Terze parti

Identificazione dei requisiti di sicurezza per l'accesso di fornitori/clienti ad informazioni o beni aziendali	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, ad opera di soggetti esterni.
Contromisure	Devono essere considerati e identificati tutti i requisiti di sicurezza prima di concedere ai partners, fornitori/clienti, anche in fase di trattativa, l'accesso a informazioni o beni dell'organizzazione ospitati nel sistema/piattaforma. Effettuare un'analisi dei rischi per valutare l'impatto sul business aziendale (a livello economico, d'immagine, di continuità operativa, eccetera) nel caso di violazioni della sicurezza, divulgazione non autorizzata (es. a concorrenti), illecito trattamento delle informazioni, effettuati da tali soggetti che accedono ad informazioni.

Identificazione dei requisiti di sicurezza negli accordi con i fornitori/clienti	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, ad opera di soggetti esterni.
Contromisure	Gli accordi con terze parti che prevedono accesso, elaborazione, comunicazione, aggiunte o, in generale, gestione delle informazioni ospitate nel sistema/piattaforma dell'organizzazione, devono considerare tutti i requisiti di sicurezza pertinenti. Prevedere, in particolare, misure preventive per evitare violazioni o illeciti delle terze parti nella gestione delle informazioni. Definire con precisione le attività, le modalità, le responsabilità e la periodicità, per l'esercizio di diritti di audit o comunque di verifiche sull'attività dei fornitori/clienti. Gli accessi logici privilegiati da parte di soggetti esterni devono essere subordinati alla nomina di tali soggetti ad amministratori di sistema, e tale nomina deve essere a sua volta legata ad uno specifico contratto con la ditta di appartenenza comprendente accordi di riservatezza e regole per il corretto uso delle risorse informatiche vincolanti per il fornitore e per i suoi dipendenti. Ovviamente gli accessi logici devono essere monitorati da parte di fornitori devono essere completamente monitorati. In ogni caso gli accessi privilegiati da parte di soggetti esterni non devono mai avvenire da sedi esterne (es. sede fornitore).

5.1.2 Autenticazione

Gestione delle informazioni segrete di autenticazione degli utenti	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	L'assegnazione agli utenti delle informazioni segrete di autenticazione (es. password) deve essere controllata attraverso un processo di gestione. Il processo dovrebbe prevedere: - l'uso di user ID e password individuali per sostenere il principio di accountability; - le modalità di assegnazione temporanea delle informazioni segrete di autenticazione, da cambiare al primo uso; - procedure per verificare l'identità di un utente, prima di fornire, modificare o sostituire nuove informazioni; - le modalità per assicurare il rispetto dell'utente della riservatezza delle informazioni segrete di autenticazione. Per quest'ultimo punto l'organizzazione dovrebbe informare l'utente delle sue responsabilità ed acquisire dallo stesso un formale impegno a mantenere riservate le informazioni (ad es. mediante specifica lettera da sottoscrivere).