5.6.3 Strumenti

Compilatori, editor ed altri strumenti di sviluppo non devono essere presenti nei sistemi di produzione in cui l'applicazione risiede.

5.6.4 Profili utente

I profili utente dell'applicazione che risiede nei sistemi di produzione devono essere differenti da quelli configurati e utilizzati nei sistemi di sviluppo e test. L'applicazione deve implementare un meccanismo di avviso della tipologia di profilatura, ruoli e permessi assegnati all'utente a seguito dell'accesso (vedasi per maggior dettaglio "Procedura di accesso dell'applicazione" Cfr. [paragrafo 5.7.3]).

5.6.5 Trattamento dei dati

I dati personali e critici, gestiti dall'applicazione, che risiedono nell'ambiente di esercizio, non devono essere copiati negli ambienti di test e sviluppo. In caso di utilizzo dell'applicazione al solo fine di test questi devono essere rimossi immediatamente dopo il completamento di detta fase.

5.6.6 Protezione dei sorgenti e delle librerie

I sorgenti dell'applicazione e delle librerie correlate, fatta eccezione per i linguaggi interpretati, non devono risiedere in testo chiaro all'interno dei sistemi di esercizio, bensì sotto forma di oggetti compilati. Nel caso di linguaggi interpretati, il sorgente dell'applicazione che risiede nei sistemi di esercizio deve essere offuscato.
Una copia non offuscata deve comunque sempre essere conservata su un supporto diverso (esempio copia su CD o DVD).

5.7 Autenticazione, Autorizzazione e Gestione degli accessi

Per le politiche degli accessi si raccomanda l'adozione dei criteri riportati di seguito.

5.7.1 Policy standard "Everything is generally forbidden unless expressly permitted"

L'applicazione deve implementare un meccanismo di access control adeguato. Tutte le operazioni svolte dagli utenti e le fasi di autorizzazione e assegnazione dei permessi devono essere subordinate alla policy standard : "Ogni azione è negata se non espressamente consentita".

5.7.2 Assegnazione dei privilegi utente

L'applicazione non deve assegnare alcun privilegio/permesso all'utente fin quando il processo di autenticazione e autorizzazione non è stato completato.

5.7.3 Procedura di accesso dell'applicazione

La procedura di accesso e log-on dell'applicazione deve ridurre al minimo le informazioni fornite agli utenti non ancora autenticati e prevedere determinati comportamenti. In particolare:

- Non deve con messaggi specifici fornire alcun tipo di aiuto, né rendere comprensibile se il processo di autenticazione è fallito a causa del nome utente o della password errata;
- Non deve fornire alcuna chiara indicazione sui ruoli e sui permessi assegnati a un utente fin quando il processo di autenticazione non viene completato;
- Deve visualizzare un messaggio di avviso sulle sanzioni derivate dall'accesso fraudolento all'applicazione;
- Deve prevedere il mascheramento della password digitata dall'utente non rendendola visibile o nascondendola attraverso simboli (ad esempio con asterischi);
- Non deve trasmettere in rete la password in chiaro;
- Deve "processare" le informazioni fornite dall'utente per l'accesso solo quando sono complete;
- Deve prevedere procedure configurabili di blocco momentaneo dell'account dopo una serie di tentativi d'accesso infruttuosi;