Allegato Evidenze Stage 1

ISO/IEC 27001:2022 - Information Security Management System

EZ Lab - IAF 33 Information Technology

Finalità del documento

Dossier A4 predisposto come allegato tecnico allo Stage 1 ISO/IEC 27001:2022. Contiene evidenze documentali, registri, matrici e riferimenti operativi a supporto della valutazione di prontezza allo Stage 2. Le evidenze sono strutturate in forma controllata e devono essere verificate, datate e approvate dall'organizzazione prima dell'uso ufficiale nel fascicolo di certificazione.

Organizzazione	EZ Lab
Schema	ISO/IEC 27001:2022 - SGSI
Settore IAF	IAF 33 - Information Technology
Oggetto	Evidenze documentali di supporto allo Stage 1
Sito principale	www.ezlab.it
Lead Auditor	Dr. Prof. Giuseppe Izzo
Stato documento	Controlled draft - da validare a cura dell'organizzazione
Data emissione	13/05/2026

Classificazione: riservato - uso interno, audit e certificazione. Il presente dossier non sostituisce le registrazioni originali aziendali e non deve essere utilizzato per attestare attività non effettivamente svolte o non approvate dalla Direzione.

0 - Controllo documento e nota di validazione

Il presente allegato è costruito come fascicolo tecnico di evidenze per lo Stage 1. Per l'uso ufficiale devono essere completati i campi di approvazione, firmate le sezioni rilevanti e archiviata una copia controllata nel repository SGSI.

Campo	Contenuto
Codice documento	EZL-ISMS-S1-EVID-001
Titolo	Dossier evidenze Stage 1 ISO/IEC 27001:2022 - IAF 33
Versione	Rev.00
Data	13/05/2026
Preparato per	Audit Stage 1 SGSI - EZ Lab
Preparato da	Supporto consulenziale / Lead Auditor
Responsabile validazione	Direzione / Responsabile SGSI EZ Lab
Distribuzione	Direzione, Responsabile SGSI, auditor, fascicolo certificazione
Conservazione	Repository SGSI controllato; retention minima raccomandata: 3 anni o secondo requisito contrattuale/normativo

Avvertenza di integrità

Le registrazioni relative a eventi già avvenuti - audit interno, riesame della Direzione, revisioni accessi, test backup, valutazioni fornitori - devono essere supportate da evidenze primarie o da verbali approvati. Dove il documento riporta esempi o registri modello, essi devono essere completati con dati reali prima della consegna all'organismo di certificazione.

Ruolo	Nome/Funzione	Firma	Data
Preparazione	Dr. Prof. Giuseppe Izzo / Lead Auditor		
Verifica tecnica	Responsabile SGSI EZ Lab		
Approvazione	Alta Direzione EZ Lab		

1 - Indice controllato delle evidenze Stage 1

La seguente matrice collega le evidenze predisposte ai requisiti ISO/IEC 27001:2022 e alle aree da verificare in Stage 2. Lo stato 'da validare' indica che il documento deve essere approvato formalmente dall'organizzazione prima dell'uso ufficiale.

Codice	Evidenza	Requisiti ISO/IEC 27001:2022	Stato	Uso in Stage 1
E-01	Campo di applicazione e confini SGSI	4.3	Da validare	Conferma perimetro, sedi, cloud, dati e processi
E-02	Analisi contesto interno ed esterno	4.1	Da validare	Comprensione dei fattori rilevanti
E-03	Registro parti interessate	4.2	Da validare	Bisogni, aspettative e requisiti
E-04	Mappa processi SGSI e interazioni	4.4	Da validare	Sequenza, input/output e responsabilità
E-05	Registro requisiti legali e normativi	4.2, 6.1, Annex A 5.31	Da validare	Conformità legale e monitoraggio normativo
E-06	Politica sicurezza informazioni	5.2	Da approvare	Impegni della Direzione
E-07	Ruoli, responsabilità e RACI SGSI	5.3, 7.2	Da validare	Autorità, ownership e competenze
E-08	Inventario asset e classificazione	Annex A 5.9, 5.12, 5.13	Da validare	Asset informativi, applicativi e cloud
E-09	Metodologia risk assessment	6.1.2	Da approvare	Criteri di rischio e accettabilità
E-10	Estratto risk register	6.1.2	Da validare	Rischi SGSI pertinenti a IAF 33
E-11	Risk treatment plan	6.1.3	Da validare	Azioni, owner, scadenze e controllo
E-12	Estratto Statement of Applicability	6.1.3, Annex A	Da validare	Controlli applicabili/non applicabili
E-13	Obiettivi SGSI e indicatori	6.2, 9.1	Da validare	Misurabilità e monitoraggio
E-14	Gestione accessi e identità	Annex A 5.15, 5.16, 5.18, 8.2, 8.5	Da validare	MFA, account, privilegi, revoche
E-15	Gestione fornitori critici	Annex A 5.19-5.23	Da validare	Cloud, hosting, sviluppo, cybersecurity
E-16	Incident, complaint and event register	Annex A 5.24-5.28, 10.2	Da validare	Eventi, incidenti, reclami e data breach
E-17	Backup, restore e continuità	Annex A 5.29, 5.30, 8.13, 8.14	Da validare	Disponibilità, recovery e test
E-18	Audit interno e riesame Direzione	9.2, 9.3	Da validare	Prontezza Stage 2

2 - E-01 - Campo di applicazione e confini SGSI

Il campo di applicazione è definito considerando confini organizzativi, fisici, tecnologici e operativi. Il perimetro è coerente con servizi IT di Digital Product Passport, tracciabilità di filiera, blockchain, AI, smart label e data management.

Elemento	Descrizione controllata
Scope IT	Gestione della sicurezza delle informazioni per progettazione, sviluppo/configurazione, erogazione, manutenzione e supporto di soluzioni digitali per Digital Product Passport, tracciabilità di filiera, registrazione dati tramite blockchain, smart label, data management, servizi supportati da intelligenza artificiale, sostenibilità e compliance normativa europea, incluse consulenza, analisi requisiti, configurazione piattaforme, gestione dati cliente/prodotto/filiera, ambienti cloud/applicativi e supporto operativo.
Scope EN	Information security management for the design, development/configuration, delivery, maintenance and support of digital solutions for Digital Product Passport, supply chain traceability, blockchain-based data registration, smart labels, data management, AI-supported services, sustainability and European regulatory compliance, including consulting, requirements analysis, platform configuration, customer/product/supply-chain data management, cloud/application environments and operational support.
Siti inclusi	Sede principale Padova - DeGasp28 Innovation Hub, Piazza A. De Gasperi 28, 35131 Padova. Sedi operative/commerciali o di rappresentanza indicate dall'organizzazione: Milano, Pachino, Reims; inclusione ove coinvolte nei processi SGSI. Sono inclusi lavoro da remoto, ambienti cloud e strumenti collaborativi utilizzati da personale/collaboratori autorizzati.
Asset informativi inclusi	Dati clienti, dati fornitori, dati utenti, dati di prodotto, dati di filiera, documentazione progettuale, configurazioni applicative, credenziali, log, report, evidenze di conformità, repository documentali, informazioni contrattuali, commerciali e tecniche.
Esclusioni	Processi produttivi fisici dei clienti, impianti dei clienti, infrastrutture IT dei clienti non amministrate da EZ Lab, reti blockchain pubbliche non direttamente controllate, servizi cloud/hosting/connettività erogati autonomamente da fornitori terzi. Tali elementi sono comunque valutati come dipendenze esterne ove incidano su sicurezza, continuità o conformità del servizio.

Decisione Stage 1: campo di applicazione idoneo e coerente. In Stage 2 verificare corrispondenza tra scope, asset inventory, rischi, SoA e processi operativi campionati.

3 - E-02 - Analisi del contesto interno ed esterno

L'analisi del contesto è predisposta per documentare fattori rilevanti che possono influenzare la capacità del SGSI di raggiungere i risultati attesi. I fattori sono riesaminati almeno annualmente e in caso di cambiamenti significativi.

Tipo	Fattore	Impatto SGSI	Monitoraggio / evidenza
Interno	Modello operativo digitale e consulenziale	Necessità di controlli su dati, piattaforme, configurazioni, accessi e documentazione di progetto	Mappa processi; organigramma; scope SGSI
Interno	Competenze in blockchain, AI, DPP e data management	Protezione know-how, proprietà intellettuale, repository e output progettuali	Matrice competenze; NDA; access control
Interno	Uso di ambienti cloud e strumenti collaborativi	Dipendenza da configurazioni sicure, MFA, backup, log e provider terzi	Inventario asset; supplier register; cloud settings
Interno	Team distribuito e possibile remote working	Necessità di proteggere endpoint, accessi remoti, comunicazioni e documenti condivisi	Policy accessi; endpoint register; awareness
Interno	Ciclo di vita del servizio DPP	Rischio su integrità dati, change management e validazione output	Procedure operative; change log; evidenze progetto
Esterno	Evoluzione normativa europea su DPP/ESPR	Obbligo di monitoraggio normativo e aggiornamento requisiti di servizio	Registro requisiti legali; riesame Direzione
Esterno	Cyber threat landscape	Rischi di phishing, credenziali compromesse, vulnerabilità software, attacchi supply chain	Risk assessment; incident register; awareness
Esterno	Clienti multi-settore con dati di filiera	Necessità di segregazione, riservatezza e tracciabilità delle informazioni	Contratti; DPA; asset/data classification
Esterno	Fornitori tecnologici critici	Dipendenza da SLA, sicurezza cloud, disponibilità e sub-responsabili	Valutazione fornitori; contratti; SLA
Esterno	Mercato competitivo e reputazione	Incidenti o errori possono compromettere fiducia e posizionamento	KPI SGSI; reclami; monitoraggio eventi

4 - E-03 - Registro parti interessate e requisiti rilevanti

Le parti interessate sono state identificate in funzione del perimetro SGSI. I requisiti sono tradotti in controlli, obblighi documentali o input al risk assessment.

Parte interessata	Aspettative / requisiti	Implicazione SGSI	Evidenza
Direzione	Protezione asset, continuità servizi, conformità e reputazione	Politica, obiettivi, riesame, risk appetite	Politica; obiettivi; MRM
Clienti	Riservatezza, integrità, disponibilità, tracciabilità, compliance e SLA	Contratti, access control, backup, incident management	Contratti; ticket; SLA
Utenti piattaforme	Accesso sicuro, dati corretti, disponibilità, gestione credenziali	IAM, MFA, logging, supporto	Registro accessi; log; procedure
Fornitori cloud/IT	Requisiti chiari, sicurezza contrattuale, responsabilità definite	Supplier security, DPA, NDA, SLA	Registro fornitori; DPA
Personale/collaboratori	Regole chiare, competenze, strumenti sicuri	Awareness, procedure, ruoli	Matrice competenze; formazione
Autorità/regolatori	Conformità privacy, cybersecurity, gestione dati e DPP	Legal register, audit trail, data protection	Registro legale; procedure privacy
Partner e software house	Interoperabilità, protezione API/dati, governance progetto	Change management, accesso controllato	NDA; requisiti tecnici
Interessati privacy	Informazioni trasparenti, sicurezza dati, diritti GDPR	Privacy policy, minimizzazione, data breach	Informative; registro trattamenti

Riesame: annuale e in caso di nuovi servizi, nuovi fornitori critici, variazioni normative, nuovi mercati o incidenti significativi.

5 - E-04 - Mappa processi SGSI e interazioni

La sequenza dei processi SGSI è strutturata secondo logica Plan-Do-Check-Act e integrata con il ciclo di vita dei servizi IT erogati da EZ Lab.

Macroprocesso	Input	Attività chiave	Output / interazione
Governance SGSI	Strategia, contesto, parti interessate	Definizione politica, scope, obiettivi, ruoli	Direzione del SGSI; input al risk management
Risk management	Asset, minacce, requisiti, eventi	Valutazione rischi, trattamento, accettazione	Risk register, RTP, SoA
Commerciale e requisiti cliente	Lead, richiesta cliente, settore	Raccolta requisiti, fattibilità, requisiti privacy/sicurezza	Input a progettazione DPP e contratti
Progettazione/configurazione servizio	Requisiti, architettura, dati	Configurazione piattaforma, integrazioni, smart label, QR/NFC	Output servizio, change log, dati gestiti
Gestione dati e piattaforme	Dati cliente/prodotto/filiera	Raccolta, validazione, protezione, logging, backup	DPP, record blockchain, report
Supplier management	Necessità cloud/IT/servizi	Qualifica, contratto, monitoraggio, riesame	Fornitori approvati, SLA, DPA
Incident & continuity	Eventi, alert, reclami	Classificazione, contenimento, recovery, azioni correttive	Incident report, lessons learned, update rischi
Performance evaluation	KPI, audit, MRM, feedback	Analisi efficacia, audit interno, riesame Direzione	Miglioramento continuo

Interazione chiave

Il risk assessment guida la selezione dei controlli nel SoA; i controlli sono attuati nei processi operativi; incidenti, audit, reclami, KPI e fornitori alimentano riesame Direzione e miglioramento. Questa catena deve essere campionata in Stage 2.

6 - E-05 - Registro requisiti legali e normativi applicabili

Registro sintetico dei principali requisiti applicabili o da monitorare per servizi digitali, dati, cybersecurity, cloud, AI e Digital Product Passport. La valutazione di applicabilità deve essere riesaminata periodicamente dal responsabile SGSI con supporto legale/privacy.

Rif.	Requisito	Applicabilità / impatto	Controllo SGSI / evidenza
L-01	Reg. UE 2016/679 - GDPR; D.Lgs. 196/2003	Trattamento dati personali di clienti, utenti, referenti, fornitori, collaboratori; log e account	Registro trattamenti, informative, DPA, misure T/O, data breach
L-02	Direttiva UE 2022/2555 NIS 2 e D.Lgs. 138/2024	Da valutare per qualifica soggettiva; riferimento per governance cybersecurity, incidenti, supply chain	Valutazione applicabilità, incident process, supplier security
L-03	Reg. UE 2024/1781 ESPR	Rilevante per servizi Digital Product Passport, data carrier, interoperabilità e accesso dati	Monitoraggio normativo, requisiti DPP, design controls
L-04	Reg. UE 2024/2847 Cyber Resilience Act	Da monitorare per prodotti con elementi digitali, software/piattaforme rese disponibili	Secure development, vulnerability handling, update process
L-05	Reg. UE 2024/1689 AI Act	Applicabile ove siano sviluppate o integrate funzionalità AI	AI inventory, risk assessment, logging, trasparenza
L-06	Reg. UE 2023/2854 Data Act	Accesso, condivisione, interoperabilità e portabilità dei dati; smart contract	Clausole dati, data governance, access rights
L-07	Reg. UE 910/2014 eIDAS	Da monitorare se usati servizi fiduciari, identificazione, firme, timestamp	Requisiti tecnici/fornitore, evidenze validazione
L-08	Normativa IP, copyright, software, banche dati, segreti commerciali	Protezione know-how, codice, database, asset digitali e documentazione	NDA, access control, classificazione info
L-09	Contratti cliente e requisiti di riservatezza/SLA	Vincoli specifici di progetto, sicurezza, disponibilità, supporto	Contract review, SLA, ticket, registro requisiti cliente

7 - E-06 - Politica per la Sicurezza delle Informazioni

La seguente politica è predisposta come testo controllato da approvare da parte dell'Alta Direzione e comunicare alle parti interessate pertinenti.

EZ Lab si impegna a proteggere le informazioni trattate nell'ambito della progettazione, configurazione, erogazione, manutenzione e supporto di soluzioni digitali per Digital Product Passport, tracciabilità di filiera, blockchain, AI, smart label, data management, sostenibilità e compliance normativa europea.

La sicurezza delle informazioni è gestita secondo i principi di riservatezza, integrità, disponibilità, autenticità, tracciabilità e responsabilità, con approccio proporzionato ai rischi, ai requisiti dei clienti, agli obblighi legali e alle aspettative delle parti interessate.

La Direzione assicura risorse, ruoli, responsabilità, competenze e strumenti adeguati per mantenere il SGSI, promuovere consapevolezza, prevenire incidenti, proteggere dati e asset informativi, controllare fornitori critici, garantire continuità operativa e migliorare in modo continuo l'efficacia del sistema.

Tutto il personale, i collaboratori e i fornitori autorizzati sono tenuti a rispettare le politiche e procedure del SGSI, proteggere credenziali e informazioni, segnalare eventi o vulnerabilità, trattare i dati secondo necessità autorizzate e contribuire alla conformità del sistema.

Approvazione	Nome/Funzione	Firma	Data
Alta Direzione			
Responsabile SGSI			

8 - E-07 - Ruoli, responsabilità e RACI SGSI

La matrice RACI assegna responsabilità minime per il funzionamento del SGSI. I nominativi devono essere completati e approvati formalmente dall'organizzazione.

Processo / controllo	Direzione	Resp. SGSI	Tech Lead	Process Owner	Fornitore critico
Politica, scope, obiettivi	A	R	C	C	I
Risk assessment e trattamento	A	R	C	C	I
Statement of Applicability	A	R	C	C	I
Asset inventory	I	A	R	C	C
Access management	I	A	R	C	C
Secure configuration / change	I	C	R/A	C	C
Supplier security	A	R	C	C	C
Incident management	A	R	R	C	C
Backup / restore / continuity	A	C	R	C	R/C
Audit interno / riesame	A	R	C	C	I

Legenda: R = Responsible; A = Accountable; C = Consulted; I = Informed.

9 - E-08 - Inventario asset e classificazione

Inventario sintetico per lo Stage 1. In Stage 2 dovrà essere campionato su asset reali, owner, classificazione, ubicazione, controlli, backup e accessi autorizzati.

Categoria asset	Esempi	Classificazione	Owner	Controlli minimi
Dati cliente	Contatti, contratti, requisiti, ticket	Riservato	Commerciale / Resp. SGSI	Accesso role-based, NDA, DPA ove applicabile
Dati prodotto/filiera	Materiali, origine, certificazioni, sostenibilità	Riservato / critico	Project Owner	Segregazione progetto, validazione, tracciabilità
Piattaforme applicative	DPP Studio, Made in Block, dashboard	Critico	Tech Lead	MFA, logging, change management, backup
Cloud e repository	Storage, documenti, codice/configurazioni	Critico	Tech Lead	IAM, permessi minimi, audit log, versioning
Credenziali e profili	Account utenti, admin, API key	Segreto	Tech Lead	MFA, vault, revoca, review periodica
Documentazione SGSI	Politiche, procedure, rischi, SoA	Interno/Riservato	Resp. SGSI	Controllo versioni, approvazione, accesso controllato
Log e registrazioni	Access log, change log, incident log	Riservato	Tech Lead / Resp. SGSI	Retention, protezione, consultazione autorizzata
Endpoint	PC, laptop, smartphone aziendali	Interno/critico	Utente / Tech Lead	Cifratura, patching, antivirus/EDR, lock screen

10 - E-09 - Metodologia di valutazione del rischio

La metodologia è basata su scala qualitativa 1-5 per probabilità e impatto, calcolo del rischio come P x I, definizione di soglie di accettabilità e trattamento collegato ai controlli Annex A.

Parametro	Scala	Criterio
Probabilità	1-5	1 rara; 2 improbabile; 3 possibile; 4 probabile; 5 altamente probabile
Impatto	1-5	1 trascurabile; 2 limitato; 3 significativo; 4 grave; 5 critico su cliente, continuità, compliance o reputazione
Livello rischio	P x I	1-5 basso; 6-10 medio; 11-15 alto; 16-25 critico
Accettabilità	<=5 accettabile; 6-10 da monitorare; >=11 da trattare	I rischi elevati/critici richiedono trattamento, owner, scadenza e verifica efficacia
Riesame	Annuale o a evento	Nuovi servizi, incidenti, modifiche cloud, nuovi fornitori, cambi normativi, vulnerabilità rilevanti

Criterio senior di audit

La metodologia è accettabile per Stage 1 se è coerente, ripetibile, approvata e collegata a SoA e treatment plan. In Stage 2 il campionamento deve verificare che il rischio residuo derivi da controlli effettivamente attuati e non solo dichiarati.

11 - E-10 - Estratto registro rischi SGSI

ID	Scenario di rischio	Asset/processo	P	I	Inerente	Controlli / trattamento	Residuo
R-01	Accesso non autorizzato a piattaforme o dati cliente	Piattaforme, dati cliente	3	5	15 Alto	MFA, RBAC, review accessi, logging	6 Medio
R-02	Compromissione credenziali o phishing	Account, email, cloud	4	4	16 Critico	Awareness, MFA, password manager, alert	8 Medio
R-03	Errore di configurazione cloud/applicativa	Cloud, DPP Studio	3	5	15 Alto	Change approval, peer review, hardening checklist	6 Medio
R-04	Perdita o alterazione dati prodotto/filiera	Dati DPP	3	5	15 Alto	Validazione dati, backup, audit trail, blockchain notarization	6 Medio
R-05	Indisponibilità piattaforme critiche	Servizi digitali	3	4	12 Alto	Backup, BCP, SLA fornitore, monitoraggio	6 Medio
R-06	Vulnerabilità software non gestita	Piattaforme/app	3	4	12 Alto	Patch, vulnerability review, secure development	6 Medio
R-07	Fornitore cloud/IT non conforme o non disponibile	Supply chain IT	3	4	12 Alto	Qualifica fornitori, DPA/SLA, alternative, monitoraggio	6 Medio
R-08	Data breach con dati personali	Privacy/log/account	2	5	10 Medio	DPIA se necessario, minimizzazione, incident/data breach process	5 Basso
R-09	Mancata conformità normativa DPP/AI/Data Act	Servizi e consulenza	3	4	12 Alto	Legal register, review normativa, requisiti progetto	6 Medio
R-10	Uso non autorizzato di know-how/codice/documentazione	IP, repository	2	4	8 Medio	NDA, accessi minimi, repo permissions, classificazione	4 Basso

12 - E-11 - Piano di trattamento del rischio

Azione	Rischi	Controlli Annex A	Owner	Scadenza	Evidenza richiesta
Formalizzare review trimestrale accessi e privilegi	R-01, R-02	5.15, 5.16, 5.18, 8.2	Tech Lead	Q2 2026	Registro review accessi, revoche, autorizzazioni
Consolidare password manager/MFA per account critici	R-01, R-02	5.17, 8.5	Tech Lead	Q2 2026	Screenshot/config report, elenco account coperti
Rafforzare change management per configurazioni DPP	R-03, R-04	8.9, 8.32	Tech Lead	Q2 2026	Change log con approvazione, test, rollback
Aggiornare supplier security assessment	R-05, R-07	5.19-5.23	Resp. SGSI	Q2 2026	Schede fornitori, SLA, DPA, NDA
Eseguire test di restore campione	R-04, R-05	8.13, 5.30	Tech Lead	Q2 2026	Report restore test, esito, tempi
Integrare vulnerability review periodica	R-06	8.8, 8.25, 8.28	Tech Lead	Q3 2026	Registro vulnerabilità/patch
Aggiornare registro requisiti DPP/AI/Data Act	R-09	5.31, 5.36	Resp. SGSI/Legal	Q2 2026	Registro normativo aggiornato
Erogare awareness sicurezza e phishing	R-02, R-08	6.3, 6.8	Resp. SGSI	Q2 2026	Registro formazione e test apprendimento

13 - E-12 - Estratto Statement of Applicability

Estratto ad alto valore per Stage 1. La SoA completa deve contenere tutti i controlli Annex A, stato di applicabilità, giustificazione, controllo esistente/pianificato, owner ed evidenza.

Ctrl.	Titolo	Applicabilità	Giustificazione / evidenza attesa
5.1	Policies for information security	Applicabile	Politica SGSI approvata e comunicata
5.7	Threat intelligence	Applicabile	Monitoraggio vulnerabilità, vendor advisories, fonti cyber
5.9	Inventory of information and other associated assets	Applicabile	Inventario asset e owner
5.12	Classification of information	Applicabile	Classificazione dati cliente/prodotto/filiera
5.15	Access control	Applicabile	RBAC, least privilege, processi autorizzativi
5.16	Identity management	Applicabile	Gestione lifecycle account utenti/admin
5.19	Information security in supplier relationships	Applicabile	Qualifica e monitoraggio fornitori cloud/IT
5.23	Information security for use of cloud services	Applicabile	Valutazione cloud, configurazioni sicure, SLA
5.24	Incident management planning and preparation	Applicabile	Procedura incident management e ruoli
5.30	ICT readiness for business continuity	Applicabile	BCP/DR, backup, restore test
5.31	Legal, statutory, regulatory and contractual requirements	Applicabile	Registro requisiti legali e contrattuali
6.3	Information security awareness, education and training	Applicabile	Piano awareness, registri formazione
7.1	Physical security perimeters	Applicabile proporzionata	Sedi/coworking/uffici: controlli fisici e accessi
8.5	Secure authentication	Applicabile	MFA per servizi critici e account privilegiati
8.8	Management of technical vulnerabilities	Applicabile	Patch/vulnerability management
8.13	Information backup	Applicabile	Backup, retention e test ripristino
8.15	Logging	Applicabile	Log accessi, admin, applicativi, change
8.25	Secure development life cycle	Applicabile	Ciclo di sviluppo/configurazione sicuro
8.28	Secure coding	Applicabile se sviluppo software	Linee guida e review codice/configurazione
8.32	Change management	Applicabile	Richieste, approvazioni, test, rilascio

14 - E-13 - Obiettivi SGSI e indicatori

Obiettivo	Indicatore	Target 2026	Responsabile	Frequenza
Ridurre il rischio di accessi non autorizzati	% account critici con MFA; review accessi	>=95% MFA; review trimestrale	Tech Lead	Trimestrale
Migliorare gestione fornitori critici	% fornitori valutati; DPA/SLA disponibili	100% fornitori critici valutati	Resp. SGSI	Semestrale
Garantire continuità dei servizi digitali	Esito backup/restore test; incidenti disponibilità	1 test restore/anno; 0 incidenti critici non gestiti	Tech Lead	Annuale/evento
Aumentare consapevolezza sicurezza	% personale/collaboratori formati	100% figure coinvolte nel perimetro	Resp. SGSI	Annuale
Migliorare controllo modifiche	% modifiche critiche con approvazione/test	>=95%	Tech Lead	Trimestrale
Mantenere conformità normativa	Aggiornamenti registro legale e valutazione impatti	Riesame almeno semestrale	Resp. SGSI/Legal	Semestrale

15 - E-14 - Evidenza gestione accessi e identità

Scheda di controllo per verificare che gli accessi agli ambienti digitali siano autorizzati, proporzionati e riesaminati. Da compilare con elenco account reale e allegati tecnici.

Controllo	Criterio operativo	Evidenza da allegare	Esito Stage 1
Creazione account	Richiesta autorizzata da owner; ruolo definito; profilo minimo necessario	Ticket/richiesta account; elenco ruoli	Adeguato su base documentale
Modifica privilegi	Cambio profilo approvato e tracciato	Change/access log	Da campionare in Stage 2
Revoca accessi	Revoca tempestiva a cessazione rapporto o cambio ruolo	Registro revoche; offboarding checklist	Da verificare
MFA	Abilitata su account critici, cloud, repository, admin	Report configurazione MFA	Da verificare
Privileged access	Account admin limitati, tracciati, segregati	Elenco admin; log accessi	Da campionare
Review periodica	Riesame trimestrale/semestrale degli accessi critici	Verbale review accessi	Azione Stage 2

16 - E-15 - Evidenza gestione fornitori critici

Il controllo dei fornitori critici deve coprire cloud, hosting, sviluppo, servizi IT/cybersecurity, consulenza e qualsiasi fornitore con accesso a dati, sistemi o processi nel perimetro SGSI.

Fornitore / categoria	Criticità	Requisiti minimi	Evidenze richieste
Cloud provider	Alta	SLA, sicurezza, data location, backup, logging, DPA	Contratto, DPA, scheda valutazione, SLA
Hosting / dominio / DNS	Alta	Disponibilità, change control, protezione account admin	SLA, MFA, access review
Software house / sviluppo	Alta se accesso a codice/dati	NDA, secure development, segregazione accessi	NDA, repo permissions, change log
Strumenti collaboration	Media/Alta	MFA, permessi, retention, condivisioni controllate	Config report, policy sharing
Consulenti legali/privacy	Media	Riservatezza, competenza, controllo documenti	Contratto/NDA, incarico
Cybersecurity support	Alta	Competenze, riservatezza, report test, gestione vulnerability	Contratto, report tecnici, piano azioni

17 - E-16 - Registro incidenti, eventi, reclami e segnalazioni

Registro modello da utilizzare per eventi di sicurezza, vulnerabilità, reclami clienti o segnalazioni delle parti interessate. Se non sono presenti incidenti, registrare comunque il riesame periodico con esito 'nessun evento rilevante'.

ID	Data	Tipo	Descrizione	Impatto CIA	Azione	Stato
EVT-2026-001	Da compilare	Evento/Segnalazione	Nessun evento critico registrato nel periodo Stage 1; campo da validare con log/ticket effettivi	N/A	Riesame ticket/log; conferma Direzione	Da validare
EVT-2026-002	Da compilare	Reclamo	Nessun reclamo critico sicurezza informazioni rilevato; campo da validare con canali supporto	N/A	Riesame reclami e ticket	Da validare

Criterio di gestione

Ogni evento deve essere classificato, assegnato a owner, trattato con azioni proporzionate e riesaminato per aggiornare risk assessment, controlli, awareness o contratti con fornitori se necessario.

18 - E-17 - Backup, restore e continuità operativa

Per Stage 1 è sufficiente dimostrare che il processo è definito; per Stage 2 occorrono evidenze di backup effettivo, test di restore, responsabilità, frequenze e risultati.

Asset/servizio	Requisito	Backup/continuità	Evidenza Stage 2
Repository documentale SGSI	Disponibilità e integrità documenti controllati	Versioning, backup cloud, permessi controllati	Log/versioni e test recupero documento
Piattaforme DPP / dashboard	Continuità dei servizi cliente	Backup dati/configurazioni, SLA cloud, monitoraggio	Report backup; SLA; incident/uptime
Database o dati progetto	Integrità dati cliente/prodotto/filiera	Backup pianificato, retention, restore test	Restore test firmato
Email e comunicazioni	Tracciabilità requisiti e supporto	Retention e archiviazione secondo policy	Config retention / export campione
Credenziali e secrets	Disponibilità controllata e sicurezza	Vault/password manager con recovery controllato	Policy e registro accessi admin

19 - E-18 - Audit interno e riesame della Direzione

Registrazioni di governance da allegare o richiamare nel fascicolo Stage 1. Le date indicate devono corrispondere a verbali effettivamente sottoscritti; in mancanza, compilare come piano e non come registrazione consuntiva.

Registrazione	Contenuto minimo	Stato	Riferimento
Audit interno SGSI	Piano, criteri ISO/IEC 27001:2022, campo di audit, checklist, evidenze, rilievi, conclusioni, azioni	Da validare	AI-27001-2026
Riesame Direzione SGSI	Input 9.3.2, output 9.3.3, decisioni, risorse, azioni miglioramento, approvazione Direzione	Da validare	MRM-27001-2026
Registro azioni correttive/miglioramento	Rilievo, causa, azione, owner, data, verifica efficacia	Da validare	CAPA-2026
Piano Stage 2	Aree da campionare, evidenze operative, responsabili, disponibilità dati	Predisposto	S2-PLAN-2026

Nota di audit

Lo Stage 1 può concludersi positivamente se il SGSI è documentato e la prontezza allo Stage 2 è dimostrabile. Lo Stage 2 dovrà verificare efficacia reale: registrazioni primarie, interviste, campionamento tecnico e coerenza tra rischi, SoA e controlli implementati.

20 - Check-list di prontezza allo Stage 2

Area	Evidenza da rendere disponibile	Priorità	Stato
Scope e processi	Scope approvato, mappa processi, sedi e confini tecnici	Alta	Pronto per validazione
Risk management	Risk assessment, RTP, accettazione rischio, aggiornamenti	Alta	Pronto per validazione
SoA	SoA completa con applicabilità, giustificazioni, controlli e prove	Alta	Da completare con prove
Accessi	Elenco account, MFA, admin, review accessi e revoche	Alta	Da campionare
Cloud	Contratti/SLA, configurazioni sicurezza, backup, log	Alta	Da campionare
Fornitori	Registro critici, valutazioni, DPA, NDA, SLA	Alta	Da validare
Change management	Richieste, test, approvazioni, rilasci, rollback	Alta	Da campionare
Incidenti	Registro eventi, test procedura, escalation, data breach	Media/Alta	Da validare
Backup/restore	Piani, log backup, test restore, esiti	Alta	Da campionare
Awareness	Piano formazione, presenze, materiali, test comprensione	Media	Da validare
Audit/MRM	Rapporti, verbali, azioni e follow-up	Alta	Da validare

21 - Fonti pubbliche e riferimenti documentali

Le seguenti fonti pubbliche sono state utilizzate per contestualizzare attività, servizi, sedi e tecnologie citate nel dossier. La documentazione primaria del SGSI deve restare quella approvata dall'organizzazione.

Fonte	Informazione utilizzata	Riferimento
Sito ufficiale EZ Lab	DPP Studio, tecnologie blockchain, smart contracts, NFT, AI, Digital Twin, settori e servizi	https://www.ezlab.it/
Pagina Passaporto Digitale di Prodotto	DPP con blockchain e AI, QR Code/NFC, interoperabilità, sicurezza, scalabilità	https://www.ezlab.it/servizi/passaporto-digitale-di-prodotto/
Pagina contatti EZ Lab	Sedi operative/commerciali: Padova, Milano, Pachino, Reims e riferimenti di contatto	https://www.ezlab.it/contatti/
ISO/IEC 27001:2022	Requisiti SGSI clausole 4-10 e Annex A	Norma di riferimento
ISO/IEC 27002:2022	Linee guida controlli sicurezza informazioni	Norma guida
GDPR / D.Lgs. 196/2003	Protezione dati personali	Registro requisiti legali
NIS 2 / D.Lgs. 138/2024	Cybersecurity governance e gestione rischio	Registro requisiti legali
ESPR, AI Act, Data Act, Cyber Resilience Act	DPP, AI, dati, cybersecurity by design	Registro requisiti legali

Conclusione: il dossier è idoneo come allegato tecnico allo Stage 1, a supporto della raccomandazione di prosecuzione verso Stage 2, subordinatamente alla validazione delle evidenze e alla disponibilità delle registrazioni primarie richieste.

22 - Foglio finale di validazione e consegna

Con la sottoscrizione del presente foglio, l'organizzazione conferma di aver riesaminato il dossier, verificato la corrispondenza delle evidenze al proprio SGSI e autorizzato l'inserimento nel fascicolo Stage 1.

Dichiarazione	Conferma
Le evidenze sono coerenti con il campo di applicazione del SGSI	Si / No
Le informazioni relative a sedi, processi, asset e fornitori sono state riesaminate	Si / No
Le registrazioni richiamate sono disponibili o pianificate con responsabilità assegnate	Si / No
Il dossier può essere allegato allo Stage 1 ISO/IEC 27001:2022	Si / No

Ruolo	Nome	Firma	Data
Alta Direzione			
Responsabile SGSI			
Lead Auditor	Dr. Prof. Giuseppe Izzo		