	in una apposita sezione di rete.

Continuità elettrica delle PdL	
Minaccia	Negazione dei servizi - Black out elettrico o mancanza improvvisa di energia elettrica
Contromisure	Verificare che sia garantita l'alimentazione delle PdL in caso di interruzione della corrente elettrica, tramite l'utilizzo di dispositivi UPS che garantiscano anche la protezione dalle sovratensioni, prevedendo uno shutdown automatico allo scadere del periodo di autonomia dell'UPS. Effettuare un monitoraggio delle batterie degli UPS e prevederne la sostituzione qualora si ravvisi un degrado della loro capacità.

Protezione fisica dei dispositivi (fissi e mobili)	
Minaccia	- Cancellazione o furto di informazioni. - Danneggiamento, perdita o furto di un asset fisico. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Assicurare un cavo di acciaio galvanizzato, non meno di 3,5 mm di spessore, munito di chiusura a chiave o a combinazione al computer da proteggere o, in alternativa, utilizzare delle gabbie di sicurezza facilmente ancorabili, in cui riporre i dispositivi. Accertare che il cavo sia assicurato ad un elemento fisso non smontabile, facendone passare un'estremità nell'occhiello posto ad un capo del cavo ed inserire il lucchetto di sicurezza nell'apposito foro presente nel computer.

5.4.2 Hardening

Hardening del sistema operativo installato sulla PDL	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Eseguire l'hardening del sistema operativo che gira sulla PDL [rif. 5.2.2].

Hardening del/i web browser/s installato/i sulla PDL	
Minaccia	- Accesso non autorizzato alle informazioni. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware)
Contromisure	I principi per la sicurezza del web browser sono oggetto di un paragrafo precedente. Effettuare controlli periodici al fine di verificare che i browser installati sulle PdL siano effettivamente quelli autorizzati e con le configurazioni di sicurezza previste (es. funzionalità di blocco dei popup, degli script, ecc.).

Hardening del sistema	
Minaccia	Negazione dei servizi (per spam su sistemi di messaggistica).
Contromisure	Se è autorizzato l'uso di sistemi di messaggistica immediata, dotarsi di strumenti specifici "IM spam blockers".