	- Tentativi di frode. - Uso non autorizzato di privilegi.
Contromisure	Richiedere l'autenticazione per svolgere qualsiasi tipo di attività di rilievo (compreso lo shutdown del sistema). Utilizzare tecniche di identificazione e autenticazione a due fattori, ad es. basate su pin e token o su pin e impronta biometrica, non solo per l'accesso amministrativo a sistemi critici ed apparati di rete e di sicurezza, ma anche per l'accesso ad applicativi che trattano dati personali sensibili, dati di traffico telematico e telefonico, dati bancari.

5.2.5 Autorizzazione

Ai principi generali introdotti nel paragrafo [rif. 5.1.3], si aggiungono le indicazioni, di cui di seguito:

Gestione delle informazioni segrete di autenticazione degli utenti	
Minaccia	- Perdita di riservatezza delle informazioni. - Furto di credenziali di autenticazione. - Falsificazione di identità.
Contromisure	Per i file contenenti le password e altre informazioni riservate relative agli account utente, valgono le seguenti restrizioni: - Possono essere salvati solo su file system che supportano meccanismi di controllo accessi a livello di singolo utente. - Devono essere protetti con diritti di accesso il più possibile restrittivi. - Devono contenere le password in formato hashed (non invertibile) protetto con un codice ("salt") e non tramite crittografia reversibile. L'hash non deve essere basato su MD5, né SHA-1. Preferibilmente deve essere usato l'algoritmo SHA-2 512. Questa impostazione ad es. è possibile per il file delle password sui moderni sistemi operativi UNIX-like e Linux.

Autorizzazioni basate sui ruoli	
Minaccia	Perdita di riservatezza delle informazioni
Contromisure	Per le informazioni di autorizzazione valgono le seguenti regole: - Utilizzare meccanismi autorizzazione di sistema e applicativa basata sui ruoli per garantire che solo gli utenti con il livello appropriato di autorizzazione siano autorizzati ad accedere a dati sensibili e che tali autorizzazioni discendano da un ruolo organizzativo e non da una abilitazione "ad hoc" che è spesso sinonimo di eccezione non tracciata e non autorizzata formalmente. - Utilizzare la protezione basata sui ruoli con il massimo livello possibile di granularità, per distinguere tra utenti che possono creare, visualizzare, aggiornare e cancellare dati, distinguendo anche tra le diverse tipologie di dati e di funzionalità applicative. - A livello di sistema, utilizzare ruoli distinti per diversi compiti amministrativi come il backup, l'esecuzione di applicativi, l'avvio di specifici servizi di rete, la configurazione dell'audit e la visualizzazione dei log, ecc.

5.2.6 Crittografia

Valgono i principi generali introdotti nel paragrafo [rif. 5.1.4].