Unione Europea
FONDI STRUTTURALI EUROPEI
PON 2007-2013
MIUR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
D.G. per gli Affari Internazionali - Ufficio IV
Programmazione e gestione dei fondi strutturali europei e nazionali per lo sviluppo e la coesione sociale
COMPETENZE PER LO SVILUPPO (FSE) - AMBIENTI PER L' APPRENDIMENTO (FESR)

SCUOLA SECONDARIA STATALE 1^ GRADO "T. TASSO"
Via M. Iannicelli - **84126** SALERNO - C.F.: 80024690655- C.M.SAMM181002
Email – samm181002@istruzione.it – P.E.C. : samm181002@pec.istruzione.it
Sito web: www.scuolasecondariatassosalerno.it - Tel. 089/405294- Fax. 089/799550

Prot.n. 1881-C/2

Salerno, 13.09.2014
Al Direttore dei S.G. e A.
Al Personale Amministrativo

ALBO SEDE
Al Sito-Web istituzionale
ATTI

OGGETTO: Norme basilari di comportamento-D.Lgs.n. 196/2003.

Con la presente, si trasmettono le norme basilari di comportamento che le SS.LL. sono tenute a rispettare ai sensi di quanto disposto dal D. Lgs.n.196/2003.

Distinti saluti

Il DIRIGENTE SCOLASTICO
Dott.ssa Elvira Vittoria BONINFANTE

NORME BASILARI DI COMPORTAMENTO

Al fine di evitare problemi correlati a virus informatici, gli utenti rispettano come misura minima le seguenti prescrizioni:

a) mantenere costantemente aggiornato il programma antivirus.

b) ovunque possibile, accertarsi della provenienza dei messaggi do posta elettronica contenenti allegati.

c) aprire gli allegati di posta elettronica solo dopo averli salvati e controllati con il programma antivirus.

d) sottoporre a controllo tutti i supporti di provenienza esterna o incerta, prima di eseguire o caricare uno qualsiasi dei files in esso contenuti.

e) non utilizzare il proprio "disco sistema" su di un altro computer se non in condizione di "protezione in scrittura".

f) proteggere in "scrittura" tutti i propri floppy disk di sistema o contenenti programmi eseguibili, dati o back-up.

g) se si utilizza un computer che necessita di un "bootstrap" da floppy, usare un floppy disk protetto in scrittura e verificato come non infetto.

h) non attivare mai da floppy un sistema basato su hard disk a meno di utilizzare un disco di sistema, protetto in scrittura e sicuramente non infetto.

i) limitare la trasmissione di files eseguibili e di sistema (tra cui .COM, .EXE, .BIN, .OVL, .OVR, .SYS) tra computer in rete.

j) non utilizzare i server come stazioni di lavoro.

k) non aggiungere mai dati o files ai supporti contenenti programmi originali.

l) non intraprendere azioni di modifica sui sistemi informativi a seguito di diffusione di messaggi e segnalazioni di virus, da qualsiasi fonte provenienti. Le uniche azioni eventualmente necessarie vengono comunicate dalla Direzione Informatica.

m) evitare di scaricare da rete programmi o files non inerenti le attività d'ufficio o comunque sospetti.

REGOLE OPERATIVE

1. Tutti i computer dell' Ente devono essere dotati di programma antivirus. I programmi vengono aggiornati con cadenza almeno quindicinale. Ove ritenuto necessario, può essere assegnata a cura del R.S.I. (Responsabile Sistema Informativo) una frequenza di aggiornamento superiore.
2. Ogni computer è costantemente sottoposto a controllo anti-virus, attraverso la scansione del software in dotazione.
3. Ogni qualvolta si renda necessario, i responsabili della sicurezza provvedono a immediati aggiornamenti dell'antivirus e all'applicazione di altre misure di sicurezza su indicazione del R.S.I.
4. I responsabili della sicurezza si assicurano che i computer delle società esterne, qualora interagiscano con i propri sistemi informatici, siano dotati di adeguate misure di protezione antivirus.
5. Il personale delle ditte addette alla manutenzione dei supporti informatici usa solo supporti preventivamente controllati, singolarmente, ogni volta.
6. I supporti provenienti dall'esterno vengono sottoposti a verifica da attuare con un PC non collegato in rete (macchina da quarantena), ed inoltre vengono individuate le aree dell' Ente che, in relazione alla loro particolare attività, sono da considerare a più alto rischio nei riguardi dell'infezione da virus.
7. All'atto della individuazione di una infezione da virus l'utente segue le raccomandazioni emanate in proposito dal R.S.I; ne dà immediata comunicazione al responsabile della sicurezza.
8. Gli utenti si rivolgono al R.S.I. per la eliminazione dei virus qualora il livello di infezioni risulti superiori alla capacità dell'antivirus installato.
9. Il personale deve essere a conoscenza che la diffusione dei virus è punita dall'art. 615 quinquies del Codice Penale.
10. Il software acquisito viene sempre controllato contro i virus e verificato perché sia di uso sicuro prima di essere installato.
11. Il salvataggio dei documenti su file viene effettuato in formati standard (p.e. RTF per il testo), evitando ovunque possibile il salvataggio in formati proprietari. Ciò allo scopo di ridurre il rischio di contaminazioni da macro virus, problemi di compatibilità tra versioni e dimensioni dei documenti.
12. La distribuzione di documenti in formato elettronico avviene tramite formati generali, compatibili e possibilmente compressi (p.e. PDF).

REGOLAMENTO INTERNO PER GLI INCARICATI

- Gli incaricati si assumono la responsabilità del corretto utilizzo delle macchine, salvaguardandone la funzionalità ed utilizzandole esclusivamente per fini di lavoro.
- Gli incaricati sono tenuti ad informare il R.S.I. (interno o ditta esterna) di eventuali malfunzionamenti o presenze di virus.
- Gli incaricati sono tenuti a mantenere ordinata l'area di lavoro; non possono essere consumati cibi e bevande in prossimità dei P.C.
- Gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- Gli incaricati che volessero installare nuovi software devono dare previa comunicazione al responsabile del sistema informatico interno che eseguirà direttamente le fasi di implementazione.
- Gli incaricati sono tenuti a fare una scansione con l'apposito antivirus di tutti i supporti di memorizzazione e lettura esterni (CD-rom, DVD, Floppy disk, Pen Drive, Zip).

Ogni incaricato può essere dotato di tre tipologie di password:

1. Bios
2. rete/sistema operativo
3. software applicativo

ogni password deve essere costituita da almeno 8 caratteri alfanumerici, oppure nel caso in cui lo strumento elettronico non lo permetta un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili all'incaricato; deve essere consegnata in busta chiusa al Responsabile della sicurezza dei dati (DSGA) e, infine, deve essere aggiornata ogni trimestre.

Gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento

MANUTENZIONE ORDINARIA INCARICATI

L'incaricati di ogni postazione informatico-amministrativa è tenuto a fare settimanalmente le seguenti operazioni:

- SCAN DISK, DEFRAG (deframmentazione disco fisso) e PULITURA DISCO FISSO.
- AGGIORNAMENTO DELL'ANTIVIRUS
- SCANSIONE DELL'INTERO SISTEMA CON L'ANTIVIRUS