

SGSI - Politica per la Sicurezza delle Informazioni

1. Scopo e campo di applicazione

Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) del Gruppo Frigerio Viaggi definisce le regole per la protezione della riservatezza, integrità e disponibilità di tutti i dati critici e delle risorse informative del business.

Il SGSI si applica al perimetro costituito dalle attività di progettazione ed erogazione di servizi di business travel e trasporto turistico, incluso lo sviluppo e la manutenzione dell'applicativo proprietario FriTravelApp e delle relative integrazioni con i sistemi GDS globali.

Tutte le regole aziendali in questo ambito seguono lo standard ISO/IEC 27001:2022 e le linee guida ISO/IEC 27002:2022. Ad esse si aggiungono le misure previste dal Regolamento Europeo per la protezione dei dati (Reg. UE 2016/679 — GDPR) e dalla normativa italiana di recepimento.

La presente Politica costituisce il documento di più alto livello del SGSI ed è vincolante per tutto il personale, i collaboratori e i fornitori che operano nel perimetro definito.

2. Impegno della Direzione

La Direzione aziendale del Gruppo Frigerio Viaggi considera la sicurezza delle informazioni un fattore critico per il settore di business nel quale opera e si impegna attivamente a:

- a) intraprendere iniziative e progetti strutturati per identificare, valutare e ridurre i rischi per la sicurezza delle informazioni, con priorità ai rischi classificati come ALTI o CRITICI;
- b) assicurare l'adempimento degli obblighi contrattuali, normativi e regolamentari applicabili, con particolare riferimento al GDPR, alla ISO/IEC 27001:2022 e alla Direttiva NIS2 (UE 2022/2555) ove applicabile;
- c) adottare le migliori pratiche di settore e adeguarsi agli standard tecnologici più avanzati, inclusi quelli relativi alla sicurezza dello sviluppo software e alle integrazioni con sistemi GDS e piattaforme di pagamento;
- d) garantire le risorse umane, tecnologiche e finanziarie necessarie al funzionamento e al miglioramento continuo del SGSI;

- e) promuovere una cultura della sicurezza delle informazioni a tutti i livelli dell'organizzazione, attraverso formazione, sensibilizzazione e comunicazione interna;
- f) riesaminare periodicamente la presente Politica e gli obiettivi di sicurezza, al fine di verificarne l'adeguatezza e l'efficacia in relazione al contesto organizzativo e al panorama delle minacce.

3. Principi di applicazione

All'interno del Gruppo, tutto il personale, i collaboratori e i fornitori sono tenuti a conoscere e osservare i seguenti principi fondamentali:

- a) La sicurezza informativa è dovere e responsabilità di ciascuno: ogni individuo che opera nel perimetro del SGSI è responsabile della protezione delle informazioni cui accede o tratta, indipendentemente dal ruolo e dalla modalità di lavoro (sede, remoto, trasferta).
- b) Principio del minimo privilegio (need-to-know): ogni utente del sistema informativo deve poter accedere alle sole informazioni necessarie per lo svolgimento delle proprie mansioni. Le autorizzazioni di accesso sono differenziate in base al ruolo, agli incarichi e al profilo di rischio associato.
- c) Gestione e classificazione degli asset: gli asset aziendali devono essere catalogati e a ciascun asset deve essere assegnato un responsabile (owner). Le risorse devono essere utilizzate e protette secondo i requisiti di sicurezza della classificazione assegnata.
- d) Difesa in profondità (defence in depth): un singolo livello di controllo può rivelarsi insufficiente. Un approccio a più livelli di protezione deve essere adottato nei casi in cui una perdita di funzionalità del sistema informativo sia classificata come critica per il business.
- e) Privacy e Security by Design: la protezione dei dati personali e la sicurezza delle informazioni devono essere integrate fin dalla fase di progettazione di nuovi sistemi, servizi, processi e applicativi software, in conformità all'art. 25 del GDPR e ai controlli A.8.25–A.8.34 della ISO/IEC 27001:2022.
- f) Continuità operativa e resilienza: è essenziale sottoporre a esercitazioni e test periodici la capacità di risposta agli incidenti, la continuità del servizio (Business Continuity) e il ripristino dei servizi critici con danno minimo (Disaster Recovery), con cadenza almeno annuale.
- g) Miglioramento continuo: il SGSI è soggetto a monitoraggio costante, audit interni periodici e riesame da parte della Direzione, al fine di garantire la sua adeguatezza, adeguatezza e efficacia nel tempo.

4. Gestione del rischio e propensione al rischio

Il Gruppo Frigerio Viaggi adotta un approccio sistematico e documentato alla gestione del rischio per la sicurezza delle informazioni, in conformità ai requisiti del punto 6.1 della ISO/IEC 27001:2022 e alle linee guida della ISO/IEC 27005:2022.

Il processo di valutazione del rischio viene condotto con cadenza almeno annuale e ogniqualvolta intervengano modifiche significative al contesto organizzativo, tecnologico o normativo.

La Direzione stabilisce i seguenti criteri di accettazione del rischio (risk appetite):

- Rischi classificati come BASSI (punteggio 1–4 su scala 5×5): accettabili senza piano di trattamento obbligatorio, soggetti a monitoraggio periodico.
- Rischi classificati come MEDI (punteggio 5–12): accettabili con monitoraggio rafforzato e misure di mitigazione programmate entro 90 giorni.
- Rischi classificati come ALTI (punteggio 13–19): non accettabili. Devono essere oggetto di piano di trattamento formale con responsabile e scadenza definiti, con approvazione del RSSI e della Direzione, prima di poter essere accettati come rischio residuo.
- Rischi classificati come CRITICI (punteggio 20–25): non accettabili in nessun caso. Richiedono azione immediata e blocco dell'attività associata fino all'adozione di misure di contenimento efficaci.

I risultati della valutazione del rischio, il piano di trattamento e i rischi residui accettati dalla Direzione sono documentati nel Registro dei Rischi (Risk Register) del SGSI e ne viene dato riscontro nell'ambito del riesame della Direzione.

5. Sicurezza nello sviluppo software

Il Gruppo Frigerio Viaggi gestisce internamente lo sviluppo e la manutenzione evolutiva dell'applicativo proprietario FriTravelApp, integrato con sistemi GDS globali e piattaforme di pagamento. Questa attività costituisce un ambito di rischio specifico che richiede l'applicazione di controlli dedicati.

Tutti i processi di sviluppo, test e rilascio in produzione del software devono essere condotti secondo i seguenti principi, in conformità ai controlli A.8.25–A.8.34 della ISO/IEC 27001:2022 e alle linee guida NIST SP 800-218 (Secure Software Development Framework — SSDF):

- a) Security by Design: i requisiti di sicurezza devono essere definiti e documentati nella fase di analisi di ogni progetto di sviluppo, prima dell'avvio delle attività di codifica.
- b) Secure Coding: il codice deve essere sviluppato secondo le linee guida di codifica sicura (OWASP, CERT), con particolare attenzione alla validazione degli input, alla

gestione delle sessioni, alla protezione contro le vulnerabilità più comuni (es. SQL injection, XSS, CSRF).

c) Test di sicurezza: ogni rilascio in produzione deve essere preceduto da test di sicurezza applicativa (SAST, DAST) e dalla compilazione della Checklist di Security Review Pre-Deploy. Le vulnerabilità critiche identificate devono essere risolte prima del rilascio.

d) Gestione degli ambienti: gli ambienti di sviluppo, test e produzione devono essere separati e gestiti con controlli di accesso differenziati. I dati reali di produzione non devono essere utilizzati in ambienti di test senza adeguata pseudonimizzazione.

e) Gestione delle vulnerabilità: le vulnerabilità identificate devono essere classificate per gravità (CVSS) e trattate nei tempi stabiliti dalla policy aziendale: critiche entro 72 ore, alte entro 7 giorni, medie entro 30 giorni. Il Piano di Trattamento delle Vulnerabilità deve essere aggiornato a ogni identificazione.

Il Manager IT è responsabile della supervisione del processo di sviluppo sicuro. Il DPO deve essere coinvolto nelle fasi di progettazione che riguardano il trattamento di dati personali.

6. Sicurezza nella catena di fornitura

Il Gruppo Frigerio Viaggi riconosce che i fornitori e i partner con accesso ai propri sistemi informativi, dati o infrastrutture rappresentano un'estensione del perimetro di rischio del SGSI. Pertanto, in conformità ai controlli A.5.19–A.5.22 della ISO/IEC 27001:2022, la gestione della sicurezza nella catena di fornitura è parte integrante del SGSI.

Sono considerati fornitori critici in ambito SGSI, a titolo esemplificativo e non esaustivo:

- I sistemi GDS (Global Distribution Systems): Amadeus, Sabre, Travelport — fornitori di infrastruttura per la prenotazione di servizi travel, con accesso in lettura/scrittura a dati di viaggio e PNR;
- I fornitori di servizi cloud e infrastruttura (IaaS/SaaS) utilizzati per l'hosting dell'applicativo FriTravelApp;
- I fornitori di servizi di pagamento e tokenizzazione, soggetti anche ai requisiti PCI DSS;
- I consulenti e collaboratori esterni con accesso a sistemi o dati classificati.

Per tutti i fornitori critici, il Gruppo Frigerio Viaggi si impegna a: inserire clausole contrattuali di sicurezza (DPA, NDA, requisiti minimi di sicurezza); effettuare una valutazione del rischio fornitore in fase di selezione; monitorare periodicamente il rispetto dei requisiti di sicurezza pattuiti; garantire procedure di gestione delle modifiche e della cessazione del rapporto contrattuale che includano la restituzione o cancellazione sicura dei dati.

7. Gestione degli incidenti di sicurezza

Il Gruppo Frigerio Viaggi adotta una procedura strutturata per la gestione degli eventi e degli incidenti di sicurezza delle informazioni, in conformità ai controlli A.5.24–A.5.28 della ISO/IEC 27001:2022.

Tutti gli incidenti di sicurezza, reali o sospetti, devono essere segnalati tempestivamente al RSSI (o al referente designato) attraverso i canali di comunicazione interni definiti.

La gestione degli incidenti si articola nelle seguenti fasi: rilevamento e segnalazione; classificazione e valutazione dell'impatto; contenimento e ripristino; analisi delle cause e azioni correttive; documentazione e chiusura nel Registro Incidenti.

Obblighi di notifica al Garante per la protezione dei dati personali (GDPR art. 33): qualora un incidente di sicurezza comporti una violazione dei dati personali (data breach), il Titolare del trattamento è tenuto a notificare l'evento all'Autorità Garante entro 72 ore dal momento in cui ne viene a conoscenza, salvo che sia improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche.

Il DPO è responsabile della valutazione dell'obbligo di notifica e della relativa comunicazione.

Qualora la violazione presenti un rischio elevato per i diritti degli interessati, è altresì obbligatoria la comunicazione agli interessati stessi (GDPR art. 34), senza ingiustificato ritardo.

8. Continuità operativa e Disaster Recovery

Il Gruppo Frigerio Viaggi garantisce la continuità operativa dei servizi critici attraverso un Piano di Business Continuity (BCP) e un Piano di Disaster Recovery (DRP), in conformità ai controlli A.5.29 e A.5.30 della ISO/IEC 27001:2022.

I piani definiscono le strategie, le procedure e le responsabilità necessarie a garantire la continuità dei processi essenziali e il ripristino dei sistemi in caso di interruzione.

Per ciascun servizio e sistema critico sono definiti:

- RTO (Recovery Time Objective): tempo massimo accettabile di interruzione del servizio prima che il ripristino debba essere completato;
- RPO (Recovery Point Objective): massima perdita di dati accettabile, espressa in unità di tempo dalla precedente procedura di backup.

I piani di Business Continuity e Disaster Recovery sono soggetti a test e simulazioni con cadenza almeno annuale. Gli esiti delle simulazioni sono documentati nel Verbale di Simulazione Disaster Recovery e le eventuali criticità emerse devono essere oggetto di azioni correttive entro 30 giorni. I piani devono essere aggiornati a seguito di ogni simulazione, cambiamento organizzativo rilevante o incidente che ne abbia messo alla prova l'efficacia.

9. Obiettivi di sicurezza e indicatori di prestazione

In conformità al punto 6.2 della ISO/IEC 27001:2022, il Gruppo Frigerio Viaggi definisce, documenta e monitora obiettivi di sicurezza delle informazioni misurabili, coerenti con la presente Politica. Gli obiettivi sono comunicati a tutto il personale interessato e sottoposti a verifica nell'ambito del riesame annuale della Direzione.

Gli obiettivi di sicurezza per il periodo in corso comprendono, a titolo indicativo:

1. Formazione del personale: garantire che il 100% del personale interno abbia completato il programma annuale di formazione e sensibilizzazione sulla sicurezza delle informazioni entro il 31 dicembre di ogni anno.
2. Gestione delle vulnerabilità critiche: assicurare la risoluzione del 100% delle vulnerabilità classificate come critiche (CVSS $\geq$ 9.0) entro 72 ore dall'identificazione.
3. Gestione degli incidenti: garantire la chiusura formale del 100% degli incidenti di sicurezza registrati entro i tempi definiti nella procedura di incident management, con documentazione completa nel sistema.
4. Test di Business Continuity: condurre almeno una simulazione di Disaster Recovery all'anno, con documentazione degli esiti e piano di azioni correttive per le criticità emerse.
5. Audit interno: eseguire almeno un ciclo completo di audit interno del SGSI per anno, con chiusura formale di tutte le non conformità rilevate entro i termini stabiliti nel piano di azioni correttive.
6. Sicurezza nello sviluppo software: garantire che il 100% dei rilasci in produzione di FriTravelApp sia preceduto dalla compilazione e superamento della Checklist di Security Review Pre-Deploy.

10. Responsabilità

Tutto il personale interno, i collaboratori e i fornitori devono conformarsi a quanto previsto dalla presente Politica e alle procedure operative del SGSI. Inadeguati livelli di sicurezza possono arrecare danni all'immagine aziendale, generare insoddisfazione del cliente, comportare rischi di incorrere in sanzioni e danni di natura economica e finanziaria. Chiunque, in modo intenzionale o per negligenza, disattenda le regole di sicurezza provocando un danno al Gruppo, potrà essere perseguito nelle opportune sedi civili, penali e disciplinari. Tutto il personale è responsabile della segnalazione di eventuali anomalie, vulnerabilità o violazioni di cui dovesse venire a conoscenza.

Le responsabilità specifiche nell'ambito del SGSI sono così distribuite:

- Direzione (General Director): approva la presente Politica, gli obiettivi di sicurezza e le risorse del SGSI; presiede il riesame della Direzione; approva il trattamento dei rischi residui ALTI e CRITICI.

- **Amministratore di Sistema:** responsabile della gestione operativa dell'infrastruttura, della configurazione sicura dei sistemi, della gestione dei backup e del monitoraggio degli accessi privilegiati.
- **Manager IT:** responsabile della sicurezza dell'infrastruttura tecnologica e del processo di sviluppo sicuro del software, coordina il team di sviluppo, supervisiona la gestione degli accessi e l'applicazione dei controlli tecnici.
- **RSSI (Responsabile del Sistema di Sicurezza delle Informazioni):** coordina il SGSI, supervisiona la valutazione e il trattamento dei rischi, gestisce gli audit interni, verifica l'efficacia dei controlli e propone azioni di miglioramento.
- **DPO (Data Protection Officer):** supervisiona la conformità al GDPR, valuta gli obblighi di notifica in caso di data breach, verifica l'applicazione dei principi di Privacy by Design nei processi e nei sistemi, e supporta le valutazioni di impatto (DPIA).
- **Tutto il personale:** rispetta le policy di sicurezza, segnala prontamente incidenti e anomalie, partecipa ai programmi di formazione obbligatori.

11. Riferimenti normativi e documentali

La presente Politica si fonda sui seguenti riferimenti normativi, regolamentari e di standard internazionali:

- **UNI CEI EN ISO/IEC 27001:2022** — Sicurezza delle informazioni, cybersecurity e protezione della privacy — Sistemi di gestione per la sicurezza delle informazioni — Requisiti
- **ISO/IEC 27002:2022** — Sicurezza delle informazioni, cybersecurity e protezione della privacy — Controlli di sicurezza delle informazioni
- **ISO/IEC 27005:2022** — Linee guida per la gestione del rischio per la sicurezza delle informazioni
- **ISO/IEC 27701:2019** — Estensione a ISO/IEC 27001 e 27002 per la gestione delle informazioni sulla privacy — Requisiti e linee guida
- **ISO/IEC 27034:2011** — Information Technology — Security Techniques
- **D.Lgs. 196/2003 e s.m.i. (Codice Privacy italiano, aggiornato dal D.Lgs. 101/2018)**
- **Direttiva (UE) 2022/2555 — NIS2** — Misure per un elevato livello comune di cibersicurezza nell'Unione (ove applicabile al perimetro del Gruppo)
- **NIST SP 800-218** — Secure Software Development Framework (SSDF) v1.1

12. Revisione, aggiornamento e controllo del documento

La presente Politica è sottoposta a revisione formale con cadenza annuale, nell'ambito del riesame della Direzione del SGSI, e ogniqualvolta intervengano modifiche rilevanti al contesto organizzativo, normativo o tecnologico (es. introduzione di nuovi sistemi, cambiamenti strutturali, incidenti significativi, aggiornamenti di standard di riferimento).

La responsabilità della revisione è in capo al RSSI, con il supporto del DPO per gli aspetti relativi alla protezione dei dati. La Politica aggiornata deve essere approvata dal General Director prima della distribuzione e deve essere comunicata a tutto il personale.

Il presente documento è soggetto a controllo di versione.

Registro delle revisioni:

Rev. 1 — 22.09.2024 — Prima emissione — Approvata da Simone Frigerio, General Director

Rev. 2 — 30.06.2026 — Revisione e aggiornamento: aggiunta sezioni Gestione del rischio e risk appetite, Sicurezza nello sviluppo software, Sicurezza nella catena di fornitura, Gestione degli incidenti, Continuità operativa e DR, Obiettivi di sicurezza e KPI. Aggiornamento riferimenti normativi (ISO/IEC 27005:2022, NIS2). Allineamento ISO/IEC 27001:2022 completo — Approvata da Simone Frigerio, General Director

Giussano, 30 giugno 2026

Simone Frigerio
General Director — Gruppo Frigerio Viaggi

