Evidenze oggettive senior

Dossier tecnico A4 per audit Stage 2, certificazione ISO/IEC 27001:2022 con estensione ISO/IEC 27017:2015

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-EVID-01
Data: Maggio 2026

Dossier evidenze oggettive senior

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 dossier raccoglie evidenze oggettive, criteri di audit e valutazioni professionali a supporto della certificazione ISO/IEC 27001:2022 con estensione ISO/IEC 27017:2015, alla luce delle risultanze di Stage 1 e Stage 2. Il taglio e volutamente orientato alla valutazione senior del sistema, con enfasi su tracciabilita, proporzionalita, applicabilita dei controlli e coerenza con il settore IT/cloud.

1. Contesto dell'organizzazione e parti interessate

Sono state verificate le evidenze relative all'analisi del contesto interno ed esterno dell'organizzazione, con riferimento alla natura di EPTA TECH S.R.L. quale societa operante nel settore Information Technology, con attivita prevalente di programmazione informatica, sviluppo software, servizi web, hosting, housing, posta elettronica, registrazione e mantenimento domini e servizi cloud.

L'analisi considera la struttura organizzativa snella, il numero limitato di addetti, la centralita delle competenze tecniche interne, la dipendenza da infrastrutture IT e cloud, la gestione di dati aziendali e dati dei clienti, nonche i requisiti normativi, contrattuali e tecnologici applicabili.

E stata campionata la mappatura delle parti interessate, comprendente direzione, personale interno, collaboratori, clienti, fornitori IT, cloud provider, hosting provider, registrar, partner tecnologici, autorita competenti, organismo di certificazione e soggetti interessati alla protezione delle informazioni. I requisiti risultano collegati a riservatezza, integrita, disponibilita, continuita dei servizi, protezione del codice sorgente, gestione degli accessi, sicurezza dei servizi cloud, protezione dei dati personali, obblighi contrattuali e SLA.

2. Campo di applicazione e limiti del SGSI

Il campo di applicazione risulta documentato e coerente con le attivita effettivamente presidiate: progettazione, sviluppo, realizzazione, commercializzazione, manutenzione e assistenza di soluzioni software, applicazioni web based, app, sistemi informatici, servizi digitali, servizi web, posta elettronica, hosting, housing, registrazione e mantenimento domini e servizi cloud, inclusi SaaS, DaaS, HaaS, PaaS e IaaS.

Il perimetro fisico e riferito alla sede di Via San Carlo n. 40, Frazione Prodolone, 33078 San Vito al Tagliamento (PN), Italia. Sono inclusi processi direzionali, tecnici, operativi e di supporto, personale e collaboratori coinvolti, sistemi informativi, postazioni di lavoro, ambienti cloud, piattaforme applicative, codice sorgente, dati aziendali e dei clienti, credenziali, log, backup e fornitori rilevanti.

Le attivita impiantistiche, elettriche, fotovoltaiche, videosorveglianza fisica o installazioni generiche non direttamente governate dal SGSI sono mantenute fuori dal perimetro certificativo, salvo evidenza documentata di processi, asset, responsabilita, rischi e controlli specifici. La delimitazione risulta coerente con la visura e con l'effettivo perimetro IT/cloud sottoposto a certificazione.

3. Leadership, ruoli e responsabilita

Sono state verificate le evidenze relative all'impegno della direzione, alla Politica per la Sicurezza delle Informazioni, all'attribuzione dei ruoli e alla formalizzazione delle responsabilita SGSI. Considerata la struttura snella, l'audit ha approfondito chiarezza delle responsabilita, segregazione minima dei ruoli compatibile con la dimensione aziendale e capacita della direzione di garantire supervisione, risorse, indirizzo e controllo.

La Politica per la Sicurezza delle Informazioni risulta coerente con il contesto aziendale, con i servizi IT/cloud erogati e con gli obiettivi di protezione delle informazioni. Sono state verificate evidenze di comunicazione della politica al personale e ai collaboratori pertinenti, nonche ruoli formalizzati per gestione SGSI, risk treatment, accessi, backup, incidenti, fornitori, sviluppo software e servizi cloud.

4. Valutazione dei rischi per la sicurezza delle informazioni

E stata verificata la metodologia di valutazione dei rischi, con criteri di identificazione, analisi, valutazione, trattamento e accettazione. La metodologia risulta applicata agli asset informativi e ai processi critici, inclusi dati aziendali, dati dei clienti, codice sorgente, ambienti di sviluppo, sistemi applicativi, server, workstation, credenziali, configurazioni, log, backup, repository, piattaforme cloud, servizi web e fornitori terzi.

Il Registro dei Rischi risulta riesaminato e aggiornato rispetto alle aree di attenzione emerse nello Stage 1. Sono considerati rischi pertinenti quali perdita di riservatezza, accesso non autorizzato, indisponibilita dei servizi cloud, compromissione delle credenziali, errore umano nello sviluppo o rilascio software, vulnerabilita applicative, errata configurazione cloud, perdita o corruzione dei backup, indisponibilita di fornitori critici, incidenti di sicurezza, carenze nei log e segregazione degli ambienti.

La valutazione dei rischi alimenta il Piano di Trattamento e la Dichiarazione di Applicabilita, consentendo la tracciabilita tra rischio identificato, controllo applicabile, misura adottata, responsabilita e stato di attuazione.

5. Piano di trattamento del rischio e Dichiarazione di Applicabilita

Sono state verificate le evidenze relative al Piano di Trattamento del Rischio e alla Dichiarazione di Applicabilita. Il piano risulta coerente con i rischi identificati e include misure tecniche, organizzative, procedurali e contrattuali proporzionate alla dimensione dell'organizzazione e alla criticita dei servizi IT/cloud erogati.

La SoA indica controlli applicabili, non applicabili, motivazioni, stato di implementazione e collegamento con i rischi. Le non applicabilita risultano motivate rispetto al perimetro certificativo, alle responsabilita effettivamente assunte e alla distinzione tra ambienti gestiti direttamente, ambienti cloud di terze parti e sistemi del cliente non amministrati da EPTA TECH.

Per ISO/IEC 27017 e stata verificata la coerenza tra SoA, matrice cloud e ruoli effettivamente svolti come Cloud Service Provider e/o Cloud Service Customer, considerando responsabilita condivise, contratti, segregazione logica, logging, portabilita, cancellazione sicura, incidenti e continuita dei servizi cloud.

6. Obiettivi di sicurezza delle informazioni

Sono state verificate evidenze relative alla definizione degli obiettivi di sicurezza, coerenti con politica, rischi, processi e campo di applicazione. Gli obiettivi risultano misurabili, assegnati a responsabili, monitorabili e collegati a indicatori proporzionati alla dimensione aziendale.

Gli obiettivi includono disponibilita dei servizi IT/cloud, efficacia dei backup, tempestivita nella gestione degli incidenti, controllo degli accessi privilegiati, consapevolezza del personale, gestione dei fornitori critici, aggiornamento del Registro dei Rischi, riesame periodico, monitoraggio delle vulnerabilita e miglioramento della tracciabilita documentale.

7. Competenze, formazione e consapevolezza

Sono state verificate le competenze del personale e dei collaboratori coinvolti nei processi SGSI, con attenzione alla coerenza tra ruoli assegnati, competenze tecniche, attivita svolte e responsabilita in materia di sicurezza delle informazioni.

Sono state campionate evidenze relative a formazione o sensibilizzazione su sicurezza delle informazioni, gestione credenziali, phishing, protezione dei dati, uso sicuro degli strumenti informatici, classificazione delle informazioni, gestione incidenti, backup, sicurezza nello sviluppo software e responsabilita connesse ai servizi cloud.

8. Controllo delle informazioni documentate

Sono state verificate le modalita di controllo delle informazioni documentate, includendo identificazione, approvazione, revisione, distribuzione, conservazione, accessibilita, protezione da modifiche non autorizzate e gestione delle versioni.

Sono state campionate evidenze relative a Manuale SGSI, Politica, Registro dei Rischi, Piano di Trattamento, SoA, procedure operative, registri, verbali di audit interno, riesame della direzione, incidenti, backup, fornitori e azioni correttive. Rispetto allo Stage 1, l'organizzazione ha rafforzato tracciabilita documentale e disponibilita delle registrazioni necessarie a dimostrare l'effettiva implementazione del sistema.

9. Pianificazione e controllo operativo

Sono state verificate evidenze relative alla pianificazione e al controllo operativo dei processi inclusi nel SGSI. I controlli operativi risultano applicati a sviluppo software, gestione servizi web/cloud, accessi, asset, backup, incidenti, fornitori, vulnerabilita, configurazioni e rilascio di applicazioni o servizi.

Sono state campionate procedure operative, registrazioni di attivita, log, ticket, verifiche backup, controlli accessi, gestione modifiche, registrazioni fornitori e controlli su servizi cloud. Il controllo operativo risulta proporzionato alla dimensione aziendale e alla complessita tecnica dei servizi erogati.

10. Gestione degli asset informativi

Sono state verificate evidenze relative all'inventario degli asset informativi, alla loro classificazione e all'assegnazione delle responsabilita. Gli asset includono dati aziendali, dati dei clienti, codice sorgente, repository, ambienti di sviluppo, ambienti applicativi, server, postazioni di lavoro, servizi cloud, credenziali, configurazioni, log, backup, documentazione tecnica, strumenti di collaborazione e piattaforme di erogazione dei servizi.

L'inventario risulta coerente con campo di applicazione e rischi identificati. Per gli asset critici sono stati verificati responsabilita, modalita di protezione, criteri di accesso, backup e collegamento con i controlli della SoA.

11. Controllo accessi, autenticazione e privilegi

Sono state verificate evidenze relative alla gestione degli accessi agli ambienti informatici, applicativi e cloud: autorizzazione, assegnazione, modifica, riesame e revoca degli accessi, con attenzione a utenti privilegiati, account amministrativi, credenziali condivise, repository, ambienti di sviluppo, servizi cloud, posta elettronica e strumenti collaborativi.

L'organizzazione applica regole per la gestione delle credenziali, limitazione degli accessi secondo il principio del minimo privilegio, protezione degli account critici e riesame periodico degli utenti attivi. Le evidenze risultano coerenti con i rischi di accesso non autorizzato, compromissione credenziali, esposizione di dati cliente e accesso improprio a codice sorgente.

12. Backup, ripristino e continuita ICT

Sono state verificate evidenze relative a backup, responsabilita, frequenze, conservazione, protezione delle copie e prove di ripristino. Sono state considerate le esigenze di disponibilita di dati aziendali, dati dei clienti, codice sorgente, configurazioni, sistemi applicativi e ambienti rilevanti per l'erogazione dei servizi IT/cloud.

Sono state campionate registrazioni di backup e test di ripristino, nonche misure di continuita operativa e prontezza ICT proporzionate alla dimensione dell'organizzazione e alla criticita dei servizi erogati. Il processo e

collegato a asset critici, priorita di ripristino, responsabilita, fornitori rilevanti e procedure di escalation.

13. Gestione degli incidenti di sicurezza

Sono state verificate evidenze relative alla procedura di gestione degli incidenti e al registro. La procedura considera identificazione, classificazione, registrazione, valutazione impatto, escalation, comunicazione interna/esterna, risposta, contenimento, risoluzione, lesson learned e azioni correttive.

Sono considerate tipologie di evento coerenti con il settore IT/cloud: accessi non autorizzati, indisponibilita servizi, compromissione credenziali, perdita o alterazione di dati, vulnerabilita critiche, configurazioni errate, sospetta violazione di dati personali, disservizi di fornitori cloud, errori di rilascio software e anomalie nei log.

14. Sviluppo software sicuro

Sono state verificate evidenze relative al ciclo di sviluppo software sicuro: progettazione, sviluppo, test, rilascio, manutenzione e gestione modifiche. Sono stati considerati requisiti di sicurezza applicativa, controllo codice sorgente, separazione degli ambienti, gestione versioni, autorizzazione modifiche, riesame codice, gestione vulnerabilita e tracciabilita dei rilasci.

Le evidenze risultano coerenti con lo scope, che include sviluppo e manutenzione di soluzioni software, applicazioni web based, app, sistemi informatici e servizi digitali. Sono state considerate misure a tutela del codice sorgente, credenziali di sviluppo, configurazioni applicative, dati di test e ambienti cloud.

15. Gestione vulnerabilita e sicurezza tecnica

Sono state verificate evidenze relative alla gestione delle vulnerabilita tecniche: identificazione, valutazione, priorita, trattamento e verifica per sistemi, applicazioni, ambienti cloud, server, workstation, repository, librerie software, componenti applicative e strumenti utilizzati per i servizi.

Sono state considerate fonti informative tecniche, aggiornamenti, patch, controlli di configurazione, test applicativi e misure di hardening proporzionate alla dimensione aziendale. Dove applicabile, sono state valutate evidenze di vulnerability assessment, penetration test o verifiche tecniche equivalenti, con attenzione agli asset esposti su Internet e alle applicazioni web based.

16. Crittografia e gestione delle chiavi

Sono state verificate evidenze relative all'utilizzo di controlli crittografici per proteggere dati, credenziali, comunicazioni, backup e servizi cloud ove applicabile. Sono stati considerati protocolli sicuri, protezione delle credenziali, cifratura o protezione logica degli ambienti, gestione delle chiavi, responsabilita di custodia e misure per prevenire accessi non autorizzati.

In considerazione dell'osservazione emersa nello Stage 2 sui controlli crittografici e sulla gestione delle chiavi, si raccomanda di rafforzare ulteriormente la formalizzazione della politica crittografica, includendo criteri di utilizzo, responsabilita, inventario delle chiavi/certificati rilevanti, rinnovo, revoca, conservazione e rotazione.

17. Gestione fornitori, cloud provider e terze parti

Sono state verificate evidenze relative a identificazione, valutazione, qualificazione e monitoraggio dei fornitori rilevanti per il SGSI. Il perimetro comprende fornitori IT, cloud provider, hosting/housing provider, registrar, posta elettronica, strumenti collaborativi, servizi infrastrutturali, consulenti e terze parti che possono incidere su sicurezza, disponibilita o continuita dei servizi.

I criteri di valutazione considerano criticita del servizio, accesso a dati o sistemi, impatto sulla continuita, localizzazione o trattamento dei dati, SLA, DPA ove applicabile, requisiti contrattuali di riservatezza, sicurezza, disponibilita, gestione incidenti, backup, subfornitura e cessazione del servizio.

18. Sicurezza dei servizi cloud - ISO/IEC 27017

Sono state verificate evidenze relative all'applicabilita dei controlli ISO/IEC 27017, con particolare riferimento alla distinzione dei ruoli svolti come Cloud Service Provider e/o Cloud Service Customer. La valutazione considera responsabilita condivise, servizi cloud erogati o utilizzati, contratti con fornitori, responsabilita verso clienti, accessi cloud, segregazione logica, logging, monitoraggio, portabilita, cancellazione sicura, backup, incidenti cloud e continuita.

La matrice ISO/IEC 27017 risulta collegata alla SoA e al Registro dei Rischi. I controlli cloud pertinenti risultano valutati in base ai servizi effettivamente gestiti e alle responsabilita operative o contrattuali assunte. I controlli non pertinenti risultano esclusi o limitati con motivazione documentata.

19. Monitoraggio, misurazione e valutazione prestazioni

Sono state verificate evidenze relative al monitoraggio e alla misurazione delle prestazioni del SGSI. Gli indicatori considerano stato degli obiettivi, andamento rischi, stato azioni di trattamento, efficacia backup, incidenti o eventi di sicurezza, vulnerabilita, formazione, stato fornitori critici, audit interni, non conformita e azioni correttive.

Le registrazioni risultano coerenti con la dimensione dell'organizzazione e supportano il riesame della direzione. Le evidenze consentono un controllo periodico del SGSI basato su elementi documentati e non su valutazioni meramente descrittive.

20. Audit interno e riesame della direzione

Sono state verificate evidenze relative ad audit interno e riesame della direzione. L'audit interno verifica conformita del SGSI a ISO/IEC 27001, SoA, procedure interne e controlli applicabili. Il riesame considera cambiamenti del contesto, risultati di audit, stato azioni, prestazioni SGSI, rischi, opportunita, incidenti, fornitori, obiettivi e miglioramento.

Le risultanze dello Stage 1 sono state prese in carico e rivalutate nello Stage 2. Le registrazioni dimostrano la chiusura o gestione delle aree di attenzione relative a contesto, parti interessate, processi SGSI, politica, risk assessment, SoA, piano trattamento, obiettivi, controllo operativo, monitoraggio, incidenti, continuita ICT e fornitori.

21. Non conformita, azioni correttive e miglioramento

Sono state verificate evidenze relative alla gestione di non conformita, azioni correttive e opportunita di miglioramento. Il processo prevede identificazione del rilievo, analisi della causa, definizione dell'azione, responsabilita, tempi, attuazione e verifica di efficacia.

Le aree di attenzione emerse nello Stage 1 sono state considerate come input di miglioramento del SGSI. In Stage 2 risultano prese in carico e gestite, senza evidenza di problemi irrisolti ostativi alla certificazione.

22. Conformita legislativa e requisiti cogenti

Sono state verificate evidenze relative all'identificazione dei requisiti legislativi, regolamentari e contrattuali applicabili alla sicurezza delle informazioni. Per il settore IT/cloud sono considerati GDPR e D.Lgs. 196/2003, normativa contrattuale, proprieta intellettuale e diritto d'autore sul software, requisiti di riservatezza, SLA, DPA, obblighi verso clienti e fornitori, NIS 2 ove applicabile, Cyber Resilience Act ove pertinente e requisiti relativi ai servizi cloud.

La conformita legislativa risulta integrata nella valutazione dei rischi, nei controlli applicabili, nella gestione fornitori, nella gestione incidenti, nella protezione dei dati e nella definizione del campo di applicazione.

Sintesi conclusiva

Sulla base delle evidenze documentali, operative e testimoniali campionate, il Sistema di Gestione per la Sicurezza delle Informazioni di EPTA TECH S.R.L. risulta implementato, mantenuto e controllato in modo coerente con il campo di applicazione definito per le attivita IT, software, servizi web, hosting, housing e servizi cloud. Le aree di attenzione emerse durante lo Stage 1 sono state prese in carico e rivalutate in Stage 2. Non emergono elementi ostativi alla raccomandazione per la certificazione, fermo restando il mantenimento del monitoraggio periodico, dell'aggiornamento della valutazione dei rischi, della verifica dei controlli cloud e del miglioramento continuo.