

# Analisi del contesto interno ed esterno e SWOT

|                 |                    |               |   |
|-----------------|--------------------|---------------|---|
| Organizzazione  | CWNET S.R.L.       | Sede          | Via Degli Oliveti 110, 54100 Massa (MS), Italia |
| Norma           | ISO/IEC 27001:2022 | Audit         | Audit Stage 2 - AR_01.2                         |
| Codice evidenza | EV-01              | Periodo audit | 15-17/04/2026                                   |

## Finalita del documento

Documentare i fattori interni ed esterni che possono influenzare il raggiungimento degli obiettivi del SGSI.

## Collegamento al rapporto Stage 2

Il rapporto Stage 2 CWNET evidenzia un SGSI ISO/IEC 27001:2022 applicato ai processi, agli asset e ai sistemi utilizzati per progettazione, attivazione, erogazione, gestione tecnica, monitoraggio, supporto e assistenza dei servizi di accesso a Internet e telecomunicazioni. Le evidenze sono predisposte in coerenza con le risultanze e le risposte del cliente emerse in audit.

## Fattori interni

| Ambito         | Fattore  | Impatto SGSI   |
|----------------|--|--|
| Governance     | Sede unica, CdA e direzione coinvolta                                | Maggiore chiarezza decisionale e responsabilita accentrate                   |
| Processi       | Erogazione servizi Internet, telecomunicazioni e servizi digitali    | Necessita di continuita, monitoraggio e protezione dati clienti              |
| Risorse IT     | 10 server, 21 utenti, 21 postazioni, 4 addetti sviluppo/manutenzione | Perimetro tecnologico rilevante per accessi, backup, patching e monitoraggio |
| Documentazione | SGSI formalizzato dopo Stage 1                                       | Necessita di mantenere versioning e riesami periodici                        |

## Fattori esterni

| Ambito      | Fattore   | Impatto SGSI  |
|-------------|---|---|
| Mercato     | Servizi ISP e ICT con aspettativa di disponibilita                                | Rilevanza di continuita operativa e gestione incidenti    |
| Normativo   | Privacy, contratti clienti, requisiti tecnici e D.M. 37/2008 ove pertinente       | Rilevanza di compliance e competenze                      |
| Terze parti | Fornitori con possibile impatto su servizio, connettivita, infrastrutture e cloud | Rilevanza di valutazione e monitoraggio fornitori critici |
| Minacce     | Phishing, accessi non autorizzati, indisponibilita sistemi, vulnerabilita         | Rilevanza di controlli Annex A e risk treatment           |

## SWOT sintetica

Punti di forza: sede unica, perimetro chiaro, leadership attiva, SGSI formalizzato, risk assessment e SoA disponibili. Debolezze: necessita di consolidare versioning, KPI, tracciabilita fornitori e test periodici. Opportunita: automazione reporting, rafforzamento audit fornitori, formazione ricorrente. Minacce: indisponibilita infrastrutture, incidenti cyber, dipendenza da fornitori critici, errori configurativi.

## Approvazione e validazione

| Ruolo             | Nominativo      | Firma | Data |
|-------------------|-----------------|-------|------|
| Responsabile SGSI |                 |       |      |
| Direzione         | Marco Bondielli |       |      |