

SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Politica Sicurezza Informazioni

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-POL-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

Impegno della direzione

Principi di riferimento

Campo di applicazione

Obiettivi

Riesame

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.

IMPEGNO DELLA DIREZIONE

La Direzione di EPTA TECH S.R.L. si impegna a proteggere la riservatezza, l'integrità e la disponibilità delle informazioni, garantendo risorse adeguate, responsabilità chiare e monitoraggio dell'efficacia del SGSI.

PRINCIPI DI RIFERIMENTO

- approccio basato sul rischio;
- principio del minimo privilegio;
- separazione dei compiti;
- controllo dei fornitori e dei servizi cloud;
- formazione continua del personale;
- gestione tempestiva degli incidenti.

CAMPO DI APPLICAZIONE

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.

OBIETTIVI

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.

RIESAME

La presente politica è riesaminata periodicamente, in occasione di modifiche organizzative rilevanti, incidenti significativi o aggiornamenti normativi e contrattuali.