	apparecchiature in manutenzione, tenendo anche conto se tale manutenzione è fatta da personale in sito o all'esterno dell'organizzazione; - ove necessario, si dovrebbero eliminare le informazioni critiche dall'apparecchiatura oppure il personale di manutenzione dovrebbe essere sufficientemente selezionato;

Patching

Controllo di vulnerabilità tecniche	
Minaccia	- Abuso di risorse. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Crittografia debole o non validata. - Divulgazione di informazioni riservate. - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Ottenere tempestive informazioni sulle vulnerabilità tecniche dei sistemi di informazione in uso, valutare l'esposizione dell'azienda a tali vulnerabilità e prendere appropriate misure per indicare il rischio associato. A tale scopo è necessario mantenere un inventario aggiornato e completo dei beni quali il rivenditore del software, il numero della versione, i software installati e i sistemi su cui sono installati, e i referenti interni all'azienda responsabili del software. In particolare è necessario: - definire i ruoli e le responsabilità per la gestione delle vulnerabilità tecniche; - definire i mezzi di informazione che saranno usati per identificare le vulnerabilità tecniche; - identificare i rischi associati e le azioni da intraprendere una volta che una potenziale vulnerabilità tecnica è stata identificata; - gestire le patch disponibili valutando anche i rischi associati alla loro installazione; - controllare il processo di gestione delle vulnerabilità tecniche e valutare la sua efficacia ed efficienza.

Software Patching	
Minaccia	- Abuso di risorse. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Crittografia debole o non validata. - Divulgazione di informazioni riservate. - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Verificare che sia applicata una procedura di gestione delle patch composto almeno