5.4.3 Utenze

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1].

5.4.4 Autenticazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.2].

5.4.5 Autorizzazione

Valgono i principi generali già introdotti nel paragrafo [rif.5.1.3].

5.4.6 Crittografia

Ai principi generali introdotti nel paragrafo [rif. 5.1.1.4], si aggiungono le indicazioni, di cui di seguito:

Crittografia	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	Per l'accesso ai dati critici o sensibili definire requisiti di sicurezza più stringenti applicando tecniche di cifratura o altri meccanismi di sicurezza per rafforzare la protezione dagli accessi non autorizzati.

5.4.7 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1.5].

5.4.8 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1.6].

5.4.9 Procedure

Ai principi generali introdotti nel paragrafo [rif. 5.1.7], si aggiungono le indicazioni, di cui di seguito:

Politica per la gestione delle postazioni di lavoro	
Minaccia	- Abuso di privilegi da parte dell'utente. - Abuso di risorse. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Danneggiamento, perdita o furto di un asset fisico. - Uso non autorizzato di privilegi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.) - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Verificare l'esistenza e l'applicazione di una formale politica di sicurezza che specifichi dei principi e delle linee guida per il corretto utilizzo delle postazioni di lavoro (workstation, desktop, notebook) da parte degli utenti, al fine di garantire la salvaguardia dell'informazione aziendale. Tale politica di sicurezza deve, nel rispetto della politica di sicurezza generale dell'azienda, specificare: - i requisiti di sicurezza fisica da soddisfare durante l'utilizzo dei dispositivi (ad

	esempio, il corretto posizionamento delle PdL); - i requisiti relativi alla corretta gestione della password, al backup, alla protezione contro i virus, alla configurazione del sistema operativo e delle applicazioni; - gli utilizzi non consentiti, estranei agli incarichi lavorativi, della propria postazione di lavoro; - i requisiti relativi al riutilizzo o alla rottamazione della PdL; - i requisiti relativi alla restituzione della PdL in caso di cessazione del rapporto di lavoro e/o cambio mansione. Eseguire delle attività di controllo e degli audit periodici sull'utilizzo della PdL da parte degli utenti, anche tramite tecnologie di controllo compatibili con quanto disposto dalle norme di legge.

Misure tecniche di garanzia di effettiva cancellazione dei dati o di loro non intellegibilità in caso di reimpiego o riciclo dell'apparecchiatura elettronica	
Minaccia	Accesso non autorizzato alle informazioni / ai dati personali contenuti in apparecchiature elettroniche dismesse.
Contromisure	Adottare misure tecniche che garantiscano la non intellegibilità dei dati o l'effettiva cancellazione. Le prime possono consistere, tra l'altro, nella cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. La cancellazione sicura delle informazioni, è ottenibile mediante misure tecniche consistenti in: - utilizzo di programmi informatici (quali wiping program o file shredder); - demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici); - distruzione fisica dei dispositivi di memoria dismessi.

Politica di protezione da accesso fisico non autorizzato	
Minaccia	- Accesso non autorizzato alle informazioni. - Danneggiamento, perdita o furto di un asset fisico. - Violazione della sicurezza (riservatezza, integrità, disponibilità) delle informazioni.
Contromisure	Deve essere adottata una politica di sospensione della sessione per inattività su PC e notebook che preveda almeno che i terminali: - non debbano essere lasciati incustoditi durante e fuori orario di lavoro; - siano protetti da accessi non autorizzati con la sospensione della sessione mediante un salva-schermo che richieda l'autenticazione per continuare. Le informazioni critiche, riportate su carta o su supporti informatici e i dispositivi critici quando non utilizzati, dovrebbero essere chiusi a chiave (in cassaforte o armadio o altri mobili con caratteristiche di sicurezza) soprattutto quando l'ufficio è vuoto. Devono essere adottate regole e accorgimenti per evitare il danneggiamento/ distruzione delle apparecchiature.

Sensibilizzazione del personale sui rischi di divulgazione di informazioni riservate	
Minaccia	- Divulgazione di informazioni riservate (codici di accesso). - Furto di credenziali di autenticazione.
Contromisure	Effettuare opere di sensibilizzazione nei confronti del personale perché non divulghi a terze parti informazioni riservate o critiche quali, ad esempio, dati personali e password.