Piano di chiusura Stage 1 - Stage 2

Matrice di chiusura rilievi, evidenze e presidi futuri 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-CLOSE-03
Data: Maggio 2026

Piano di chiusura Stage 1 e consolidamento Stage 2

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.

Il presente documento trasforma le aree di attenzione emerse in Stage 1 in evidenze di chiusura e mantenimento verificate in Stage 2. La finalita e fornire una traccia professionale, utilizzabile nel fascicolo di certificazione e nelle sorveglianze successive.

Clausola/Area	Rilievo Stage 1	Evidenza Stage 2	Stato	Presidio futuro
4.1 Contesto	Analisi contesto parziale o da aggiornare	Analisi aggiornata con fattori interni/esterni, requisiti tecnologici, normativi e contrattuali	Accettata	Mantenere riesame periodico e collegamento a rischi/opportunita
4.2 Parti interessate	Mappatura non pienamente aggiornata	Registro parti interessate aggiornato con clienti, fornitori, cloud provider, personale, autorita e requisiti	Accettata	Aggiornare in caso di nuovi servizi, clienti critici o cambi normativi
4.4 Processi SGSI	Descrizione processi e interazioni non pienamente disponibile	Mappa processi direzionali, tecnici, operativi e supporto con interazioni e responsabilita	Accettata	Usare la mappa come base per audit interno e riesame
5.2 Politica	Politica non pienamente disponibile/aggiornata	Politica approvata e comunicata, coerente con scope IT/cloud	Accettata	Riesame annuale o in caso di cambiamenti
6.1.2 Risk assessment	Risultati valutazione rischi non pienamente disponibili	Registro rischi aggiornato su asset, minacce, vulnerabilita, impatti, criteri	Accettata	Riesame dopo modifiche a servizi, fornitori, infrastruttura
6.1.3 Trattamento e SoA	Piano trattamento, SoA, rischi residui da rafforzare	Piano trattamento, SoA e accettazione rischi residui formalizzati e collegati	Accettata con attenzione	Migliorare dettaglio controlli 27017 e crittografia/chiavi
6.2 Obiettivi	Obiettivi sicurezza non pienamente disponibili	Obiettivi misurabili con indicatori, responsabilita e monitoraggio	Accettata	Riesame indicatori nel management review
6.3 Modifiche	Pianificazione modifiche non pienamente disponibile	Modalita di change planning per SGSI, asset, servizi e ambienti IT/cloud	Accettata	Integrare con ticket/change request tecnici
7.4 Comunicazione	Piano comunicazione parziale	Piano interno/esterno con destinatari, canali, responsabilita, incidenti e obblighi	Accettata	Testare canali incident reporting e comunicazione clienti
7.5.3 Documenti	Controllo informazioni documentate da rafforzare	Controllo versioni, approvazioni, conservazione e tracciabilita registrazioni	Accettata	Mantenere indice documentale e storico versioni
8.1 Controllo operativo	Pianificazione/controllo operativo non pienamente disponibili	Procedure ed evidenze su sviluppo, accessi, backup, fornitori, incidenti, cloud	Accettata	Campionare output operativi a ogni audit interno
8.2/8.3 Rischi e trattamento	Risultati aggiornati ed evidenze attuazione da completare	Evidenze di misure tecniche, organizzative, contrattuali e procedurali	Accettata	Aumentare evidenza fotografica/logica dei controlli implementati
9.1 Monitoraggio	Registrazioni monitoraggio non pienamente disponibili	KPI, registrazioni su obiettivi, backup, incidenti, fornitori, vulnerabilita	Accettata	Consolidare dashboard SGSI trimestrale
9.3 Riesame	Registrazioni riesame direzione non pienamente disponibili	Riesame con input/output, decisioni, azioni, rischi, opportunita	Accettata	Documentare follow-up delle decisioni
10.2 NC/AC	Gestione NC e verifica efficacia da completare	Processo NC/AC con analisi cause, azioni, responsabilita, tempi, verifica	Accettata	Applicare anche a incidenti e rilievi interni
A.5.24-A.5.27 Incidenti	Procedura e registro incidenti non pienamente disponibili	Procedura incidenti aggiornata e registro disponibile	Accettata	Effettuare simulazione annuale

Clausola/Area	Rilievo Stage 1	Evidenza Stage 2	Stato	Presidio futuro
A.5.30 Continuita ICT	Piano continuita e prontezza ICT non pienamente disponibile	Misure di backup, ripristino, responsabilita, priorita e verifiche	Accettata	Definire scenari di indisponibilita cloud/provider
A.5.19-A.5.22 Fornitori	Valutazione sicurezza fornitori e accordi da rafforzare	Registro fornitori, criteri sicurezza, SLA/DPA, requisiti contrattuali	Accettata	Formalizzare riesame fornitori critici
ISO/IEC 27017	Chiarire ruoli CSP/CSC e controlli cloud	Matrice 27017 allineata a SoA e servizi effettivi	Accettata	Mantenere aggiornata con nuovi servizi cloud

Valutazione finale di chiusura

Le aree rilevate in Stage 1 risultano gestite mediante aggiornamento documentale, applicazione operativa e campionamento delle evidenze in Stage 2. Le opportunita residue hanno natura di rafforzamento della maturita del sistema e non incidono negativamente sulla raccomandazione alla certificazione. Il monitoraggio deve concentrarsi su controlli cloud, crittografia/chiavi, evidenze di vulnerability management, riesame fornitori critici e prova periodica di incident response/continuita ICT.