SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Piano di Trattamento del Rischio

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-TRT-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.

PIANO DI TRATTAMENTO DEL RISCHIO

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Portale clienti / area riservata, con owner Responsabile IT / Commerciale e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT / Commerciale	2026-07-04	planned
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione	HR	2026-07-04	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
			operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.			
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Archivi cartacei riservati, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Amministrazione / Direzione	2026-07-04	planned
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Piattaforma documentale / DMS, con owner Qualità / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Qualità / IT	2026-07-04	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Marketing / IT	2026-07-04	planned
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Documenti contrattuali e amministrativi, con owner Amministrazione / Direzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Amministrazione / Direzione	2026-07-04	planned
Perdita di disponibilità dell’asset / Procedure di gestione non formalizzate o misure di protezione non proporzionate		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell’esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Sito web aziendale, con owner Marketing / IT e presidio del controllo Controlli	Marketing / IT	2026-07-04	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
			organizzativi e tecnici proporzionati.			
Smarrimento o furto del dispositivo / Cifratura disco assente o controllo remoto non attivo		mitigate	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Dispositivi mobili aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-06-04	planned
Smarrimento o furto del dispositivo / Cifratura disco assente o controllo remoto non attivo		mitigate	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per PC e laptop dipendenti, con owner Responsabili di funzione e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabili di funzione	2026-06-04	planned
Malware, ransomware o indisponibilità infrastrutturale / Patching incompleto, hardening insufficiente o monitoraggio debole		mitigate	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Workspace cloud collaborativo, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-05-20	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
Malware, ransomware o indisponibilità infrastrutturale / Patching incompleto, hardening insufficiente o monitoraggio debole		mitigate	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Firewall e apparati di rete, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-05-20	planned
Corruzione o modifica impropria dei dati / Mancanza di segregazione ruoli, log e controlli di integrità		mitigate	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per CRM / ERP, con owner Responsabile di processo e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile di processo	2026-05-20	planned
Accesso non autorizzato ai dati / Credenziali deboli, MFA non attiva o privilegi eccessivi		mitigate	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per CRM / ERP, con owner Responsabile di processo e presidio del controllo	Responsabile di processo	2026-05-20	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
			Controlli organizzativi e tecnici proporzionati.			
Impossibilità di ripristino / Backup non testati o retention inadeguata		mitigate	Mitigare il rischio implementando backup periodici, test di ripristino, retention definita e monitoraggio dell'esito dei job. Controlli suggeriti: A.8.13 Information backup; A.5.30 ICT readiness for business continuity. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Backup aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-05-20	planned
Malware, ransomware o indisponibilità infrastrutturale / Patching incompleto, hardening insufficiente o monitoraggio debole		mitigate	Mitigare il rischio con patch management, protezioni endpoint, filtro e-mail/web e monitoraggio centralizzato degli eventi di sicurezza. Controlli suggeriti: A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.16 Monitoring activities. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Server / infrastruttura virtuale, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile IT	2026-05-20	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
Corruzione o modifica impropria dei dati / Mancanza di segregazione ruoli, log e controlli di integrità		mitigate	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile commerciale / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile commerciale / IT	2026-05-20	planned
Accesso non autorizzato ai dati / Credenziali deboli, MFA non attiva o privilegi eccessivi		mitigate	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights. Azione operativa suggerita: definire attività, evidenze, verifiche e responsabilità per Database clienti, con owner Responsabile commerciale / IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.	Responsabile commerciale / IT	2026-05-20	planned
Phishing e compromissione account / Formazione insufficiente, MFA assente, filtri antispam non adeguati		mitigate	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning. Controlli suggeriti: A.5.15 Access control; A.8.5 Secure authentication; A.8.2 Privileged access rights; A.6.3 Information security awareness, education and training; A.5.10 Acceptable use of information and other associated assets. Azione operativa suggerita: definire	Responsabile IT	2026-05-20	planned

Rischio	Controllo	Tipo	Azione	Responsabile	Scadenza	Stato
			attività, evidenze, verifiche e responsabilità per Caselle e-mail aziendali, con owner Responsabile IT e presidio del controllo Controlli organizzativi e tecnici proporzionati.			