Istituto Nazionale Previdenza Sociale

Direzione Generale
Direzione Centrale Organizzazione
Direzione Centrale Risorse Umane
Direzione Centrale Sistemi Informativi e Tecnologici

Roma, 03/12/2012

Circolare n. 135

Ai Dirigenti centrali e periferici
Ai Responsabili delle Agenzie
Ai Coordinatori generali, centrali e periferici dei Rami professionali
Al Coordinatore generale Medico legale e Dirigenti Medici

e, per conoscenza,

Al Presidente
Al Presidente e ai Componenti del Consiglio di Indirizzo e Vigilanza
Al Presidente e ai Componenti del Collegio dei Sindaci
Al Magistrato della Corte dei Conti delegato all'esercizio del controllo
Ai Presidenti dei Comitati amministratori di fondi, gestioni e casse
Al Presidente della Commissione centrale per l'accertamento e la riscossione dei contributi agricoli unificati
Ai Presidenti dei Comitati regionali
Ai Presidenti dei Comitati provinciali

Allegati n.1

OGGETTO: **disciplinare per l'utilizzo degli strumenti informatici**

SOMMARIO:

1. PREMESSA

La continua evoluzione tecnologica e l'utilizzo sempre più intensivo degli strumenti informatici per lo svolgimento di tutte le attività istituzionali inducono all'adozione di misure idonee indirizzate alla protezione delle infrastrutture informatiche.

In considerazione del rischio aziendale sotteso all'uso improprio della posta elettronica e della navigazione Internet, l'Istituto ha ritenuto di predisporre un insieme di misure idonee indirizzate alla riduzione del rischio derivante dall'uso improprio degli strumenti forniti in dotazione.

Ancorchè molteplici siano state le misure tecnologiche ed organizzative introdotte dall'INPS a garanzia dell'integrità e della riservatezza dei dati e delle transazioni informatiche, si ritiene che il livello di rischio in tale ambito possa essere ulteriormente ridotto intervenendo anche sulle regole comportamentali in relazione all'uso degli asset informatici, richiamando le regole del loro impiego e monitorando la loro applicazione.

Con la presente circolare si portano a conoscenza di tutto il personale dell'Istituto le norme sull'utilizzo delle strumentazioni e delle procedure informatiche che ciascun dipendente è tenuto ad osservare.

Il disciplinare si rivolge anche al personale esterno che utilizzi strumenti e servizi informatici all'interno delle Sedi dell'Istituto.

2. DISPOSIZIONI OPERATIVE

Atteso che l'Istituto, per l'attuazione delle politiche di sicurezza informatica, al fine di difendere il proprio patrimonio informativo ed individuare eventuali utilizzi illeciti e/o fraudolenti, sottopone a tracciatura - log - tutte le transazioni informatiche, conservando altresì i log di navigazione internet e di posta elettronica (in questi ultimi i dati vengono trattati in maniera anonima così da garantire la privacy dell'utente che ha effettuato gli accessi);

tenuto conto che tali log sono consultabili solo dagli amministratori di sistema - specificamente incaricati secondo la normativa vigente - esclusivamente su richieste collegate ad azioni relative a finalità investigative per la repressione di illeciti o su richiesta delle autorità inquirenti,

al fine di definire i principi generali per il corretto utilizzo degli strumenti informatici dell'Istituto e la conseguente tutela del proprio patrimonio informativo, è stato predisposto il documento "*Disciplinare per l'utilizzo degli strumenti informatici*", allegato alla presente circolare, a cui tutto il personale dovrà attenersi.

Tale documento, in particolare, definisce:

- i ruoli e le responsabilità delle principali strutture dell'Istituto coinvolte nel processo di gestione dei servizi informatici;
- le raccomandazioni generali e le regole comportamentali cui devono attenersi gli utenti interni, al fine di garantire l'utilizzo in sicurezza dei servizi informatici e degli strumenti, in coerenza con la politica dell'Istituto e con la normativa in vigore;
- le attività di monitoraggio e di tracciamento dei servizi di posta elettronica e di navigazione Internet degli utenti, in conformità con le indicazioni del Garante stabilite nel Provvedimento Generale del 1 marzo 2007, "Linee guida del Garante per posta elettronica e internet".

Si ritiene opportuno, per facilità di lettura, riportare di seguito le principali indicazioni generali e disposizioni.

A. Il personale è responsabile di tutte le attività che svolge utilizzando le risorse informatiche dell'Istituto assegnate (computer, telefono, procedure informatiche, ecc.), il cui utilizzo deve sempre ispirarsi al principio di diligenza e correttezza. In particolare, il Personal Computer (postazioni fisse e notebook) deve essere utilizzato esclusivamente per scopi professionali ed in relazione alle attività di presidio del proprio ruolo.

B. Al fine di non compromettere le funzionalità ed il livello di sicurezza della postazione di lavoro, non sono consentite l'installazione o la rimozione di hardware o software, né la modifica delle configurazioni impostate (ad es. parametri di rete, configurazioni di sistema, ecc.), se non espressamente autorizzate dalla Direzione Centrale Sistemi Informativi e Tecnologici (di seguito DCSIT).

C. Devono essere consentiti l'aggiornamento dell'antivirus e l'installazione degli aggiornamenti di sistema almeno ogni 15 giorni; tali aggiornamenti vengono di norma effettuati automaticamente dal sistema ma, in particolar modo per gli strumenti portatili (notebook), occorre consentire il collegamento con la rete aziendale per il tempo necessario al completamento delle operazioni.

D. E' necessario assicurarsi che il software antivirus sia installato e attivo.

E. I supporti di memoria rimovibili (floppy disk, CD/DVD, chiavi USB, hard disk esterni, ecc.) contenenti dati sensibili o giudiziari devono essere conservati in luoghi protetti (ad esempio, armadi e cassettiere chiusi a chiave) o protetti da una chiave di accesso di protezione. I dati in essi contenuti devono essere cancellati, quando non sono più necessari, o, nel caso non fosse possibile cancellarli, i supporti devono essere distrutti.

F. In caso di furto o smarrimento di risorse informatiche o di supporti contenenti dati dell'Istituto, oltre che presentarne denuncia alle autorità di pubblica sicurezza, l'utente deve tempestivamente darne comunicazione anche alla DCSIT.

G. Senza una specifica autorizzazione della DCSIT, l'utente non deve utilizzare modem o dispositivi affini che consentono la connessione diretta della postazione di lavoro a reti esterne pubbliche (Internet) o private (sistemi di altre società), ivi incluso il collegamento tramite telefoni cellulari o apparati hardware wireless (ad es. router wireless o access point). In nessun caso, inoltre, il modem ed i dispositivi affini possono essere utilizzati quando la postazione di lavoro è collegata contemporaneamente alla rete dell'Istituto.

H. Laddove possibile il monitor delle postazioni di lavoro dovrà essere posizionato in modo da non rendere possibile, se non per il suo utilizzatore, la lettura delle informazioni visualizzate. Qualora il monitor sia ubicato a ridosso di finestre o presso gli sportelli al pubblico è necessario verificarne l'orientamento al fine di garantire la riservatezza delle informazioni.

I. L'Istituto mette a disposizione del lavoratore un indirizzo di posta elettronica aziendale da utilizzare per finalità inerenti all'attività lavorativa. Nell'ambito della corrispondenza elettronica, l'utente avrà cura di trasmettere comunicazioni concise, professionali e rispettose, nei toni, della dignità dei destinatari, utilizzando un linguaggio appropriato e una forma espositiva adeguata. Gli utenti hanno l'obbligo di comunicare con i vari livelli della struttura aziendale seguendo le stesse vie gerarchiche utilizzate per la posta convenzionale.

J. L'utente del servizio di posta elettronica è tenuto ad adottare comportamenti mirati ad evitare l'utilizzo della posta elettronica dell'Istituto per motivi personali.

K. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'utente interessato può delegare un altro utente affinché verifichi il contenuto dei

messaggi e inoltri al responsabile del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Allorquando l'utente non conferisca tale delega, il responsabile del trattamento, alla presenza dei richiamati presupposti , può accedere alle comunicazioni di servizio presenti nella mailbox dell'utente con modalità selettive.

L. Pur essendo consentito l'acceso web a caselle di posta personali, i dipendenti sono tenuti ad evitare il download di allegati che possono essere veicolo di virus o di elementi dannosi per l'integrità del sistema informativo.

M. E' vietato modificare il proprio client di posta elettronica standard messo a disposizione dall'Istituto. L'Help Desk non è tenuto a fornire assistenza in caso di utilizzo di client di posta difformi da quelli standard.

N. Il dipendente ha l'obbligo di segnalare la ricezione di messaggi con contenuto potenzialmente pericoloso alle strutture preposte.

O. Non è consentito condividere la propria casella personale con collaboratori esterni.

P. Non è consentito utilizzare i servizi forniti dall'Istituto per effettuare attività che possano provocare malfunzionamenti, arrecare danni ad altri utenti, costituire abusi o illeciti, causare la riduzione di efficienza del servizio o arrecare danni, anche in termini di immagine all'Istituto, ad altri utenti e/o a terzi.

Q. La connessione ad Internet è messa a disposizione del lavoratore da parte dell'Istituto ai fini dello svolgimento dell'attività lavorativa. E' tuttavia tollerata in via eccezionale l'utilizzo della navigazione internet per finalità non direttamente correlate alla prestazione lavorativa, purché ciò avvenga per una durata limitata e tale da non incidere sulla propria prestazione lavorativa e, comunque, in modo da non mettere a repentaglio l'integrità e la riservatezza dei dati e del sistema informatico dell'Istituto ovvero provochi per lo stesso un danno di immagine.

R. E' vietato scaricare sulla propria postazione di lavoro software, file e qualsiasi tipologia di materiale multimediale che viola, o per mezzo dei quali può essere violata, la normativa in tema di diritto d'autore.

S. Non è consentito utilizzare e duplicare software senza un'idonea licenza all'uso né installare software gratuiti (freeware o shareware), se non con preventiva autorizzazione di DCSIT.

Rientra nel dovere di diligenza e di osservanza delle norme per l'esecuzione e la disciplina del lavoro consultare con regolarità i messaggi pubblicati su HERMES e le email pervenute nella propria casella di posta elettronica.

3. Attività di supporto e monitoraggio

Le Direzioni regionali, attraverso i Gruppi regionali di assistenza informatica, svolgono azioni di monitoraggio e supporto ai fini dell'applicazione delle disposizioni contenute nella presente circolare.

La Direzione Centrale Sistemi Informativi e Tecnologici svolge azioni di monitoraggio anche attraverso l'utilizzo di sistemi automatizzati.

Inoltre, nell'ambito della Direzione Centrale Sistemi Informativi e Tecnologici opera una struttura funzionale denominata IRT (Incident Response Team), con compiti di ricezione,

analisi e gestione delle segnalazioni pervenute dagli utenti per sospette violazioni di sicurezza.

La presente circolare dovrà essere notificata, con le consuete modalità, a tutto il personale dell'Istituto.

La aziende fornitrici di servizi all'Istituto che utilizzino strumenti informatici dovranno ricevere copia della presente circolare affinché ne venga data diffusione a tutti i propri collaboratori.

Il Direttore Generale
Nori

Sono presenti i seguenti allegati:

Allegato N.1

Cliccare sull'icona "ALLEGATI"  per visualizzarli.