Matrice controlli ed evidenze

Annex A ISO/IEC 27001:2022 e controlli cloud ISO/IEC 27017:2015 - formato A4 senior

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-MAT-02
Data: Maggio 2026

Matrice controlli ed evidenze - Annex A e ISO/IEC 27017

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.

La matrice seguente sintetizza i controlli principali, le evidenze campionate e le raccomandazioni di mantenimento/miglioramento per il perimetro IT/cloud di EPTA TECH S.R.L. La lettura e orientata alla dimostrazione dell'efficacia del SGSI in Stage 2 e alla preparazione delle successive sorveglianze.

Area	Controlli	Evidenze verificate	Valutazione senior	Follow-up consigliato
Asset informativi	A.5.9, A.5.10, A.5.12, A.5.13	Inventario asset; classificazione informazioni; assegnazione responsabilita; regole di uso accettabile e protezione.	Coerente con dati clienti, codice sorgente, credenziali, log, backup, repository, ambienti cloud e piattaforme applicative.	Mantenere riesame periodico degli asset critici e aggiornamento in caso di nuovi servizi o fornitori.
Controllo accessi	A.5.15-A.5.18, A.8.2, A.8.3, A.8.5	Autorizzazioni, modifica, riesame e revoca accessi; gestione privilegi; autenticazione; protezione credenziali.	Applicato ad ambienti IT, repository, strumenti collaborativi, posta elettronica, servizi cloud e account amministrativi.	Rafforzare evidenza dei riesami accessi privilegiati e tracciabilita delle revoche.
Backup e ripristino	A.8.13	Piano backup, frequenze, responsabilita, protezione copie, test di ripristino, registrazioni esiti.	Adeguato per dati aziendali, dati clienti, codice sorgente, configurazioni e asset critici.	Mantenere test di ripristino documentati e collegare priorita di ripristino a BIA/continuita ICT.
Sviluppo sicuro	A.8.25-A.8.29	Requisiti di sicurezza, controllo codice, gestione versioni, test, rilascio controllato, separazione ambienti.	Coerente con sviluppo software, web app, app, portali e servizi digitali in scope.	Formalizzare criteri minimi di secure coding, review, gestione dipendenze e vulnerabilita applicative.
Incident management	A.5.24-A.5.27	Procedura incidenti, classificazione, escalation, registro, risposta, comunicazione, lesson learned.	Applicabile ad accessi non autorizzati, indisponibilita servizi, violazioni dati, errori di configurazione, anomalie log e incidenti cloud.	Mantenere simulazioni o test periodici della procedura e collegamento con GDPR, clienti e fornitori.
Continuita ICT	A.5.29, A.5.30, A.8.14	Misure di continuita, disponibilita, backup, ripristino, responsabilita, fornitori critici.	Proporzionato alla dimensione aziendale e ai servizi software/cloud erogati.	Evolvere verso scenari di continuita per servizi SaaS/web e indisponibilita provider.
Fornitori e terze parti	A.5.19-A.5.23	Registro fornitori, valutazione criticita, requisiti contrattuali, SLA/DPA, monitoraggio e riesame.	Rilevante per cloud provider, hosting/housing provider, registrar, email, strumenti collaborativi e servizi infrastrutturali.	Rafforzare scorecard fornitori critici, evidenze SLA e clausole di sicurezza/incident notification.
Logging e monitoraggio	A.8.15, A.8.16, A.8.17	Log applicativi, eventi sicurezza, monitoraggio anomalie, sincronizzazione temporale ove applicabile.	Coerente con servizi web/cloud, gestione incidenti e accountability tecnica.	Definire periodo di conservazione log e responsabilita di review per eventi critici.
Vulnerabilita tecniche	A.8.8	Identificazione, valutazione, trattamento e verifica vulnerabilita per sistemi, applicazioni, librerie, servizi esposti e ambienti cloud.	Processo coerente con sviluppo software e servizi digitali, da mantenere proporzionato al rischio.	Programmare scansioni periodiche e verifiche dopo modifiche rilevanti o nuovi rilasci.
Crittografia e chiavi	A.8.24	Uso di protocolli sicuri, protezione credenziali, cifratura/controlli logici, certificati, gestione chiavi.	Presente come controllo tecnico rilevante; Stage 2 evidenzia opportunita di maggiore formalizzazione.	Formalizzare policy crittografica, inventario certificati/chiavi, rinnovo, revoca, rotazione e custodia.

Area	Controlli	Evidenze verificate	Valutazione senior	Follow-up consigliato
Responsabilita cloud	ISO/IEC 27017	Matrice ruoli CSP/CSC, modello responsabilita condivisa, controlli applicabili, non applicabilita motivate.	Applicabilita trattata in relazione a servizi erogati/utilizzati, fornitori e responsabilita contrattuali.	Mantenere matrice 27017 allineata a SoA, contratti e servizi cloud attivi.
Segregazione e isolamento cloud	ISO/IEC 27017	Segregazione logica, ambienti clienti, accessi amministrativi, separazione ambienti sviluppo/test/produzione ove applicabile.	Rilevante per hosting, housing, SaaS, PaaS, IaaS e applicazioni web based.	Documentare controlli di segregazione per ambienti multi-tenant o servizi gestiti per clienti.
Portabilita e cancellazione	ISO/IEC 27017	Cancellazione sicura, restituzione dati, portabilita, gestione fine contratto, responsabilita cliente/fornitore.	Controllo pertinente per servizi cloud, dati clienti e cessazione rapporti di servizio.	Rafforzare clausole contrattuali e procedure operative di offboarding cliente/servizio.

Nota professionale

La matrice conferma che i controlli prioritari sono stati valutati in funzione del rischio, del perimetro certificativo e del ruolo effettivamente svolto dall'organizzazione nei servizi cloud. Le opportunita di miglioramento non configurano elementi ostativi, ma rafforzano la maturita del sistema in vista del mantenimento della certificazione e delle successive sorveglianze.