DELIBERAZIONE n. 7

allegata al **VERBALE n. 92** della seduta del **CONSIGLIO DI AMMINISTRAZIONE** del **22-12-2009.**

OGGETTO: Adozione del ***Regolamento per la posta elettronica.***

Sono presenti i Signori:

Il Presidente Prof. Enrico **GARACI**;

I Componenti Dott. Salvatore Paolo **CANTARO;**

Dr.ssa Francesca **BASILICO D'AMELIO;**

Dott. Mario **MORLACCO;**

Prof. Calogero **SURRENTI;**

Risultano *assenti giustificati:*

Il Vice Presidente Prof. Adelfio Elio **CARDINALE;**

I Componenti Prof. Fabio **MIDULLA;**

Prof. Sergio **PECORELLI.**

Prof. Stefano **ZURRIDA;**

Partecipano, altresì, del Collegio dei Revisori dei Conti, i Signori:

I Componenti Dott. Angelo **MENDITTO;**

Dott. Giulio **DI CLEMENTE.**

Risulta *assente giustificato:*

Il Presidente Dott. Alessandro **RIDOLFI.**

Partecipano, inoltre:

- la Dott.ssa Monica **BETTONI**, Direttore Generale dell'Istituto;
- la Dott.ssa Rosa M. **MARTOCCIA**, Direttore Centrale degli Affari Amm.vi e delle R. E. dell'ISS;
- il Dott. Maurizio **PASQUALI**, Direttore Centrale delle Risorse Umane e Affari Generali dell'ISS.

Svolge le funzioni di *Segretario* la Dott.ssa Giuliana **ERAMO**, Dirigente dell'Ufficio Organi Collegiali dell'Istituto.

Relatore: **IL PRESIDENTE.**

Il Relatore rappresenta al Consiglio che l'I.S.S., nell'ambito della gestione dei servizi di posta elettronica e di rete, cura la funzionalità dei sistemi informativi, adotta le misure di sicurezza necessarie a garantire la disponibilità e l'integrità dei sistemi e dei dati, indica le modalità d'uso delle risorse informatiche per assicurare il corretto impiego da parte dei lavoratori e prevenire utilizzi indebiti.

Al riguardo, il Presidente rappresenta l'opportunità di adottare un disciplinare riguardante l'utilizzo degli strumenti informatici, della rete e della **posta elettronica**.

A tal fine, sottopone al Consiglio per l'approvazione il testo concernente: "Disciplinare interno per l'utilizzo degli strumenti informatici, della rete e della posta elettronica dell'Istituto superiore di sanità " (Allegato n. 1).

Il Presidente precisa che il succitato disciplinare è stato elaborato in ossequio alla vigente normativa di riferimento. In particolare, evidenzia che lo stesso definisce le regole tecniche, organizzative e di utilizzazione delle risorse informatiche, telematiche e dei servizi di posta elettronica e di rete dell'Istituto Superiore di Sanità conformemente alle *Linee guida per posta elettronica ed Internet,* definite dal Garante per la protezione dei dati personali con provvedimento a carattere generale del 1/03/2007, pubblicato nella G.U. n. 58 del 10 marzo 2007.

Tanto premesso, il Presidente invita il Consiglio ad esprimersi .

IL CONSIGLIO

Udito il relatore;

Esaminato il documento presentato recante "Disciplinare interno per l'utilizzo degli strumenti informatici, della rete e della posta elettronica dell'Istituto superiore di sanità "(Allegato n. 1);

Sentito il parere favorevole del Direttore Generale;

Dopo ampia ed approfondita discussione;

All'unanimità

DELIBERA

di **approvare,** come innanzi proposto, l'adozione del "Disciplinare interno per l'utilizzo degli strumenti informatici, della rete e della posta elettronica dell'Istituto superiore di sanità" contenuto nel documento facente parte integrante della presente deliberazione (Allegato n. 1).

Letto, confermato e sottoscritto.

IL SEGRETARIO

IL PRESIDENTE

DISCIPLINARE INTERNO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI, DELLA RETE E DELLA POSTA ELETTRONICA DELL'ISTITUTO SUPERIORE DI SANITA'

INDICE

1 – INTRODUZIONE

1.1 – Oggetto

Il presente disciplinare definisce le regole tecniche, organizzative e di utilizzazione delle risorse informatiche, telematiche e dei servizi di posta elettronica e di rete dell'Istituto Superiore di Sanità conformemente alle *Linee guida per posta elettronica ed Internet,* definite dal Garante per la protezione dei dati personali con provvedimento a carattere generale del 1/03/2007, pubblicato nella G.U. n. 58 del 10 marzo 2007.
Nell'ambito della gestione dei servizi di posta elettronica e di rete, l'I.S.S. cura la funzionalità dei sistemi informativi, adotta le misure di sicurezza necessarie a garantire la disponibilità e l'integrità dei sistemi e dei dati, indica le modalità d'uso delle risorse informatiche per assicurare il corretto impiego da parte dei lavoratori e prevenire utilizzi indebiti.
La gestione dei servizi oggetto del presente disciplinare è di competenza del Settore Informatico.
Il Presidente dell'ISS, quale Titolare per il trattamento dei dati, nomina - ai sensi dell'art. 29 del D.lgs 196/2003 (*Codice in materia di protezione dei dati personali)* - il Responsabile della sicurezza informatica il quale fornisce idonea garanzia del rispetto delle norme vigenti in materia di trattamento con strumenti elettronici, ivi compreso il profilo della sicurezza.
In considerazione della delicatezza della materia che attiene ai diritti individuali e che richiede un giusto bilanciamento con il potere di controllo dell'amministrazione, le attività di verifica finalizzate al controllo della sicurezza dei sistemi e del traffico di *rete,* ove operate, sono svolte su dati aggregati e comunque trattati in forma anonima, riferiti all'intera struttura lavorativa o ad alcune aree specialistiche, nel rispetto del principio di proporzionalità, pertinenza e non eccedenza.
Nei casi di accertata violazione dei principi fissati nel presente disciplinare, l'I.S.S. potrà procedere all'applicazione dei provvedimenti sanzionatori individuati nella normativa del rapporto di lavoro, con le modalità ivi previste per il personale dipendente e all'applicazione delle sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti.

1.2 – Soggetti preposti al controllo: Amministratori di Sistema

Al Responsabile della sicurezza informatica è affidato il compito di:

- nominare gli amministratori dei sistemi di posta e di rete come prescritto dal provvedimento del Garante per la protezione dei dati personali del 27/11/2008 (G.U. 300/24.12.2008) avente per oggetto: *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema,* successivamente modificato in data 25/06/2009 (G.U.149/30.06.2009)
- assicurare che le attività svolte dagli amministratori di sistema, finalizzate alla verifica sulla funzionalità e sicurezza dei sistemi e al controllo dell'utilizzo dei servizi da parte dei lavoratori, siano conformi alle vigenti leggi in materia di sicurezza e protezione dei dati personali
- assicurare che le operazioni eseguite sui sistemi siano strettamente necessarie al perseguimento delle finalità prescritte
- verificare almeno annualmente la rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza, previste dalle norme vigenti sul trattamento dei dati personali
- vigilare sulla corretta applicazione del presente regolamento.

L'individuazione nominativa degli amministratori di sistema e l'elencazione analitica degli ambiti di operatività individuali, in base al profilo di autorizzazione assegnato, sono riportati nel D.P.S., (Documento Programmatico della Sicurezza) aggiornato annualmente ai sensi del Dlgs 196/2003 e pubblicato sul sito intranet dell'ISS.
L'ISS adotta sistemi di controllo che consentano la registrazione degli accessi logici effettuati dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici. Tali registrazioni, con i riferimenti temporali e la descrizione dell'evento che le ha generate, sono conservate con caratteristiche di completezza, inalterabilità e integrità per un periodo non inferiore a sei mesi.

1.3 - Fonti normative

Le fonti normative prese in esame sono:

- Le norme istitutive e regolatrici dell'ISS
- Legge n. 300/1970 - Statuto dei Lavoratori
- Decreto Legislativo 196/2003 – Codice in materia di trattamento di dati personali
- Linee guida per posta elettronica e internet - deliberazione del Garante per la protezione dei dati personali n° 13 del 1° marzo 2007 – G.U. n. 58 del 10 marzo 2007
- Provvedimenti e Comunicati del Garante in materia
- Codice dell'amministrazione digitale (D.lgs. 7.3.2005 e successive modificazioni)
- Codice di comportamento dei dipendenti della Pubblica Amministrazione (D.M. 28.11.2000)
- CCNL degli Enti di ricerca pubblica

2 – PERSONAL COMPUTER

2.1 - Utilizzo del Personal Computer

L'I.S.S. è proprietario delle apparecchiature informatiche, assegnate come strumenti di lavoro ai dipendenti con rapporto di lavoro a tempo indeterminato e determinato, i quali sono tenuti al dovere di diligenza e vigilanza evitando manomissioni e danneggiamenti.
Le stazioni di lavoro, fisse e portatili, sono dotate di dispositivi (*hardware*) e programmi (*software*) tali da consentirne il corretto funzionamento. Qualsiasi utilizzo non conforme all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.
Il dipendente è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale; pertanto, sulle apparecchiature assegnate, non può installare *hardware e/o software* né duplicare o utilizzare *software* non conformi all'attività istituzionale. E' tenuto a non salvare, nelle cartelle di *rete* su cui viene eseguito giornalmente il *back-up,* file audio e video non inerenti l'attività lavorativa o comunque sanzionabili dalla legge sul diritto d'autore e file non istituzionali di ogni tipo. In ogni caso è vietata la riproduzione o la duplicazione di programmi informatici su licenza ai sensi della Legge n. 128 del 21.05.2004.
Il dipendente, si impegna:

- a non concedere l'uso della propria stazione di lavoro a persone non autorizzate
- a non usare stazioni di lavoro diverse dalla propria senza autorizzazione
- a non lasciare incustodita ed accessibile la propria stazione di lavoro
- a non alterare la configurazione del proprio computer.

Non è consentita l'attivazione della password d'accensione (*BIOS*), senza preventiva autorizzazione.
Salvo documentata necessità, il P.C. deve essere spento ogni sera e deve essere impostato il parametro per il risparmio energetico in caso di assenze prolungate dal servizio.
L'utilizzo di una stazione di lavoro, a disposizione in occasione di convegni, conferenze, ospitalità e simili è sotto la responsabilità dell'organizzatore dell'evento, previa la necessaria autorizzazione del Settore Informatico.

2.2 - Utilizzo di P. C. portatili

Il dipendente assegnatario del P.C. portatile è responsabile della sua custodia.
Ai P.C. portatili, connessi alla *rete* I.S.S., si applicano le regole di utilizzo previste per le stazioni fisse. Si consiglia di collegarsi periodicamente alla *rete* interna per consentire l'aggiornamento dell'antivirus, con cadenza almeno semestrale.
E' obbligo del dipendente rimuovere eventuali archivi residenti su disco prima della riconsegna del P.C. portatile.
Il collegamento di P.C. portatili privati alla *rete* dell'I.S.S. deve essere autorizzato dal Settore Informatico.

3 – LA RETE

3.1 – La rete dell'I.S.S.

La *rete* istituzionale, la cui gestione è demandata al Settore Informatico, è protetta e per accedere è obbligatorio usare credenziali di accesso personali e non cedibili a terzi, assegnate esclusivamente ai dipendenti con rapporto di lavoro a tempo indeterminato e determinato e al personale con contratto di collaborazione.
Il dipendente, cui sono assegnate credenziali di accesso personali (codice utente e *parola chiave*), si impegna:

- a non cedere le proprie credenziali
- a non utilizzare credenziali di altri utenti
- a conservare diligentemente le proprie credenziali
- ad adottare una *parola chiave* non banale (ad es. senza riferimenti personali), come prescritto al punto 5 dell'Allegato B del Dlgs 196/2003

Le credenziali cessano d'ufficio quando non sussiste più la condizione per cui sono state rilasciate oppure in caso di accertata violazione degli obblighi di legge.
L'I.S.S., tramite gli amministratori della *rete* e degli apparati di sicurezza, può disciplinare l'accesso alla *rete*

- adottando misure di tipo organizzativo e tecnologico per prevenire utilizzi impropri e ridurre il rischio di impieghi abusivi
- predisponendo l'utilizzazione di filtri per prevenire comportamenti impropri.

Per motivi di sicurezza può essere attuato il blocco della navigazione verso siti particolari, aventi contenuti e/o finalità vietati dalla legge, anche utilizzando prodotti *software* specifici che ne forniscano *Blacklist* aggiornate.
L'I.S.S. può svolgere verifiche su dati aggregati e generali, inerenti l'accesso alla rete dei propri dipendenti, trattati sempre in forma anonima.
Tali verifiche, ove operate, sono finalizzate alla sicurezza, efficienza e integrità dei sistemi informativi, nel rispetto dei principi di proporzionalità, pertinenza e non eccedenza.

3.2. – Uso della rete e dei relativi servizi

L'utilizzo della *rete* è consentito esclusivamente per fini istituzionali.
Il collegamento a Internet, reso disponibile sulle stazioni di lavoro fisse o mobili, è finalizzato allo svolgimento dell'attività lavorativa.
E' vietato lo scarico di *software* di carattere non istituzionale, prelevato da siti esterni anche di tipo *freeware.*
L'accesso alla *rete* dell'I.S.S. è consentito esclusivamente attraverso i canali istituzionali e qualsiasi altro dispositivo di accesso deve essere esplicitamente autorizzato dal Settore Informatico.
E' vietata la partecipazione a *Forum* non professionali, l'utilizzo di *chat-line* (esclusi gli strumenti autorizzati) e di bacheche elettroniche.
Il dipendente è direttamente e totalmente responsabile dell'accesso alla *rete* e ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che immette e delle modalità con cui opera.

E' vietata l'installazione, non concordata con il Settore Informatico, di strumenti che aumentino la possibilità di connessione alla rete – *Hub e Switch* - perché possono causare grave nocumento alle prestazioni della rete stessa. Ai fini della sicurezza e' inoltre vietato effettuare *Tunneling*.

3.3. – Protezione antivirus

L'I.S.S. fornisce un *software* antivirus di ultima generazione, costantemente aggiornato, installato in tutte le stazioni di lavoro e disponibile in rete; salvo documentate motivazioni tecniche, è obbligatorio usufruire del suddetto *software* antivirus per ridurre il rischio di attacco al sistema informatico istituzionale.

Nel caso che il *software* antivirus rilevi la presenza di un *virus* che non è riuscito a rimuovere, è necessario sospendere ogni elaborazione in corso e, senza spegnere il computer, segnalare l'accaduto al Settore Informatico.

Ogni dispositivo di provenienza esterna all'I.S.S. deve essere sottoposto a verifica mediante il programma antivirus prima dell'utilizzo e, nel caso venga rilevato un *virus* non eliminabile, non deve essere connesso alla rete.

4 - POSTA ELETTRONICA

4.1 – Assegnazione della casella postale

Il servizio di posta elettronica consiste nella disponibilità di una casella postale, accessibile tramite le credenziali personali di accesso alla rete, assegnata dal Settore Informatico esclusivamente ai dipendenti con rapporto di lavoro a tempo indeterminato e determinato e al personale con contratto di collaborazione.
L'indirizzo è univoco sulla rete ed ha la forma standard seguente:

nome.cognome@iss.it

dove "iss.it" è il nome del *dominio*.
E' consentito, su istanza motivata, il rilascio di indirizzi alternativi non standard (*alias* di *account)* nel *dominio* iss.it.
L'I.S.S.:

- può assegnare una casella istituzionale di riferimento ad ogni singola struttura
- può imporre la presenza, nei messaggi in uscita, di una nota a piè di pagina di natura istituzionale.

L'invio interno dei messaggi di posta può essere rivolto:

- ad un singolo
- ad un gruppo
- alla totalità della popolazione I.S.S. (*e-mail all*) o a gruppi preconfigurati (*mailing-list*).

Le *e-mail* di tipo *all* e a gruppi preconfigurati sono momentaneamente trattenute dal sistema di posta e sottoposte all'approvazione dell'Amministratore di sistema al fine di valutarne l'esclusivo uso istituzionale.

4.2 – Regole d'uso

La casella di posta elettronica è destinata ad un esclusivo utilizzo istituzionale, coerente con la prestazione lavorativa e conforme alle norme che disciplinano il lavoro alle dipendenze della P.A. e pertanto l'autore del messaggio si assume le responsabilità disciplinari, civili e penali derivanti dalla propria comunicazione.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
In caso di assenza, programmata e per lunghi periodi, è opportuno attivare una risposta automatica per garantire la continuità dell'attività lavorativa.
Il dipendente è tenuto ad osservare una condotta prudente, sapendo che:

- le comunicazioni tramite posta elettronica hanno la stessa efficacia di quelle divulgate secondo i canali tradizionali (corrispondenza epistolare, telefonica, fax)
- le liste di destinatari (*mailing-list*) devono essere sempre verificate
- i messaggi possono essere modificati e ritrasmessi in versione alterata
- i messaggi possono diventare documenti permanenti
- i messaggi, anche se cancellati, possono essere potenzialmente recuperati

- gli allegati possono contenere anche materiale insicuro (programmi e/o comandi) e/o file di dimensioni eccessive
- i messaggi trasmessi per posta elettronica possono essere usati come prove in procedimenti civili e penali.

Non è consentita la trasmissione di materiale e/o pubblicità non richiesti (*spamming*), catene di Sant'Antonio e simili.
Non è consentito inviare o memorizzare messaggi (interni o esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, o che costituiscano comunque condotta illecita e in ogni caso le comunicazioni non devono recare pregiudizio all'I.S.S..

4.3 – Antispam e gestione degli spam

L'I.S.S. pone la sua attenzione sul fenomeno dello *spam* in posta elettronica attivando misure di sicurezza nell'intera infrastruttura informatica.
I sistemi antispam sono gestiti centralmente dal Settore Informatico e monitorati quotidianamente.
Il sistema provvede ad intercettare le *e-mail* considerate *spam* e a metterle in quarantena ma, come tutti i sistemi automatici, pur garantendo un'alta affidabilità nel riconoscimento delle *e-mail* di *spam*, non è esente da falsi positivi.
Per questo motivo è predisposto un meccanismo di report, periodicamente inviati alla casella postale, con indicate le *e-mail* messe in quarantena. E' compito del dipendente controllare i report e reindirizzare alla propria casella di posta eventuali *e-mail* accantonate dal sistema.
I messaggi identificati come *spam* e lasciati in quarantena sono rimossi automaticamente dopo trenta giorni.

5 – GLOSSARIO

ACCOUNT: iscrizione registrata su un server che, tramite credenziali, consente l'accesso alla *rete* e ai suoi servizi;

BIOS: Basic I/O System (PC): è il primo codice che viene eseguito da un PC dopo l'accensione, ed ha la funzione principale di localizzare e caricare il Sistema Operativo nella RAM;

BACK-UP: operazione tesa a duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server.

BLACK LIST: registro contenente elenco di "risorse" non fruibili

CHAT LINE: servizio che consente di dialogare, attraverso computer e Internet, con una o più persone, in tempo reale;

DOMINIO: indirizzo su Internet identificato da un nome registrato presso le autorità nazionali ed internazionali competenti;

E-MAIL: messaggio in formato elettronico composto al computer e trasmesso a un altro computer utilizzando una *rete* locale o Internet;

FIREWALL: sistema di sicurezza destinato a impedire l'accesso da una *rete* esterna a un computer oppure a un Local Area Network (LAN);

FORUM: pagina internet che commenti e pareri su svariati argomenti.

FREEWARE: software gratuito, di libera distribuzione ed utilizzo;

HARDWARE: indica la parte fisica di un personal computer ovvero tutte le parti magnetiche, ottiche, meccaniche ed elettroniche che ne consentono il funzionamento;

HUB: dispositivo che funge da nodo di smistamento di una *rete* di comunicazione dati;

INTRANET: rete locale simile a quella Internet, con accesso riservato ai dipendenti forniti di credenziali;

LOG: archivio storico delle attività registrate automaticamente da un computer ;

NOME UTENTE (USER NAME): identificativo con il quale si accede alle risorse o a un sistema. Il nome utente e la password rappresentano le credenziali di un utente;

PAROLA CHIAVE (PASSWORD): sequenza segreta di caratteri (lettere, numeri, ecc) che, combinata con nome utente, consente l'accesso a una determinata area;

RETE: sistema di computer connessi per stabilire una comunicazione e per facilitare lo scambio di informazioni tra utenti. Può essere semplice o complessa;

SITO: termine generale con il quale si indica un "luogo virtuale", costituito da un insieme di pagine web, raggiungibile attraverso un indirizzo Internet (URL);

SPAM: invio di posta elettronica indesiderata, con annunci pubblicitari o catene di S. Antonio, a un gran numero di utenti contemporaneamente;

STAZIONE DI LAVORO: personal computer collegato alla rete istituzionale tramite il quale l'utente accede ai servizi;

SOFTWARE: indica l'insieme dei programmi in grado di far dì funzionare un computer;

SWITCH: dispositivo di rete usato per connettere ad una singola porta del computer più periferiche;

TUNNELING: è una tecnica utilizzata nel campo della trasmissione di dati digitali per veicolare informazioni che normalmente utilizzano metodologie diverse per incapsulare un protocollo trasmissivo. Tale tecnica viene utilizzata anche per bypassare i *firewall*, utilizzando tipologie di connessioni non bloccate per effettuare altre operazioni che normalmente verrebbero filtrate.

VIRUS: programma in grado di danneggiare, anche irreversibilmente, i dati e le applicazioni di un computer. Può essere introdotto da un messaggio di posta elettronica o scaricando da Internet file non sicuri;

WHITE LIST: registro contenente elenco di "risorse" fruibili;

WWW: World Wide Web – rete telematica mondiale. Sistema di informazioni globale, basato sulla combinazione di ricerca e recupero delle informazioni e tecniche ipertestuali. IL WWW è stato creato nel 1994 al CERN di Ginevra. Letteralmente significa "ragnatela mondiale".

Il Presidente

Il Segretario