

### Dati identificativi

- Organizzazione: SAMTEL NETWORK SRL
- Sede verificata: Via Roma 5, 84060 Perdifumo (SA) / sito operativo indicato in audit.
- Contesto: ISP territoriale, FTTH/FWA, servizi mobile, gestione rete, assistenza clienti e dati cliente.
- Codice evidenza: EV-39

### Finalita dell evidenza

Dimostrare controllo delle vulnerabilita su sistemi, apparati, workstation e servizi utilizzati.

### Clausole e riferimenti

ISO/IEC 27001:2022 - A.8.8, A.8.9, A.8.16

### Evidenze oggettive considerate

Registro vulnerability, update log, configurazioni, evidenze IT, SoA.

### Note operative e valutazione senior

- Il processo identifica vulnerabilita note, aggiornamenti, patch critiche, firmware apparati e prioritari di remediation.
- Le vulnerabilita sono valutate in funzione di esposizione, criticita asset, impatto su servizio e probabilita di sfruttamento.
- Le azioni di correzione sono pianificate e tracciate, con verifica successiva.
- Per apparati ISP e FWA la gestione patch deve essere bilanciata con continuita del servizio e finestre operative.

### Presidio / azione richiesta

Mantenere registro mensile vulnerabilita/patch con stato, eccezioni motivate e verifica post-aggiornamento.

### Registrazioni minime attese

Patch log; vulnerability register; firmware list; ticket change

### Stato di controllo

- Esito atteso: evidenza coerente con Stage 2 e utilizzabile per follow-up.
- Stato documento: fac-simile operativo da validare, datare e approvare internamente.
- Responsabile: Direzione / Referente SGQ-SGSI / funzione tecnica competente.
- Frequenza riesame: annuale, a seguito di incidente o a seguito di cambiamenti significativi.
- Rilievi collegati: KPI 9.1, incident management A.5.24, logging A.8.15, azioni correttive 10.2 ove pertinente.