SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Manuale SGSI

EPTA TECH S.R.L. è una società italiana con sede legale a San Vito al Tagliamento (PN), operante nel settore dell'information technology, con attività prevalente di produzione e sviluppo di software non connesso all'edizione. L'azienda svolge attività di progettazione, realizzazione, commercializzazione, manutenzione e assistenza di soluzioni software, applicazioni web based, app e sistemi informatici, anche su commissione e su iniziativa propria.

La società opera inoltre nell'ambito della consulenza informatica, della gestione di servizi web, posta elettronica, hosting, housing, registrazione e mantenimento domini, nonché nella fornitura e gestione di servizi cloud quali SaaS, DaaS, HaaS, PaaS e IaaS. Rientrano inoltre nelle attività aziendali la realizzazione e gestione di siti internet, portali web, e-commerce, banche dati, reti dati, sistemi di telecomunicazione e soluzioni di sicurezza, sorveglianza e videosorveglianza.

In considerazione della natura delle attività svolte, EPTA TECH S.R.L. gestisce informazioni, infrastrutture tecnologiche, servizi digitali e ambienti cloud che richiedono adeguate misure di sicurezza, riservatezza, integrità, disponibilità e continuità operativa, in coerenza con i requisiti delle norme ISO/IEC 27001 e ISO/IEC 27017.

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

EPTA TECH S.R.L. è una società italiana con sede legale a San Vito al Tagliamento (PN), operante nel settore dell'information technology, con attività prevalente di produzione e sviluppo di software non connesso all'edizione. L'azienda svolge attività di progettazione, realizzazione, commercializzazione, manutenzione e assistenza di soluzioni software, applicazioni web based, app e sistemi informatici, anche su commissione e su iniziativa propria.

La società opera inoltre nell'ambito della consulenza informatica, della gestione di servizi web, posta elettronica, hosting, housing, registrazione e mantenimento domini, nonché nella fornitura e gestione di servizi cloud quali SaaS, DaaS, HaaS, PaaS e IaaS. Rientrano inoltre nelle attività aziendali la realizzazione e gestione di siti internet, portali web, e-commerce, banche dati, reti dati, sistemi di telecomunicazione e soluzioni di sicurezza, sorveglianza e videosorveglianza.

In considerazione della natura delle attività svolte, EPTA TECH S.R.L. gestisce informazioni, infrastrutture tecnologiche, servizi digitali e ambienti cloud che richiedono adeguate misure di sicurezza, riservatezza, integrità, disponibilità e continuità operativa, in coerenza con i requisiti delle norme ISO/IEC 27001 e ISO/IEC 27017.

DESCRIZIONE DEL SERVIZIO

Il servizio di consulenza ha ad oggetto il supporto specialistico a EPTA TECH S.R.L. per la progettazione, implementazione, mantenimento e miglioramento di un Sistema di Gestione per la Sicurezza delle Informazioni conforme alla norma ISO/IEC 27001, con estensione ai controlli e alle buone pratiche specifiche per i servizi cloud previste dalla ISO/IEC 27017.

L'attività comprende l'analisi del contesto aziendale, dei processi IT e cloud, delle infrastrutture tecnologiche, delle applicazioni software, dei servizi digitali erogati e delle informazioni trattate, al fine di individuare rischi, minacce, vulnerabilità e requisiti di sicurezza applicabili. La consulenza include inoltre il supporto nella definizione del campo di applicazione del sistema di gestione, nella valutazione dei rischi, nella redazione della documentazione richiesta, nella predisposizione delle procedure operative, nella selezione e applicazione dei controlli di sicurezza e nella preparazione all'eventuale audit di certificazione.

Particolare attenzione viene dedicata alla sicurezza dei servizi cloud, alla gestione delle responsabilità tra fornitore e cliente, alla protezione dei dati, al controllo degli accessi, alla continuità dei servizi, alla gestione degli incidenti, alla sicurezza delle infrastrutture, alla conformità normativa e contrattuale e al miglioramento continuo delle misure organizzative e tecniche adottate dall'azienda.

INDICE DEL DOCUMENTO

TERMINI IN USO

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

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 EPTA TECH 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

EPTA TECH S.R.L. è una società italiana con sede legale a San Vito al Tagliamento (PN), operante nel settore dell'information technology, con attività prevalente di produzione e sviluppo di software non connesso all'edizione. L'azienda svolge attività di progettazione, realizzazione, commercializzazione, manutenzione e assistenza di soluzioni software, applicazioni web based, app e sistemi informatici, anche su commissione e su iniziativa propria.

La società opera inoltre nell'ambito della consulenza informatica, della gestione di servizi web, posta elettronica, hosting, housing, registrazione e mantenimento domini, nonché nella fornitura e gestione di servizi cloud quali SaaS, DaaS, HaaS, PaaS e IaaS. Rientrano inoltre nelle attività aziendali la realizzazione e gestione di siti internet, portali web, e-commerce, banche dati, reti dati, sistemi di telecomunicazione e soluzioni di sicurezza, sorveglianza e videosorveglianza.

In considerazione della natura delle attività svolte, EPTA TECH S.R.L. gestisce informazioni, infrastrutture tecnologiche, servizi digitali e ambienti cloud che richiedono adeguate misure di sicurezza, riservatezza, integrità, disponibilità e continuità operativa, in coerenza con i requisiti delle norme ISO/IEC 27001 e ISO/IEC 27017.

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 EPTA TECH S.R.L. si applica alle attività di progettazione, sviluppo, realizzazione, commercializzazione, manutenzione e assistenza di soluzioni software, applicazioni web based, app, sistemi informatici e servizi digitali, nonché alle attività di consulenza informatica, gestione di servizi web, posta elettronica, hosting, housing, registrazione e mantenimento domini e servizi cloud quali SaaS, DaaS, HaaS, PaaS e IaaS.

Il perimetro del SGSI comprende i processi direzionali, commerciali, tecnici, operativi e di supporto connessi all'erogazione dei servizi IT e cloud, inclusi la gestione dei clienti, la gestione dei progetti, lo sviluppo software, la manutenzione applicativa, l'assistenza tecnica, la gestione delle infrastrutture tecnologiche, la gestione degli accessi, la protezione dei dati, la continuità operativa, la gestione degli incidenti di sicurezza e il controllo dei fornitori rilevanti.

Sono compresi nello scopo le informazioni aziendali, i dati dei clienti e degli utenti, la documentazione tecnica e contrattuale, il codice sorgente, le configurazioni di sistema, le credenziali, i log, i backup, le informazioni amministrative e ogni altro dato trattato nell'ambito dei servizi erogati.

Il campo di applicazione comprende la sede di EPTA TECH S.R.L. sita in Via San Carlo n. 40, frazione Prodolone, 33078 San Vito al Tagliamento (PN), Italia, nonché i sistemi informativi, le postazioni di lavoro, le infrastrutture di rete, gli ambienti cloud, i server, le piattaforme applicative, gli strumenti di collaborazione, gli archivi digitali e gli eventuali sistemi di terze parti utilizzati per l'erogazione, gestione e protezione dei servizi aziendali.

Il SGSI è definito tenendo conto dei requisiti della norma ISO/IEC 27001 e dei controlli specifici per la sicurezza dei servizi cloud previsti dalla ISO/IEC 27017.

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

EPTA TECH S.R.L. è una società operante nel settore dell'information technology, con attività prevalente di produzione e sviluppo software e con servizi connessi alla consulenza informatica, ai servizi web, ai servizi cloud, alle reti dati, alle telecomunicazioni e ai sistemi di sicurezza.

La struttura organizzativa è di dimensioni contenute e prevede una gestione accentrata, con Amministratore Unico e personale tecnico coinvolto nelle attività operative. Tale configurazione consente rapidità decisionale, controllo diretto dei processi e flessibilità operativa, ma richiede una chiara attribuzione di ruoli, responsabilità, autorizzazioni e segregazione delle attività critiche.

I principali processi interni rilevanti per la sicurezza delle informazioni riguardano lo sviluppo e la manutenzione software, la gestione dei servizi cloud e web, l'assistenza tecnica, la gestione delle infrastrutture informatiche, la gestione degli accessi, la protezione dei dati, la gestione dei backup, la continuità operativa, la gestione degli incidenti, la selezione e controllo dei fornitori e la gestione documentale.

I principali asset interni comprendono sistemi informatici, applicazioni software, codice sorgente, ambienti cloud, dispositivi aziendali, credenziali, configurazioni, documentazione tecnica, dati dei clienti, dati amministrativi e strumenti di comunicazione e collaborazione.

Le competenze interne in ambito software, sistemi informatici, servizi cloud e consulenza IT rappresentano un elemento rilevante per il presidio della sicurezza. Le principali criticità interne sono riconducibili alla necessità di formalizzare processi, responsabilità, procedure, controlli documentati, monitoraggio dei rischi, continuità operativa e consapevolezza del personale in materia di sicurezza delle informazioni.

4.2 Analisi del contesto esterno

EPTA TECH S.R.L. opera in un mercato caratterizzato da elevata digitalizzazione, crescente utilizzo di servizi cloud, forte dipendenza da infrastrutture tecnologiche e aumento delle esigenze di sicurezza, affidabilità, continuità e conformità normativa da parte dei clienti.

Il contesto esterno è influenzato da clienti che richiedono servizi IT sicuri, continui e affidabili, da fornitori tecnologici e cloud provider che possono incidere sulla disponibilità e protezione dei servizi erogati, da partner tecnici, consulenti, enti di certificazione, autorità pubbliche e soggetti regolatori.

Sono rilevanti gli obblighi normativi e contrattuali in materia di protezione dei dati personali, sicurezza delle informazioni, riservatezza, continuità dei servizi, responsabilità nella gestione dei dati, contratti con clienti e fornitori, proprietà intellettuale, licenze software e requisiti applicabili ai servizi cloud.

Le principali minacce esterne includono attacchi informatici, malware, ransomware, phishing, accessi non autorizzati, perdita o indisponibilità dei dati, interruzioni dei servizi cloud, vulnerabilità software, compromissione delle credenziali, errori di configurazione, incidenti presso fornitori terzi e violazioni della riservatezza, integrità o disponibilità delle informazioni.

Il SGSI tiene conto di tali fattori esterni al fine di definire controlli adeguati, ridurre i rischi, assicurare la continuità dei servizi e garantire il rispetto dei requisiti normativi, contrattuali e di sicurezza applicabili.

4.3 Parti interessate e relative esigenze

Le parti interessate rilevanti per il Sistema di Gestione per la Sicurezza delle Informazioni di EPTA TECH S.R.L. sono le seguenti:

Clienti: si aspettano la protezione dei dati affidati, la riservatezza delle informazioni, la continuità dei servizi, la disponibilità delle piattaforme, la gestione tempestiva degli incidenti, il rispetto degli accordi contrattuali e l'adozione di misure di sicurezza adeguate.

Utenti finali dei servizi: si aspettano servizi digitali sicuri, accessibili, affidabili e protetti da accessi non autorizzati, perdita di dati o interruzioni operative.

Direzione aziendale: si aspetta il governo dei rischi informativi, la conformità ai requisiti applicabili, la protezione del know-how aziendale, la continuità operativa, la tutela reputazionale e il miglioramento dell'efficienza dei processi.

Personale interno e collaboratori: si aspettano regole chiare, strumenti sicuri, responsabilità definite, formazione adeguata, procedure operative comprensibili e protezione delle informazioni trattate nello svolgimento delle attività aziendali.

Fornitori tecnologici e cloud provider: si aspettano una corretta gestione dei rapporti contrattuali, requisiti di sicurezza definiti, responsabilità chiare, comunicazioni efficaci e rispetto delle condizioni di utilizzo dei servizi.

Partner commerciali e tecnici: si aspettano affidabilità, protezione delle informazioni condivise, rispetto degli accordi di riservatezza e continuità nella collaborazione.

Autorità pubbliche e organismi regolatori: si aspettano il rispetto delle norme applicabili in materia di protezione dei dati personali, sicurezza delle informazioni, obblighi societari, contrattuali e tecnici.

Organismi di certificazione e auditor: si aspettano evidenze documentate, applicazione efficace dei requisiti ISO/IEC 27001 e ISO/IEC 27017, gestione dei rischi, monitoraggio dei controlli e miglioramento continuo del SGSI.

Socio unico e proprietà: si aspettano tutela del valore aziendale, continuità dei servizi, protezione degli asset informativi, riduzione dei rischi operativi e reputazionali e conformità agli obblighi applicabili.

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	Via San Carlo n. 40 San Vito al Tagliamento	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://eptatech.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

Gli obiettivi del Sistema di Gestione per la Sicurezza delle Informazioni di EPTA TECH S.R.L. sono i seguenti:

Garantire la riservatezza, integrità e disponibilità delle informazioni aziendali, dei dati dei clienti, dei sistemi informatici, delle applicazioni software e dei servizi cloud gestiti dall'organizzazione.
Identificare, valutare e trattare periodicamente i rischi di sicurezza delle informazioni, con riesame almeno annuale o in occasione di modifiche significative ai processi, ai sistemi, ai servizi o al contesto aziendale.
Ridurre il livello di rischio residuo attraverso l'adozione di controlli organizzativi, tecnici e procedurali coerenti con ISO/IEC 27001 e ISO/IEC 27017.
Definire e mantenere ruoli, responsabilità e autorizzazioni per la gestione sicura delle informazioni, dei sistemi, degli accessi e dei servizi cloud.
Migliorare la gestione degli accessi logici, assicurando che gli utenti dispongano esclusivamente delle autorizzazioni necessarie allo svolgimento delle attività assegnate.
Garantire la continuità dei servizi IT e cloud attraverso misure di backup, ripristino, protezione delle infrastrutture, gestione degli incidenti e pianificazione della continuità operativa.
Assicurare che gli incidenti di sicurezza delle informazioni siano rilevati, registrati, valutati, gestiti e risolti in modo tempestivo, con analisi delle cause e definizione di azioni correttive.
Incrementare la consapevolezza del personale e dei collaboratori sui temi della sicurezza delle informazioni, della protezione dei dati, dell'utilizzo sicuro degli strumenti informatici e della gestione dei servizi cloud.
Monitorare e valutare periodicamente l'efficacia dei controlli di sicurezza adottati, attraverso verifiche interne, riesami, indicatori, audit e azioni di miglioramento.
Garantire il rispetto dei requisiti normativi, contrattuali e regolamentari applicabili, con particolare riferimento alla protezione dei dati, alla sicurezza delle informazioni, alla gestione dei fornitori e alla sicurezza dei servizi cloud.
Migliorare progressivamente il livello di maturità del SGSI, riducendo le non conformità, rafforzando la documentazione, consolidando i processi e aumentando la capacità dell'organizzazione di prevenire, rilevare e gestire eventi di sicurezza.

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.