DOSSIER DELLE EVIDENZE OGGETTIVE

Stage 2 - Trasferimento ed estensione di scopo

ISO/IEC 27001:2022 con estensione ISO/IEC 27017 e ISO/IEC 27018

Organizzazione: ITLAB S.R.L.
Redazione tecnica: Dott. Anthony D'Angelo
Data: 05/05/2026

Documento riservato - predisposto per il fascicolo di certificazione, trasferimento e ampliamento del perimetro SGSI.

1. Controllo del documento

Campo	Valore
Organizzazione	ITLAB S.R.L.
Documento	Dossier delle evidenze oggettive - Stage 2, trasferimento ed estensione di scopo
Standard	ISO/IEC 27001:2022 - ISO/IEC 27017 - ISO/IEC 27018
Oggetto	Evidenze oggettive a supporto della certificazione, del trasferimento e dell'estensione ai controlli cloud e privacy cloud
Audit di riferimento	Stage 2 - Audit speciale - Modalita' mista - Attivita' di estensione: ISO 27017 - ISO 27018
Redazione tecnica	Dott. Anthony D'Angelo
Data documento	05/05/2026
Stato documento	Bozza professionale per fascicolo di audit - da allegare alle evidenze SGSI e validare dalla Direzione

Nota metodologica

Il presente dossier raccoglie e organizza, in forma professionale e verificabile, le evidenze oggettive rilevanti per il completamento dello Stage 2, con riferimento al trasferimento della certificazione e all'estensione del campo ai riferimenti ISO/IEC 27017 e ISO/IEC 27018. Il documento non sostituisce le registrazioni originali, gli allegati tecnici, i contratti, i log o le schermate di sistema, ma costituisce indice ragionato e sintesi tecnica di accompagnamento alle evidenze operative da mantenere nel fascicolo SGSI.

Il documento e' redatto in modo da supportare la valutazione senior dell'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni, con particolare attenzione a servizi ICT, sviluppo software, piattaforme cloud, trattamento dati, telemedicina, protezione dei dati personali e gestione delle responsabilita' condivise con provider e partner tecnologici.

2. Riferimenti di audit e perimetro

Elemento	Evidenza sintetica
Organizzazione	ITLAB S.R.L., sede legale in Via Pietro Giannone 9, 20154 Milano (MI).
Sedi considerate	Sede legale Milano; unita' operativa Francavilla al Mare, Via Nazionale Adriatica Nord 278; ufficio Napoli, Via Toledo 289.
Personale / complessita' IT	3 utenti, 1 server, 3 workstation/PC/laptop, 2 addetti sviluppo e manutenzione applicativa, 1 rete, 2 connessioni Internet.
Audit	Stage 2 - audit speciale - modalita' mista - 3 man/day - estensione ISO 27017 e ISO 27018.
Campo	Progettazione, sviluppo, gestione, manutenzione, assistenza e supporto di soluzioni software, piattaforme digitali, sistemi informatici, servizi ICT, hosting specializzato, trattamento dati e servizi digitali anche in ambito sanitario/telemedicina.
Esclusioni	Non risultano esclusioni generali dall'Allegato A. Eventuali controlli non applicabili devono essere motivati nello Statement of Applicability e approvati dalla Direzione.
Normative rilevanti	ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, GDPR, D.Lgs. 196/2003 e s.m.i., D.Lgs. 138/2024 NIS2 se applicabile, requisiti contrattuali e requisiti specifici dei clienti.

Sintesi senior

Il perimetro risulta congruente con un SGSI ad alta rilevanza informativa, nel quale le principali aree di rischio sono connesse a trattamento dati, sviluppo software, gestione accessi, continuita' dei servizi, sicurezza cloud, privacy cloud, fornitori critici e dipendenze tecnologiche. L'estensione ISO/IEC 27017 e ISO/IEC 27018 richiede una dimostrazione specifica della governance cloud e della protezione dei dati personali trattati in ambienti cloud.

3. Matrice riepilogativa delle evidenze

Codice	Processo / area	Clausole	Esito	Evidenze chiave
EV-01	Campo, contesto e parti interessate	4.1 / 4.2 / 4.3 / 4.4	C	Contesto, perimetro, sedi, servizi, requisiti parti interessate.
EV-02	Leadership e responsabilita' SGSI	5.1 / 5.2 / 5.3	C	Politica, organigramma, ruoli, riesame direzione.
EV-03	Risk assessment e trattamento	6.1.1 / 6.1.2 / 6.1.3	C/O	Metodologia, risk assessment, piano trattamento, rischi cloud/privacy.
EV-04	Statement of Applicability integrato	6.1.3 / Annex A / 27017 / 27018	C	SoA aggiornato, motivazioni, stato attuazione, evidenze.
EV-05	Obiettivi SGSI e KPI	6.2 / 9.1	C	KPI accessi, incidenti, backup, formazione, fornitori, controlli cloud.
EV-06	Gestione documentale	7.5	O	Elenco documenti, versioni, approvazioni, conservazione.
EV-07	Asset inventory e classificazione	A.5.9 / A.5.10 / A.5.12 / A.5.13	C	Asset, sistemi, dati, ambienti cloud, repository, dispositivi.
EV-08	Accessi e privilegi	A.5.15-5.18 / A.8.2 / A.8.3 / A.8.5	C	Utenze, privilegi, revoche, MFA, riesami accessi.
EV-09	Sicurezza operativa	A.8.6-8.17	C	Backup, restore, log, monitoraggio, vulnerabilita', malware, continuita'.
EV-10	Sviluppo software sicuro	A.8.25-8.32	C	Change log, repository, test, rilasci, segregazione ambienti.
EV-11	Fornitori e provider cloud	A.5.19-5.22 / 27017	O	Classificazione fornitori, SLA, NDA, DPA, requisiti cloud.
EV-12	Protezione dati personali in cloud	A.5.34 / 27018 / GDPR	C	Registro trattamenti, DPA, subfornitori, data breach, cancellazione/restituzione.
EV-13	Incident management	A.5.24-5.28	C	Procedura incidenti, registro, escalation, azioni correttive.
EV-14	Formazione e consapevolezza	7.2 / 7.3 / A.6.3	C	Piano formazione, registri, awareness cloud/privacy.
EV-15	Audit interno e riesame	9.2 / 9.3 / 10.1 / 10.2	C	Audit interno, riesame Direzione, NC, azioni correttive.

Legenda esito: C = conforme; NC maggiore/minore = non conformita'; O = osservazione/opportunita' di miglioramento. Le osservazioni indicate non costituiscono elementi ostativi se trattate nel processo di miglioramento continuo e supportate da evidenze oggettive.

4. Evidenze dettagliate per processo

EV-01 - Contesto, parti interessate e campo di applicazione

Campo	Contenuto
Codice evidenza	EV-01
Area / processo	Contesto, parti interessate e campo di applicazione
Standard e clausole	ISO/IEC 27001: 4.1, 4.2, 4.3, 4.4; ISO/IEC 27017 e ISO/IEC 27018 per aspetti cloud/privacy cloud
Tipo evidenza	Documentale, intervista, coerenza perimetrale
Evidenza oggettiva predisposta / verificata	Sono disponibili elementi documentali che descrivono identita' dell'organizzazione, sedi, processi, clienti, fornitori, servizi ICT, software, hosting specializzato, trattamento dati, telemedicina e supporto tecnologico. Il campo include dati aziendali, tecnici, amministrativi, contrattuali e commerciali, dati di clienti, fornitori, partner, utenti, personale e collaboratori, nonche' dati personali e, ove applicabile, informazioni connesse a servizi sanitari o di telemedicina.
Esito professionale	Conformita' sostanziale. Il campo e' adeguato a rappresentare il perimetro certificativo e l'estensione cloud/privacy cloud.
Fonte informativa	Audit Report Stage 2; visura camerale; documento campo SGSI; analisi contesto; elenco parti interessate.
Nota del redattore	Da mantenere evidenza del riesame periodico del campo, soprattutto in caso di nuovi servizi SaaS, variazioni di provider cloud, nuove sedi o modifiche ai trattamenti.

EV-02 - Leadership, politica e responsabilita'

Campo	Contenuto
Codice evidenza	EV-02
Area / processo	Leadership, politica e responsabilita'
Standard e clausole	ISO/IEC 27001: 5.1, 5.2, 5.3
Tipo evidenza	Documentale e intervista direzionale
Evidenza oggettiva predisposta / verificata	La Direzione risulta coinvolta nella definizione del SGSI, della politica per la sicurezza delle informazioni, degli obiettivi, delle responsabilita' e del riesame. Anthony D'Angelo e' indicato nel rapporto come partecipante all'audit con ruolo CEO / Top Management e come Technical Expert nel team di audit.
Esito professionale	Conformita' rilevata. La leadership e' adeguata, con raccomandazione di rendere sempre tracciabili le decisioni su rischi residui, risorse, priorita' e integrazione 27017/27018.
Fonte informativa	Politica SGSI; organigramma; mansionario; verbale riesame; audit attendance sheet; deleghe/nomine interne.
Nota del redattore	Formalizzare nel riesame della Direzione le decisioni sull'estensione di scopo e sul modello di responsabilita' cloud.

EV-03 - Valutazione dei rischi e piano di trattamento

Campo	Contenuto
Codice evidenza	EV-03
Area / processo	Valutazione dei rischi e piano di trattamento
Standard e clausole	ISO/IEC 27001: 6.1.1, 6.1.2, 6.1.3; ISO/IEC 27017; ISO/IEC 27018
Tipo evidenza	Documentale e campionamento controlli
Evidenza oggettiva predisposta / verificata	Il risk assessment considera i rischi rilevanti per accessi, credenziali, sviluppo software, fornitori, continuita' operativa, dati personali, ambienti cloud e servizi ICT critici. Il piano di trattamento collega rischi, controlli, responsabilita', tempi e verifica dell'efficacia.
Esito professionale	Conformita' con osservazione di rafforzamento. L'impianto e' idoneo allo Stage 2, ma deve restare aggiornato rispetto a modifiche tecnologiche, nuovi fornitori e variazioni di trattamento dati.
Fonte informativa	Metodologia risk assessment; risk assessment; risk treatment plan; SoA; interviste Responsabile SGSI e area tecnica.
Nota del redattore	Inserire nel piano di trattamento un tracciamento puntuale delle azioni cloud: ownership, scadenza, evidenza di chiusura e riesame efficacia.

EV-04 - Statement of Applicability integrato ISO 27001 / 27017 / 27018

Campo	Contenuto
Codice evidenza	EV-04
Area / processo	Statement of Applicability integrato ISO 27001 / 27017 / 27018
Standard e clausole	ISO/IEC 27001: 6.1.3 e Annex A; ISO/IEC 27017; ISO/IEC 27018
Tipo evidenza	Documentale
Evidenza oggettiva predisposta / verificata	Lo Statement of Applicability deve includere controlli ISO/IEC 27001 applicabili e controlli integrativi riferiti a sicurezza cloud e protezione dei dati personali trattati in cloud. Per ciascun controllo devono risultare applicabilita', motivazione, stato, responsabilita' ed evidenze.
Esito professionale	Conformita' condizionata alla disponibilita' del SoA aggiornato. L'assenza di esclusioni generali e' coerente con il perimetro dichiarato.
Fonte informativa	SoA aggiornato; piano di trattamento; risk assessment; evidenze di attuazione controlli; matrice 27017/27018.
Nota del redattore	Mantenere una colonna specifica per controlli 27017/27018 e per responsabilita' condivise cliente/provider.

EV-05 - Obiettivi SGSI, KPI e monitoraggio performance

Campo	Contenuto
Codice evidenza	EV-05
Area / processo	Obiettivi SGSI, KPI e monitoraggio performance
Standard e clausole	ISO/IEC 27001: 6.2, 9.1
Tipo evidenza	Documentale e registrazioni
Evidenza oggettiva predisposta / verificata	Sono stati definiti obiettivi e KPI coerenti con gestione rischi, formazione, riesame accessi, gestione incidenti, backup, restore test, fornitori critici, audit interno, NC, azioni correttive e controlli cloud/privacy.
Esito professionale	Conformita'. Gli indicatori sono idonei a misurare efficacia e miglioramento del SGSI, inclusa estensione di scopo.
Fonte informativa	Piano obiettivi SGSI; dashboard KPI; verbale riesame Direzione; report formazione; registro incidenti; registro fornitori.
Nota del redattore	Integrare KPI specifici cloud: percentuale configurazioni riesaminate, backup cloud riusciti, restore test, tempi revoca account cloud, fornitori cloud valutati.

EV-06 - Gestione documentale e informazioni documentate

Campo	Contenuto
Codice evidenza	EV-06
Area / processo	Gestione documentale e informazioni documentate
Standard e clausole	ISO/IEC 27001: 7.5.1, 7.5.2, 7.5.3
Tipo evidenza	Documentale
Evidenza oggettiva predisposta / verificata	La documentazione necessaria al SGSI include politiche, procedure, registri, verbali, risk assessment, SoA, piani di trattamento, registri formazione, asset, fornitori, incidenti, audit interno e riesame. Il rapporto evidenzia la necessita' di controllo versioni, approvazioni, conservazione e disponibilita'.
Esito professionale	Osservazione. La struttura documentale e' adeguata, ma va presidiata la rintracciabilita' delle versioni e delle approvazioni per tutti i documenti collegati all'estensione 27017/27018.
Fonte informativa	Elenco documenti SGSI; procedure controllo documenti; registrazioni approvazioni; repository documentale.
Nota del redattore	Applicare codifica univoca, revisione, data, owner, stato e livello di riservatezza su ogni documento SGSI.

EV-07 - Gestione asset informativi e classificazione

Campo	Contenuto
Codice evidenza	EV-07
Area / processo	Gestione asset informativi e classificazione
Standard e clausole	ISO/IEC 27001 Annex A: 5.9, 5.10, 5.12, 5.13
Tipo evidenza	Documentale e campionamento
Evidenza oggettiva predisposta / verificata	L'inventario deve coprire software, piattaforme, ambienti cloud, dispositivi, account, database, repository, archivi documentali, dati personali, dati clienti e fornitori critici. Le informazioni devono essere classificate per riservatezza, integrita', disponibilita' e requisiti normativi.
Esito professionale	Conformita' se inventario, ownership e classificazione risultano aggiornati e coerenti con il perimetro.
Fonte informativa	Inventario asset; elenco software; elenco piattaforme cloud; registro trattamenti; interviste area tecnica.
Nota del redattore	Collegare ogni asset critico al rischio, al controllo SoA e al responsabile operativo.

EV-08 - Gestione accessi, credenziali e privilegi

Campo	Contenuto
Codice evidenza	EV-08
Area / processo	Gestione accessi, credenziali e privilegi
Standard e clausole	ISO/IEC 27001 Annex A: 5.15, 5.16, 5.17, 5.18, 8.2, 8.3, 8.5; ISO/IEC 27017
Tipo evidenza	Tecnica e documentale
Evidenza oggettiva predisposta / verificata	Gli accessi devono essere nominativi, autorizzati, proporzionati al ruolo, riesaminati periodicamente e revocati tempestivamente. Per gli ambienti cloud devono essere considerate MFA ove applicabile, segregazione dei ruoli, privilegi amministrativi limitati e tracciabilita' degli accessi.
Esito professionale	Conformita' sulla base delle evidenze rese disponibili. Controllo rilevante per l'estensione cloud.
Fonte informativa	Policy accessi; elenco utenti; autorizzazioni; log; evidenze revoca; configurazioni accessi cloud; interviste tecniche.
Nota del redattore	Conservare evidenza del riesame periodico degli accessi e della revoca delle utenze non piu' necessarie.

EV-09 - Sicurezza operativa, backup, logging, monitoring e continuita'

Campo	Contenuto
Codice evidenza	EV-09
Area / processo	Sicurezza operativa, backup, logging, monitoring e continuita'
Standard e clausole	ISO/IEC 27001 Annex A: 8.6, 8.7, 8.8, 8.13, 8.15, 8.16, 8.17; ISO/IEC 27017
Tipo evidenza	Tecnica, registrazioni e campionamento
Evidenza oggettiva predisposta / verificata	Sono richieste evidenze relative a backup, test di ripristino, logging, monitoraggio, protezione malware, gestione vulnerabilita', configurazioni sicure, continuita' dei servizi ICT/cloud e dipendenze da provider cloud o hosting.
Esito professionale	Conformita' con focus su dimostrazione operativa. Le evidenze devono mostrare controllo effettivo, non solo policy.
Fonte informativa	Policy backup; report backup; test restore; log; sistemi monitoraggio; registro incidenti; procedure operative; interviste area tecnica.
Nota del redattore	Pianificare almeno un test periodico di ripristino documentato per i servizi critici e conservare esito, tempi e anomalie.

EV-10 - Sviluppo software sicuro e gestione modifiche

Campo	Contenuto
Codice evidenza	EV-10
Area / processo	Sviluppo software sicuro e gestione modifiche
Standard e clausole	ISO/IEC 27001 Annex A: 8.25, 8.26, 8.27, 8.28, 8.29, 8.31, 8.32
Tipo evidenza	Tecnica e documentale
Evidenza oggettiva predisposta / verificata	Il processo di sviluppo software prevede requisiti di sicurezza, separazione tra ambienti, controllo del codice, test, approvazione dei rilasci, gestione modifiche e trattamento delle vulnerabilita' applicative. Il processo e' centrale per ITLAB S.R.L. in quanto l'attivita' di programmazione informatica e' parte del perimetro.
Esito professionale	Conformita'. Si raccomanda mantenimento di change log, evidenza test, autorizzazioni e tracciabilita' dei rilasci.
Fonte informativa	Procedura sviluppo sicuro; repository; change log; ticket; evidenze test; documentazione tecnica; interviste sviluppatori/responsabili tecnici.
Nota del redattore	Integrare checklist di secure coding e vulnerability review prima dei rilasci in produzione.

EV-11 - Gestione fornitori, provider cloud, hosting e partner tecnologici

Campo	Contenuto
Codice evidenza	EV-11
Area / processo	Gestione fornitori, provider cloud, hosting e partner tecnologici
Standard e clausole	ISO/IEC 27001 Annex A: 5.19, 5.20, 5.21, 5.22; ISO/IEC 27017
Tipo evidenza	Contrattuale e documentale
Evidenza oggettiva predisposta / verificata	I fornitori critici devono essere identificati, classificati, valutati, contrattualizzati e monitorati. Contratti, SLA, NDA e DPA devono includere requisiti di sicurezza, riservatezza, continuita', gestione incidenti, accessi, trattamento dati e responsabilita' cloud.
Esito professionale	Osservazione di presidio. L'area e' critica per l'estensione 27017/27018 e deve essere mantenuta con monitoraggio formale.
Fonte informativa	Registro fornitori; valutazioni fornitori; contratti; SLA; NDA; DPA; nomine privacy; evidenze monitoraggio; interviste Direzione/area tecnica.
Nota del redattore	Classificare ogni fornitore per criticita', accesso ai dati, impatto su CIA, localizzazione dati e obblighi di notifica incidenti.

EV-12 - Protezione dei dati personali trattati in ambienti cloud

Campo	Contenuto
Codice evidenza	EV-12
Area / processo	Protezione dei dati personali trattati in ambienti cloud
Standard e clausole	ISO/IEC 27018; ISO/IEC 27001 Annex A 5.34; GDPR
Tipo evidenza	Privacy, contrattuale e tecnica
Evidenza oggettiva predisposta / verificata	Devono risultare identificati i dati personali trattati in cloud, ruoli privacy, istruzioni documentate, finalita' del trattamento, misure tecniche e organizzative, subfornitori, conservazione, cancellazione/restituzione, data breach e supporto ai diritti degli interessati.
Esito professionale	Conformita' se documentazione privacy e contratti cloud risultano coerenti con i trattamenti effettivi e con ISO/IEC 27018.
Fonte informativa	Registro trattamenti; informative; DPA; nomine; misure tecniche e organizzative; procedure data breach; contratti cloud; interviste privacy/compliance.
Nota del redattore	Mantenere evidenza di istruzioni al processor, verifica sub-responsabili e modalita' di cancellazione/restituzione dati a fine servizio.

EV-13 - Gestione incidenti e data breach

Campo	Contenuto
Codice evidenza	EV-13
Area / processo	Gestione incidenti e data breach
Standard e clausole	ISO/IEC 27001 Annex A: 5.24, 5.25, 5.26, 5.27, 5.28; GDPR
Tipo evidenza	Procedurale e registrazioni
Evidenza oggettiva predisposta / verificata	Il processo deve prevedere identificazione, segnalazione, registrazione, classificazione, analisi, trattamento, escalation, comunicazione e chiusura degli incidenti, comprese implicazioni su cloud, fornitori, dati personali e continuita' operativa.
Esito professionale	Conformita'. La presenza di registro e procedura consente gestione e tracciabilita' degli eventi.
Fonte informativa	Procedura incidenti; registro incidenti; ticket; comunicazioni interne; evidenze chiusura; azioni correttive; procedura data breach.
Nota del redattore	Eseguire almeno una simulazione periodica di incidente/data breach con evidenza di tempi, ruoli, comunicazioni e lezioni apprese.

EV-14 - Formazione, competenza e consapevolezza

Campo	Contenuto
Codice evidenza	EV-14
Area / processo	Formazione, competenza e consapevolezza
Standard e clausole	ISO/IEC 27001: 7.2, 7.3; Annex A 6.3
Tipo evidenza	Registrazioni e interviste
Evidenza oggettiva predisposta / verificata	Il personale e i collaboratori devono essere formati su policy SGSI, responsabilita', credenziali, phishing, protezione dati, incident reporting, uso strumenti aziendali, sicurezza cloud e requisiti 27017/27018.
Esito professionale	Conformita'. Evidenze formative e interviste supportano la consapevolezza del personale.
Fonte informativa	Piano formazione; registri presenza; materiale didattico; test/quiz; comunicazioni awareness; interviste.
Nota del redattore	Prevedere modulo annuale specifico su sicurezza cloud, trattamento dati personali in cloud e gestione incidenti.

EV-15 - Audit interno, riesame della Direzione e miglioramento continuo

Campo	Contenuto
Codice evidenza	EV-15
Area / processo	Audit interno, riesame della Direzione e miglioramento continuo
Standard e clausole	ISO/IEC 27001: 9.2, 9.3, 10.1, 10.2
Tipo evidenza	Documentale e registrazioni
Evidenza oggettiva predisposta / verificata	Il programma di audit interno, il riesame della Direzione, le non conformita', le azioni correttive e le opportunita' di miglioramento devono includere anche estensione 27017/27018, rischi cloud, privacy cloud, fornitori critici, SLA, KPI e incidenti.
Esito professionale	Conformita'. Il processo sostiene la raccomandazione positiva se sono presenti registrazioni complete e azioni tracciate.
Fonte informativa	Programma audit interno; rapporti audit; verbale riesame; registro NC; azioni correttive; KPI; follow-up.
Nota del redattore	Assicurare che il prossimo ciclo di audit interno abbia check-list esplicita per ISO/IEC 27017 e 27018.

5. Evidenze specifiche per trasferimento e extension scope

Ambito	Evidenza da mantenere	Valutazione senior
Trasferimento certificativo	Assenza di audit precedenti disponibili o presenza di rapporti precedenti da riesaminare; verifica di eventuali NC pregresse, azioni correttive, reclami e uso marchi.	Nessun elemento ostativo se non risultano NC aperte, reclami critici o uso improprio dei marchi. Conservare dichiarazione formale e registro reclami/NC.
Extension ISO/IEC 27017	Matrice responsabilita' cloud; contratti/SLA provider; configurazioni sicure; accessi amministrativi; logging; backup; monitoraggio; continuita'.	Idonea se il modello di responsabilita' condivisa e' documentato e coerente con i servizi effettivamente erogati/utilizzati.
Extension ISO/IEC 27018	Registro trattamenti cloud; DPA; istruzioni documentate; subfornitori; cancellazione/restituzione dati; data breach; misure tecniche e organizzative.	Idonea se i trattamenti cloud sono mappati e se le responsabilita' privacy sono formalizzate.
Siti permanenti	Milano, Francavilla al Mare e Napoli, con verifica mista e focus su sede operativa di programmazione informatica.	Il perimetro fisico risulta coerente con il campo SGSI. Le evidenze tecniche possono essere verificate anche da remoto.
Decisione tecnica	Nessuna NC maggiore o minore bloccante rilevata nel dossier; osservazioni trattabili nel miglioramento continuo.	Il fascicolo e' impostato per sostenere una raccomandazione positiva, salvo decisione finale dell'Organismo di Certificazione.

Dichiarazione tecnica di accompagnamento

Sulla base delle evidenze documentali e operative organizzate nel presente dossier, il Sistema di Gestione per la Sicurezza delle Informazioni di ITLAB S.R.L. risulta strutturato per supportare il trasferimento certificativo e l'estensione di scopo ai riferimenti ISO/IEC 27017 e ISO/IEC 27018. Le osservazioni individuate sono gestibili mediante il normale processo di miglioramento continuo e non assumono, allo stato delle informazioni disponibili, natura ostativa alla prosecuzione positiva dell'iter certificativo.

6. Piano minimo di mantenimento evidenze

Frequenza	Evidenza	Responsabile suggerito
Mensile	Monitoraggio backup, log, incidenti, vulnerabilita', disponibilita' servizi cloud, anomalie e accessi privilegiati.	Responsabile tecnico / SGSI
Trimestrale	Riesame accessi, fornitori critici, KPI SGSI, avanzamento piano trattamento, configurazioni cloud e stato azioni correttive.	Responsabile SGSI / Direzione
Semestrale	Verifica contratti, SLA, DPA, subfornitori, registro trattamenti, test di restore e aggiornamento asset inventory.	SGSI / Privacy / Area tecnica
Annuale	Audit interno completo, riesame della Direzione, formazione, aggiornamento SoA, aggiornamento risk assessment e test di continuita'.	Direzione / SGSI
A evento	Nuovi servizi, nuovi provider, variazioni architetturali, incidenti, data breach, modifiche rilevanti al perimetro o ai trattamenti.	Owner del processo / SGSI

7. Attestazione finale del redattore

Il presente dossier e' stato predisposto come fascicolo professionale di evidenze oggettive a supporto dello Stage 2, del trasferimento e dell'estensione di scopo ISO/IEC 27001 con riferimenti ISO/IEC 27017 e ISO/IEC 27018. La struttura delle evidenze e' coerente con il campo dichiarato, con i processi analizzati, con le aree di interesse dello Stage 2 e con le esigenze di dimostrazione documentale tipiche di una verifica di certificazione.

Le evidenze dovranno essere conservate in forma controllata, corredate dagli allegati originali, dalle registrazioni operative e dalle eventuali firme interne richieste dalle procedure aziendali. Ogni evidenza dovra' essere resa disponibile all'Organismo di Certificazione in caso di richiesta, riesame tecnico o successiva sorveglianza.

Campo	Valore
Redazione tecnica	Dott. Anthony D'Angelo
Ruolo nel fascicolo	Referente tecnico e top management per le evidenze SGSI, cloud e privacy cloud
Organizzazione	ITLAB S.R.L.
Data	05/05/2026
Firma	_____ Dott. Anthony D'Angelo

Allegati raccomandati al fascicolo

N.	Allegato
1	Audit Report Stage 2 - AR_01.2 - ITLAB S.R.L.
2	Visura camerale aggiornata ITLAB S.R.L.
3	Campo di applicazione SGSI approvato
4	Risk assessment e piano di trattamento
5	Statement of Applicability integrato ISO 27001 / 27017 / 27018
6	Registro asset, registro fornitori, registro incidenti, registro formazione
7	Contratti, SLA, NDA, DPA, nomine privacy e documentazione provider cloud
8	Evidenze tecniche: accessi, log, backup, restore test, change log, vulnerability management
9	Audit interno, riesame Direzione, KPI, non conformita', azioni correttive e miglioramento