SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

# Registro dei Rischi

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-RSK-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

Registro dei rischi

## 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. |

## REGISTRO DEI RISCHI

| Asset | Minaccia | Vulnerabilità | Impatto | Probabilità | Score | Livello | Responsabile | Trattamento |
|---|---|---|---|---|---|---|---|---|
| Caselle e-mail aziendali | Phishing e compromissione account | Formazione insufficiente, MFA assente, filtri antispam non adeguati | 4 Alto - interruzione rilevante del servizio o danno reputazionale | 4 Alta - evento probabile nel breve periodo | 16 | Critico | Responsabile IT | 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 | 5 Molto alto - blocco operativo, perdita dati critica o violazione grave | 3 Media - evento possibile in condizioni normali | 15 | Critico | Responsabile IT | 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 | 5 Molto alto - blocco operativo, perdita dati critica o violazione grave | 3 Media - evento possibile in condizioni normali | 15 | Critico | Responsabile IT | 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 | 5 Molto alto - blocco operativo, perdita dati critica o violazione grave | 3 Media - evento possibile in condizioni normali | 15 | Critico | Responsabile di processo | 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 | 5 Molto alto - blocco | 3 Media - evento | 15 | Critico | Responsabile di processo | Mitigare il rischio applicando il principio del minimo privilegio, attivando |

| Asset | Minaccia | Vulnerabilità | Impatto | Probabilità | Score | Livello | Responsabile | Trattamento |
|---|---|---|---|---|---|---|---|---|
| | | privilegi eccessivi | operativo, perdita dati critica o violazione grave | possibile in condizioni normali | | | | 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. |
| Backup aziendali | Impossibilità di ripristino | Backup non testati o retention inadeguata | 5 Molto alto - blocco operativo, perdita dati critica o violazione grave | 3 Media - evento possibile in condizioni normali | 15 | Critico | Responsabile IT | 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 | 5 Molto alto - blocco operativo, perdita dati critica o violazione grave | 3 Media - evento possibile in condizioni normali | 15 | Critico | Responsabile IT | 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 | 5 Molto alto - blocco operativo, perdita dati critica o violazione grave | 3 Media - evento possibile in condizioni normali | 15 | Critico | Responsabile commerciale / IT | 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 | 5 Molto alto - blocco operativo, perdita dati critica o violazione grave | 3 Media - evento possibile in condizioni normali | 15 | Critico | Responsabile commerciale / IT | 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 | 4 Alto - interruzione rilevante del servizio o danno reputazionale | 3 Media - evento possibile in condizioni normali | 12 | Alto | Responsabile IT | 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 | 4 Alto - interruzione rilevante del servizio o danno reputazionale | 3 Media - evento possibile in condizioni normali | 12 | Alto | Responsabili di funzione | Mitigare il rischio con misure organizzative e tecniche proporzionate, formalizzando controlli, responsabilità e riesami periodici. |

| Asset | Minaccia | Vulnerabilità | Impatto | Probabilità | Score | Livello | Responsabile | Trattamento |
|---|---|---|---|---|---|---|---|---|
| Portale clienti / area riservata | Perdita di disponibilità dell'asset | Procedure di gestione non formalizzate o misure di protezione non proporzionate | 3 Medio - impatto operativo o economico moderato | 3 Media - evento possibile in condizioni normali | 9 | Medio | Responsabile IT / Commerciale | 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. |
| Sistema HR / anagrafiche personale | Perdita di disponibilità dell'asset | Procedure di gestione non formalizzate o misure di protezione non proporzionate | 3 Medio - impatto operativo o economico moderato | 3 Media - evento possibile in condizioni normali | 9 | Medio | HR | 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. |
| Archivi cartacei riservati | Perdita di disponibilità dell'asset | Procedure di gestione non formalizzate o misure di protezione non proporzionate | 3 Medio - impatto operativo o economico moderato | 3 Media - evento possibile in condizioni normali | 9 | Medio | Amministrazione / Direzione | 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. |
| Piattaforma documentale / DMS | Perdita di disponibilità dell'asset | Procedure di gestione non formalizzate o misure di protezione non proporzionate | 3 Medio - impatto operativo o economico moderato | 3 Media - evento possibile in condizioni normali | 9 | Medio | Qualità / IT | 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. |
| Sito web aziendale | Perdita di disponibilità dell'asset | Procedure di gestione non formalizzate o misure di protezione non proporzionate | 3 Medio - impatto operativo o economico moderato | 3 Media - evento possibile in condizioni normali | 9 | Medio | Marketing / IT | 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. |
| Documenti contrattuali e amministrativi | Perdita di disponibilità dell'asset | Procedure di gestione non formalizzate o misure di protezione non proporzionate | 3 Medio - impatto operativo o economico moderato | 3 Media - evento possibile in condizioni normali | 9 | Medio | Amministrazione / Direzione | 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. |
| Sito web aziendale | Perdita di disponibilità dell'asset | Procedure di gestione non formalizzate o misure di protezione non proporzionate | 3 Medio - impatto operativo o economico moderato | 3 Media - evento possibile in condizioni normali | 9 | Medio | Marketing / IT | 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. |