando non è strettamente necessario.

Se un utente che riceve un messaggio preme "Rispondi a tutti" la sua risposta verrà inviata solo agli indirizzi presenti nei campi "A" e "Cc" (escluso il proprio) e non a quelli presenti nel campo "Ccn".

E' importantissimo riempire sempre il campo "Oggetto" oltre che per la comodità di chi riceve il messaggio che avrà maggiore facilità ad archiviarlo ed a ritrovarlo anche per la sicurezza.

Alcuni virus sono in grado di replicarsi rinviando automaticamente posta a tutti gli indirizzi dell'agenda del PC infettato. E' quindi possibile ricevere posta "infetta" anche da persone note. Più difficile è che l'oggetto della posta infetta sia coerente (spesso è in inglese o comunque generico).

10 Criteri per Internet

10.1 Generalità

La quantità di informazioni che possono essere trasmesse tramite il canale di comunicazione con Internet è, ovviamente, limitata. Poiché tramite questo canale "passano" tutte le comunicazioni di posta elettronica, tutti gli accessi diretti ad internet e i collegamenti virtuali con le altre sedi del gruppo è necessario non "sprecare" questo canale di comunicazione per usi non lavorativi (anche dove il collegamento ad Internet avviene tramite abbonamenti a costo fisso).

10.2 Internet come principale canale di infezione da virus

Negli anni passati i virus erano trasmessi prevalentemente tramite dischetti. Oggi internet è uno dei principali canali di contaminazione.

Per nessun motivo gli utenti devono scaricare programmi senza l'autorizzazione dell'Ufficio Qualità e Sistemi Informativi.

A volte viene richiesto di scaricare programmi al fine di poter vedere immagini o scaricare musica. Anche in questo caso è necessario prima consultare l'Ufficio Qualità e Sistemi Informativi.

10.3 Scaricare illegalmente musica o filmati

La FIMI (Federazione dei discografici italiani) ha annunciato una iniziativa verso imprese pubbliche e private sui "rischi connessi all'utilizzo della rete informatica aziendale per scaricare e distribuire file musicali in termini di sicurezza, spreco di risorse tecnologiche e forza lavoro" avvertendo che vi sono server aziendali trasformati in veri e propri jukebox di file illegali e ciò espone le imprese e i propri responsabili a serie conseguenze legali.

E' opportuno non esporre l'azienda a potenziali rischi legali evitando di installare programmi peer-to-peer che, oltretutto, utilizzano pesantemente la banda internet aziendale.

10.4 Accessi alternativi ad internet

E' proibito a tutti gli utenti collegati ad una rete locale connettersi ad internet con modalità differenti da quelle previste (ad esempio con i modem presenti sui portatili) per evitare che, inconsapevolmente, si aprono falle nel sistema di sicurezza evitando i controlli previsti.

11 Criteri per i dati

11.1 Classificazione delle informazioni

Le informazioni possono essere classificate, in funzione del D.Lgs. 196/03 "Codice in materia di protezione dei dati personali", come:

- **Dati personali** - Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
- **Dati identificativi** - I dati personali che permettono l'identificazione diretta dell'interessato;
- **Dati sensibili** - Sono 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.

Il D.Lgs. 196/03 "Codice in materia di protezione dei dati personali" prescrive che sia ridotta al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

In generale, il trattamento di dati personali, è ammesso solo con il consenso espresso dell'interessato che deve essere scritto per quelli sensibili; in ogni caso i dati idonei a rivelare lo stato di salute non possono essere diffusi.

In funzione dell'utilità per l'impresa i dati possono essere suddivisi in:

Importanti - Sono le informazioni che vanno protette da eliminazioni o modifiche non autorizzate, garantendone disponibilità e integrità.

Riservati – Sono i dati destinati a essere rigorosamente utilizzati solo all'interno dell'impresa o di un ufficio. Per questa categoria di informazioni il danno maggiore potrebbe derivare da una loro divulgazione non autorizzata (fra questi rientrano i dati personali per le possibili conseguenze legali).

Dati generici - In generale, sono informazioni la cui divulgazione o perdita non avrebbe conseguenze.

11.2 Responsabilità

Sarà responsabilità di ogni utente informare tempestivamente l'Ufficio Qualità e Sistemi Informativi in caso di gestione di nuove informazioni. Senza preventiva autorizzazione del Responsabile, non è possibile creare nuove ed autonome banche dati.

11.3 Memorizzazione delle informazioni

Tutte le informazioni devono essere memorizzate nelle apposite cartelle personali o di gruppo e che sono sottoposte ad opportune modalità di copie di sicurezza.

Qualora l'utente si trovi nelle condizioni di dover memorizzare informazioni che richiedono di essere protette in modo particolare perché potrebbero essere oggetto di "attacco dall'esterno" o perché una loro diffusione non autorizzata potrebbe portare a ripercussioni legali dovrà avvisare l'Ufficio Qualità e Sistemi Informativi.

11.4 Uso di strumenti di memorizzazione removibili

E' proibito utilizzare Floppy Disk o MicroDriver USB di cui non si conosce con sicurezza l'origine. Attraverso i Floppy Disk passava il maggior numero di "infezioni" prima della diffusione di internet. In caso di necessità è possibile richiedere all'Ufficio Qualità e Sistemi Informativi di recuperare files contenuti in floppy o su MicroDriver USB non sicuri.

11.5 Conservazione ed Eliminazione dei supporti removibili

Se i supporti contengono dati Riservati è cura di chi li produce provvedere alla loro conservazione adottando misure idonee ad evitare la loro divulgazione. Analoga cura dovrà essere posta alla loro distruzione o alla cancellazione dei dati una volta cessato il motivo della duplicazione.

Qualora i supporti siano consegnati ad altro personale interno all'impresa sarà responsabilità di chi consegna i dati concordare con il destinatario le modalità di trattamento e di distruzione dei dati.

La consegna di dati riservati a personale esterno all'impresa è permesso solo dopo aver concordato le modalità con il Responsabile del trattamento dei dati e comunque previo impegno scritto da parte del destinatario sulle modalità di trattamento dei dati stessi.

11.6 Copie di dati Riservati

11.6.1 Responsabilità

La copia di dati Riservati su cartelle diverse da quelle originali o su supporti removibili (FD, CD, MicroDriver USB, ecc.) o l'invio degli stessi dati tramite posta elettronica o lo scambio di dati tramite VPN, ecc. deve avvenire con le seguenti modalità in base all'uso:

- Per copie personali sarà cura dell'utente garantire il mantenimento delle misure idonee anche sui dati copiati;
- Per invio ad altro personale dell'impresa (che potrà avvenire unicamente per necessità) sarà cura di chi ha effettuato la copia concordare con il destinatario le modalità per il mantenimento di misure idonee alla riservatezza dei dati;
- Per invio all'esterno dell'impresa sarà necessario concordare con il responsabile del trattamento dei dati le modalità per la trasmissione che comunque potrà avvenire solo a seguito di impegno scritto da parte del destinatario sulle modalità di trattamento dei dati per il mantenimento di misure idonee.

11.6.2 Misure da adottare

In base al supporto utilizzato è necessario adottare differenti misure per garantire la riservatezza dei dati copiati:

11.6.2.1 Copia su cartelle

- Assicurarsi che abbiano criteri di sicurezza idonei ai dati che vi vengono copiati;
- Provvedere all'eliminazione della copia quando non più necessaria.

11.6.2.2 Copia su FD, Nastri e CD

- Indicare il contenuto del supporto non in chiaro;
- Conservare il supporto con cura per evitarne lo smarrimento o il furto;
- Dove possibile utilizzare aree protette da password (MicroDriver USB);
- Provvedere alla cancellazione dei dati (con formattazione o con sovrascrittura) o alla distruzione del supporto quando la copia non è più necessaria.

11.6.2.3 Invio tramite posta elettronica

- L'indirizzo di posta deve essere personale o accessibile solo a personale autorizzati al trattamento ed alla consultazione dei dati inviati;
- I dati ricevuti tramite posta elettronica devono essere copiati solo su cartelle con le misure di riservatezza adeguate;
- Il messaggio di posta deve essere eliminato in modo completo quando non più necessario.

11.6.2.4 Invio tramite posta o fax

- I dati devono essere indirizzati all'attenzione del responsabile;
- L'invio tramite fax è possibile solo se si ha la certezza che il fax ricevente sia accessibile solo dal destinatario.

12 Criteri per il trattamento dei dati non elettronici

12.1 Documenti cartacei

Tutti i documenti cartacei contenenti informazioni personali o riservate prodotti o comunque trattati devono essere idoneamente custoditi dall'incaricato e conservati in locali o armadi il cui accesso sia limitato ai soli incaricati autorizzati. Nei periodi di assenza dell'incaricato i documenti devono essere riposti in modo da non essere consultabili da personale che ha accesso ai locali per altre funzioni (es. pulizie).

12.2 Posta

Gli incaricati allo smistamento della posta devono provvedere a non lasciare incustoditi i documenti prima della consegna all'incaricato al trattamento.

12.3 FAX

L'accesso ai FAX deve essere limitato ai soli incaricati al trattamento dei dati dell'unità operativa relativa. Ogni documento pervenuto per fax deve essere consegnato all'interessato o agli addetti allo smistamento della posta che provvederanno appena possibile alla consegna all'interessato.