

# Cybersecurity, priorità per le imprese italiane

Tra i principali investimenti attesi per il 2026, la sicurezza informatica è tra le priorità, insieme all'intelligenza artificiale

di Serena Fumagalli e Martina Mannino\*

**P**ochi dati sono sufficienti a mostrare quanto la sicurezza informatica sia oggi una priorità strategica per il Paese. Infatti, secondo il Rapporto Clusit 2025, nel primo semestre 2025 non è aumentato solo il numero degli incidenti cyber, ma anche la loro gravità media, confermando una tendenza ormai strutturale.

Già nel 2024, il 77% degli incidenti registrati aveva un impatto “critico” o “alto”, in forte crescita rispetto al 50% del 2020. Nei primi sei mesi del 2025 la situazione è ulteriormente peggiorata: a livello globale, l'82% degli attacchi ha avuto un impatto “grave” o “critico”.

Il processo di digitalizzazione che sta caratterizzando il sistema economico, con

una crescente pervasività di soluzioni ICT applicate in molteplici settori, dall'energia ai trasporti, dalla manifattura ai servizi, rende i processi più efficienti, ma allo stesso tempo anche più esposti agli attacchi informatici. Le organizzazioni si dovranno sempre più attrezzare per gestire eventuali attacchi, attraverso l'adozione di strategie diverse, tra cui ad esempio la separazione delle reti informatiche, l'aggiornamento continuo di tutti i dispositivi e software utilizzati, così come quello di programmi e sistemi. Sarà inoltre sempre più necessario progettare sistemi già pensati per resistere agli attacchi (resilienza “by design”), integrando la sicurezza fin dall'inizio e non solo come intervento successivo, con un ruolo crescente dell'intelligenza artificiale (IA).

Le statistiche Istat consentono di fare ul-

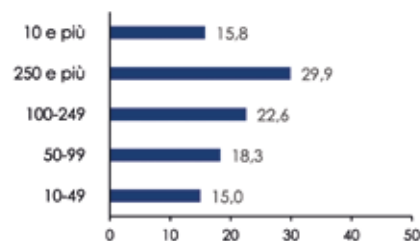
teriore luce sul fenomeno, distinguendo anche per dimensione aziendale ed evidenziando così significative differenze tra grandi e piccole imprese.

Nel 2024, il 15,8% delle imprese con almeno 10 addetti (considerando il totale delle attività economiche) ha avuto incidenti di sicurezza ICT con riflessi negativi sull'operatività delle stesse, come ad esempio l'indisponibilità dei servizi ICT, distruzione o danneggiamento dei dati o divulgazione di quelli riservati. Si tratta di una percentuale significativa, che sale addirittura al 22,6% tra le imprese con 100-249 addetti e al 29,9% tra quelle con almeno 250 addetti.

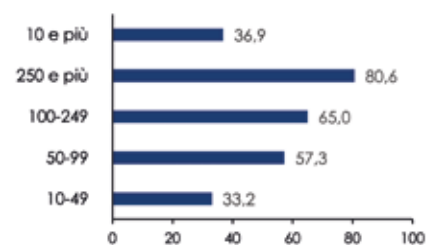
L'incidenza del fenomeno è quindi maggiore tra le imprese più grandi, anche perché è tra queste che gli investimenti in tecnologia sono più rilevanti. In queste realtà



**Tab. 1 - Imprese che in seguito a incidenti di sicurezza ICT hanno avuto indisponibilità dei servizi ICT, distruzione o danneggiamento dei dati, divulgazione di dati riservati, 2024 (%; per classi di addetti)**

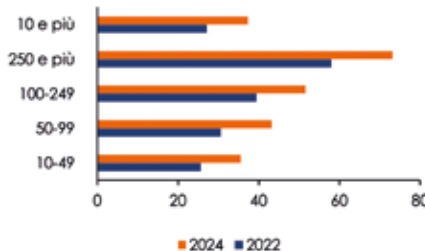


**Tab. 2 - Imprese con attività di valutazione del rischio ICT, 2024 (%; per classi di addetti)**

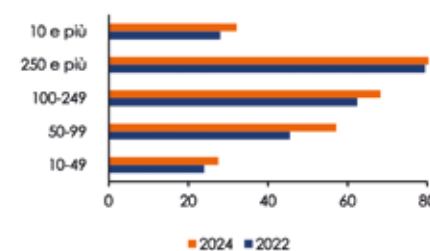


Fonte: elaborazioni Intesa Sanpaolo su dati Istat

**Tab. 3 - Imprese che utilizzano una combinazione di almeno due meccanismi di autenticazione, anni 2022 e 2024 (%; per classi di addetti)**



**Tab. 4 - Imprese che utilizzano almeno 7 misure di sicurezza ICT, anni 2022 e 2024 (%; per classi di addetti)**



è inoltre più rilevante il tema della valutazione del rischio ICT: oltre l'80% delle imprese indicano infatti che viene effettuata questa particolare attività, quasi il doppio rispetto al totale delle attività, che conferma come i soggetti più colpiti siano anche quelli più attenti alla valutazione dei rischi stessi.

La complessità dello scenario dei rischi informatici e la gravità delle conseguenze degli attacchi impongono una sempre maggiore sensibilizzazione sul tema anche all'interno delle imprese stesse.

Negli ultimi anni è aumentata la quota di aziende che rende i propri addetti consapevoli dei loro obblighi in materia di sicurezza ICT tramite formazione obbligatoria (dal 22 al 26% tra il 2022 e il 2024). Tra queste, è cresciuta la quota di imprese prevede tale formazione per contratto

*L'Intelligenza Artificiale si configura come un potente acceleratore, capace di potenziare tanto le strategie di attacco quanto quelle di difesa dalla pirateria informatica*

(dal 23,5% al 37,4%), rendendo la consapevolezza degli obblighi in materia di sicurezza informatica un dovere contrattuale specifico.

Le imprese stanno affrontando la sfida imposta dagli attacchi cyber con un mix articolato di strategie, che coinvolge sia le imprese più grandi, che stanno rafforzando ulteriormente i loro meccanismi di autenticazione e le loro politiche di contrasto a questi rischi, che quelle più piccole che stanno provando a colmare i ritardi che le caratterizzano.

Tra il 2022 e il 2024, la quota di imprese che utilizza una combinazione di almeno due meccanismi di autenticazione è passata dal 27,1% al 37,4%, con un aumento che ha riguardato sia le grandi aziende che le PMI. In particolare, per le imprese con più di 250 addetti si è passati dal



IA e cybersecurity sono tecnologie che sempre più risultano interconnesse e sinergiche. L'IA è ormai utilizzata sia in chiave offensiva sia difensiva. I cybercriminali la impiegano infatti per rendere più sofisticati phishing e malware e per automatizzare gli attacchi, mentre le imprese la sfruttano per migliorare il rilevamento delle minacce, velocizzare la risposta agli incidenti e ottimizzare le attività di sicurezza. L'IA si configura, quindi, come un potente acceleratore, capace di potenziare tanto le strategie di attacco quanto quelle di difesa. Gli investimenti in tecnologia saranno fondamentali in tutti i settori dell'economia, anche in quello del turismo dove i processi sono sempre più digitalizzati. Non è un caso che, nell'ambito dell'ampia strategia complessiva a sostegno del settore, la banca ha rinnovato



58% al 73,2%, mentre per le altre si è osservato in media un aumento di circa 12 punti percentuali, dal 32% al 44%. Anche la quota di imprese che utilizza almeno 7 misure di sicurezza ICT, quindi con un'attenzione importante al tema cybersecurity, ha mostrato un incremento, passando dal 28% al 32,2%. Le grandi imprese hanno raggiunto l'85%, ma sono soprattutto le imprese con 50-99 dipendenti a mostrare l'incremento più significativo, passando dal 47,5% al 57,1%. Anche le piccole comunque mostrano marginali progressi. La consapevolezza dell'importanza di aumentare la sicurezza informatica emerge anche dai risultati dell'indagine che Intesa Sanpaolo ha realizzato tra novembre e dicembre 2025, coinvolgendo un campione di colleghi Gestori imprese, che restituisce il sentiment del sistema produttivo su molteplici tematiche. È infatti emerso come tra i principali investimenti attesi per il 2026 la cybersecurity sia tra le priorità, insieme all'intelligenza artificiale.

nell'estate del 2024 il proprio impegno per il turismo con 10 miliardi di euro di nuovo credito, che si sono andati ad aggiungere ai circa 9 miliardi di liquidità erogati al comparto nel triennio precedente. Un plafond volto a incentivare nuovi investimenti in competitività tecnologica, efficientamento energetico e sostenibilità lungo tre assi: digitalizzazione del modello di servizio, riqualificazione e aumento degli standard qualitativi delle strutture, sostenibilità ambientale dell'offerta.

*\*Intesa Sanpaolo Research Department*

**INTESA  SANPAOLO**

L'accordo di collaborazione tra Federalberghi e Intesa Sanpaolo prevede soluzioni dedicate per accompagnare le imprese alberghiere nei loro programmi d'investimento.