# *SICUREZZA DELLE INFORMAZIONI*

## Policy in Pillole

**Gruppo TIM**

**Dicembre 2025**

# INDICE

## 1. Perchè questa Policy

La Politica di Sicurezza delle Informazioni definisce i principi e gli impegni del Gruppo TIM per proteggere le informazioni aziendali e garantirne un utilizzo corretto e responsabile.
Le informazioni rappresentano un asset strategico per il Gruppo TIM e sono essenziali per il funzionamento dei processi di business e per l'erogazione dei servizi. La loro protezione è quindi fondamentale per assicurare continuità operativa, affidabilità e tutela degli stakeholder.
Questa Policy stabilisce un quadro organizzativo e normativo di riferimento che individua ruoli, responsabilità e regole per la gestione sicura delle informazioni, con l'obiettivo di garantirne riservatezza, integrità e disponibilità, riducendo i rischi legati alla sicurezza, alla conformità normativa e alla continuità dei servizi.

## 2. Gli obiettivi che ci siamo dati

Le informazioni oggetto di questa Policy comprendono qualsiasi aggregazione di dati che abbia valore e interesse per il Gruppo TIM, indipendentemente dalla forma assunta e dalle modalità con cui viene trattata.

La Politica di Sicurezza delle Informazioni ha l'obiettivo di garantire che tali informazioni siano protette in modo coerente con il loro valore per il business, tenendo conto dei rischi di sicurezza, delle normative applicabili e delle aspettative degli stakeholder, assicurandone riservatezza, integrità e disponibilità.
Tali obiettivi sono perseguiti attraverso un insieme strutturato di processi organizzativi e responsabilità definite.
A tal fine, il Gruppo TIM si impegna a:

- definire regole, priorità, processi, ruoli e responsabilità per la sicurezza delle informazioni;
- garantire la sicurezza dei servizi e i livelli di continuità operativa previsti;
- proteggere le informazioni in funzione del loro valore e dell'impatto potenziale di incidenti di sicurezza;
- tutelare le informazioni strategiche, i dati personali e l'immagine aziendale;
- operare nel rispetto delle leggi, dei contratti e delle procedure interne del Gruppo

- promuovere la formazione e la sensibilizzazione del personale;
- monitorare, gestire e analizzare gli incidenti di sicurezza, collaborando con Enti e Istituzioni per il miglioramento continuo.

## 3. A chi si rivolge e dove si applica

La Policy si applica a TIM S.p.A. e alle Società del Gruppo TIM operanti in ambito *Domestic* e disciplina la protezione delle informazioni di valore aziendale e degli asset utilizzati per il loro trattamento, lungo l'intero ciclo di vita delle informazioni, indipendentemente dalle modalità operative, dalle tecnologie utilizzate o dal ricorso a terze parti.

## 4. Chi sono i responsabili dell'attuazione

L'attuazione della Policy è supportata da un modello di governance che assicura una gestione coordinata e coerente della sicurezza delle informazioni all'interno del Gruppo TIM, con una chiara attribuzione di ruoli e responsabilità.
La Funzione "*Chief Security Office*" svolge un ruolo di indirizzo e governo del sistema di sicurezza delle informazioni del Gruppo, assicurando il coordinamento complessivo, l'allineamento alle normative e agli standard applicabili e la coerenza delle iniziative di sicurezza.
Le Società del Gruppo TIM sono responsabili dell'attuazione operativa della Policy nell'ambito delle proprie attività, garantendo l'applicazione delle misure di sicurezza delle informazioni, la gestione dei rischi e la protezione delle informazioni trattate sui propri processi, sistemi e asset.

## 5. Il Quadro normativo a cui facciamo riferimento

La Policy è allineata agli standard internazionali e alle normative di riferimento in materia di sicurezza delle informazioni, tra cui:

- ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary
- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection
- Information security management systems - Requirements

- ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection
- Information security controls
- ISO/IEC 27035-1:2023 Information technology - Information security incident management - Part 1: Principles and process; Part 2: Guidelines to plan and prepare for incident response; Part 3: Guidelines for ICT incident response operations

## 6. I principali contenuti della Policy

La Politica di Sicurezza delle Informazioni definisce il quadro di riferimento attraverso cui il Gruppo TIM protegge il proprio patrimonio informativo, garantendo la riservatezza, l'integrità e la disponibilità delle informazioni, la continuità dei processi aziendali e il rispetto degli obblighi normativi e contrattuali.

Elemento centrale della Policy è il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), che stabilisce in modo strutturato come la sicurezza delle informazioni viene organizzata, applicata e monitorata nel tempo all'interno del Gruppo, secondo un approccio basato sull'analisi dei rischi e sul miglioramento continuo.

Il SGSI presidia i processi e le attività necessarie a garantire la sicurezza del patrimonio informativo, definendo:

- ruoli e responsabilità all'interno del Gruppo TIM, al fine di stabilire priorità di intervento e assicurare un'adeguata allocazione delle risorse necessarie all'efficace attuazione delle politiche di sicurezza;
- le esigenze di sicurezza da garantire sulla base dell'analisi dei rischi, acquisendo consapevolezza del livello di esposizione a minacce del patrimonio informativo e degli impatti potenziali di eventuali incidenti di sicurezza sul business;
- le misure di sicurezza da adottare in conformità agli standard internazionali di settore e alle normative cogenti;
- l'efficace implementazione delle misure individuate e il controllo del loro mantenimento nel tempo.

Dal **punto di vista organizzativo**, il SGSI articola la gestione della sicurezza su tre livelli tra loro coordinati:

- un **livello di indirizzo**, presidiato dalla Funzione Chief Security Office che definisce obiettivi, requisiti e regole di sicurezza in coerenza con le normative, gli standard di riferimento e le esigenze del business;
- un **livello operativo**, in capo alle funzioni competenti delle Società del Gruppo, responsabile dell'attuazione concreta delle misure di sicurezza sui processi, sui sistemi, sugli asset e lungo l'intero ciclo di vita delle informazioni;
- un **livello di controllo**, svolto dalle strutture competenti che verifica l'effettiva applicazione delle regole, la conformità ai requisiti della Policy e contribuisce al miglioramento continuo del sistema.

Dal **punto di vista operativo**, l'SGSi analizza e classifica tutti gli asset informativi e tecnologici in base al loro valore e agli impatti potenziali sul business, e li sottoponei a un processo strutturato di gestione del rischio. Sulla base della classificazione assegnata, vengono definiti e applicati livelli di protezione proporzionati, che accompagnano le informazioni e gli asset lungo l'intero ciclo di vita, dalla creazione o acquisizione fino alla dismissione. Per ciascun asset è individuato un responsabile incaricato di garantire il rispetto delle regole di sicurezza.

Il modello disciplina inoltre le principali attività operative necessarie a garantire la sicurezza delle informazioni, tra cui:

- la gestione degli accessi secondo i principi di necessità e di minimo privilegio;
- il tracciamento delle attività sugli asset, al fine di garantire controllo e verificabilità;
- la protezione delle comunicazioni, dei sistemi e delle infrastrutture;
- la gestione delle modifiche, degli aggiornamenti, degli ambienti di sviluppo e collaudo e dei backup;
- la prevenzione e la gestione degli incidenti di sicurezza, inclusi i data breach, nonché l'attivazione delle misure di business continuity per assicurare la continuità dei servizi.

Particolare attenzione è dedicata ai **rapporti con fornitori e partner**: il SGSI richiede l'adozione di livelli di sicurezza coerenti con quelli interni, attraverso specifici requisiti contrattuali, strumenti di monitoraggio e meccanismi di verifica, inclusi diritti di audit. Gli asset, inclusi quelli forniti da terze parti, devono essere progettati, sviluppati e mantenuti in conformità agli standard e alle best practices di sicurezza adottate dal Gruppo TIM; sono previsti processi

di sviluppo sicuro del software, la protezione del codice sorgente e l'esecuzione di test di sicurezza prima del rilascio in ambiente di esercizio.

A supporto dell'efficace attuazione del modello, il SGSI promuove inoltre la sensibilizzazione e la **formazione continua delle persone** che, a vario titolo, trattano informazioni e asset aziendali, al fine di rafforzare la consapevolezza dei rischi e garantire comportamenti coerenti con le regole di sicurezza definite.

Attraverso questo insieme di regole e presìdi, la sicurezza delle informazioni è gestita come un processo continuo e coordinato, finalizzato a ridurre i rischi, limitare gli impatti negativi e supportare la continuità operativa e l'affidabilità dei servizi del Gruppo.

## 7. Come la sostenibilità è integrata nella sicurezza delle informazioni

La Policy di Sicurezza delle Informazioni del Gruppo TIM affronta in modo strutturato i rischi e gli impatti negativi connessi alla gestione delle informazioni e alla resilienza dei sistemi ICT, che possono incidere sulla capacità del Gruppo di operare in modo continuativo, affidabile e responsabile nel tempo. Sul piano degli impatti verso l'esterno, eventi quali violazioni dei dati, indisponibilità dei sistemi o compromissione dell'integrità delle informazioni possono generare effetti negativi su stakeholder rilevanti, in particolare clienti e dipendenti, incidendo sulla tutela delle informazioni, sulla qualità e continuità dei servizi e sulla fiducia nei confronti del Gruppo. Sul piano dei rischi per il Gruppo, gli stessi eventi possono determinare conseguenze di natura economica, operativa e reputazionale, quali interruzioni dei servizi, costi di ripristino, sanzioni o contenziosi, con possibili effetti sulla stabilità delle attività nel medio-lungo periodo. La Policy interviene su questo quadro definendo regole, responsabilità e misure di sicurezza finalizzate a ridurre la probabilità che tali eventi si verifichino e a limitarne gli effetti. In particolare, la tutela della riservatezza, dell'integrità e della disponibilità delle informazioni e il rafforzamento della resilienza dei sistemi informativi consentono di prevenire impatti negativi sugli stakeholder e di mitigare i rischi per il Gruppo. La Policy supporta inoltre la riduzione dei rischi connessi alle modalità di utilizzo delle informazioni e degli strumenti informativi da parte dei dipendenti, attraverso iniziative di

formazione e sensibilizzazione volte a prevenire errori operativi, utilizzi non conformi alle regole di sicurezza e carenze di consapevolezza.

## 8. Parole Chiave

- **Asset:** risorsa aziendale che ha valore per il Gruppo TIM e che deve essere protetta, comprendente informazioni, sistemi, tecnologie e infrastrutture utilizzate nei processi aziendali.
- **Business Continuity:** insieme di misure e processi finalizzati a garantire la continuità operativa dei servizi e dei processi critici in caso di incidenti o eventi avversi.
- **Data breach**: violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati.
- **Principio del minimo privilegio:** principio di sicurezza secondo cui agli utenti sono concessi esclusivamente i diritti di accesso strettamente necessari allo svolgimento delle attività autorizzate.