



CYBERSECURITY

Approfondimento

Gruppo TIM

Giugno 2026



INDICE

1.	La cybersecurity al centro del nostro impegno per un digitale affidabile e sicuro.....	3
2.	Il nostro sistema di governance per la cybersecurity	4
3.	Il quadro normativo e istituzionale della cybersecurity	5
4.	La nostra policy sulla cybersecurity.....	7
5.	Il nostro sistema di gestione della cybersecurity	8



1. La cybersecurity al centro del nostro impegno per un digitale affidabile e sicuro

Siamo il principale operatore di telecomunicazioni in Italia e tra i leader a livello europeo. Questa posizione ci offre una prospettiva unica sulle minacce informatiche. Ogni giorno, monitoriamo e analizziamo centinaia di eventi per prevenire o contenere gli attacchi, lavorando senza sosta per proteggere le infrastrutture di rete, i data center, le piattaforme cloud e i servizi digitali del Gruppo TIM e, naturalmente, dei nostri clienti.

Al nostro interno operano realtà specializzate e coordinate, come la sicurezza di rete, i Centri Operativi di Sicurezza Informatica (Cyber Security Operations Center – Cyber SOC) e società come Telsy. Un ecosistema che ci permette di osservare da vicino l'evoluzione delle minacce che colpiscono indistintamente cittadini, imprese e istituzioni.

Monitoriamo altresì l'evoluzione del contesto normativo e istituzionale in tema di Cyber sicurezza per capire come si stanno rafforzando le difese e quali interventi si stanno introducendo a livello europeo e nazionale per incrementare le capacità di prevenzione e contrasto all'intensificarsi degli attacchi.

Crediamo in un mondo digitale che sia affidabile e sicuro. Per questo ci impegniamo a diffondere una vera cultura della cybersecurity, accessibile anche ai non esperti. Per questo motivo abbiamo pubblicato, nel corso del 2025, il Cyber Security Report 2024 in collaborazione con la Cyber Security Foundation, la prima fondazione no profit italiana sul mondo cibernetico.

Nel corso del 2025, il Gruppo TIM ha inoltre rafforzato il presidio delle tematiche di sicurezza delle informazioni e protezione dei dati nell'ambito del proprio Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR), integrando tali aspetti tra i principali rischi ESG monitorati dagli organi di governance e dai processi di Enterprise Risk Management.



2. Il nostro sistema di governance per la cybersecurity

Per garantire la protezione delle nostre infrastrutture e dei dati trattati dai rischi legati alla cybersecurity, operiamo attraverso un sistema di governance strutturato e coerente.

Il Consiglio di Amministrazione ha la responsabilità di indirizzo e supervisione strategica, anche in materia di controllo interno e gestione dei rischi. In questo ambito, definisce le linee guida del Sistema di Controllo Interno, ne verifica l'adeguatezza, l'efficacia e il corretto funzionamento, affinché i principali rischi aziendali, inclusi quelli legati alla cybersecurity e alla protezione dei dati, siano correttamente identificati, valutati e gestiti nel tempo. A questo scopo il modello di Enterprise Risk Management adottato consente di individuare, valutare e gestire i rischi in modo omogeneo all'interno del Gruppo.

A livello complessivo di governance, nell'espletamento delle proprie responsabilità di indirizzo e supervisione strategica, estese alle tematiche del controllo e della gestione del rischio, il Consiglio di Amministrazione (CdA) di TIM si è organizzato costituendo un comitato interno focalizzato su controlli e rischi (il Comitato per il Controllo e i Rischi). Il Comitato per il Controllo e i Rischi è un organo endoconsiliare composto da soli amministratori indipendenti. Il Comitato svolge funzioni istruttorie a supporto del Consiglio nelle valutazioni e nelle decisioni riguardanti il sistema di controllo e gestione dei rischi al quale riferisce regolarmente sulle attività svolte.

Nel 2025 il Consiglio di Amministrazione ha ulteriormente rafforzato il presidio delle competenze ESG e dei rischi di sicurezza delle informazioni, evidenziando tra i principali rischi monitorati quelli relativi alla cybersecurity, alla protezione dei dati e alla conformità normativa. Tra le aree di sua competenza rientrano anche i rischi relativi alla Cyber Security e alla Privacy, ambiti in cui il Presidente del Comitato vanta una solida esperienza operativa.

Il Chief Executive Officer (CEO), nel rispetto degli indirizzi del Consiglio di



Amministrazione, è responsabile dell'istituzione e del corretto funzionamento del sistema di controllo interno e di gestione dei rischi. A lui fa capo anche la governance in materia di Information Security e Cyber Security, inclusa la gestione dei rischi correlati.

Su attribuzione del Consiglio di Amministrazione e con l'assenso dell'Autorità di Governo, il CEO detiene la delega esclusiva in qualità di Amministratore per l'Organizzazione di Sicurezza, secondo quanto previsto dalla normativa Golden Power. Tale disciplina prevede una stretta collaborazione con il Governo sui temi legati alla sicurezza delle infrastrutture strategiche di comunicazione e impone il rafforzamento dei presidi interni di sicurezza.

Nel 2025 il Sistema di Controllo Interno e Gestione dei Rischi è stato ulteriormente consolidato attraverso il coordinamento tra funzioni Enterprise.

3. Il quadro normativo e istituzionale della cybersecurity

In qualità di operatore strategico per il Paese, TIM opera all'interno di un quadro normativo nazionale ed europeo particolarmente articolato in materia di cybersecurity, sicurezza delle infrastrutture critiche, resilienza digitale e protezione dei dati personali.

I decreti Golden Power, introdotti nel 2017, prevedono specifici obblighi per le imprese operanti in settori strategici quali le telecomunicazioni, imponendo l'adozione di misure dedicate di sicurezza e controllo e specifici obblighi di reporting verso l'Autorità di Governo.

Con il Decreto-legge 21/2022, emanato nel contesto della crisi ucraina, sono stati ulteriormente rafforzati i poteri speciali della Presidenza del Consiglio dei Ministri e introdotti requisiti più stringenti per la sicurezza delle reti 5G considerate infrastrutture critiche di interesse nazionale.

L'attuazione delle misure previste dalla normativa è sottoposta alla verifica di un



Comitato di Monitoraggio istituito presso la Presidenza del Consiglio dei Ministri, incaricato di verificare l'adempimento degli obblighi normativi e, ove necessario, applicare sanzioni.

A partire dal 2021 il quadro normativo si è ulteriormente consolidato con l'attuazione della Legge 133/2019, che ha istituito il Perimetro di Sicurezza Nazionale Cibernetica (PSNC), finalizzato a garantire elevati livelli di protezione per gli operatori che gestiscono servizi ICT essenziali per la sicurezza nazionale, tra cui TIM.

Un ulteriore elemento di evoluzione normativa è rappresentato dalla Direttiva europea 2022/2555 (NIS2), entrata in vigore nel gennaio 2023 e applicabile dal 18 ottobre 2024, che amplia significativamente l'ambito di applicazione delle norme sulla sicurezza delle reti e dei sistemi informativi, sia a settori precedentemente disciplinati da altre normative, sia a nuovi soggetti, tra cui data center e Content Delivery Network (CDN).

La Direttiva introduce requisiti più stringenti in materia di gestione del rischio cyber, sicurezza della supply chain, resilienza operativa, governance della cybersecurity e gestione e notifica degli incidenti informatici, mantenendo l'obbligo di adottare misure di sicurezza commisurate al rischio e introducendo requisiti minimi di base. In caso di inottemperanza, sono previste sanzioni che possono arrivare fino al 2% del fatturato. La NIS2 rafforza inoltre gli organi e le attività di supervisione a livello europeo e la collaborazione tra gli Stati membri, anche attraverso la condivisione delle esperienze nel contrasto alle minacce informatiche.

L'evoluzione normativa in materia di cybersecurity, resilienza digitale e compliance rappresenta uno dei principali elementi considerati nei processi di governance e gestione dei rischi del Gruppo.

In questo contesto opera anche l'Agenzia per la Cybersicurezza Nazionale (ACN), con il compito di vigilare, coordinare e rafforzare la resilienza del Paese rispetto all'evoluzione delle minacce cyber. TIM mantiene inoltre una collaborazione costante e strutturata con



le istituzioni, partecipando attraverso le proprie funzioni specializzate a gruppi di lavoro presso organismi istituzionali, tra cui la Presidenza del Consiglio dei Ministri, il Ministero dell'Interno e il Ministero della Difesa.

4. La nostra policy sulla cybersecurity

La sicurezza delle informazioni costituisce un elemento centrale del modello di governance del Gruppo TIM e la relativa policy si applica a tutte le funzioni aziendali, ai processi, alle tecnologie e agli asset che trattano informazioni per conto del Gruppo.

La policy di sicurezza delle informazioni definisce principi, obiettivi, ruoli e responsabilità finalizzati a garantire la riservatezza, l'integrità, la disponibilità e la protezione delle informazioni aziendali e dei dati personali, promuovendo un approccio orientato al miglioramento continuo e formalizzando l'impegno del management al rispetto dei requisiti di sicurezza.

Nel corso del 2025 il Gruppo ha ulteriormente rafforzato l'integrazione tra gestione dei rischi cyber, governance ESG e sistemi di controllo interno, assicurando la piena integrazione dei processi di sicurezza delle informazioni nei sistemi di governance, controllo interno e gestione del rischio.

La policy si applica a tutti gli asset aziendali e coinvolge l'intera forza lavoro del Gruppo, chiamata a contribuire attivamente al raggiungimento degli obiettivi di sicurezza attraverso comportamenti coerenti con le policy aziendali e con i requisiti normativi applicabili e l'attuazione delle azioni di sicurezza di propria competenza.

Attraverso la policy di Information Security, TIM si impegna a:

- definire processi, ruoli e responsabilità in materia di sicurezza delle informazioni;
- garantire un livello di riservatezza, integrità, disponibilità e protezione



proporzionato al valore delle informazioni per il business e alle potenziali perdite derivanti da incidenti di sicurezza

- sensibilizzare e formare il personale sui temi della cybersecurity;
- monitorare, analizzare e gestire ogni incidente, anche solo presunto, relativo alla sicurezza delle informazioni
- definire specifici requisiti di sicurezza informatica per fornitori e altre controparti esterne;
- promuovere il miglioramento continuo dei sistemi di sicurezza delle informazioni attraverso la collaborazione con enti e istituzioni nazionali e internazionali e la condivisione di metodologie e best practice.

Nei rapporti con fornitori e partner, il Gruppo prevede specifici requisiti e clausole contrattuali finalizzati a garantire la protezione delle informazioni e della proprietà intellettuale, la conformità normativa, adeguati livelli di sicurezza, la gestione degli incidenti e la possibilità di svolgere attività di audit e monitoraggio. Tali requisiti riguardano anche l'adeguatezza delle competenze del personale coinvolto, i piani di continuità operativa, i livelli di servizio e le relative penali, allineati o più stringenti rispetto a quelli previsti per i clienti.

5. Il nostro sistema di gestione della cybersecurity

Per perseguire gli obiettivi definiti dalla policy di sicurezza delle informazioni, il Gruppo TIM ha adottato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) basato su processi strutturati di prevenzione, monitoraggio, gestione del rischio e miglioramento continuo.

Il sistema comprende:

- un piano di business continuity dedicato alla sicurezza informatica e integrato nel più ampio sistema di business continuity del Gruppo, finalizzato a



salvaguardare l'operatività dei processi critici in caso di eventi che possano compromettere l'erogazione dei servizi. Il piano prevede procedure per prevenire potenziali minacce, limitarne e mitigarne gli impatti e ripristinare i processi;

- attività di rilevazione, analisi e gestione delle vulnerabilità informatiche, finalizzate a prevenire e ridurre gli incidenti di sicurezza;
- verifiche dell'infrastruttura IT volte a valutarne l'adeguatezza rispetto al quadro normativo interno, alle normative vigenti, agli standard adottati e ai requisiti di sicurezza implementati;
- audit di terza parte sul Sistema di Gestione della Sicurezza delle Informazioni;
- programmi di formazione rivolti a tutto il personale del Gruppo TIM, finalizzati ad accrescere la consapevolezza sulla sicurezza delle informazioni;
- un processo di escalation per la gestione delle segnalazioni relative a incidenti, vulnerabilità o attività sospette, raccolte dal personale del Gruppo e gestite dalle funzioni competenti.

Nel corso del 2025 il Gruppo ha ulteriormente rafforzato i processi di monitoraggio e reporting dei rischi aziendali, assicurando flussi informativi periodici verso il top management, il Comitato per il Controllo e i Rischi e il Consiglio di Amministrazione, anche con riferimento ai rischi cyber e alla resilienza delle infrastrutture digitali.

Le attività di cybersecurity comprendono inoltre il monitoraggio continuo degli eventi di sicurezza e la gestione tempestiva degli incidenti attraverso misure tecniche e organizzative preventive e correttive finalizzate a proteggere i dati personali e gli asset informativi e a contrastare minacce informatiche, vulnerabilità di processo e attacchi cyber, inclusi eventi di tipo DDoS.

A supporto di tali attività, il Gruppo mette a disposizione strumenti informativi e iniziative di sensibilizzazione rivolte ai dipendenti, finalizzate a promuovere comportamenti



consapevoli e coerenti con i requisiti di sicurezza delle informazioni.

L'efficacia delle misure adottate viene verificata attraverso specifici Key Performance Indicator (KPI) di natura sistemica e operativa, audit periodici e processi strutturati di Impact Analysis & Risk Assessment finalizzati a valutare gli impatti derivanti dalla perdita o compromissione di informazioni e sistemi e a individuare le priorità di intervento.