1 Introduzione

La presente Politica per la Sicurezza delle Informazioni è stata redatta in conformità ai requisiti del paragrafo 5.2 della norma ISO/IEC 27001, al fine di stabilire i principi, gli obiettivi e gli impegni dell'organizzazione in materia di protezione delle informazioni. Il documento rappresenta il quadro di riferimento per la gestione della sicurezza delle informazioni di TIM San Marino, garantendo l'allineamento con le normative vigenti, gli standard internazionali e le esigenze delle parti interessate. La politica è approvata dalla Direzione e diffusa a tutti i livelli dell'organizzazione, costituendo elemento fondante del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

1.1 Contesto e Scopo

TIM San Marino opera in un contesto caratterizzato da una crescente digitalizzazione e da rischi informatici in continua evoluzione.

Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di TIM San Marino si applica a tutte le attività, processi, infrastrutture e risorse coinvolte nella gestione delle informazioni aziendali, con particolare attenzione ai dati sensibili e ai sistemi critici. L'ambito del SGSI comprende sia le risorse tecnologiche che quelle umane, includendo il trattamento dei dati personali, la protezione delle comunicazioni, la gestione degli accessi e la prevenzione di incidenti di sicurezza. Sono inoltre ricompresi i rapporti con fornitori, clienti e partner, garantendo che tutte le parti interessate rispettino i requisiti di sicurezza previsti dalle normative vigenti e dalle politiche interne. L'obiettivo è assicurare la riservatezza, l'integrità e la disponibilità delle informazioni, promuovendo una cultura della sicurezza a tutti i livelli dell'organizzazione.

La protezione delle informazioni rappresenta un valore imprescindibile per assicurare la continuità operativa, la reputazione aziendale e la fiducia di clienti, partner e stakeholder. Lo scopo di questa politica è definire le linee guida fondamentali per la salvaguardia della riservatezza, integrità e disponibilità delle informazioni, assicurando un approccio proattivo e sistematico alla gestione della sicurezza.

1.2 Riferimenti Normativi

- ISO/IEC 27001:2022 – Sistemi di gestione per la sicurezza delle informazioni – Requisiti
- Norma ISO/IEC 27002:2022 – Codice di buone pratiche per i controlli di sicurezza delle informazioni
- Legge n. 171/2018 della Repubblica di San Marino – Disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e libera circolazione di tali dati (recepimento GDPR).
- Legge n. 70/1995 – Norme sulla criminalità informatica e tutela dei sistemi informatici.
- Provvedimenti e regolamenti emanati dall'Autorità Garante per la Protezione dei Dati Personali della Repubblica di San Marino.
- Politiche, procedure e regolamenti interni di TIM San Marino

2 Principi Generali della Politica di Sicurezza delle Informazioni

La politica si fonda sui seguenti principi:

- Protezione delle informazioni da qualsiasi minaccia, interna o esterna, intenzionale o accidentale
- Gestione dei rischi in modo strutturato e sistematico
- Rispetto delle leggi, regolamenti e obblighi contrattuali applicabili
- Formazione e sensibilizzazione continua del personale
- Promozione di una cultura organizzativa orientata alla sicurezza

3 Adeguatezza della Politica Rispetto allo Scopo dell'Organizzazione

La presente politica è adeguata allo scopo, al contesto e alle strategie di TIM San Marino, in linea con quanto definito nell'ambito di applicazione del Sistema di Gestione della Sicurezza delle Informazioni. Essa tiene conto delle dimensioni organizzative, della tipologia dei servizi offerti, dei processi aziendali, delle esigenze delle parti interessate interne ed esterne e dei requisiti di sicurezza applicabili. La politica sostiene attivamente il raggiungimento degli obiettivi aziendali, promuovendo l'integrazione della sicurezza delle informazioni nei processi di business e nelle attività operative quotidiane. Viene periodicamente riesaminata e aggiornata per garantirne la coerenza e l'efficacia in relazione all'evoluzione del contesto interno, del mercato e delle normative di riferimento.

4 Obiettivi di Sicurezza delle Informazioni e Quadro per la Loro Definizione

TIM San Marino si impegna a definire, documentare e riesaminare periodicamente obiettivi specifici di sicurezza delle informazioni, coerenti con la presente politica e con i requisiti identificati dalle parti interessate. Gli obiettivi vengono stabiliti considerando i rischi individuati, le opportunità di miglioramento e il contesto organizzativo, e sono misurabili, raggiungibili e allineati alle strategie aziendali. Il raggiungimento di tali obiettivi è monitorato attraverso indicatori di performance e processi di audit interni.

- La definizione degli obiettivi di sicurezza delle informazioni tiene conto dell'ambito di applicazione del SGSI. Questo garantisce che gli obiettivi siano pertinenti rispetto ai processi, alle aree operative e alle risorse coinvolte nel sistema di gestione della sicurezza delle informazioni.
- Inoltre, l'analisi del contesto e delle parti interessate, è utilizzata come strumento per identificare le esigenze e le aspettative sia interne che esterne, assicurando che gli obiettivi rispecchino le reali priorità e i fattori di rischio specifici per TIM San Marino.

- Gli obiettivi sono pertanto formulati in modo da rispondere alle esigenze delle parti interessate, ai requisiti normativi e contrattuali, alle minacce e vulnerabilità individuate, e alle opportunità di miglioramento rilevate nei processi di business.
- La misurazione e il monitoraggio degli obiettivi avvengono tramite indicatori di performance specifici, audit interni e riesami periodici, assicurando così un ciclo di miglioramento continuo e l'adeguamento tempestivo alle evoluzioni del contesto e delle esigenze aziendali.

5 Impegno a Soddisfare i Requisiti Applicabili Relativi alla Sicurezza delle Informazioni

TIM San Marino si impegna a rispettare tutte le leggi, regolamenti, normative e obblighi contrattuali applicabili in materia di sicurezza delle informazioni. Questo impegno si traduce nell'adozione di procedure operative, controlli tecnici e amministrativi volti a garantire la conformità e a prevenire violazioni che possano compromettere la riservatezza, l'integrità e la disponibilità delle informazioni. La conformità viene regolarmente verificata e aggiornata in funzione delle evoluzioni normative e di business.

6 Impegno al Miglioramento Continuo del Sistema di Gestione della Sicurezza delle Informazioni

TIM San Marino promuove il miglioramento continuo del proprio SGSI attraverso l'analisi periodica dei risultati, la valutazione dei rischi, l'attuazione di azioni correttive e preventive e il coinvolgimento di tutte le funzioni aziendali. Le revisioni della politica e degli obiettivi, i risultati degli audit, le segnalazioni di incidenti e i feedback delle parti interessate costituiscono elementi fondamentali per l'evoluzione del sistema e per il rafforzamento della cultura della sicurezza.

7 Disponibilità della Politica come Informazione Documentata

La presente politica è formalmente documentata, approvata dalla Direzione e inserita nel sistema di gestione documentale aziendale. Essa è soggetta a controllo delle versioni e viene conservata in modo che sia facilmente accessibile per consultazione da parte di tutto il personale e delle parti interessate autorizzate. Ogni modifica è tracciata e comunicata tempestivamente secondo le procedure vigenti.

8 Comunicazione Interna della Politica

La politica per la sicurezza delle informazioni è comunicata a tutti i dipendenti e collaboratori tramite canali interni ufficiali quali intranet aziendale, newsletter, sessioni formative e incontri periodici. L'organizzazione si assicura che il personale comprenda il proprio ruolo e le responsabilità in materia

di sicurezza delle informazioni, promuovendo la partecipazione attiva e il rispetto delle disposizioni contenute nella presente politica.

9 Disponibilità della Politica alle Parti Interessate

Ove appropriato, la presente politica è resa disponibile anche alle parti interessate esterne, quali clienti, partner, fornitori e autorità di controllo, su richiesta o tramite pubblicazione su canali istituzionali. Questo garantisce trasparenza, fiducia e allineamento con le aspettative degli stakeholder, rafforzando la reputazione dell'organizzazione in materia di sicurezza delle informazioni.

10 Ruoli e Responsabilità

La Direzione ha la responsabilità ultima dell'attuazione e del mantenimento della politica per la sicurezza delle informazioni. Specifici ruoli e responsabilità sono assegnati all'interno dell'organizzazione per la gestione, il monitoraggio e il miglioramento del SGSI. Tutto il personale è tenuto a rispettare le prescrizioni della politica e a segnalare tempestivamente eventuali anomalie o incidenti di sicurezza.

11 Conclusioni

La Politica per la Sicurezza delle Informazioni rappresenta l'impegno formale di TIM San Marino a proteggere i propri asset informativi e a garantire la conformità ai requisiti applicabili. La sua attuazione richiede la collaborazione attiva di tutte le parti coinvolte e costituisce un elemento chiave per il successo e la sostenibilità dell'organizzazione. La politica verrà periodicamente riesaminata e aggiornata per rispondere alle nuove sfide e opportunità.