SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Manuale SGSI

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-MAN-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

1. Scopo e finalità del manuale
2. Campo di applicazione del SGSI
3. Riferimenti normativi e criteri di conformità
4. Contesto dell’organizzazione e parti interessate
5. Leadership, governo e responsabilità
6. Sedi, unità organizzative e ambienti inclusi
7. Asset informativi e criteri di classificazione
8. Metodologia di valutazione e trattamento del rischio
9. Quadro dei rischi e priorità di intervento
10. Obiettivi SGSI, pianificazione e risorse
11. Controlli, Statement of Applicability e piano di trattamento
12. Competenza, consapevolezza, comunicazione e controllo documentale
13. Gestione operativa, monitoraggio e risposta agli eventi
14. Audit interni, riesame della direzione e miglioramento continuo
15. Allegati e documenti correlati

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.

1. SCOPO E FINALITÀ DEL MANUALE

1.1 Scopo del manuale

Il presente Manuale SGSI definisce l’architettura di governo, i criteri metodologici, i ruoli, i processi e le regole operative mediante cui iTLab S.r.l. istituisce, attua, mantiene e migliora il proprio Sistema di Gestione

per la Sicurezza delle Informazioni. Il manuale costituisce il riferimento di alto livello del sistema e raccorda contesto organizzativo, analisi dei rischi, piano di trattamento, controlli applicabili, procedure operative, riesame e miglioramento continuo, in coerenza con i requisiti della ISO/IEC 27001 e con le migliori pratiche internazionali di governance.

1.2 Profilo aziendale

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.

1.3 Campo di applicazione di alto livello

Il SGSI è concepito per proteggere informazioni, asset, processi e servizi che sostengono gli obiettivi aziendali, salvaguardando riservatezza, integrità, disponibilità, autenticità e tracciabilità dove necessario.

1.4 Politica per la sicurezza delle informazioni

La Direzione si impegna a garantire che la sicurezza delle informazioni sia allineata agli obiettivi di business, sostenuta da adeguate risorse, integrata nei processi aziendali e riesaminata periodicamente per assicurarne efficacia, pertinenza e miglioramento continuo.

2. CAMPO DI APPLICAZIONE DEL SGSI

Il Sistema di Gestione per la Sicurezza delle Informazioni di ITLAB S.R.L. si applica alla progettazione, sviluppo, gestione, manutenzione, assistenza e supporto di soluzioni software, piattaforme digitali, sistemi informatici, reti telematiche, servizi internet, hosting specializzato, trattamento elettronico e non elettronico dei dati, servizi ICT e servizi tecnologici a supporto di clienti pubblici e privati, con particolare riferimento anche all'ambito della telemedicina, del monitoraggio a distanza, dell'home care, della prenotazione di prestazioni domiciliari, della refertazione e dei servizi digitali a supporto di strutture sanitarie, professionisti sanitari e organizzazioni pubbliche e private.

Il perimetro del SGSI comprende i processi di analisi dei requisiti, progettazione e sviluppo software, configurazione e gestione applicativa, assistenza tecnica, manutenzione correttiva ed evolutiva, gestione degli ambienti informatici, gestione delle infrastrutture e degli strumenti digitali utilizzati per l'erogazione dei servizi, gestione degli accessi, gestione degli incidenti di sicurezza, continuità operativa, protezione dei dati, gestione documentale, gestione dei fornitori e gestione dei rapporti con clienti, partner e soggetti terzi coinvolti nell'erogazione dei servizi.

Sono comprese nello scopo le informazioni aziendali, tecniche, amministrative e commerciali, i dati relativi a clienti, utenti, fornitori, partner, personale e collaboratori, nonché i dati personali e, ove applicabile, le informazioni connesse a servizi sanitari, assistenziali o di telemedicina trattate nell'ambito delle attività aziendali.

Il perimetro fisico comprende la sede legale di Milano, Via Pietro Giannone 9, l'unità locale operativa di Francavilla al Mare, Via Nazionale Adriatica Nord 278, presso la quale risulta esercitata l'attività di programmazione informatica, e l'unità locale di Napoli, Via Toledo 289, adibita a ufficio. Il perimetro logico comprende sistemi informativi, applicazioni, piattaforme software, ambienti di sviluppo, sistemi di comunicazione, archivi documentali, dispositivi, credenziali, account, strumenti cloud e infrastrutture tecnologiche utilizzati per l'erogazione e il governo dei servizi.

Sono esclusi dallo scopo del SGSI i processi, le infrastrutture e le attività non sotto il controllo diretto di ITLAB S.R.L., salvo gli aspetti di sicurezza disciplinati tramite accordi contrattuali, requisiti di fornitura, controlli sui fornitori e responsabilità condivise con clienti, partner o provider tecnologici.

Il perimetro del SGSI comprende persone, processi, informazioni, tecnologie, servizi e siti inclusi nell'ambito dichiarato, nonché gli asset e i trattamenti correlati che possono influire su riservatezza, integrità e disponibilità delle informazioni rilevanti per l'organizzazione e per le parti interessate.

2.1 Confini fisici, logici e organizzativi

I confini del sistema includono le sedi, le unità organizzative, le piattaforme, le infrastrutture, i servizi e i flussi informativi ricompresi nel perimetro dichiarato. Sono inclusi anche i fornitori critici, i processi esternalizzati e gli ambienti digitali che trattano o supportano informazioni rilevanti per il business.

3. RIFERIMENTI NORMATIVI E CRITERI DI CONFORMITÀ

3.1 Riferimenti applicabili

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- GDPR / Regolamento (UE) 2016/679
- NIS2 ove applicabile
- Obblighi contrattuali e requisiti cliente
- Policy, procedure e registrazioni interne del SGSI

3.2 Criteri di conformità

Il sistema è sviluppato assumendo come quadro di riferimento la ISO/IEC 27001, la Statement of Applicability aziendale, le procedure interne, gli obblighi contrattuali, i requisiti cogenti applicabili e gli impegni assunti verso clienti, partner, personale, fornitori e altre parti interessate. Eventuali requisiti aggiuntivi di natura legale, regolatoria, settoriale o contrattuale devono essere recepiti nei registri, nei controlli e nei piani di azione del SGSI.

4. CONTESTO DELL'ORGANIZZAZIONE E PARTI INTERESSATE

4.1 Analisi del contesto interno

ITLAB S.R.L. opera come società ICT e tecnologica orientata allo sviluppo software, alla programmazione informatica, alla gestione di servizi digitali, alla consulenza organizzativa e gestionale e alla fornitura di soluzioni tecnologiche anche per il settore sanitario e della telemedicina.

La struttura organizzativa è basata su un Consiglio di Amministrazione composto da tre membri, con Presidente del Consiglio di Amministrazione e rappresentante dell'impresa. Le responsabilità relative alla sicurezza delle informazioni devono essere assegnate in modo chiaro tra direzione, funzioni tecniche, personale operativo, eventuali collaboratori, consulenti e fornitori coinvolti nei processi ICT.

I processi interni rilevanti per il SGSI comprendono sviluppo software, programmazione informatica, gestione dei sistemi e degli ambienti applicativi, assistenza tecnica, manutenzione, gestione dei dati, gestione documentale, gestione delle credenziali, gestione degli accessi, gestione dei fornitori, gestione dei rapporti con clienti e partner, formazione del personale e controllo della conformità normativa.

Gli strumenti e gli asset rilevanti includono piattaforme software, applicazioni, ambienti di sviluppo, dispositivi informatici, sistemi di comunicazione, repository documentali, archivi digitali, servizi cloud, credenziali, account utente, dati tecnici, dati contrattuali, dati personali e informazioni trattate nell'ambito dei servizi ICT e sanitari digitali.

Le competenze interne devono coprire sicurezza informatica, protezione dei dati personali, sviluppo sicuro del software, gestione degli accessi, continuità operativa, risposta agli incidenti, gestione dei fornitori, conformità GDPR e consapevolezza del personale sui rischi legati alla sicurezza delle informazioni.

Le principali criticità interne riguardano la corretta segregazione dei ruoli e degli accessi, la protezione degli ambienti di sviluppo e produzione, la gestione controllata delle modifiche software, la sicurezza dei dati trattati per clienti e utenti, la formalizzazione delle responsabilità, la gestione documentale, la continuità dei servizi digitali, la formazione del personale e il controllo delle attività eventualmente affidate a fornitori o partner.

4.2 Analisi del contesto esterno

ITLAB S.R.L. opera in un contesto esterno caratterizzato da elevata digitalizzazione, crescente domanda di servizi ICT, software, piattaforme digitali, telemedicina, monitoraggio a distanza e soluzioni tecnologiche a supporto di organizzazioni pubbliche e private, incluse strutture sanitarie e professionisti del settore.

Il mercato richiede elevati livelli di affidabilità, riservatezza, integrità, disponibilità, tracciabilità e continuità dei servizi digitali, soprattutto quando i servizi riguardano dati personali, dati aziendali riservati, servizi sanitari digitali, informazioni di clienti pubblici o privati e sistemi connessi a processi critici.

I principali fattori esterni includono requisiti di clienti e committenti, obblighi contrattuali, requisiti di sicurezza richiesti da partner e fornitori, normative applicabili in materia di protezione dei dati personali, GDPR, cybersecurity, sicurezza dei servizi ICT, continuità operativa, conservazione e gestione delle informazioni, nonché eventuali requisiti specifici derivanti dal settore sanitario e dai servizi di telemedicina.

La società dipende da fornitori esterni, provider cloud, fornitori di connettività, strumenti software, piattaforme tecnologiche, consulenti, partner commerciali e soggetti terzi eventualmente coinvolti nella progettazione, gestione, manutenzione o supporto dei servizi erogati.

Le principali minacce esterne rilevanti sono attacchi informatici, accessi non autorizzati, malware, phishing,

compromissione di credenziali, perdita o indisponibilità dei dati, vulnerabilità software, errori di configurazione, interruzioni dei servizi cloud o di connettività, indisponibilità dei fornitori critici, violazioni dei dati personali, perdita di reputazione e non conformità a requisiti normativi o contrattuali.

4.3 Parti interessate e relative esigenze

Clienti pubblici e privati: si aspettano servizi ICT affidabili, sicuri e continui, protezione delle informazioni affidate, rispetto dei requisiti contrattuali, gestione tempestiva degli incidenti, riservatezza dei dati e disponibilità delle piattaforme e dei servizi.

Strutture sanitarie, professionisti sanitari e organizzazioni operanti in ambito salute: si aspettano tutela dei dati personali e delle informazioni eventualmente connesse a servizi sanitari, continuità dei servizi digitali, tracciabilità delle attività, interoperabilità dei sistemi e rispetto dei requisiti applicabili in materia di privacy e sicurezza.

Utenti finali e pazienti, ove applicabile: si aspettano che i dati personali e le informazioni trattate tramite servizi digitali, telemedicina, home care o monitoraggio a distanza siano protetti da accessi non autorizzati, perdita, alterazione o uso improprio.

Direzione aziendale e organi amministrativi: si aspettano un sistema di gestione efficace, proporzionato ai rischi, orientato alla conformità normativa, alla continuità operativa, alla riduzione dei rischi, alla protezione del valore aziendale e alla tutela della reputazione.

Personale, collaboratori e consulenti: si aspettano ruoli e responsabilità chiari, procedure operative definite, strumenti adeguati, formazione sulla sicurezza delle informazioni, regole per l’utilizzo dei sistemi e protezione dei dati trattati nello svolgimento delle attività.

Fornitori tecnologici, provider cloud, partner e outsourcer: si aspettano requisiti di sicurezza chiari, accordi contrattuali definiti, gestione ordinata delle responsabilità, procedure di accesso controllate, collaborazione nella gestione degli incidenti e rispetto delle condizioni di servizio.

Autorità pubbliche, enti regolatori e organismi di controllo: si aspettano il rispetto degli obblighi normativi applicabili, inclusi quelli in materia di protezione dei dati personali, sicurezza delle informazioni, conservazione documentale, obblighi societari, obblighi contrattuali e gestione delle eventuali violazioni.

Soci e stakeholder societari: si aspettano tutela del patrimonio informativo, continuità dei servizi, riduzione dei rischi operativi, protezione della reputazione, affidabilità gestionale e capacità dell’organizzazione di dimostrare controllo sui processi rilevanti.

Organismo di certificazione: si aspetta che il SGSI sia documentato, attuato, mantenuto e migliorato secondo i requisiti della ISO/IEC 27001, con evidenze oggettive relative a contesto, scopo, valutazione dei rischi, controlli applicati, audit interni, riesame della direzione e miglioramento continuo.

L’organizzazione valuta periodicamente le evoluzioni del contesto e le aspettative delle parti interessate, verificandone l’impatto sul perimetro, sui rischi, sui controlli e sulla documentazione del sistema.

5. LEADERSHIP, GOVERNO E RESPONSABILITÀ

5.1 Ruoli, responsabilità e autorità

La Direzione assicura indirizzo strategico, disponibilità delle risorse, integrazione del SGSI nei processi aziendali, approvazione delle politiche e riesame periodico delle prestazioni del sistema. I responsabili di funzione e gli owner degli asset presidiano i rischi di competenza, sostengono l'attuazione dei controlli, promuovono la consapevolezza del personale e garantiscono la gestione delle evidenze documentate. Tutto il personale e i collaboratori sono tenuti ad operare secondo ruoli, autorizzazioni e responsabilità formalmente assegnate.

5.2 Risorse e competenze

Le risorse necessarie in termini di persone, competenze, tecnologie, budget e supporto operativo sono pianificate in modo coerente con priorità di rischio, obblighi di conformità e obiettivi del business.

5.3 Comunicazione

I flussi informativi interni ed esterni relativi al SGSI sono stabiliti per garantire tempestività, tracciabilità, adeguata autorizzazione e corretta gestione delle evidenze documentate.

6. SEDI, UNITÀ ORGANIZZATIVE E AMBIENTI INCLUSI

Sito	Indirizzo	Paese	Note
Sede legale ITLAB S.R.L.	Via Pietro Giannone 9, CAP 20154 Milano	Italia	

Numero siti/ambienti censiti nel perimetro: **1**.

7. ASSET INFORMATIVI E CRITERI DI CLASSIFICAZIONE

Gli asset del SGSI comprendono informazioni, servizi, applicazioni, infrastrutture, dispositivi, archivi documentali, risorse umane, sedi e altri elementi di supporto al business. Ciascun asset deve essere identificato, associato a un owner, classificato secondo i requisiti di riservatezza, integrità e disponibilità e gestito lungo il relativo ciclo di vita.

7.1 Criteri di classificazione

La classificazione degli asset e delle informazioni considera criticità per il business, requisiti contrattuali, impatti legali/regolatori e conseguenze operative in caso di compromissione o indisponibilità.

Asset	Tipo	Owner	C	I	A	Note
Archivi cartacei riservati	Archivio cartaceo	Amministrazione / Direzione	4	3	2	Contengono contratti, documenti HR, atti societari o registrazioni sensibili in formato cartaceo.
Backup aziendali	Backup	Responsabile IT	4	5	5	Copie di sicurezza necessarie al ripristino in caso di incidente, errore umano o attacco informatico.
Caselle e-mail aziendali	Servizio SaaS	Responsabile IT	4	4	4	Utilizzate per comunicazioni interne, esterne, invio documenti e gestione credenziali di servizi terzi.
CRM / ERP	Applicazione	Responsabile di processo	4	5	4	Sistema gestionale usato per processi commerciali, amministrativi e decisionali.
Database clienti	Database	Responsabile commerciale / IT	5	5	4	Contiene dati personali, storici ordini, offerte, contatti commerciali e informazioni riservate.
Dispositivi mobili aziendali	Dispositivo mobile	Responsabile IT	4	4	3	Smartphone e tablet con accesso a posta, file, autenticazione e applicazioni aziendali.
Documenti contrattuali e amministrativi	Documentazione	Amministrazione / Direzione	4	4	3	Documentazione rilevante ai fini legali, fiscali, organizzativi e di conformità.
Firewall e apparati di rete	Infrastruttura	Responsabile IT	3	5	5	Proteggono segmentazione, connettività, accessi remoti e perimetro di rete aziendale.

Asset	Tipo	Owner	C	I	A	Note
PC e laptop dipendenti	Endpoint	Responsabili di funzione	3	4	4	Strumenti di lavoro con accesso a dati, servizi cloud, documentazione e sistemi aziendali.
Piattaforma documentale / DMS	Applicazione	Qualità / IT	4	5	4	Raccoglie manuali, procedure, registrazioni, versioni e approvazioni documentali.
Portale clienti / area riservata	Sito web	Responsabile IT / Commerciale	4	5	4	Espone funzionalità applicative o documentali a clienti e partner attraverso autenticazione.
Server / infrastruttura virtuale	Infrastruttura	Responsabile IT	4	5	5	Ospita applicazioni, dati e servizi essenziali per l'operatività aziendale e la continuità del business.
Sistema HR / anagrafiche personale	Applicazione	HR	5	4	3	Gestisce dati del personale, ruoli, documenti, presenze e informazioni soggette a riservatezza elevata.
Sito web aziendale	Sito web	Marketing / IT	2	4	4	Canale istituzionale e commerciale, importante per immagine, reputazione e continuità di contatto con il mercato.
Sito web aziendale	Sito web https://www.itlab-group.it/	Marketing / IT	2	4	4	Canale istituzionale e commerciale, importante per immagine, reputazione e continuità di contatto con il mercato.
Workspace cloud collaborativo	Cloud workspace	Responsabile IT	4	4	4	Suite cloud per collaborazione, documenti, calendari, videoconferenze e condivisione file.

Legenda CIA: Confidenzialità, Integrità, Disponibilità. Numero asset censiti nel perimetro: **16**.

8. METODOLOGIA DI VALUTAZIONE E TRATTAMENTO DEL RISCHIO

8.1 Metodologia di valutazione dei rischi

L’organizzazione adotta una metodologia strutturata di risk assessment e risk treatment che prende in considerazione contesto, asset, minacce, vulnerabilità, probabilità, impatto e livello di rischio risultante. I criteri di accettazione del rischio, le priorità di intervento e le decisioni di trattamento sono definiti in modo coerente con gli obiettivi di business, la propensione al rischio dell’organizzazione, gli obblighi applicabili e le capacità operative disponibili.

8.2 Opzioni di trattamento

Le opzioni di trattamento includono riduzione, trasferimento, evitamento o accettazione motivata del rischio. La metodologia viene aggiornata quando intervengono cambiamenti rilevanti nel contesto, nel perimetro, nelle tecnologie, nei processi, nei requisiti contrattuali o nel panorama delle minacce.

9. QUADRO DEI RISCHI E PRIORITÀ DI INTERVENTO

9.1 Report di valutazione del rischio

Asset	Minaccia	Vulnerabilità	Score	Livello	Trattamento
Caselle e-mail aziendali	Phishing e compromissione account	Formazione insufficiente, MFA assente, filtri antispam non adeguati	16	Critico	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	15	Critico	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	15	Critico	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	15	Critico	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 privilegi eccessivi	15	Critico	Mitigare il rischio applicando il principio del minimo privilegio, attivando MFA, riesaminando periodicamente gli accessi e formalizzando provisioning/deprovisioning.

Asset	Minaccia	Vulnerabilità	Score	Livello	Trattamento
					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	15	Critico	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	15	Critico	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	15	Critico	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	15	Critico	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	12	Alto	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	12	Alto	Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici.

Numero complessivo dei rischi registrati: **18**.

10. OBIETTIVI SGSI, PIANIFICAZIONE E RISORSE

Garantire la riservatezza, integrità e disponibilità delle informazioni trattate nell'ambito dei servizi ICT, software, telemedicina, assistenza tecnica, programmazione informatica e gestione dei dati.

Ridurre progressivamente il livello di rischio informatico attraverso l'identificazione, valutazione, trattamento e monitoraggio periodico dei rischi relativi a dati, sistemi, applicazioni, infrastrutture, fornitori, personale e processi aziendali.

Assicurare che il 100% dei rischi classificati come non accettabili sia oggetto di un piano di trattamento approvato, con responsabilità assegnate, tempi di attuazione definiti e verifica dell'efficacia dei controlli implementati.

Mantenere sotto controllo gli accessi ai sistemi, agli ambienti applicativi, agli archivi documentali e alle informazioni aziendali, garantendo che gli accessi siano autorizzati, proporzionati al ruolo, riesaminati periodicamente e revocati tempestivamente in caso di cessazione o modifica del rapporto.

Incrementare il livello di consapevolezza del personale, dei collaboratori e delle funzioni coinvolte attraverso attività formative periodiche sulla sicurezza delle informazioni, protezione dei dati personali, phishing, gestione delle credenziali, classificazione delle informazioni, incident reporting e corretto utilizzo degli strumenti aziendali.

Garantire la gestione tempestiva degli incidenti di sicurezza, prevedendo registrazione, classificazione, analisi, trattamento, comunicazione interna, eventuale escalation e azioni correttive per prevenire il ripetersi degli eventi.

Migliorare la continuità operativa dei servizi digitali e dei processi critici, riducendo il rischio di indisponibilità dei sistemi, perdita dei dati, interruzione dei servizi ai clienti e impatti operativi derivanti da guasti, errori, attacchi informatici o indisponibilità dei fornitori.

Assicurare che i fornitori critici e i partner tecnologici siano valutati e monitorati in funzione dei rischi di sicurezza delle informazioni, della criticità dei servizi erogati, del trattamento dei dati e degli obblighi contrattuali applicabili.

Mantenere la conformità ai requisiti normativi, contrattuali e regolamentari applicabili, con particolare riferimento alla protezione dei dati personali, alla sicurezza delle informazioni, agli obblighi verso clienti e partner e ai requisiti derivanti dai servizi ICT e sanitari digitali.

Promuovere il miglioramento continuo del SGSI attraverso audit interni, riesame della direzione, analisi degli incidenti, monitoraggio degli indicatori, trattamento delle non conformità e aggiornamento periodico della valutazione dei rischi e dei controlli di sicurezza.

Fonte societaria e attività dichiarate: visura ITLAB S.R.L., con sede legale a Milano, unità locali a Francavilla al Mare e Napoli, oggetto sociale relativo a software, reti telematiche, servizi internet, trattamento dati, telemedicina e attività di programmazione informatica.

Gli obiettivi del SGSI devono essere misurabili ove possibile, coerenti con la politica per la sicurezza delle informazioni, assegnati a responsabili identificati, monitorati tramite indicatori e riesaminati periodicamente. L'organizzazione garantisce risorse adeguate in termini di persone, competenze, tecnologie, budget, tempo e supporto operativo per l'attuazione delle iniziative di sicurezza.

11. CONTROLLI, STATEMENT OF APPLICABILITY E PIANO DI TRATTAMENTO

11.1 Controlli e SoA

I controlli del SGSI sono determinati in funzione dei risultati dell'analisi del rischio, dei requisiti applicabili e delle esigenze operative dell'organizzazione. La Statement of Applicability formalizza per ciascun controllo la decisione di applicabilità, lo stato di implementazione e la relativa motivazione.

11.2 Piano di trattamento del rischio

Il piano di trattamento traduce i rischi significativi in azioni, responsabilità, scadenze e stati di avanzamento, mantenendo coerenza tra rischio, controllo, responsabili e capacità attuativa del business.

Controlli applicabili o da confermare presenti in archivio: **33**. Azioni/piani di trattamento presenti: **18**. Procedure SGSI registrate: **8**.

12. COMPETENZA, CONSAPEVOLEZZA, COMUNICAZIONE E CONTROLLO DOCUMENTALE

12.1 Competenze e consapevolezza

L'organizzazione assicura che il personale operi con adeguata competenza e consapevolezza rispetto a ruoli, responsabilità, politiche, procedure e requisiti di sicurezza.

12.2 Controllo documentale

Le informazioni documentate del SGSI sono identificate, approvate, aggiornate, protette, rese disponibili e conservate in modo controllato per garantirne integrità, reperibilità e adeguatezza d'uso. Le comunicazioni interne ed esterne rilevanti per il SGSI sono pianificate, tracciate quando necessario e gestite secondo criteri di riservatezza e autorizzazione.

13. GESTIONE OPERATIVA, MONITORAGGIO E RISPOSTA AGLI EVENTI

13.1 Attuazione operativa

Le attività operative del SGSI comprendono l'attuazione dei controlli, la gestione dei cambiamenti, il monitoraggio delle misure di sicurezza, il presidio delle vulnerabilità, la gestione degli incidenti e la conservazione delle evidenze.

13.2 Risposta agli eventi e non conformità

Eventi, anomalie, non conformità e incidenti informativi devono essere rilevati, registrati, valutati, trattati e, ove opportuno, analizzati per identificarne cause, impatti e azioni correttive.

14. AUDIT INTERNI, RIESAME DELLA DIREZIONE E MIGLIORAMENTO CONTINUO

14.1 Audit e riesame

Il SGSI è sottoposto a audit interni pianificati, riesami periodici della Direzione e verifiche dell'efficacia delle misure adottate.

14.2 Miglioramento continuo

I risultati di audit, monitoraggi, incidenti, analisi dei rischi, trattamenti, indicatori e feedback delle parti interessate alimentano il processo di miglioramento continuo. Le azioni correttive e di miglioramento devono essere proporzionate ai rilievi emersi, assegnate a responsabili identificati e verificate fino alla loro chiusura.

15. ALLEGATI E DOCUMENTI CORRELATI

Il presente manuale si integra con il registro degli asset, il registro dei rischi, il piano di trattamento del rischio, la Statement of Applicability, la politica per la sicurezza delle informazioni, le procedure operative e ogni altra informazione documentata del SGSI rilevante ai fini del governo, della conformità e dell'efficacia del sistema.