SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Statement of Applicability

ITLAB S.R.L. è una società a responsabilità limitata con sede legale a Milano, operante nel settore ICT, software, reti telematiche, servizi digitali e soluzioni tecnologiche applicate anche al settore sanitario. L'organizzazione svolge attività di progettazione, sviluppo, installazione, distribuzione, assistenza, manutenzione e commercializzazione di prodotti software, reti telematiche, banche dati, servizi internet, servizi multimediali, trasmissione dati, hosting specializzato, trattamento elettronico e non elettronico dei dati, consulenza organizzativa e gestionale, efficientamento dei processi aziendali e formazione informatica. La società opera inoltre nell'ambito della telemedicina, del monitoraggio a distanza, della prenotazione di prestazioni domiciliari, della refertazione, dell'home care e del supporto a strutture sanitarie pubbliche e private, con particolare attenzione alla protezione dei dati personali, alla sicurezza delle informazioni, all'interoperabilità dei sistemi tecnologici e alla conformità normativa applicabile, inclusa la normativa privacy e GDPR.
ITLAB S.R.L. dispone di una sede legale a Milano e di unità operative a Francavilla al Mare e Napoli. L'attività primaria dichiarata presso l'unità locale di Francavilla al Mare è l'attività di programmazione informatica.

Codice	SGSI-SOA-001
Data documento	05/05/2026
Versione	00
Approvato da	Alta direzione

PRESENTAZIONE

Il presente documento è redatto per fornire una rappresentazione organica, elegante e professionale del Sistema di Gestione per la Sicurezza delle Informazioni dell'organizzazione, collegando business, asset, rischi, controlli, responsabilità e miglioramento continuo in un impianto coerente con la ISO/IEC 27001:2022.

SCOPO

Lo scopo del documento è supportare direzione, funzioni aziendali, auditor, consulenti e parti autorizzate nella comprensione del perimetro del SGSI, della logica di governo adottata, delle priorità di rischio e delle misure poste a presidio delle informazioni e dei servizi rilevanti.

DESCRIZIONE DELL'AZIENDA

ITLAB S.R.L. è una società a responsabilità limitata con sede legale a Milano, operante nel settore ICT, software, reti telematiche, servizi digitali e soluzioni tecnologiche applicate anche al settore sanitario.
L'organizzazione svolge attività di progettazione, sviluppo, installazione, distribuzione, assistenza, manutenzione e commercializzazione di prodotti software, reti telematiche, banche dati, servizi internet, servizi multimediali, trasmissione dati, hosting specializzato, trattamento elettronico e non elettronico dei dati, consulenza organizzativa e gestionale, efficientamento dei processi aziendali e formazione informatica.
La società opera inoltre nell'ambito della telemedicina, del monitoraggio a distanza, della prenotazione di prestazioni domiciliari, della refertazione, dell'home care e del supporto a strutture sanitarie pubbliche e private, con particolare attenzione alla protezione dei dati personali, alla sicurezza delle informazioni, all'interoperabilità dei sistemi tecnologici e alla conformità normativa applicabile, inclusa la normativa privacy e GDPR.
ITLAB S.R.L. dispone di una sede legale a Milano e di unità operative a Francavilla al Mare e Napoli.
L'attività primaria dichiarata presso l'unità locale di Francavilla al Mare è l'attività di programmazione informatica.

DESCRIZIONE DEL SERVIZIO

Il servizio oggetto del Sistema di Gestione per la Sicurezza delle Informazioni riguarda la progettazione, sviluppo, gestione, manutenzione e supporto di soluzioni software, piattaforme digitali, sistemi informatici e servizi tecnologici destinati a clienti pubblici e privati, con particolare riferimento ad applicazioni ICT, servizi internet, hosting specializzato, reti telematiche, trattamento dati, telemedicina, monitoraggio a distanza, home care e servizi digitali a supporto di strutture sanitarie e professionisti del settore.
Il servizio comprende le attività di analisi dei requisiti, sviluppo e configurazione software, gestione delle infrastrutture e degli ambienti applicativi, assistenza tecnica, manutenzione evolutiva e correttiva, supporto agli utenti, gestione documentale e trattamento delle informazioni aziendali e dei dati dei clienti. Nell'ambito dei servizi erogati possono essere trattate informazioni riservate, dati personali, dati relativi a clienti, fornitori, partner, utenti e, ove applicabile, dati connessi a servizi sanitari o assistenziali.
Il servizio è erogato nel rispetto dei requisiti di riservatezza, integrità e disponibilità delle informazioni, attraverso processi organizzativi e tecnici finalizzati alla gestione dei rischi di sicurezza informatica, alla protezione dei dati, alla continuità operativa, al controllo degli accessi, alla gestione degli incidenti, alla sicurezza delle infrastrutture e alla conformità normativa applicabile.

INDICE DEL DOCUMENTO

TERMINI IN USO

Termine	Definizione
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni.
Informazione	Dato o insieme di dati rilevanti per l'organizzazione, indipendentemente dal formato o supporto.
Asset	Qualsiasi risorsa informativa, organizzativa, tecnologica, fisica o di supporto rilevante per il SGSI.
Rischio	Effetto dell'incertezza sugli obiettivi, valutato in termini di probabilità e impatto.
Controllo	Misura organizzativa, fisica o tecnica adottata per modificare o presidiare il rischio.
Trattamento del rischio	Decisione e insieme di azioni per mitigare, trasferire, evitare o accettare un rischio.
SoA	Statement of Applicability: documento che riporta i controlli applicabili, il relativo stato e la giustificazione.
Parte interessata	Soggetto interno o esterno che può influenzare, essere influenzato o percepirsi influenzato dal SGSI.

DICHIARAZIONE DI APPLICABILITÀ

La seguente tabella riporta i controlli considerati nel perimetro SGSI, l’applicabilità, lo stato di implementazione e la relativa giustificazione.

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
A.5.1	Politiche per la sicurezza delle informazioni	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.2	Ruoli e responsabilità per la sicurezza delle informazioni	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.7	Threat intelligence	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.9	Inventario degli asset informativi	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
					associati e al piano di trattamento in essere.
A.5.10	Uso accettabile degli asset	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.12	Classificazione delle informazioni	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.15	Controllo degli accessi	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.18	Diritti di accesso	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.19	Sicurezza delle informazioni nei rapporti con i fornitori	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.23	Sicurezza per l’uso dei servizi cloud	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.24	Pianificazione della gestione incidenti	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.5.29	Sicurezza durante la disruption	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
A.5.30	ICT readiness per la continuità	Organizzativi	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.6.3	Consapevolezza e formazione	Persone	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.6.5	Responsabilità a fine rapporto o cambio ruolo	Persone	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.7.1	Perimetri di sicurezza fisica	Fisici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.7.2	Controlli di accesso fisico	Fisici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.7.4	Monitoraggio sicurezza fisica	Fisici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.7.8	Collocazione e protezione apparecchiature	Fisici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.1	Dispositivi endpoint utente	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.2	Accessi privilegiati	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
					associati e al piano di trattamento in essere.
A.8.3	Restrizione accessi alle informazioni	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.5	Autenticazione sicura	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.8	Gestione vulnerabilità tecniche	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.9	Configuration management	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.10	Cancellazione delle informazioni	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.11	Data masking	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.12	Data leakage prevention	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.13	Backup delle informazioni	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.

Codice	Controllo	Dominio	Applicabile	Stato	Giustificazione
A.8.15	Logging	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.16	Monitoring activities	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.23	Web filtering	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.
A.8.24	Uso della crittografia	Tecnologici	Sì	planned	Controllo applicabile in relazione agli asset del perimetro SGSI, ai rischi associati e al piano di trattamento in essere.