Allegato alla delibera C-6.
n° 627 del 14/03/08

Comune di Taranto

Politiche di Sicurezza del sitema Informativo del Comune di Taranto

Regolamento del Comune di Taranto per il Corretto Utilizzo delle Risorse Informatiche e Telematiche

Predisposto da:

DIREZIONE DECENTRAMENTO COMUNICAZIONE E INNOVAZIONE

Servizio Comunicazione – URP e Innovazione

Versione 1.0

Indice

1.- PREMESSA..... pag. 3

2.- PRINCIPI GENERALI DELLE POLITICHE DI SICUREZZA..... pag. 3

3.- CONTENUTI DELLE POLITICHE DI SICUREZZA DEL COMUNE DI TARANTO..... pag. 4

4.- REGOLAMENTI E PROCEDURE DERIVANTI DALLE POLITICHE DI SICUREZZA..... pag. 5

5.- UTILIZZO DEL PERSONAL COMPUTER..... pag. 6

6.- UTILIZZO DELLA RETE..... pag. 8

7.- GESTIONE DELLE PASSWORD..... pag. 8

8.- UTILIZZO DEI SUPPORTI MAGNETICI..... pag. 9

9.- UTILIZZO DEI PC PORTATILI..... pag. 9

10.- UTILIZZO DELLA POSTA ELETTRONICA..... pag. 9

11.- UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI..... pag.10

12.- PROTEZIONE ANTIVIRUS..... pag.11

13.- OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY..... pag.12

14.- NON OSSERVANZA DEL REGOLAMENTO..... pag.12

15.- AGGIORNAMENTO E REVISIONE..... pag.12

1. - PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche per lo svolgimento delle attività del Civico Ente, ed il libero accesso alla rete Internet dai Personal Computer, comporta la necessità di regolamentare l'utilizzo delle risorse informatiche e telematiche, al fine di evitare comportamenti inconsapevolmente scorretti da parte del personale dipendente.

Inoltre, il presente Regolamento interno è diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza del trattamento dei dati disciplinato dal D. Lgs n.196 del 30.06.2003.

Il presente Regolamento deve essere rispettato da tutto il personale dipendente (Dirigenza e comparto) nonché dal personale dipendente di aziende terze operanti, in forza di specifici rapporti contrattuali, nell'ambito dei servizi e delle strutture del Comune di Taranto.

L'utilizzo di strumenti informatici o telematici di proprietà del Comune di Taranto o da Esso acquisiti o utilizzati sotto forma di leasing, di comodato d'uso, di noleggio o sotto altra forma, deve conformarsi al presente Regolamento.

2. - PRINCIPI GENERALI DELLE POLITICHE DI SICUREZZA

Un aspetto fondamentale della realizzazione di un Sistema di gestione della sicurezza delle informazioni conforme alle norme di settore vigenti, è la definizione delle politiche di sicurezza che il Comune di Taranto intende adottare.

Per "politiche" si intendono gli obiettivi, le linee guida, i criteri generali che un'organizzazione pone alla base delle proprie azioni in tema di sicurezza.

Le politiche, inoltre, devono tenere conto:

- della normativa di legge (per esempio della legge n. 196/2003), dei regolamenti (norme o standard dettate da Regione, Ministero o altri organismi), in tema di sicurezza;
- del valore del patrimonio informativo da proteggere, valutato con il processo di analisi dei rischi, in modo che le misure di sicurezza definite dalle politiche siano coerenti con tale valore;
- dell'indipendenza dalla tecnologia.

L'individuazione degli obiettivi di Sicurezza del Comune di Taranto si traduce in obiettivi di Sicurezza del Sistema Informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento.

Su questa base il Comune di Taranto procederà operativamente, dove necessario, alla scelta e implementazione di dispositivi e tecnologie.

COMUNE DI TARANTO

3. - CONTENUTI DELLE POLITICHE DI SICUREZZA DEL COMUNE DI TARANTO

a. La sicurezza deve essere considerata una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, da uso improprio o da distruzione da parte di tutti i dipendenti e dalle società informatiche e telematiche, operanti nel Comune di Taranto.

b. L' Amministrazione comunale ha intrapreso una valutazione dei rischi e su tale base ha considerato le priorità e gli obiettivi del proprio Sistema di gestione della sicurezza delle informazioni.

c. Le Politiche di Sicurezza si basano sul principio che le risorse informatiche (dati, risorse hardware, software, ecc.) sono un patrimonio che deve essere protetto dal momento in cui viene creato/installato, durante il suo utilizzo, fino al momento in cui viene distrutto.

d. Classificazione delle informazioni: le informazioni, in qualsiasi forma esse si presentino (posta elettronica, archivi informatici, programmi, ecc.), devono essere protette con normative e misure tecniche commisurate sia alla importanza che esse rappresentano per il Comune di Taranto (riservatezza, criticità, valore economico diretto o indiretto), sia a specifici requisiti (norme di legge, ecc), criteri su cui si baserà il sistema di classificazione.

e. Protezione fisica delle risorse: l'obiettivo è la definizione di misure di sicurezza per la predisposizione e il mantenimento dell'efficacia ed efficienza dell'ambiente di lavoro e la riduzione dei rischi di interruzione dei servizi.

f. Tale obiettivo viene raggiunto attraverso misure proporzionate ai rischi e al valore dei beni e delle informazioni presenti nell'ambiente da proteggere. Ne fanno parte le seguenti componenti:
   - la classificazione delle aree del Comune di Taranto legate al sistema da proteggere (es.: aree riservate, aree interne, aree pubbliche);
   - l'accesso controllato alle aree considerate critiche;
   - la sicurezza fisica (relativa agli impianti) e la sorveglianza di queste aree;
   - la rilevazione tempestiva di eventuali incidenti di sicurezza.

g. Protezione logica delle informazioni: con misure proporzionate al "valore" delle informazioni, copriranno i seguenti aspetti di sicurezza:
   - il controllo degli accessi alle informazioni;
   - il mantenimento della loro integrità e riservatezza;
   - le comunicazioni interne ed esterne;
   - la sicurezza delle stazioni di lavoro;
   - lo sviluppo, manutenzione e messa in esercizio delle applicazioni;
   - la gestione operativa dei dispositivi (dai PC a firewall, router, server);
   - la rilevazione tempestiva di eventuali incidenti di sicurezza.

h. Definizione della struttura organizzativa della sicurezza, ovvero la catena di ruoli e responsabilità per tutte le attività necessarie al funzionamento e alla gestione del sistema di gestione della sicurezza.

i. Conseguenze della violazione delle politiche; accanto alla attribuzione dei ruoli e delle

responsabilità occorre prevedere la violazione delle norme collegate e le sanzioni o azioni correttive da intraprendere in proposito.

j. Norme per il Personale: tutti i dipendenti concorrono alla realizzazione della Sicurezza; pertanto, dovranno proteggere le informazioni assegnate loro per lo svolgimento dell'attività lavorativa nel rispetto di quanto stabilito dalle Politiche almeno in termini di:
   - utilizzo delle risorse informatiche;
   - accesso ai sistemi e ai dati;
   - uso della password.

k. Piano di Continuità Operativa: l'obiettivo è quello di garantire la continuità del servizio e la disponibilità di informazioni con un conveniente grado di aggiornamento, evitando o limitando i danni al patrimonio informativo a fronte di una emergenza. Questo può essere raggiunto sia con un Piano di Ripristino del servizio, che porta alla ripresa delle attività in seguito ad una emergenza prevedendone gli aspetti organizzativi e normativi, le modalità e le risorse di backup necessarie (centro di calcolo, risorse hardware, software, personale, ecc.); si potrà prevedere anche l'attivazione di eventuali sistemi alternativi di gestione del servizio, anche in modalità degradata, fino al ripristino della gestione originale (è il caso in cui si può prevedere l'uso del canale telefonico in caso di emergenza e blocco del servizio Internet).

l. Gestione degli incidenti: i rischi informatici devono essere sempre costantemente controllati e monitorati. Saranno, quindi, definite le responsabilità e le modalità con cui gestire eventuali incidenti di sicurezza.

m. Revisione delle politiche: sarà messo in atto un meccanismo di manutenzione delle Politiche, a intervalli di tempo predefiniti, o al mutare di determinate condizioni (variazioni dell'ambito di certificazione, modifiche interne all'organizzazione, risultato di un *penetration test*).

4. - REGOLAMENTI E PROCEDURE DERIVANTI DALLE POLITICHE DI SICUREZZA

Dai punti sopra evidenziati emergono quei documenti che sono necessari alla formalizzazione del funzionamento del sistema di gestione della sicurezza, ovvero tutte quelle procedure, regolamenti, disposizioni, emanati in applicazione e comunque in conformità alle politiche di sicurezza.

Questi documenti, in linea generale, indirizzeranno tutte le attività che utenti e gestori del sistema di sicurezza svolgono, senza arrivare al dettaglio tecnologico di manuali tecnici o di sistema.

Tutte le volte che lo standard fa riferimento a controlli che per la loro natura si prestano a contromisure di carattere prevalentemente organizzativo, l'evidenza dell'implementazione del controllo è appunto documentale, la descrizione formalizzata della procedura da seguire e la prova della sua avvenuta pubblicazione e diffusione a tutte le persone ed enti interessati.

E quindi si tratta di documenti del tipo:

- identificazione e autenticazione degli utenti;
- *userid (naming convention*, assegnazione, ecc.);
- *password* (regole di assegnazione, lunghezza, sintassi, scadenza, ecc.) o altri strumenti di autenticazione (es. *smart card*);
- classificazione e livelli di protezione delle risorse;

- protezione e personalizzazione del software di base;
- classificazione, protezione e accessi alle risorse utente;
- crittografia (algoritmi, distribuzione, ecc.);
- registrazione, conservazione e consultazione dei *log* ;
- individuazione e rapporto in merito a tentativi di intrusione;
- autorità di System e Security Administration;
- ecc.

Processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza, quali le utenze, le password, le chiavi di crittografia, i certificati digitali, i *log*, gli allarmi, ecc.

Alcuni dei principali processi gestionali riguardano:

- definizione e cancellazione di *userid* ;
- assegnazione di privilegi;
- assegnazione delle password;
- autorizzazioni di accesso ai dati/transazioni;
- gestione chiavi di crittografia;
- richiesta/gestione/rinnovo certificati digitali;
- analisi e gestione dei *log*.

Sono queste categorie tecnologiche per raccogliere le informazioni e i relativi documenti.

Nel presente documento vengono definite le prime Regole per il Corretto Utilizzo delle Tecnologie Informatiche e Telematiche nell'ambito della definizione delle Politiche per la gestione della sicurezza del sistema informativo del Comune di Taranto.

Con ulteriori specifici documenti il Comune di Taranto procederà a completare il quadro delle Politiche di Sicurezza.

5. - UTILIZZO DEL PERSONAL COMPUTER

5.1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

5.2. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per l'accesso a qualsiasi applicazione, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Responsabile del sistema informativo.

5.3. Il Responsabile del sistema informativo per l'espletamento delle sue funzioni, ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

5.4. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Responsabile del sistema informativo, perché sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

5.5. Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Comune di Taranto (D.Lgs n°518/92 sulla tutela giuridica del software e Legge n°248/2000 nuove norme di tutela del diritto d'autore).

5.6. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Responsabile del sistema informativo.

5.7. Non è consentito utilizzare strumenti software e/o hardware atti ad interpretare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.

5.8. Sui pc dotati di scheda audioe/o di lettura cd non è consentito l'ascolto di programmi, files o audio musicali,...se non a fini prettamente lavorativi.

5.9. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

5.10. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc...), se non con l'autorizzazione espressa del Responsabile del sistema informativo.

5.11. Prima di procedere ad accendere la postazione di lavoro l'utente è tenuto ad accertarsi che non vi siano supporti removibili (ad esempio floppy) nei rispettivi alloggiamenti. Vi sono infatti sistemi che prima di accedere al disco fisso accedono agli alloggiamenti dei supporti removibili. Se nei supporti citati sono contenuti file, questi vengono letti prima e quindi il sistema non può avviarsi correttamente o essere infettato.

5.12. Agli utenti incaricati del trattamento dei dati sensibili è vietato l'accesso contemporaneo con lo stesso account da più PC.

5.11. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile del sistema informativo nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 9 del presente Regolamento relativo alle procedure di protezione antivirus.

5.13. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

5.14. Nella ipotesi che un utente debba allontanarsi dalla propria postazione di lavoro ma sia certo di ritornarvi entro la fine della giornata lavorativa, è tenuto ad accertarsi di aver chiuso tutti i documenti aperti per evitare che un estraneo possa accedere ai documenti cui l'utente lavora o per permettere ai colleghi di utilizzare lo stesso documento se condiviso su server di rete.

5.15. Inoltre, in caso di allontamento della propria postazione di lavoro, l'utente deve bloccare il sistema / attivare la funzione di log out:

a) ove prevista la possibilità esplicita di bloccare il sistema, l'utente deve utilizzarla (ad es. su Windows 2000 la combinazione di tasti CRTL + ALT + CANC);

b) qualora possibile, costituisce una misura ancora più efficace l'effettuazione del log out dal sistema;

c) in ogni caso l'utente è invitato ad impostare l'attivazione dello screen saver entro pochi minuti di inattività, per rendere impossibile la lettura dei dati, specialmente di quelli a elevata riservatezza; è necessario che l'accesso al sistema dopo l'intervento dello screen saver sia vincolato all'autenticazione dell'utente (tramite password, smart card, ...) in modo tale che un estraneo, se non possiede tali informazioni, non possa accedere ai dati; si tenga presente che questa misura non è da ritenersi sufficiente nel caso che non sia prevista una password di avvio della postazione.

6. - UTILIZZO DELLA RETE

6.1. Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup da parte del Responsabile del sistema informativo.

6.2. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

6.3. Il Responsabile del sistema informativo può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

6.4. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

6.5. E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. E' buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

7. - GESTIONE DELLE PASSWORD

7.1. Gli utenti (user-id) di ingresso alla rete e di accesso ai programmi, sono previsti ed attribuiti dal Responsabile del sistema informativo. È consentita comunque l'autonoma sostituzione da parte degli incaricati al trattamento, con contestuale comunicazione al Responsabile del sistema informativo.

7.2. La password è la forma di protezione più importante che l'utente possiede per evitare che estranei accedano ai suoi dati pertanto l'utente, quando la inserisce, si accerti di non essere osservato.

7.3. Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema.

7.4. Le password utilizzate dagli incaricati al trattamento hanno una durata massima di 4 mesi(così come previste dalla normativa vigente), trascorsi i quali le password devono essere sostituite.

7.5 Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile del sistema informativo.

8. - UTILIZZO DEI SUPPORTI MAGNETICI

8.1. Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce, CD-RW) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (art. 22 allegato B del D.Lgs. n°196/2003). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

8.2. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

8.3. Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

8.4. Tutti i files di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo da parte del Responsabile del sistema informativo.

9. - UTILIZZO DEI PC PORTATILI

9.1. L'utente è responsabile del PC portatile assegnatogli dal Responsabile del sistema informativo e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

9.2. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

9.3. I PC portatili utilizzati all'esterno (convegni, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

10. - UTILIZZO DELLA POSTA ELETTRONICA

10.1. La casella di posta, assegnata dal Comune di Taranto all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

10.2. E' fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

10.3. E' buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

10.4. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune di Taranto, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dalla Direzione. In ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

10.5. La posta elettronica diretta all'esterno della rete informatica comunale può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti di lavoro "strettamente riservati".

10.6. Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica

10.7. E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

10.8. Per la trasmissione di file all'interno di intranet del Comune di Taranto è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

10.9. E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

10.10. E' vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Responsabile del sistema informativo. Non si deve in alcun caso attivare gli allegati di tali messaggi.

11. - UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

11.1. Internet è la più grande rete telematica mondiale ed è un insieme di tecnologie e standard che consentono ad ogni singolo computer connesso di essere collegato in tempo reale con un qualsiasi altro computer connesso per lo scambio di dati e informazioni. Può supportare diverse forme di comunicazione, come la posta elettronica, il world wide web, i newsgroup.

11.2. Intranet è la rete interna al Comune di Taranto che supporta lo stesso standard di comunicazione di Internet e viene creata per consentire la condivisione delle risorse e delle informazioni fra tutti i collaboratori interni autorizzati ad accedervi.

11.3. Il PC abilitato alla navigazione in Internet costituisce uno strumento del Comune di Taranto necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

11.4. E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile del sistema informativo.

11.5. E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

11.6. E' da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

11.7. E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

11.8. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica

11.9. L'accesso ad Internet deve avvenire esclusivamente utilizzando gli strumenti autorizzati dal Comune di Taranto.

11.10. Non è consentito l'utilizzo di reti telefoniche del Comune di Taranto per accedere a fornitori di servizi Internet esterni e non autorizzati.

11.11. L'accesso alle risorse Internet può avvenire:

a) *usando gli indirizzi dei siti:* le risorse sono identificate da un nome o da un indirizzo univoco (ad esempio www.comune.taranto.it). Per accedere a tali risorse l'utente deve scrivere l'indirizzo nell'apposito *Web browser* (Navigatore di Rete);

b) *usando i motori di ricerca:* l'utente che non conosca gli indirizzi, o i siti, che trattano un particolare argomento può utilizzare i motori di ricerca (per esempio: www.yahoo.com, www.lycos.com, www.altavista.com, www.google.com, www.msn.com, ecc.) per reperire le informazioni ed i nomi dei siti effettuando una ricerca basata su parole chiave;

c) *usando i metamotori di ricerca:* si tratta di siti che consentono all'utente di effettuare più ricerche su più motori (inserendo la parola chiave una sola volta), aggregandone e selezionandone i risultati (ad esempio www.metacrawler.com, www.metafind.com, www.surfwax.com, ...);

d) *usando gli agenti di ricerca:* sono strumenti particolarmente evoluti di ricerca online, sulla base di spider "più intelligenti" rispetto a quelli dei motori di ricerca classici, che consentono di comparare informazioni presenti sulla Rete relative a determinati oggetti;

e) *i link (o collegamenti):* i siti possono includere collegamenti ipertestuali con pagine web aventi contenuti correlati, selezionandoli il browser provvede ad aprire le pagine relazionate senza conoscerne o digitarne l'indirizzo;
   - links presenti nei documenti in esame potrebbero non trattare argomenti analoghi (ad esempio Banner pubblicitari);
   - esiste la possibilità che si aprano finestre per effetto di determinati eventi (per esempio chiusura di una finestra oppure passaggio del mouse su determinate zone del documento) ovvero senza esplicita richiesta da parte dell'utente.

   In tal caso è opportuno chiudere le pagine non interessate.

f) *i preferiti (o segnalibri):* vi è la possibilità di registrare gli indirizzi dei siti di maggiore interesse in apposite zone del browser dette "Preferiti."

11.11. Prima di eseguire un trasferimento di dati accertarsi che:

a) ove esista la possibilità di scelta fra differenti siti ed esista una indicazione sulle loro performance eseguire il trasferimento dal sito più efficiente;

b) i dati che si stanno scaricando siano effettivamente utili per il lavoro;

c) la dimensione dei file che deve essere trasferita è tale da non rallentare il lavoro della rete del Comune di Taranto (si ricorda che per accedere ad Internet si sta utilizzando la rete del Comune di Taranto che non deve essere mai rallentata);

d) non si stiano scaricando file che contengono dei virus (tenere sempre attivo ed aggiornato l'antivirus. Si ricorda che la presenza di virus può arrecare danni al lavoro dell'utente oltre che alla rete comunale;

e) siano in ogni caso rispettati i termini di licenza del software scaricato a seguito di autorizzazione; si ricorda che i software "shareware" prevedono un periodo di prova, al termine del quale l'utilizzazione libera non è più consentita.

12. - PROTEZIONE ANTIVIRUS

12.1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico Comune di Taranto mediante virus o mediante ogni altro software aggressivo.

12.2. Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

12.3. Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente: a) sospendere ogni elaborazione in corso senza spegnere il computer; b) segnalare l'accaduto al Responsabile del sistema informativo.

12.4. Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici di provenienza ignota.

12.5. Ogni dispositivo magnetico di provenienza esterna al Comune di Taranto dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato al Responsabile del sistema informativo.

13. - OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

13.1. E' obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di individuazione di incaricato del trattamento dei dati ai sensi del D.Lgs n.196/2003.

14.- Non osservanza del Regolamento

14.1. Il Comune di Taranto verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

14.2. Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

14. - AGGIORNAMENTO E REVISIONE

15.1. Il presente Regolamento è soggetto ad aggiornamento e revisione con frequenza periodica ove necessario.