Presentazione di messaggi di avvertimento	
Minaccia	Accesso non autorizzato ad informazioni causato dal personale utente per inadeguati meccanismi, strumenti, procedure o abilità tecniche atti a prevenire l'accesso non autorizzato al sistema o a proteggere i dati di autenticazione quando memorizzati o trasmessi.
Contromisure	Includere nella schermata di log-on l'avvertimento che l'accesso è consentito ai soli utenti autorizzati. Richiamare nella schermata le norme interne o di legge che verrebbero violate in caso di accesso non autorizzato e le relative sanzioni. Informare chi si accinge ad accedere al sistema che le attività saranno monitorate e che ogni accesso non autorizzato ed ogni abuso saranno perseguiti a norma di legge.

Sincronizzazione degli orologi	
Minaccia	- Accesso non autorizzato al sistema (macchina, configurazione, ecc.). - Abuso di privilegi da parte degli utenti.
Contromisure	Sincronizzare l'orologio interno di tutti i sistemi e gli apparati di rete attraverso il protocollo NTP con un server "fidato" posizionato sulla propria intranet. Laddove tecnicamente possibile (sistemi UNIX e apparati di rete evoluti) abilitare l'autenticazione verso il server NTP. Laddove tecnicamente realizzabile, il server NTP deve a sua volta ottenere l'ora esatta attraverso un segnale radio proveniente da stazione terrestre o satellitare (GPS). Per le reti di piccole dimensioni, laddove non sia possibile avere un server NTP proprio, utilizzare comunque un server NTP "fidato" unico per tutti i sistemi, come ad es. quello dell'Istituto Nazionale di Ricerca Metrologica (INRIM) (ex Istituto Elettrotecnico Nazionale Galileo Ferraris).

5.2.3 Utenze

Accesso privilegiato nominativo	
Minaccia	- Abuso di privilegi da parte degli utenti. - Abuso di risorse. - Accesso non autorizzato alle informazioni. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
Contromisure	Disabilitare la possibilità di accesso ai sistemi (locale o remoto) utilizzando utenze amministrative impersonali come "root" o "Administrator". Gli amministratori devono accedere con utenze nominative abilitate ai rispettivi compiti (ad es. abilitate all'uso del comando "su" su Unix, o appartenenti al gruppo Administrators su Windows).

Valgono inoltre i principi generali già introdotti nel paragrafo [rif. 5.1.1].

5.2.4 Autenticazione

Ai principi generali introdotti nel paragrafo [rif. 5.1.2], si aggiungono le indicazioni, di cui di seguito:

Identificazione e autenticazione degli utenti a livello di sistema	
Minaccia	- Abuso di privilegi da parte dell'utente. - Accesso non autorizzato alle informazioni. - Falsificazione di identità.