La direzione di **Trasimeno Servizi Ambientali TSA S.p.A** nell'ambito dei propri processi ha previsto l'implementazione e l'attuazione di misure organizzative, tecniche e procedurali per proteggere e salvaguardare le informazioni.

Data la natura delle attività e le continue evoluzioni normative, TSA S.p.A. considera fondamentale garantire la sicurezza delle informazioni interne ed esterne, tutelando i principi di:

- **Riservatezza:** Protezione contro accessi non autorizzati.
- **Integrità:** Salvaguardia da modifiche non autorizzate.
- **Disponibilità:** Accesso garantito alle informazioni per gli utenti autorizzati quando necessario.

TSA S.p.A. ha implementato un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** conforme alla norma **UNI CEI ISO/IEC 27001:2022**, con l'obiettivo di garantire:

1. **Protezione del patrimonio informativo aziendale**, inclusi i dati dei clienti e dei fornitori, da minacce interne, esterne, accidentali o deliberate.
2. **Riduzione dei rischi** per i clienti derivanti dai servizi erogati.

## Obiettivi di Sicurezza delle informazioni

La direzione ha quindi definito i seguenti macro-obiettivi per la sicurezza delle informazioni:

- Identificare e proteggere le informazioni e i beni critici per le proprie attività;
- Prevenire la perdita, la compromissione o la divulgazione non autorizzata dei dati sensibili;
- l'operato dell'azienda deve rispondere pienamente alle indicazioni delle normative vigenti e cogenti (es. Regolamento Ue 2016/679);
- Monitorare e analizzare continuamente le vulnerabilità e le violazioni della sicurezza;
- Implementare soluzioni tecnologiche e procedurali per assicurare la protezione delle informazioni;
- Sensibilizzare e formare il personale sul ruolo della sicurezza delle informazioni, favorendo una cultura aziendale orientata alla protezione dei dati.

## Principi e Azioni per la Sicurezza delle Informazioni

Per raggiungere gli obiettivi sopra indicati, TSA S.p.A. si impegna a:

- Garantire la conformità normativa, rispettando i requisiti cogenti e contrattuali applicabili.
- Promuovere sistematicamente la formazione del personale con particolare riferimento ai temi inerenti alla sicurezza dell'informazione e al rischio aziendale.
- Proteggere le credenziali di accesso e le risorse aziendali, prevenendo accessi non autorizzati ai sistemi e alle attrezzature.
- Implementare misure di sicurezza avanzate per tutelare i dati sensibili e la continuità operativa.
- Analizzare e mitigare i rischi associati alla gestione delle informazioni attraverso un processo strutturato di valutazione e gestione.

- Promuovere il miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni, attraverso audit periodici, analisi dei risultati e revisione delle strategie aziendali.
- Assicurare la tracciabilità e la trasparenza delle attività, anche attraverso la gestione documentale conforme alla normativa di riferimento.

La Direzione Generale guida e sostiene l'implementazione del SGSI, assumendo i seguenti impegni:

1. **Definire e approvare il "Piano Obiettivi Aziendali"** annuale, contenente azioni, risultati attesi, responsabilità e risorse assegnate.
2. **Monitorare l'adeguatezza e l'efficacia** del SGSI attraverso il Riesame della Direzione e l'analisi degli audit interni ed esterni.
3. **Diffondere la politica aziendale** e le sue finalità a tutti i dipendenti, collaboratori, clienti e fornitori.
4. **Garantire che le risorse interne siano formate e consapevoli** del loro ruolo nella protezione delle informazioni.
5. **Limitare l'uso di dispositivi rimovibili** come chiavette USB e hard disk esterni, consentendone l'utilizzo solo in casi eccezionali, autorizzati e adeguatamente tracciati. Questa misura mira a prevenire la perdita o il furto di dati e a ridurre i rischi derivanti da accessi non autorizzati o dalla diffusione di malware.
6. **Riesaminare periodicamente tale Politica** in sede di Riesame della Direzione per verificarne l'adeguatezza ed eventualmente revisionarla anche alla luce di cambiamenti negli assets.

La Direzione