



Liceo - "Pietro Siciliani"  
Via di Leuca, 2/L - 73100 LECCE ☎ 0832-246023-246020-305664  
E-mail:LEPM01000Q@istruzione.it

Prot. N. 7378/CI

02.09.2015

AI DOCENTI  
AL PERSONALE ATA  
AL DSGA

ALL'ALBO

**Oggetto: ISTRUZIONE PER MINIMIZZARE I RISCHI DA VIRUS**  
**decreto legislativo 30 giugno 2003, n° 196**

---

#### IL DIRIGENTE SCOLASTICO

in qualità di Titolare del Trattamento dei dati Personali, in accordo con la D.S.G.A. Iolanda Quarta, Responsabile della Gestione e Manutenzione degli Strumenti Elettronici, con il presente documento intende fornire le principali direttive che tutti devono rispettare per minimizzare il rischio di intrusione di virus informatici nelle strutture informatiche messe a disposizione dall'Istituto Scolastico per le attività lavorative assegnate.

Per minimizzare il rischio da virus informatici, è fondamentale che gli utilizzatori dei PC adottino le seguenti regole:

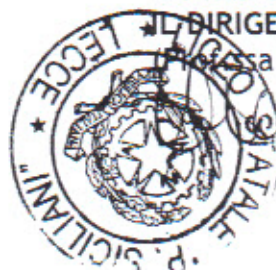
	REGOLE	DESTINATARI
1	Limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS	Tutti
2	Controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti	Tutti
3	Evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento	Tutti

*h*

4	Non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti")	Tutti
5	Non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta (potrebbe essere falso e portare a un sito truffa)	Tutti
6	Non utilizzare le chat	Tutti
7	Seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto)	Tutti
8	Avvisare il Responsabile della Gestione e manutenzione degli strumenti elettronici nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema)	Tutti
9	Disattivare o limitare il download dei file per gli utenti del browser Internet Explorer;	Responsabile della Gestione e manutenzione degli strumenti elettronici
10	Attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail;	Responsabile della Gestione e manutenzione degli strumenti elettronici

REGOLE		DESTINATARI
11	Conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge	Responsabile della Gestione e manutenzione degli strumenti elettronici
12	Conservare la copia originale del sistema operativo e la copia di backup consentita per legge	Responsabile della Gestione e manutenzione degli strumenti elettronici
13	Conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore)	Responsabile della Gestione e manutenzione degli strumenti elettronici
14	Consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate	Tutti

Il titolare del trattamento  
 IL DIRIGENTE SCOLASTICO  
 Prof.ssa Vittoria ITALIANO)



*[Handwritten signature]*