- La possibilità di individuare e rimuovere virus in assenza di comandi utente, possibilità di esecuzione ad intervalli regolari.
- L'impossibilità per l'utente di cambiare la configurazione del programma a meno che non disponga dell'apposita password.
- La possibilità di fornire reporting su rete, aggiornare il file di log ad ogni esecuzione con l'indicazione dell'identificativo della workstation.
- La possibilità di produrre certificazioni esterne per integrità.
- La capacità di fornire chiare indicazioni sul proprio corretto funzionamento. Questa caratteristica è di fondamentale importanza, in quanto la consapevolezza del funzionamento di un anti virus, si ha solo al momento della scoperta del virus stesso.
- Il programma anti virus deve disporre di un metodo di auto validazione dopo l'installazione che fornisca l'assoluta certezza di funzionalità e non contaminazione.
- La possibilità di personalizzare i messaggi verso l'utente: la messaggistica all'utente riveste un ruolo di primaria importanza in quanto le operazioni da effettuare, una volta scoperto il virus, sono diverse. Come informativa minima, deve essere prodotto un rapporto sui rischi connessi al tipo di virus individuato, lo stato di avanzamento dell'infezione, le istruzioni per la rimozione e debbono essere date chiare indicazioni sulla necessità o meno di un immediato fermo macchina.

6. GESTIONE DEI SUPPORTI

L'Amministrazione deve assicurare che tutti i supporti informatici e cartacei vengano gestiti nel rispetto cosciente del bene aziendale (informazione) ivi contenuto e in ottemperanza ai dettati della legge sulla privacy e della gestione degli incidenti e delle emergenze.

Deve essere tenuto in considerazione dagli addetti, in sede di sviluppo delle applicazioni, il tema del "back-up" su supporto elettronico, predisponendo le applicazioni stesse in modo da essere trasportabili in caso di disastro o facilmente ripristinabili in fase d'emergenza.