

CRITICITÀ RILEVATE - CATANIA MULTISERVIZI SPA

Azioni da intraprendere

Risposta al rischio residuo

Contesto	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo	NOTE	Accettato	Ridotto	Evitato	Trasferito
Backup dei dati	Backup effettuato con frequenza almeno settimanale (alcune con cadenza giornaliera)	Adeguito	Medio	Revisionato con Referente IT (Spaccabit)	Criptografati, accessi controllati, report giornaliero con contestuale controllo eventuali anomalie, copia esterna su Cloud			
Gestione incidenti	Manutenzione	Adeguito	Medio	Revisionare con Referente ICT		Controllo Monitoraggio dei log		
Raccolta di log e monitoraggio	Monitoraggio almeno semestrale degli access log degli Amministratori di sistema / Autorizzati che svolgono tali funzioni	Parziale	Medio	Revisionare con Referente ICT			Formazione	
Sicurezza fisica	Antivirus, Firewall, Gruppo di continuità, manutenzione e controllo dei Server	Adeguito	Basso	Revisionato con Referente IT (Spaccabit)	Sistemi efficaci pe salvaguardare gli "accessi" esterni			
Sicurezza Data Center	Manutenzione e controlli costanti	Adeguito	Basso	Revisionato con Referente IT (Spaccabit)	Assistenza e manutenzione costante			
Sicurezza della rete	Test degli aggiornamenti o modifiche evolutive	Adeguito	Basso	Revisionato con Referente IT (Spaccabit)	Test effettuati con cadenza mensile/bimestrale			
Sicurezza degli applicativi	Sicurezza degli Uffici, Backup	Adeguito	Basso	Revisionato con Referente IT (Spaccabit)	Controllo effettuato			
Sicurezza logica	Antivirus / Firewall Penetration test, Backup, Policy Data Breach	Parziale	Medio	Revisionato con Referente IT (Spaccabit)		Previsto un report sulla rete "interna"		