CYBERSECURITY

Approfondimento

Gruppo TIM

Giugno 2025

INDICE

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge

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.

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

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge

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. 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 presìdi interni di sicurezza.

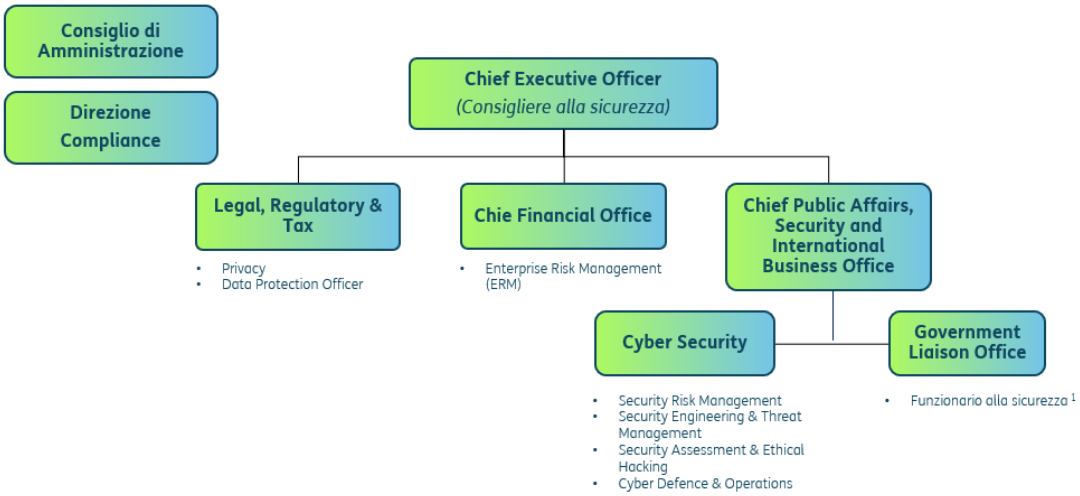
Nella governance in materia di Information Security e Cyber security il **CEO si avvale delle seguenti strutture**:

- Il **Chief Public Affairs & Security Officer** (**CPASO**) è responsabile della Sicurezza Fisica e Cyber per il Gruppo TIM. Attraverso le strutture organizzative della sua Direzione, che comprendono la Cyber Security e il Funzionario alla Sicurezza (FAS), garantisce il presidio delle tematiche di sicurezza, in coerenza con la normativa Golden Power e su delega del Consiglio di Amministrazione. Il CPASO è il referente unico per tutte le questioni di

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge

sicurezza, supervisiona le misure di prevenzione e contrasto dei rischi cyber, riporta direttamente all'Amministratore Delegato, riferisce al Comitato per il Controllo e i Rischi ed è il punto di contatto con gli Organi Istituzionali.

- la **struttura Cyber Security**, all'interno della Direzione Public Affairs & Security Office, articolata nelle funzioni di **Security Risk Management**, **Security Engineering & Threat Management**, **Security Assessment & Ethical Hacking e Cyber Defence & Operations**. Sempre nella stessa Direzione è collocata la funzione Government Liaison Office, a cui fa capo il **Funzionario alla Sicurezza**.
- la funzione Enterprise Risk Management (ERM), nella Direzione Chief Financial Office, ha un ruolo centrale nella valutazione e nel monitoraggio dei rischi aziendali, compresi quelli legati alla sicurezza informatica. In quest'ambito, ERM riceve periodicamente dalla funzione **Security Risk Management** i risultati delle analisi sul rischio cyber, che rappresentano un input fondamentale per il **modello di quantificazione del rischio** basato sulla metodologia **FAIR** (Factor Analysis of Information Risk). Si tratta di un approccio riconosciuto a livello internazionale che consente di stimare in termini economici l'impatto potenziale di minacce e vulnerabilità informatiche, traducendo il rischio in metriche comprensibili e comparabili. Il profilo di rischio aggiornato, elaborato da ERM a partire da questi input, non solo alimenta il sistema di controllo interno, ma si integra direttamente nel processo di pianificazione industriale.



(1) Il funzionario alla Sicurezza a cui fa capo la funzione è responsabile per le attività legate all'Organizzazione di Sicurezza ex DPCM 16 ottobre 2017 e alle normative Golden Power in piena autonomia, sia economica che gestionale, e riporta direttamente all'Amministratore Delegato

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge

All'interno del nostro modello di governance, la gestione della compliance ICT e della protezione dei dati personali è affidata a funzioni specializzate, che operano in modo coordinato all'interno del sistema di controllo aziendale, nel rispetto delle normative di riferimento e delle best practice internazionali.

In particolare, adottiamo il principio della segregazione dei ruoli, che distingue nettamente le attività operative, svolte dalle funzioni tecnologiche, che rispondono gerarchicamente al Chief Executive Officer da quelle di controllo, affidate alla **Direzione Compliance**. Quest'ultima opera con responsabilità centrale di indirizzo e di controllo verso il vertice e gli organi societari della conformità delle normative di riferimento e del monitoraggio delle procedure aziendali di attuazione. Il Piano annuale delle attività della Direzione Compliance è sottoposto all'approvazione del Consiglio di Amministrazione.

Accanto alla Direzione Compliance opera il **Data Protection Officer (DPO)**, figura indipendente prevista dal Regolamento UE 2016/679 (GDPR), responsabile della vigilanza sulla protezione dei dati personali trattati da TIM e dalle Società del Gruppo. Il DPO si relaziona direttamente con l'Autorità Garante per la protezione dei dati personali e supervisiona il rispetto della normativa in materia. La sua attività è supportata dal piano dei controlli privacy, eseguito dalla Direzione Compliance nell'ambito del proprio Piano annuale.

3. Il quadro normativo e istituzionale della cybersecurity

Oltre alla nostra struttura di governance dedicata alla cybersecurity, in quanto operatore strategico per il Paese, siamo soggetti a un quadro normativo nazionale ed europeo complesso, che riguarda sia la sicurezza delle infrastrutture critiche, sia la protezione dei dati e della privacy.

I **decreti Golden Power**, introdotti nel 2017, stabiliscono obblighi specifici per le imprese attive in settori strategici come le telecomunicazioni. In particolare, ci viene richiesto di:

- adottare misure di sicurezza e controllo dedicate;
- fornire report periodici all'Autorità di Governo sull'attuazione di tali misure.

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge

Con il **Decreto-legge 21/2022**, emanato in risposta alla crisi ucraina, sono stati rafforzati i poteri speciali della Presidenza del Consiglio e introdotte regole più stringenti per le reti 5G, considerate infrastrutture critiche per la sicurezza nazionale.

Il nostro impegno sul fronte della sicurezza è riconosciuto anche a livello istituzionale. L'attuazione delle misure previste dalla normativa è sottoposta alla verifica di un **Comitato di Monitoraggio istituito presso la Presidenza del Consiglio dei Ministri**, che ha il compito di controllare l'adempimento degli obblighi normativi e, se necessario, applicare sanzioni. Le attività di verifica svolte da questo Comitato hanno confermato in TIM l'adozione di elevati standard di sicurezza, realizzati grazie al coinvolgimento trasversale delle diverse Funzioni aziendali e al coordinamento garantito dalla Chief Public Affairs & Security Office, che presidia l'attuazione delle misure a tutela degli interessi nazionali.

A partire dal 2021, il quadro normativo si è ulteriormente rafforzato con l'attuazione della Legge 133/2019, che ha istituito il **Perimetro di Sicurezza Nazionale Cibernetica (PSNC).** Si tratta di un insieme di regole volto a garantire un elevato livello di protezione per gli operatori che gestiscono servizi ICT essenziali per la sicurezza nazionale, tra cui TIM, regolarmente iscritta al perimetro.

Infine, la **nuova Direttiva 2022/2555 (NIS2)**, che sostituisce l'attuale Direttiva 2016/1148 (NIS), è entrata in vigore il 16 gennaio 2023 ed è stata trasposta negli ordinamenti nazionali entro il 17 ottobre 2024 diventando applicabile dal 18 ottobre 2024.

La NIS2 prevede l'ampliamento dell'ambito di applicazione delle norme in materia di sicurezza delle reti e dei sistemi informativi, includendo da un lato settori attualmente coperti da altre normative, che vengono contestualmente abrogate (i.e. le misure di sicurezza delle reti e dei servizi di comunicazione elettronica, attualmente incluse nel Codice delle Comunicazione elettroniche europeo) ed estendendo dall'altro le norme a nuovi soggetti (e.g. Data center, CDN, ecc.).

La Direttiva mantiene l'obbligo di adottare misure di sicurezza commisurate al rischio, introducendo tuttavia una serie di requisiti minimi di base, inclusa la gestione della sicurezza

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge

della catena di approvvigionamento, e rivede le procedure di notifica obbligatoria degli incidenti informatici.

Le sanzioni in caso di inottemperanza possono arrivare fino al 2% del fatturato.
La Direttiva prevede, inoltre, il potenziamento degli organi e delle attività di supervisione a livello comunitario, con l'obiettivo di migliorare la collaborazione per contrastare la minaccia informatica globale, grazie alla condivisione delle esperienze tra gli stati membri.
In questo contesto è stata creata anche l'Agenzia per la Cybersecurity Nazionale (ACN), con il compito di vigilare, coordinare e rafforzare la resilienza dell'Italia rispetto all'evoluzione delle minacce cyber, sempre più complesse e pervasive.
La nostra collaborazione con le Istituzioni in materia di cybersecurity è costante e strutturata. Partecipiamo attivamente a numerosi gruppi di lavoro presso Organismi istituzionali, tra cui la Presidenza del Consiglio, il Ministero dell'Interno e il Ministero della Difesa, attraverso la presenza delle nostre funzioni specializzate in ambito cybersecurity.

4. La nostra policy sulla cybersecurity

La policy di sicurezza delle informazioni si applica a tutte le funzioni del Gruppo TIM e ha i seguenti obiettivi:

- definire gli obiettivi di sicurezza delle informazioni;
- esprimere il nostro impegno, attraverso il management, a soddisfare i requisiti di sicurezza secondo un processo di miglioramento continuo;
- indicare i requisiti di sicurezza delle informazioni che intendiamo adottare.

La policy si estende a tutti gli asset aziendali – processi e tecnologie – che trattano informazioni per nostro conto. Si applica inoltre a tutta la forza lavoro: ogni funzione, e quindi ogni persona che ne fa parte, è responsabile nel contribuire al raggiungimento degli obiettivi della policy attraverso l'attuazione di azioni specifiche.
Attraverso questa policy, ci impegniamo a:

- definire processi, ruoli e responsabilità per la sicurezza delle informazioni;

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge

- garantire un livello di riservatezza, integrità, protezione e disponibilità proporzionato al valore delle informazioni per il business e alle potenziali perdite dirette o indirette derivanti da incidenti di sicurezza sui servizi erogati ai nostri clienti;
- sensibilizzare e formare il personale sulla sicurezza delle informazioni;
- monitorare, analizzare e gestire ogni incidente, anche solo presunto, relativo alla sicurezza delle informazioni;
- definire i requisiti di sicurezza informatica per le controparti esterne, come i fornitori. Nei contratti e negli accordi con le terze parti, inseriamo requisiti e clausole per garantire la protezione delle informazioni e della proprietà intellettuale del Gruppo, la conformità alle normative vigenti, l'adeguatezza delle competenze del personale coinvolto, livelli di sicurezza coerenti con le nostre policy, strumenti di monitoraggio e controllo (inclusi piani di continuità e gestione degli incidenti), diritti di audit e livelli di servizio e penali allineati o più stringenti rispetto a quelli previsti per i nostri clienti;
- collaborare con enti e istituzioni per condividere metodologie e best practice utili al miglioramento continuo delle nostre policy e dei nostri sistemi di sicurezza delle informazioni, al fine di proteggere e creare valore per il Gruppo.

5. Il nostro sistema di gestione della cybersecurity

Per raggiungere gli obiettivi definiti nella nostra policy, abbiamo adottato un Sistema di Gestione della Sicurezza delle Informazioni che garantisce il governo dei processi e delle attività specifiche legate alla sicurezza del patrimonio informativo.

Questo sistema prevede:

- l'introduzione di un piano di business continuity legato alla sicurezza informatica, integrato nel più ampio sistema di gestione della business continuity adottato dal Gruppo, volto a salvaguardare l'operatività dei processi critici in caso di eventi che possano compromettere l'erogazione dei servizi. Il piano comprende un insieme di procedure per prevenire potenziali minacce, limitare e mitigare eventuali danni e ripristinare i processi;

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge

- la rilevazione, l'analisi e la gestione delle vulnerabilità informatiche per prevenire e ridurre gli incidenti di sicurezza;
- attività di verifica della nostra infrastruttura IT per valutarne il livello di adeguatezza rispetto al quadro normativo interno, alle normative vigenti, agli standard adottati e ai requisiti di sicurezza implementati;
- audit di terza parte sul nostro Sistema di Gestione della Sicurezza delle Informazioni; a questo proposito segnaliamo che abbiamo ottenuto la certificazione ISO 27001, con validità fino al 12/06/2026;
- la realizzazione di corsi di formazione, rivolti a tutto il personale del Gruppo TIM, per accrescere la consapevolezza sulla sicurezza delle informazioni;
- la definizione e l'attivazione di un processo di escalation per la gestione di segnalazioni relative a incidenti, vulnerabilità o attività sospette, raccolte dal personale del Gruppo e gestite dalla funzione IT e Crisis Management.

Nel corso del 2024, abbiamo registrato 16 eventi classificabili come incidenti o violazioni IT relativi a dati personali.

Tutti i diritti sono riservati a TIM S.p.A.
Ogni utilizzo non autorizzato potrà essere perseguito a termine di legge