Modulo E: Sicurezza Perimetrale, Firewall e Gateway Email

(es. LibraCyber, prima LibraEsva)

Le presenti condizioni si applicano alla fornitura, configurazione e gestione di servizi di sicurezza informatica, inclusi, a titolo esemplificativo, firewall hardware o software e sistemi di filtraggio del traffico di posta elettronica (Gateway Antispam/Antimalware).

- **Efficacia dei Sistemi e Minacce Inedite (Zero-Day):** i sistemi di protezione perimetrale e di filtraggio operano mediante tecniche, regole, firme, analisi euristiche e altri meccanismi di rilevazione propri delle tecnologie utilizzate. Il Fornitore configura e gestisce tali sistemi secondo il perimetro del servizio concordato, ma non può garantire un'efficacia di blocco o intercettazione pari al 100%, in particolare rispetto a minacce non ancora note o classificate, attacchi mirati, vulnerabilità zero-day o nuove varianti di malware e ransomware.
- **Falsi Positivi e Quarantena:** i sistemi antispam e antimalware possono occasionalmente classificare come indesiderate o sospette comunicazioni legittime. Quando il servizio prevede report periodici, quarantena o pannelli di gestione, il Cliente è tenuto a verificarli con regolarità e a segnalare eventuali anomalie. Il Fornitore gestisce i sistemi di filtraggio secondo le configurazioni concordate; eventuali responsabilità relative alla mancata, ritardata o errata consegna di comunicazioni elettroniche restano disciplinate dalle Condizioni Generali e dal perimetro del servizio sottoscritto.
- **Sicurezza degli Endpoint:** l'adozione di un gateway email o di un firewall perimetrale non sostituisce le misure di sicurezza necessarie sui dispositivi e sui sistemi del Cliente. Salvo che tali attività siano espressamente comprese nel servizio, resta a carico del Cliente assicurare l'adozione, il mantenimento e l'aggiornamento di adeguate misure di protezione sugli endpoint, quali antivirus, EDR o strumenti equivalenti, in funzione del proprio contesto operativo e del livello di rischio.