	- una registrazione di tutti i privilegi assegnati; - i requisiti per la scadenza dei diritti; - riesame regolare delle competenze degli utenti; - per le UserId amministrative generiche (da evitare se non indispensabile per l'esecuzione del servizio), dovrebbe essere mantenuta la riservatezza delle informazioni segrete di autenticazione quando questa è condivisa.

Riesame dei diritti di accesso degli utenti	
Minaccia	- Accesso non autorizzato alle informazioni. - Abuso di privilegi da parte dell'utente.
Contromisure	I diritti di accesso degli utenti dovrebbero essere riesaminati regolarmente (al massimo ogni sei mesi) e dopo ogni cambiamento (es. cessazione del rapporto di lavoro, cambio di ruolo, di mansione, all'interno dell'organizzazione). Le autorizzazioni per i diritti di accesso privilegiati dovrebbero essere riesaminate ad intervalli più frequenti e gli eventuali cambiamenti tracciati. Per ogni cambiamento di privilegi deve esserne registrato il richiedente, l'approvatore e la motivazione. In caso di cessazione del rapporto di lavoro, sia di personale interno sia esterno, è necessario verificare i requisiti per la rimozione, o sospensione dei diritti di accesso al sistema/piattaforma. Tali diritti dovrebbero essere ridotti o rimossi prima della cessazione o della variazione del rapporto di lavoro, a seconda della valutazione di fattori di rischio come: - criticità delle informazioni cui si accedeva; - ruolo della persona, - motivazione della cessazione/cambiamento. Prevedere controlli o misure di sicurezza per limitare il rischio che: - in caso di licenziamento o fine contratto, dei dipendenti scontenti o degli utenti di terze parti esterne possano deliberatamente corrompere informazioni o commettere illeciti; - in caso di persone dimissionarie o in uscita, esse possano essere tentate di recuperare/copiare informazioni per uso futuro.

Utenze tecniche

Protezione delle informazioni strumentali all'accesso	
Minaccia	- Divulgazione di informazioni riservate. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Furto di credenziali di autenticazione.
Contromisure	- Utilizzare ACL forti per proteggere le risorse di sistema. - Utilizzare algoritmi standard di crittografia per memorizzare i dati sensibili nei file di configurazione (utenze tecniche, non legate a persone fisiche: processi di sistema, porzioni di DB, ecc.). - Utilizzare algoritmi di comprovata robustezza come. Ad esempio AES, l'algoritmo simmetrico ritenuto al momento più sicuro, consente di scegliere una chiave crittografica di 128, 192 o 256 bit. La scelta della lunghezza della chiave crittografica deve essere commisurata al tipo di algoritmo e al livello di riservatezza delle informazioni da proteggere. Per quanto riguarda AES, anche la chiave a 128 bit è considerata sicura. Algoritmi asimmetrici come RSA richiedono chaivi crittografiche più lunghe. Nel caso di RSA la lunghezza ad oggi considerata sicura e raccomandata dal NIST è 2048.