SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Gestione fornitori e terze parti

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	PROC-SUP-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.

PROC-SUP-001 - GESTIONE FORNITORI E TERZE PARTI

Procedura Gestione fornitori e terze parti

Scopo
Stabilire regole operative coerenti con il SGSI di EPTA TECH S.R.L..

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.

Riferimenti al contesto
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.

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.