PROCEDURA OPERATIVA DI EMERGENZA (SOP)

Sicurezza Impianti Frigoriferi e Mitigazione Accessi Remoti Non Autorizzati

Codice: SOP-OT-042
Destinatari: Direttori Store / Capi Reparto Freschi
Revisione: 1.0 (Novembre 2026)

AVVISO DI CRITICITÀ OPERATIVA: A fronte delle intrusioni cibernetiche accertate sulla catena del freddo della GDO europea, i controllori di refrigerazione industriale e i banchi frigo non devono rimanere accessibili su reti aperte. Attuare immediatamente le misure sottostanti e registrarne l'esito.

CHECKLIST OPERATIVA DI BONIFICA E CONTROLLO

#	Ambito di Controllo	Istruzioni Operative Dettagliate	Verifica
01	**Censimento varchi di rete**	Mappare ogni gateway IoT, teleostato e centralina frigorifera. Verificare che nessun apparato abbia IP pubblico diretto accessibile via web.	☐ Eseguito
02	**Revoca credenziali default**	Modificare all'istante le password di fabbrica su tutti i pannelli e terminali (sostituire admin/admin, 1234, password costruttore).	☐ Eseguito
03	**Blocco software desktop remoto**	Disinstallare o disattivare dai PC di supervisione interna software non approvati (AnyDesk, TeamViewer, porte RDP/VNC non protette).	☐ Eseguito
04	**Regolazione accessi fornitori**	Revocare le connessioni h24 dei manutentori terzi. Gli accessi remoti devono essere autorizzati solo su richiesta ("Just-in-Time") e chiusi a fine intervento.	☐ Eseguito
05	**Isolamento di rete (VLAN)**	Richiedere a IT centrale la segregazione rigida: la rete degli impianti non deve comunicare con registratori di cassa, PC ufficio o Wi-Fi clienti.	☐ Eseguito
06	**Autenticazione a due fattori (MFA)**	Rendere obbligatoria l'autenticazione a più fattori per chiunque si colleghi al portale di monitoraggio o alla VPN aziendale.	☐ Eseguito
07	**Watchdog soglie di allarme**	Bloccare la sovrascrittura remota delle soglie termiche critiche (+4 °C fresco, -18 °C surgelati) e impedire sbrinamenti continui forzati via software.	☐ Eseguito
08	**Allarme out-of-band (GSM)**	Accertare il funzionamento di almeno una sonda autonoma con SIM GSM e batteria tampone per linea, non dipendente dalla connessione internet del punto vendita.	☐ Eseguito
09	**Controllo storico sbrinamenti**	Inserire nella routine di apertura/chiusura il controllo dei log notturni: allarmi disattivati o temperature anomale richiedono verifica immediata.	☐ Eseguito
10	**Disconnessione fisica d'emergenza**	Individuare e contrassegnare il cavo Ethernet/switch di collegamento della centrale alla rete. In caso di attacco in corso, scollegare fisicamente (Air-Gap).	☐ Eseguito

CONTATTI DI EMERGENZA E SEGNALAZIONE

Referente IT / Cybersecurity Aziendale:
Telefono H24: _____
Email Incidenti: _____

Ditta Manutenzione Frigorifera Reperibile:
Tecnico di Zona: _____
Centrale Operativa: _____