SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Registro dei Rischi

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-RSK-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.

REGISTRO DEI RISCHI

Asset	Minaccia	Vulnerabilità	Impatto	Probabilità	Score	Livello	Responsabile	Trattamento
Caselle e-mail aziendali	Phishing e compromissione account	Formazione insufficiente, MFA assente, filtri antispam non adeguati	4 Alto - interruzione rilevante del servizio o danno reputazionale	4 Alta - evento probabile nel breve periodo	16	Critico	Responsabile IT	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.
Workspace cloud collaborativo	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile IT	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.
Firewall e apparati di rete	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile IT	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.
CRM / ERP	Corruzione o modifica impropria dei dati	Mancanza di segregazione ruoli, log e controlli di integrità	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile di processo	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici.
CRM / ERP	Accesso non autorizzato ai dati	Credenziali deboli, MFA non attiva o	5 Molto alto - blocco	3 Media - evento	15	Critico	Responsabile di processo	Mitigare il rischio applicando il principio del minimo privilegio, attivando

Asset	Minaccia	Vulnerabilità	Impatto	Probabilità	Score	Livello	Responsabile	Trattamento
		privilegi eccessivi	operativo, perdita dati critica o violazione grave	possibile in condizioni normali				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.
Backup aziendali	Impossibilità di ripristino	Backup non testati o retention inadeguata	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile IT	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.
Server / infrastruttura virtuale	Malware, ransomware o indisponibilità infrastrutturale	Patching incompleto, hardening insufficiente o monitoraggio debole	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile IT	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.
Database clienti	Corruzione o modifica impropria dei dati	Mancanza di segregazione ruoli, log e controlli di integrità	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile commerciale / IT	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici.
Database clienti	Accesso non autorizzato ai dati	Credenziali deboli, MFA non attiva o privilegi eccessivi	5 Molto alto - blocco operativo, perdita dati critica o violazione grave	3 Media - evento possibile in condizioni normali	15	Critico	Responsabile commerciale / IT	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.
Dispositivi mobili aziendali	Smarrimento o furto del dispositivo	Cifratura disco assente o controllo remoto non attivo	4 Alto - interruzione rilevante del servizio o danno reputazionale	3 Media - evento possibile in condizioni normali	12	Alto	Responsabile IT	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici.
PC e laptop dipendenti	Smarrimento o furto del dispositivo	Cifratura disco assente o controllo remoto non attivo	4 Alto - interruzione rilevante del servizio o danno reputazionale	3 Media - evento possibile in condizioni normali	12	Alto	Responsabili di funzione	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici.

Asset	Minaccia	Vulnerabilità	Impatto	Probabilità	Score	Livello	Responsabile	Trattamento
Portale clienti / area riservata	Perdita di disponibilità dell'asset	Procedure di gestione non formalizzate o misure di protezione non proporzionate	3 Medio - impatto operativo o economico moderato	3 Media - evento possibile in condizioni normali	9	Medio	Responsabile IT / Commerciale	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.
Sistema HR / anagrafiche personale	Perdita di disponibilità dell'asset	Procedure di gestione non formalizzate o misure di protezione non proporzionate	3 Medio - impatto operativo o economico moderato	3 Media - evento possibile in condizioni normali	9	Medio	HR	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.
Archivi cartacei riservati	Perdita di disponibilità dell'asset	Procedure di gestione non formalizzate o misure di protezione non proporzionate	3 Medio - impatto operativo o economico moderato	3 Media - evento possibile in condizioni normali	9	Medio	Amministrazione / Direzione	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.
Piattaforma documentale / DMS	Perdita di disponibilità dell'asset	Procedure di gestione non formalizzate o misure di protezione non proporzionate	3 Medio - impatto operativo o economico moderato	3 Media - evento possibile in condizioni normali	9	Medio	Qualità / IT	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.
Sito web aziendale	Perdita di disponibilità dell'asset	Procedure di gestione non formalizzate o misure di protezione non proporzionate	3 Medio - impatto operativo o economico moderato	3 Media - evento possibile in condizioni normali	9	Medio	Marketing / IT	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.
Documenti contrattuali e amministrativi	Perdita di disponibilità dell'asset	Procedure di gestione non formalizzate o misure di protezione non proporzionate	3 Medio - impatto operativo o economico moderato	3 Media - evento possibile in condizioni normali	9	Medio	Amministrazione / Direzione	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.
Sito web aziendale	Perdita di disponibilità dell'asset	Procedure di gestione non formalizzate o misure di protezione non proporzionate	3 Medio - impatto operativo o economico moderato	3 Media - evento possibile in condizioni normali	9	Medio	Marketing / IT	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.