5.3.5 Procedure

Alle linee guida 'Procedure generali' (Change management, Maintenance, Patching, Secure testing, Disposal) introdotti nel paragrafo [rif. 5.1.7], si aggiungono, per l'ambito specifico, le indicazioni di cui di seguito:

Patching	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Cancellazione o furto di informazioni (ad es. da ransomware, ecc.). - Compromissione delle comunicazioni. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware) - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	È necessario controllare periodicamente il sito web del fornitore per gli aggiornamenti. A tal fine si fa notare che: - Alcuni browser controllano automaticamente gli aggiornamenti disponibili - Alcuni fornitori offrono la notifica automatica degli aggiornamenti tramite una mailing list.

Sensibilizzare il personale sui rischi che la navigazione in Internet via Browser comporta	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	Sensibilizzare il personale sui rischi che la navigazione in Internet via Browser comporta. Di seguito le principali norme comportamentali da seguire: - Non fare clic su collegamenti senza considerare i rischi che ne potrebbero derivare (evitare di cliccare su link sospetti presenti nelle pagine). - Prestare attenzione al fatto che gli indirizzi di pagine Web potrebbero essere mascherati e portare in un sito imprevisto. - Considerare che ogni volta che un sito web richiede che vengano abilitate determinate funzionalità o installati software e aggiornamenti, si mette a rischio il computer. Ad es. non aggiornare mail il Flash Player su richiesta di una pagina web ma solo da pannello di controllo. - Non riutilizzare la stessa password per siti diversi. - Non fornire mai online informazioni personali a meno di non essere certi che il sito sia valido e le transazioni sicure: prima di inserire qualsiasi informazione personale, controllare la barra degli URL del browser al fine di accertarsi che il sito sia quello atteso e che sia presente la dicitura "https:" e un'icona a forma di lucchetto ad indicare che la connessione al sito è protetta e che il certificato server è valido. - Evitare Wi-Fi pubblici o gratuiti: l'attaccante spesso utilizza sniffers wireless per rubare le informazioni degli utenti quando vengono inviate su reti non protette. Il modo migliore per proteggersi da questo attacco è evitare di utilizzare queste reti, oppure utilizzarle solo con una VPN che incapsuli tutto il traffico in un tunnel cifrato. - In caso di individuazione di una "falsa" pagina di autenticazione segnalarla al team di sicurezza interna all'organizzazione per procedere all'oscuramento della medesima e possibilmente all'individuazione dei responsabili.