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

Il presente Manuale è stato realizzato da

Criteri e le procedure per assicurare l'integrità dei dati.

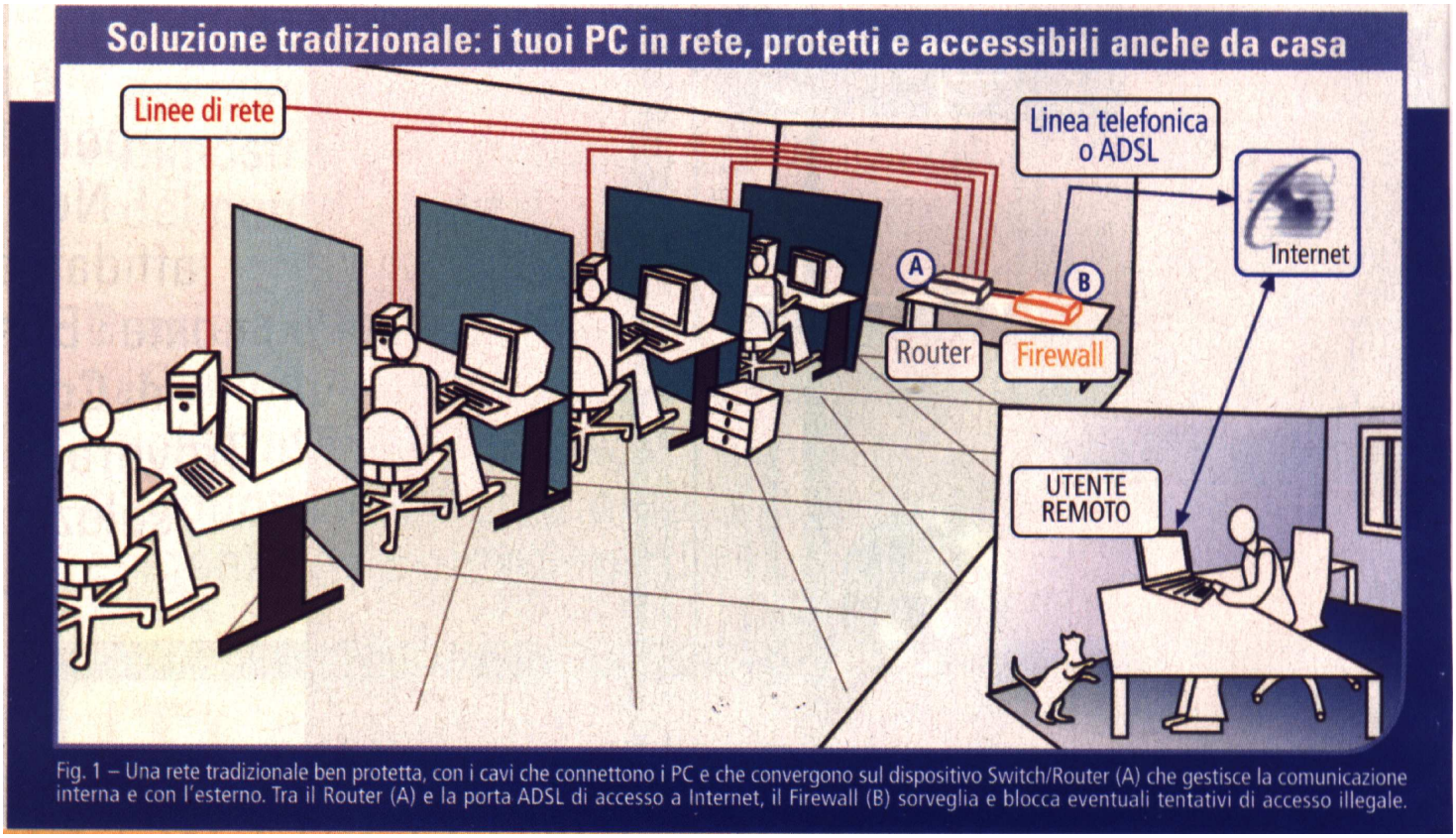
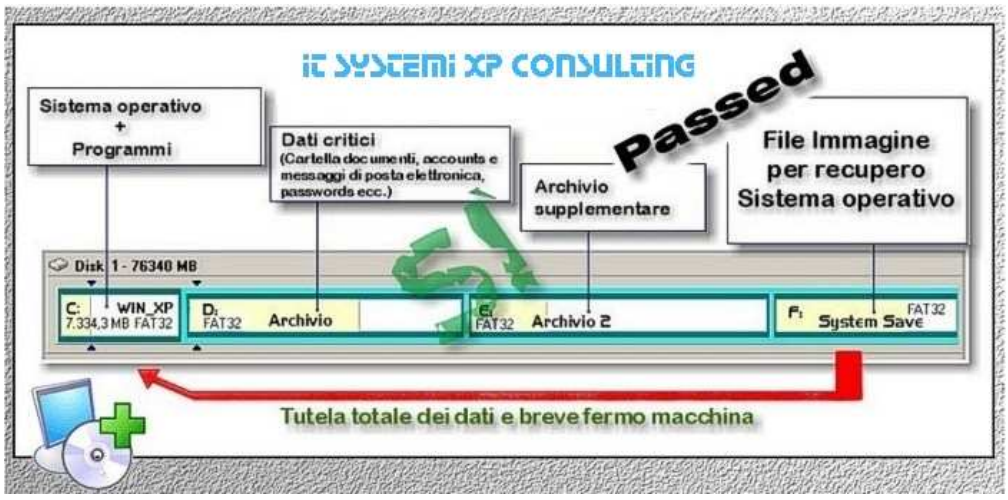


Fig. 1 – Una rete tradizionale ben protetta, con i cavi che connettono i PC e che convergono sul dispositivo Switch/Router (A) che gestisce la comunicazione interna e con l'esterno. Tra il Router (A) e la porta ADSL di accesso a Internet, il Firewall (B) sorveglia e blocca eventuali tentativi di accesso illegale.

PC CON FUNZIONI DI SICUREZZA CONTROLLO DI ACCESSO (SERVER)	**SISTEMA OPERATIVO RICHIESTO WINDOWS 2000 O WINDOWS XP; (si consiglia Windows 2000 per la provata e consolidata funzionalità e stabilità espresse nel tempo (deriva direttamente da WINDOWS NT SERVER ed è riproposto da Microsoft in tutte le versioni server) "vedi immagini 1 e 2 in basso".** **N.B. : IL DISCO DEL SERVER, CONTENENTE I TUTTI I DATI DELLO STUDIO, DOVRA' IN OGNI CASO ESSERE RESO ESTRAIBILE E DOVRA' ESSERE RIMOSSO DALLO STESSO ALLA CHIUSURA DELLE ATTIVITA' LAVORATIVE.** **NEL SERVER DOVRA' ESSERE MONTATA ANCHE UNA UNITA' DI SALVATAGGIO E BACKUP. (Es. 2° Hard Disk, Unità di Masterizzazione ecc. ecc.)**

	  **1) ERRATA MESSA IN SICUREZZA DEI DATI**  **2) CORRETTA MESSA IN SICUREZZA DEI DATI** 
PC CLIENT	**SI POSSONO CONTINUARE AD USARE I VARI SISTEMI OPERATIVI DELLA FAMIGLIA WINDOWS (98,98SE,ME ecc. ecc.) RIPULENDO TALI PC DA TUTTE LE INFORMAZIONI E DATI DI RILEVANTE IMPORTANZA (documenti, dati sensibili ecc. ecc.) CHE DOVRANNO ESSERE SALVATI SOLO ED ESCLUSIVAMENTE IN UN'AREA UTENTE RESIDENTE SUL SERVER AD ACCESSO NON LIBERO MA AUTENTICATO.**

ANTIVIRUS **Norton INTERNET SECURITY ™ 2005**	**OGNI POSTAZIONE DOVRA' ESSERE CORREDATA E CONFIGURATA CON UN ANTIVIRUS AGGIORNATO CON CADENZA ALMENO SETTIMANALE. SI CONSIGLIA DI INSTALLARE UN ANTIVIRUS DIVERSO SU OGNI POSTAZIONE COSI' DA AUMENTARE LE POSSIBILITA' DI DEBELLARE UNA QUALSIVOGLIA INFEZIONE.** **ANTIVIRUS CONSIGLIATI :** **http://www.symantec.it/region/it/product/nis_index.html** ➢ **Norton INTERNET SECURITY ™ 2005 di Symantec (pacchetto Licenza Singolo PC, per 3 o 5 Computer)** 
NOD32 per Windows 95 / 98 / ME **NOD32 per Microsoft Windows NT / 2000 / XP**	**http://www.nod32.it/home/home.htm** ➢ **NOD32 per Windows 95 / 98 / ME Fornisce "protezione on demand" per PC home o d'ufficio con il sistemi operativi Microsoft Windows 95 / 98 o ME.**

	➢ **NOD32 per Microsoft Windows NT / 2000 / XP Fornisce "protezione on demand" per PC home o d'ufficio con il sistemi operativi Microsoft Windows NT / 2000 o XP (disponibile versione per Server).**
McAfee **ANTIVIRUS**	**http://it.mcafee.com**
PANDA ANTIVIRUS **SOFTWARE**	**http://www.pandasoftware.it** **L'unico sistema di difesa è l'utilizzo di una buona soluzione antivirus, che si aggiorni quotidianamente, in grado di individuare e bloccare ogni tipo di minaccia.** **Prevenire l'attacco di virus e codici maligni è determinante per la salvaguardia dei dati e delle infrastrutture, sempre più strategiche per l'operatività delle aziende e dei singoli utenti.** **Con le soluzioni** Panda Software **tutti possono proteggersi in modo efficace dalle sempre nuove minacce che attaccano le reti ed i singoli Personal Computer.**
F-PROT **ANTIVIRUS**	**http://www.f-prot.it** F-Prot è un pacchetto software progettato per proteggere i vostri dati da nuove infezioni e programmi dannosi e per rimuovere ogni virus pronto ad infettare il vostro sistema. F-Prot per Windows può cercare, identificare e

	rimuovere circa 100.000 tipi di virus differenti. F-Prot è un antivirus molto apprezzato per valide ragioni: ha un modesto impatto sul sistema, è compatibile con tutte le versioni di Windows (95 compreso) e ha un costo limitato; riconosce e neutralizza decine di migliaia di virus e programmi dannosi; comprende un motore euristico; ha la capacità di analizzare files compressi e documenti di Office. Il software è disponibile per tutte le piattaforme più diffuse.
Kaspersky Personal Pro Suite	**http://www.kaspersky.it** **Kaspersky Personal Pro Suite - antivirus e firewall - 4.5 Ita** PROTEZIONE AVANZATA CONTRO VIRUS, HACKER E SPAM
PC-cillin Internet Security	**http://it.trendmicro-europe.com/** **PC-cillin Internet Security** **PC-cillin Internet Security – Per piccoli uffici che richiedono la protezione sul singolo PC.**
FIREWALL HARDWARE	**NEGLI UFFICI, OVE PRESENTE UNA CONNESSIONE A BANDA LARGA ADSL, E' NECESSARIO INSTALLARE ANCHE UN ROUTER CON FIREWALL INTEGRATO PER PROTEGGERSI DA ATTACCHI ESTERNI.** 

FIREWALL SOFTWARE	**PER LE CONNESSIONI DI TIPO DIAL-UP (connessioni effettuate con modem Analogico o ISDN) E' NECESSARIO INSTALLARE UN FIREWALL SOFTWARE. SI CONSIGLIA WINGATE.** **http://www.wingate.it** **http://www.achab.it/prod/intern.cfm/Ita/WinGate/1_0_1.htm**
ANTI-SPYWARE **ANTI-ADWARE**	**Software per la rimozione dal sistema di tutti quei programmi, detti spyware (software "spioni", quelli cioè che portano fuori dal computer dei dati che l'utilizzatore non si aspetterebbe), che possono violare la privacy del proprio sistema. Se qualunque informazione riguardante una persona potesse circolare da un soggetto all'altro, all'insaputa dell'interessato e al di fuori del suo controllo, venendo archiviata e usata per scopi arbitrari, la vita di quella persona rischierebbe di incorrere in tante brutte sorprese.** **A RIGUARDO SI SEGNALA QUESTO ARTICOLO** **http://punto-informatico.it/p.asp?i=34276**
BACKUP E GESTIONE DEI DISCHI E DEI DATI IN SICUREZZA	Norton Ghost 9.0 Ora con la tecnologia di Drive Image! **http://www.symantec.com/region/it/product/ng_index.html** **Fornisce funzioni avanzate di backup e di ripristino per il PC.** Norton Ghost™ 9.0 di Symantec protegge i dati creando un backup del contenuto dell'hard disk senza richiedere il riavvio di Windows® e consente di risparmiare tempo e spazio su disco tramite backup incrementali. È anche possibile pianificare

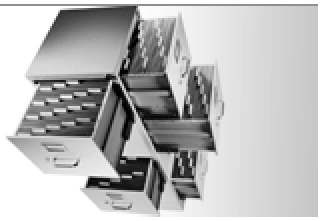
l'esecuzione automatica dei backup e ripristinare rapidamente singoli file, cartelle selezionate o l'intero hard disk.

Caratteristiche principali:

- **NOVITÀ!** L'imaging a sistema attivo consente di creare immagini di backup senza riavviare Windows®*.
- **NOVITÀ!** Gli aggiornamenti incrementali del backup fanno risparmiare tempo e spazio su disco.
- **NOVITÀ!** I backup pianificati mantengono automaticamente aggiornate le immagini di backup*.
- Esegue il backup di tutto il contenuto di un hard disk o di una partizione.
- Funziona con un'ampia gamma di hard disk e supporti rimovibili, tra cui unità CDR/RW e DVD+-R/RW, periferiche USB e FireWire® (IEEE 1394) e unità Iomega® Zip® e Jaz®**.
- Ripristina i dati dalle immagini create con PowerQuest™ Drive Image™ 7.0 e con le versioni precedenti di Norton Ghost*.
- Symantec Recovery Disk consente di ripristinare i dati da un'immagine di backup anche quando è impossibile avviare il computer in Windows.
- LiveUpdate™ mantiene aggiornato Norton Ghost automaticamente attraverso Internet.
- Norton Ghost 2003 è stato incluso per consentire il backup e il ripristino dei dati in sistemi Windows® 9x, Me, NT, Linux® e DOS.

* *Questa funzione non è disponibile in Norton Ghost 2003.*

Norton PartitionMagic™ 8.0



Norton PartitionMagic™ 8.0 di Symantec consente di organizzare facilmente l'hard disk

Norton PartitionMagic™ 8.0 di Symantec consente di organizzare facilmente l'hard disk attraverso la creazione, il ridimensionamento, la copia e l'unione di partizioni del disco. La separazione di sistema operativo, applicazioni, documenti, musica, fotografie, videogiochi e file di backup riduce il rischio di perdite di dati nel caso di blocchi del sistema. È anche possibile utilizzare più partizioni per eseguire sistemi operativi diversi in tutta sicurezza ed efficienza.

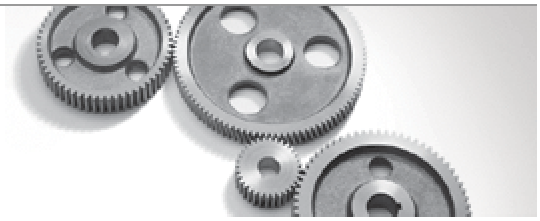
Caratteristiche

1. Divide un singolo hard disk in due o più partizioni.
2. Consente di eseguire in modo affidabile più sistemi operativi sullo stesso computer.
3. BootMagic™ semplifica il passaggio tra diversi sistemi operativi.
4. Consente di copiare, spostare, ridimensionare, dividere o unire partizioni in base alle esigenze, senza causare perdite di dati.
5. Procedure guidate illustrano dettagliatamente all'utente il processo di partizione.
6. Un browser intuitivo basato su Windows® consente di individuare, copiare e incollare i file nelle partizioni Windows e Linux®.
7. Consente di creare e modificare partizioni fino a 300 GB.*
8. Supporta unità esterne USB 2.0, USB 1.1 e FireWire®.**
9. Supporta i file system FAT, FAT32, NTFS, Ext2 ed Ext3.
10. Converte partizioni tra FAT, FAT32 e NTFS senza perdite di dati.
11. Consente di aumentare la dimensione di una partizione NTFS senza riavviare il computer.
12. Ridimensiona i cluster del sistema NTFS in base alla dimensione più appropriata.

*****Supporta l'esecuzione di operazioni su partizioni di dimensioni pari a 300 GB in cui i dati occupano il 90% dello spazio disponibile. Per hard disk più grandi potrebbe essere necessario disporre di ulteriore memoria.

******Per queste periferiche è possibile eseguire operazioni sulle partizioni se i file non sono aperti.

Norton SystemWorks 2005



Il modo più intelligente per risolvere i problemi del computer

Norton SystemWorks™ 2005 di Symantec è il modo più intelligente per risolvere i problemi del computer e proteggere i tuoi dati importanti. Questo software di facile utilizzo aiuta a eliminare i virus, prevenire i problemi del computer e ripristinare il sistema in uno stato di efficienza. La funzionalità One Button Checkup è stata migliorata per rendere più semplice la ricerca e la riparazione dei problemi del computer.

Caratteristiche principali

- One Button Checkup consente di identificare rapidamente e risolvere comuni problemi del PC.
- LiveUpdate™ scarica automaticamente gli aggiornamenti della protezione per difendere il PC dalle nuove minacce†.

Norton AntiVirus™

- **NOVITÀ!** Norton™ Internet Worm Protection blocca i worm direttamente al punto di ingresso.
- **NOVITÀ!** QuickScan rileva e rimuove i virus dopo l'installazione di nuovi aggiornamenti della protezione.
- Rimuove automaticamente virus, worm e Trojan Horse.
- Esamina e ripulisce allegati di messaggi istantanei, e-mail in entrata e in uscita e altri file.

- Rileva spyware e minacce non virali quali adware e programmi che registrano quanto digitato dall'utente.

Norton Utilities™

- Ottimizza l'archiviazione dei file per migliorare le prestazioni dell'hard disk.
- Rileva e ripara automaticamente numerosi problemi di Windows® e del disco.

Norton GoBack™

- **NOVITÀ!** La modalità SafeTry crea un ambiente temporaneo che consente di testare nuovi programmi e accettare o rifiutare le modifiche al sistema.
- **NOVITÀ!** Una barra di ricerca familiare e intuitiva facilita l'individuazione dei file o delle cartelle da ripristinare.
- Ripristina l'hard disk in una condizione di efficienza dopo un crash di sistema, un'installazione di software non riuscita, un errore dell'utente, un attacco di virus o un altro problema**.
- Consente di ripristinare solo i file e le cartelle necessari o un intero hard disk.

CheckIt® Diagnostics

- **NOVITÀ!** Fornisce una valutazione veloce e accurata dell'hardware del PC.

System Optimizer

- **NOVITÀ!** Semplifica la gestione e la personalizzazione delle impostazioni di Windows® XP tramite una semplice interfaccia.

Strumenti aggiuntivi per la risoluzione dei problemi

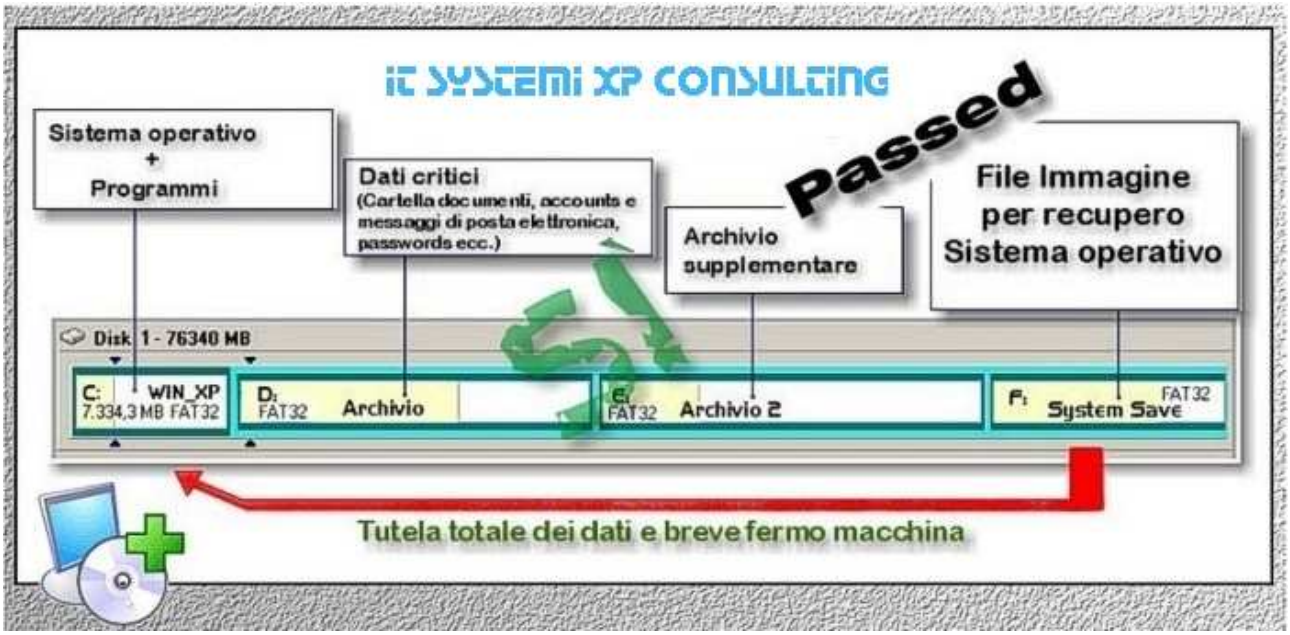
- **NOVITÀ!** Norton™ Cleanup ora elimina i file temporanei e le ultime pagine visualizzate oltre ad altri file non necessari accumulati durante le sessioni in Internet.
- Connection Keep Alive aiuta a impedire l'interruzione delle sessioni Internet su linea commutata.

** Prodotto software antivirus più venduto dal dicembre 2000 al giugno 2004 in base alla classifica Top Selling Business Software di NPD Group.*

*** La quantità di informazioni cronologiche memorizzate dipende dallo spazio disponibile su disco. La cronologia massima sui file system FAT32 è di 4 GB.*

1) ERRATA MESSA IN SICUREZZA DEI DATI

2) CORRETTA MESSA IN SICUREZZA DEI DATI



- **A) Criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi.**

Protezione delle aree e dei locali interessati

1. Le macchine server vanno collocate in un apposito locale (sala server).

2. La sala server deve essere dotata di:

   a) Impianto antincendio adeguato a locali contenenti apparati informatici;
   b) Impianto di condizionamento ambientale, opportunamente dimensionato;
   c) Porte e finestre blindate;
   d) Impianto elettrico a norma;
   e) Gruppo di continuità.

3. L’accesso alla sala server è consentito solo al responsabile del trattamento, o alle persone espressamente autorizzate.
4. In assenza del personale autorizzato, la sala server deve essere tenuta chiusa a chiave.
5. I supporti di backup vanno tenuti in armadi blindati, posti in locali distanti dalla sala server, non trasportabili e dotati di impianto antifurto.
6. Tutte le chiavi vanno custodite dalla vigilanza o da personale delegato dal Capo dell’Ufficio.

➢ B) Criteri e le procedure per assicurare l'integrità dei dati.

Sicurezza del software.

1. Presso ciascun Ufficio è consentita l’installazione esclusiva delle seguenti tre categorie di software:
    1. Software commerciale, dotato di licenza d’uso;
    2. Software Ministeriali realizzati specificamente per la gestione dello STUDIO e dei relativi adempimenti, a livello nazionale;
    3. Software realizzato specificamente per l’Ufficio, a livello locale.

2. L’installazione di software diversi da quelli indicati va autorizzato dal responsabile del trattamento.
3. Il software deve essere installato solo da supporti fisici originali o dei quali sia nota la provenienza.
4. Tramite l’Ufficio del Responsabile per i Sistemi Informativi Automatizzati si provvede alla distribuzione di un software antivirus aggiornato.
5. In mancanza di procedure automatiche, il responsabile del trattamento garantisce l’effettuazione dell’Aggiornamento del software antivirus su tutte le postazioni di lavoro, con cadenza almeno quindicinale.

Integrità dei dati.

13. Il responsabile, con la collaborazione degli Amministratori di Sistema, mantiene un elenco, da aggiornare con cadenza almeno semestrale, di tutte le attrezzature informatiche dell’ufficio, dello scopo cui sono destinate, della loro locazione fisica, delle misure di sicurezza su esse adottate e delle eventuali misure di adeguamento pianificate.
14. Il responsabile del trattamento individua i volumi logici o le aree di disco da sottoporre a backup, sui vari server.
15. A ciascun utente viene assegnata una directory, in un’area disco di un server che sia sottoposta a backup, dove mantenere i dati che debbono essere mantenuti in maniera sicura. L’accesso a queste directory è consentita esclusivamente all’utente proprietario, nonché agli incaricati del backup.
16. Il responsabile del trattamento individua, tra gli amministratori di sistema, uno o più incaricati del backup.
17. Laddove il backup venga effettuato localmente nell’ambito dell’ufficio, gli incaricati effettuano le seguenti operazioni:
    a) Esecuzione quotidiana del backup, eventualmente attraverso procedure automatiche;
    b) Verifica almeno settimanale della corretta esecuzione dei backup;
    c) Mantenimento di un elenco dei backup effettuati;
    d) Archiviazione dei supporti secondo le disposizione della sezione “**A**” “Protezione delle aree e dei locali interessati” punto N° 5 (**I supporti di backup vanno tenuti in armadi blindati ecc. ecc.**).
    e) Verifica, con cadenza almeno mensile, della procedura di recovery dai supporti di backup;
    f) Effettivo ripristino dei dati in caso di necessità.

➢ C) Criteri e procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica.

Controllo degli accessi.

1. Tutte le stazioni di lavoro debbono essere protette da una password di accensione.
2. L'inserimento della password di accensione va effettuato a cura dell'utente, affidandone una copia, in busta chiusa, al responsabile del trattamento, che le custodirà sotto chiave.
3. Ai fini dell'assistenza sistemistica, la password di accensione può venire comunicata agli incaricati, e sostituita al termine dell'intervento.
4. La password di accensione va modificata con cadenza annuale.
5. L'accesso alla rete di sistema va protetto tramite un nome utente e una password.
6. Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo, rispetto alle risorse del sistema informatico. A ciascun profilo è associato un gruppo di utenti, che condividono gli stessi privilegi di accesso e utilizzo.
7. Il responsabile del trattamento fornisce ai preposti alla custodia delle parole chiave i nominativi e la qualifica degli utenti autorizzati, nonché i loro privilegi di utilizzo del sistema informatico. I preposti provvedono:

   a) A definire, per ciascun utente, il nome utente e la password per il primo accesso;
   b) A definire i gruppi necessari per rispettare i privilegi di utilizzo;
   c) A consegnare agli interessati il nome utente e la password, unitamente a una copia del Manuale per la sicurezza.

8. Non poter utilizzare lo stesso nome utente per accedere contemporaneamente al sistema da due postazioni di lavoro distinte.
9. La password di accesso alla rete:
   8. Non deve derivare dal nome utente o dai dati personali dell'utente;
   9. Deve avere una lunghezza di almeno otto caratteri;
   10. Non deve essere una semplice parola rintracciabile in un dizionario;
   11. Deve contenere almeno un carattere non alfabetico, oppure un misto di lettere minuscole e maiuscole.

10. Gli applicativi utilizzati per il trattamento possono sfruttare l'autenticazione di cui al punto 5, oppure richiedere a loro volta un nome utente e una password per una propria autenticazione
11. Alle eventuali password di accesso agli applicativi si applicano le indicazioni di cui ai punti 7, 8 e 9. Per gli applicativi che non consentano di automatizzare i controlli di cui al punto 8 va previsto un adeguamento, i cui tempi vanno indicati nel documento di cui al punto "B1" paragrafo "**INTEGRITA' DEI DATI**".
12. I preposti alla custodia delle parole chiave provvedono, con cadenza almeno trimestrale, alla verifica degli elenchi degli utenti, e provvedono, previa verifica con il responsabile del trattamento, alla disattivazione delle utenze su cui risultasse qualche problema (mancato utilizzo da più di sei mesi, un elevato numero di tentativi di accesso non riusciti, o simili).
13. Nome utente e password sono strettamente personali. L'utente è tenuto:

    a) A non comunicare a terzi le password;
    b) A non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi;
    c) A scegliere la password di accensione diversa dalle altre due password;
    d) Ad attenersi a tutte le indicazioni contenute nel manuale per la sicurezza.

14. Ogni incaricato provvederà alla periodica sostituzione della propria parola chiave, previa comunicazione al soggetto preposto alla custodia delle parole chiave.

Ulteriori misure di sicurezza relative a elaboratori accessibili in rete:

a) I codici identificativi personali per l'utilizzazione dell'elaboratore devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi.
b) I programmi in dotazione, di protezione contro il rischio di intrusione o danneggiamento ad opera di

terzi, devono essere verificati, quanto a efficacia ed aggiornamento, con cadenza almeno semestrale.

c) Nel caso in cui l'elaboratore contenga i dati sensibili di cui all'articolo 22 della legge n. 675 del 1996 o i dati particolari di cui all'articolo 24 della citata legge n. 675 del 1996:
   - l'accesso all'elaboratore sarà consentito sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione; se si tratta di elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico;
   - l'autorizzazione, se riferita agli strumenti, dovrà individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento;
   - le autorizzazioni all'accesso sono rilasciate e revocate solo dal titolare e dal responsabile;
   - periodicamente, e comunque almeno una volta l'anno, dovrà essere verificata la sussistenza delle condizioni per le autorizzazioni all'accesso;
   - l'autorizzazione all'accesso deve in ogni caso intendersi limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
   - la validità delle richieste di accesso ai dati personali deve essere verificata prima di consentire l'accesso stesso;
   - è vietata l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

Misure di sicurezza relative a documentazione e archivi cartacei (o comunque a "strumenti diversi da quelli elettronici o comunque automatizzati"):

a) I fascicoli cartacei, nelle fasi di trasporto all'interno dell'ufficio, devono permanere nei corridoi il tempo strettamente necessario alla loro consegna.
b) Gli incaricati devono avere accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.
c) Nessuno può accedere all'archivio se non autorizzato.
d) I fascicoli se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.
e) Nel caso in cui i documenti o l'archivio contengano i dati sensibili di cui all'articolo 22 della legge n. 675 del 1996 o i dati particolari di cui all'articolo 24 della citata legge n. 675 del 1996:
   - gli atti e i documenti contenenti i dati se affidati agli incaricati del trattamento, devono essere conservati, fino alla restituzione, in contenitori muniti di serratura;
   - l'accesso all'archivio deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura dell'archivio stesso;
   - i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono conservati e custoditi con le modalità suddette.

Trasmissione dei dati

1. Le connessioni telematiche verso le banche dati degli uffici, provenienti dall'esterno dello stesso ufficio, sono distinti in tre categorie:
   a) Connessioni provenienti da altri uffici e/o aree adibite al trattamento dei dati;
   b) Connessioni provenienti dall'interno dell'ufficio, su postazioni di lavoro pubblicamente disponibili;
   c) Connessioni provenienti da utenti e postazioni di lavoro non appartenenti all'ambito dell'area di trattamento dei dati.

2. Le connessioni di tipo "**a**" vengono controllate attraverso il Sistema Informatico di Sicurezza della Rete dello Studio, secondo le regole seguenti:
3. Sul collegamento dell'ufficio verso la Rete dello STUDIO è installato un apparato di controllo (firewall);

4. In maniera predefinita, il firewall è configurato in maniera da permettere alle postazioni di lavoro interne all'ufficio di accedere ai servizi disponibili sulla rete, bloccando i tentativi di accesso provenienti dall'esterno verso l'ufficio;
5. Qualora un ufficio voglia rendere disponibili dei servizi ad altri uffici interni e/o esterni all'Ambito locale di trattamento, dovrà richiedere all'Ufficio del Responsabile per i Sistemi Informativi Automatizzati l'apertura dei canali di comunicazione necessari sul firewall.
6. Le procedure per la sicurezza delle connessioni di tipo b) sono stabilite dal responsabile del trattamento. Qualora le postazioni pubbliche consentano l'accesso ai dati sensibili di cui all'art. 22 della legge 675/99, o ai dati riservati di cui all'art. 24 della medesima legge, occorrerà stabilire rigorose procedure per l'autenticazione degli utenti (firma digitale, personale di presidio alla postazione, o simili).
7. Qualora siano necessarie connessioni effettuate tramite modem da postazioni collegate alla rete dell'ufficio senza l'ausilio di detti sistemi di controllo ed autenticazione (Firewall, router, antivirus ecc ecc) queste andranno effettuate da locali dedicati, le cui postazioni non siano connesse alla rete dell'ufficio. Per questi locali andranno previste adeguate misure di controllo degli accessi.

➢ D) Piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

Manuale per la sicurezza

1. I responsabili di trattamento provvedono all'eventuale personalizzazione del manuale per la sicurezza, con la collaborazione degli amministratori di sistema.
2. Il manuale per la sicurezza viene consegnato agli utenti contestualmente ai codici (nome utente e password) per l'accesso al sistema.

Piano di intervento e formazione

1. Gli amministratori di sistema provvedono a informare tempestivamente i responsabili del trattamento di ogni eventuale problema di sicurezza di cui dovessero venire a conoscenza.
2. I soggetti responsabili del trattamento provvederanno, anche per tramite degli amministratori di sistema, a informare tempestivamente gli incaricati:
    a) della presenza di virus negli elaboratori dell'ufficio;
    b) di prassi da parte del personale non conformi alle disposizioni di sicurezza;
    c) della periodica necessità di variazione delle parole chiave da parte degli incaricati;
    d) della disponibilità di programmi di aggiornamento relativi all'antivirus.