Sintesi direzionale

Valutazione executive, raccomandazione e presidi di mantenimento per certificazione SGSI

EPTA TECH S.R.L.

Standard: ISO/IEC 27001:2022 + ISO/IEC 27017:2015
Sito: Via San Carlo n. 40, Frazione Prodolone, 33078 San Vito al Tagliamento (PN), Italia
Settore: Information Technology - programmazione informatica, sviluppo software, servizi web, hosting, housing e servizi cloud
Documento: EPTA-SGSI-EXEC-04
Data: Maggio 2026

Sintesi direzionale e raccomandazione

Organizzazione	EPTA TECH S.R.L.
Standard	ISO/IEC 27001:2022 + ISO/IEC 27017:2015
Sede verificata	Via San Carlo n. 40, Frazione Prodolone, 33078 San Vito al Tagliamento (PN), Italia
Settore e codici	Information Technology - ATECO 62.10.00 / NACE 62.10 - Area IAF 33
Perimetro	Sviluppo software, applicazioni web based, app, sistemi informatici, servizi digitali, web, hosting, housing, posta elettronica, domini e servizi cloud SaaS, DaaS, HaaS, PaaS e IaaS.
Base informativa	Rapporto Stage 1, Rapporto Stage 2 e visura camerale ordinaria.

Questo documento sintetizza, in forma direzionale e professionale, gli esiti del percorso Stage 1 - Stage 2 per la certificazione ISO/IEC 27001:2022 con estensione ISO/IEC 27017:2015 di EPTA TECH S.R.L. L'impostazione e pensata per top management, organismo di certificazione, reviewer tecnico e fascicolo finale di audit.

Esito generale	Lo Stage 2 ha fornito evidenze sufficienti di implementazione, applicazione ed efficacia del SGSI nel campo di applicazione verificato. Non risultano non conformita maggiori o minori ostative alla raccomandazione per la certificazione. Le osservazioni hanno natura di miglioramento e di consolidamento del sistema.
Coerenza del perimetro	Il perimetro certificativo e coerente con sede, attivita effettive, visura camerale, servizi IT/cloud e documentazione SGSI. Le attivita non IT/non cloud non presidiate dal SGSI restano escluse. Il sito verificato e la sede di Via San Carlo n. 40, Frazione Prodolone, 33078 San Vito al Tagliamento (PN).
Punti di forza	Sono emersi come punti di forza la focalizzazione sui servizi IT/software/cloud, la struttura snella con competenze tecniche dirette, la coerenza tra rischi e controlli, il completamento delle aree Stage 1, la maggiore tracciabilita delle registrazioni e l'integrazione del tema cloud nella SoA e nella matrice ISO/IEC 27017.
Aree di attenzione	Le aree da mantenere sotto controllo riguardano formalizzazione dei controlli crittografici e gestione chiavi, vulnerability management, evidenze di riesame accessi privilegiati, simulazioni incident/continuita ICT, clausole e monitoraggio dei fornitori critici, aggiornamento della matrice cloud in caso di nuovi servizi.
Raccomandazione	Alla luce delle evidenze campionate, il SGSI appare adeguato alla dimensione aziendale, al contesto organizzativo e alla complessita dei servizi erogati. Si ritiene sostenibile la raccomandazione per la certificazione, con monitoraggio delle opportunita di miglioramento nelle successive sorveglianze.

Elementi probanti chiave

- Rapporto Stage 1 con identificazione delle aree di attenzione documentali e operative da chiudere prima dello Stage 2.
- Rapporto Stage 2 con verifica dell'effettiva implementazione del SGSI, valutazione dei processi, risultanze e raccomandazione alla certificazione.
- Visura camerale ordinaria per conferma di denominazione, sede, attivita prevalente, codici ATECO/NACE, addetti e assenza di ulteriori unita locali.
- Documentazione SGSI: Manuale, Politica, Registro rischi, Piano di trattamento, SoA, procedure operative, audit interno, riesame della direzione e registrazioni di controllo.

- Evidenze tecniche e operative: asset, accessi, backup, incidenti, fornitori, sviluppo sicuro, vulnerabilita, servizi cloud e controlli ISO/IEC 27017 applicabili.

Giudizio professionale finale

Il sistema presenta un livello di maturita adeguato alla certificazione iniziale per una piccola organizzazione IT/cloud con struttura snella. Il passaggio da Stage 1 a Stage 2 mostra un rafforzamento documentale e operativo sostanziale, con particolare attenzione alla chiusura delle aree di concern, alla tracciabilita dei controlli e all'allineamento tra rischio, SoA e processi. La certificazione e sostenibile se l'organizzazione mantiene il ciclo di monitoraggio e migliora progressivamente le evidenze tecniche piu specialistiche, in particolare su crittografia, vulnerabilita, logging, controlli cloud e fornitori critici.

Raccomandazioni per la prima sorveglianza

- Verificare aggiornamento del Registro dei Rischi e della SoA rispetto a nuovi clienti, servizi o fornitori cloud.
- Campionare accessi privilegiati, MFA ove applicabile, revoche e riesami periodici degli account.
- Verificare almeno un test di ripristino backup e una simulazione di incident response o scenario di continuita ICT.
- Richiedere evidenza di vulnerability management e remediation su applicazioni web o servizi esposti.
- Riesaminare la politica crittografica, gestione certificati/chiavi e protezione delle credenziali.
- Verificare contratti, SLA, DPA e requisiti di sicurezza dei fornitori critici e cloud provider.