5.2.7 Documentazione

Valgono i principi generali introdotti nel paragrafo [rif. 5.1.5].

5.2.8 Logging

Valgono i principi generali introdotti nel paragrafo [rif.5.1.6].

5.2.9 Antivirus

Prevenzione e individuazione di codice malevolo sul sistema operativo	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, causata da Malware. - Negazione dei servizi causata da Malware. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Su sistemi sia client sia server è necessario installare un software antivirus e antimalware di riconosciuta efficacia, in grado di rilevare e rimuovere keylogger, spyware, trojans, worms, ransomware ed ogni altro tipo di malware conosciuto. I sistemi devono essere configurati in modo che l'antivirus/antimalware: - sia eseguito in modo automatico all'avvio della macchina senza possibilità di disattivazione da parte di utenti non autorizzati; - esegua in automatico l'aggiornamento della lista di definizione dei virus (DAT) anche più volte al giorno mediante un'infrastruttura di sistemi dedicati alla distribuzione del DAT; - esegua una scansione approfondita del disco fisso almeno una volta alla settimana, in orari che riducano l'impatto sulle attività lavorative (ad es. durante la pausa pranzo); - esegua una scansione anche dei file compressi fino a 3 livelli di nidificazione; - preveda una gestione remota per la segnalazione di infezioni virali; - abbia funzionalità di tipo euristico per la rilevazione dei virus che consenta di inserire in "quarantena" tutti i file ritenuti sospetti dal motore euristico; - si integri nel sistema operativo al livello di file system e nel software di gestione della posta; - notifichi, durante la fase di shutdown, se è presente un dispositivo removibile. L'amministratore di sistema deve verificare (e se necessario effettuare manualmente) l'effettivo aggiornamento dei sistemi anti-virus con cadenza almeno mensile.

5.2.10 Procedure

Alle linee guida 'Procedure generali' (Change management, Maintenance, Patching, Secure testing, Disposal) introdotti nel paragrafo [rif. 5.1.7], si aggiungono, per l'ambito specifico, le indicazioni di cui di seguito:

Controlli sulla regolamentazione dell'uso del codice mobile per Sistemi Operativi	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, causata da Malware. - Negazione dei servizi causata da Malware. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Nel caso in cui si utilizzi "mobile code" (ad es. JavaScript / VBScript scaricati da siti web, Java applets, controlli ActiveX, codice Adobe Flash o Shockwave, documenti PDF attivi