SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Procedure 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-PRC-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

Pack procedure SGSI

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.

PACK PROCEDURE SGSI

Le procedure riportate di seguito definiscono i controlli operativi minimi per la gestione del SGSI.

PROC-BCK-001 - Backup e ripristino

Procedura Backup e ripristino

Scopo
Stabilire regole operative coerenti con il SGSI di iTLab S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Workspace cloud collaborativo: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- CRM / ERP: Corruzione o modifica impropria dei dati [Critico]
- CRM / ERP: Accesso non autorizzato ai dati [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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.
- Mitigare: 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 Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-CLS-001 - Classificazione delle informazioni

Procedura Classificazione delle informazioni

Scopo
Stabilire regole operative coerenti con il SGSI di iTLab S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Workspace cloud collaborativo: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- CRM / ERP: Corruzione o modifica impropria dei dati [Critico]
- CRM / ERP: Accesso non autorizzato ai dati [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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.
- Mitigare: 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 Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-BCP-001 - Continuità operativa e continuità ICT

Procedura Continuità operativa e continuità ICT

Scopo
Stabilire regole operative coerenti con il SGSI di iTLab S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Workspace cloud collaborativo: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- CRM / ERP: Corruzione o modifica impropria dei dati [Critico]
- CRM / ERP: Accesso non autorizzato ai dati [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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.
- Mitigare: 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 Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-ACC-001 - Gestione accessi

Procedura Gestione accessi

Scopo
Stabilire regole operative coerenti con il SGSI di iTLab S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Workspace cloud collaborativo: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- CRM / ERP: Corruzione o modifica impropria dei dati [Critico]
- CRM / ERP: Accesso non autorizzato ai dati [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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.
- Mitigare: 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 Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-AST-001 - Gestione asset informativi

Procedura Gestione asset informativi

Scopo
Stabilire regole operative coerenti con il SGSI di iTLab S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Workspace cloud collaborativo: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- CRM / ERP: Corruzione o modifica impropria dei dati [Critico]
- CRM / ERP: Accesso non autorizzato ai dati [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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.
- Mitigare: 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 Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-SUP-001 - Gestione fornitori e terze parti

Procedura Gestione fornitori e terze parti

Scopo
Stabilire regole operative coerenti con il SGSI di iTLab S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Workspace cloud collaborativo: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- CRM / ERP: Corruzione o modifica impropria dei dati [Critico]
- CRM / ERP: Accesso non autorizzato ai dati [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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.
- Mitigare: 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 Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-INC-001 - Gestione incidenti di sicurezza

Procedura Gestione incidenti di sicurezza

Scopo
Stabilire regole operative coerenti con il SGSI di iTLab S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Workspace cloud collaborativo: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- CRM / ERP: Corruzione o modifica impropria dei dati [Critico]
- CRM / ERP: Accesso non autorizzato ai dati [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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.
- Mitigare: 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 Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.

PROC-VUL-001 - Gestione vulnerabilità

Procedura Gestione vulnerabilità

Scopo
Stabilire regole operative coerenti con il SGSI di iTLab S.r.l..

Campo di applicazione
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.

Riferimenti al contesto
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.

Asset rilevanti
- Archivi cartacei riservati (Archivio cartaceo)
- Backup aziendali (Backup)
- Caselle e-mail aziendali (Servizio SaaS)
- CRM / ERP (Applicazione)
- Database clienti (Database)
- Dispositivi mobili aziendali (Dispositivo mobile)
- Documenti contrattuali e amministrativi (Documentazione)
- Firewall e apparati di rete (Infrastruttura)

Rischi rilevanti
- Caselle e-mail aziendali: Phishing e compromissione account [Critico]
- Workspace cloud collaborativo: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Firewall e apparati di rete: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- CRM / ERP: Corruzione o modifica impropria dei dati [Critico]
- CRM / ERP: Accesso non autorizzato ai dati [Critico]
- Backup aziendali: Impossibilità di ripristino [Critico]
- Server / infrastruttura virtuale: Malware, ransomware o indisponibilità infrastrutturale [Critico]
- Database clienti: Corruzione o modifica impropria dei dati [Critico]

Controlli / SoA correlati
- A.5.1 Politiche per la sicurezza delle informazioni (planned)
- A.5.2 Ruoli e responsabilità per la sicurezza delle informazioni (planned)
- A.5.7 Threat intelligence (planned)
- A.5.9 Inventario degli asset informativi (planned)
- A.5.10 Uso accettabile degli asset (planned)
- A.5.12 Classificazione delle informazioni (planned)
- A.5.15 Controllo degli accessi (planned)
- A.5.18 Diritti di accesso (planned)

Piano di trattamento collegato
- Mitigare: 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.
- Mitigare: 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 Sistema HR / anagrafiche personale, con owner HR e presidio del controllo Controlli organizzativi e tecnici proporzionati.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.
- Mitigare: 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.

Responsabilità
La Direzione, i process owner e i responsabili indicati nei trattamenti assicurano attuazione, evidenze e riesame.

Modalità operative
1. Verificare asset, rischi, controlli e responsabilità applicabili.
2. Attuare le misure definite nel piano di trattamento.
3. Registrare evidenze, eccezioni, non conformità e avanzamento.
4. Riesaminare periodicamente efficacia, stato e aggiornamento documentale.
5. Aggiornare la procedura in caso di variazioni di contesto, asset o rischio.