CINQUE CONTROLLI PER LA SMART HOME

Scheda privata di verifica · edizione 11 novembre 2026

Scopo: raccogliere informazioni verificabili relative ai tuoi dispositivi. Non è una certificazione di sicurezza, non è un audit né una consulenza. Conserva questa scheda in privato, non allegarla integralmente ai commenti del video e non scrivere password o dati sensibili.

Data della verifica: _____ Categoria dispositivo: _____

Produttore e modello (facoltativi): _____

Indicazioni di esito: **CONFERMATO** = evidenza pertinente trovata; **DA CORREGGERE** = elemento da rivedere; **NON VERIFICABILE** = informazioni insufficienti o prova non appropriata.

1. Supporto e aggiornamenti

Domanda: fino a quando riceverò correzioni di sicurezza? Versione firmware nota?

Esito: ☐ Confermato ☐ Da correggere ☐ Non verificabile

Fonte o evidenza (sito ufficiale / nota del produttore): _____

Azione successiva e data: _____

2. Accessi remoti e account

Domanda: so chi può entrare da app/cloud? MFA e condivisioni sono verificate?

Esito: ☐ Confermato ☐ Da correggere ☐ Non verificabile

Evidenza non sensibile (non trascrivere credenziali): _____

Azione successiva e data: _____

3. Rete e isolamento

Domanda: i dispositivi IoT hanno regole di accesso appropriate verso computer e file personali?

Esito: ☐ Confermato ☐ Da correggere ☐ Non verificabile

Evidenza (documentazione router e impostazione): _____

Azione successiva e data: _____

4. Dipendenza da Internet e cloud

Domanda: il dispositivo non critico può funzionare con sola rete locale? Esiste un comando manuale?

Esito: ☐ Confermato ☐ Da correggere ☐ Non verificabile

Evidenza (condizioni del test sicuro / istruzioni): _____

Azione successiva e data: _____

5. Privacy, dati e dismissione

Domanda: so dove sono i dati, per quanto vengono conservati e come posso cancellarli?

Esito: ☐ Confermato ☐ Da correggere ☐ Non verificabile

Evidenza (privacy policy, app, manuale): _____

Azione successiva e data: _____

Regole di prudenza

- Non eseguire prove offline su serrature, allarmi, dispositivi medici o impianti critici.
- Un esito «confermato» riguarda soltanto la verifica specifica e non la sicurezza complessiva.
- Non condividere pubblicamente password, IP, SSID, seriali, link di accesso o riprese private.

L’articolo tecnico di accompagnamento e le fonti sono disponibili sul sito insieme al prospetto.

Guida ai ruoli: chi deve fare cosa?

Questo prospetto è un aiuto per l'utente, non un'attestazione di conformità del prodotto o del servizio. Le norme europee individuano destinatari diversi per obblighi diversi.

Soggetto	Che cosa verificare o gestire
Fabbricante	Sicurezza e gestione delle vulnerabilità del prodotto secondo gli obblighi applicabili; informazioni sul supporto e aggiornamenti.
Fornitore di servizi cloud	Protezione del servizio e, quando tratta dati personali, obblighi GDPR in base al ruolo effettivo.
Utilizzatore domestico	Installa le correzioni disponibili, protegge account e accessi, configura in modo prudente e rispetta i terzi.
Organizzazione interessata dalla NIS2	Obblighi di gestione del rischio per i soggetti individuati dalla normativa; non per ogni famiglia.

Esempio: un ripristino di fabbrica può cancellare dati sul dispositivo, ma non certifica la cancellazione delle registrazioni conservate nel cloud. Prima di cedere l'oggetto, rimuovilo dall'account e consulta la procedura del fornitore.

Nota: il GDPR normalmente esclude i trattamenti strettamente personali o domestici, ma la ripresa stabile di aree pubbliche può far uscire dal perimetro dell'esenzione. Il CRA ha scadenze e disposizioni transitorie; non equivale a obblighi generali per il consumatore. ETSI EN 303 645 è uno standard tecnico.

Guida esemplificativa, non esaustiva; l'applicabilità delle disposizioni dipende dai fatti e dai soggetti.