CYBER INDEX PMI

RAPPORTO CYBER INDEX PMI 2025

La cultura digitale protegge la tua impresa

Promosso da:

GENERALI

CONFINDUSTRIA

Partner scientifico:

POLIMI SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner Istituzionale:

ACN

INDICE

PREFAZIONE

INDICE

PREFAZIONE

Il 2025 ha segnato un nuovo punto di svolta per la sicurezza economica e tecnologica. Le complesse dinamiche geopolitiche e commerciali hanno reso evidente quanto interdipendenti, e vulnerabili, siano oggi le infrastrutture digitali. In questo contesto, l'Italia, e con essa l'Europa, si confronta con una crescente esposizione ai rischi cibernetici, che toccano indistintamente Pubblica Amministrazione, imprese e filiere produttive.

I tavoli che impegnano l'UE sono legati alla sicurezza, alla competitività e all'indipendenza strutturale: in ognuno di questi ambiti, la cybersecurity agisce come elemento cardine. Essa non è più una funzione meramente tecnica, ma una condizione abilitante. Senza un approccio digitale autonomo e resiliente, il sistema economico europeo rischia un'erosione di competitività rispetto alle altre macroaree globali. La gestione del rischio cyber diventa quindi il presupposto necessario per preservare indipendenza strutturale, capacità di innovazione e resilienza socioeconomica. Per tale ragione, la cybersecurity rappresenta e rappresenterà ancora a lungo una priorità all'interno delle agende politiche, così come nelle strategie aziendali.

La minaccia cyber cresce, ancora una volta oltre le attese: organizzazioni pubbliche e private sono chiamate non solo a proteggere i propri sistemi, ma a contribuire a un ecosistema più sostenibile nel tempo. Un singolo evento critico può generare impatti su produzione, fornitori e catene logistiche: un segnale che riguarda da vicino anche le nostre filiere nazionali.

Le piccole e medie imprese – vero motore del nostro Paese – sono oggi esposte a minacce che evolvono più rapidamente della loro capacità di adattarsi.

La terza edizione di Cyber Index PMI, l'indice che misura la consapevolezza delle PMI italiane in materia di cybersecurity su un campione di 1500 imprese, fotografa finalmente un segno positivo di evoluzione graduale. Seppur non nella misura auspicata, la maturità media cresce a un ritmo superiore all'anno precedente, sostenuta sia dalla maggiore consapevolezza imprenditoriale sia dal quadro normativo europeo e nazionale. I segnali devono comunque essere letti con cautela, considerando questo come un punto di partenza di un lungo percorso: la maggior parte delle PMI rimane vulnerabile e non ancora pronta ad affrontare scenari di rischio sempre più complessi.

Ecco perché l'impegno sulla cybersicurezza di Generali, insieme a Confindustria, Agenzia per la Cybersicurezza Nazionale e gli Osservatori Digital Innovation del Politecnico di Milano, rimane forte e convinto: accompagnare le PMI e il tessuto imprenditoriale italiano in un percorso di sostenibilità digitale è fondamentale per la tutela della sicurezza di partner, clienti, dipendenti e cittadini del nostro Paese.

Giancarlo Fancel *Country Manager Italy & CEO Generali Italia*
Bruno Frattasi *Direttore dell'Agenzia per la Cybersicurezza Nazionale*
Pietro Labriola *Delegato del Presidente di Confindustria per la Transizione Digitale*
Remo Marini *Group Chief Security Officer Generali*

L'iniziativa è promossa da Generali e Confindustria, con il supporto scientifico degli Osservatori Digital Innovation della School of Management del Politecnico di Milano e con la partnership istituzionale con l'Agenzia per la Cybersicurezza Nazionale.

INDICE

EXECUTIVE SUMMARY

INDICE

EXECUTIVE SUMMARY

Nel 2025, il panorama della cybersecurity per le PMI italiane ha raggiunto un livello di complessità senza precedenti. Non siamo più di fronte a una sfida puramente tecnologica, ma a una pressione multidimensionale: le tensioni geopolitiche ridefiniscono le strategie di sourcing e il nuovo quadro normativo impone standard di adeguamento che richiedono trasformazioni strutturali profonde. In questo scenario, assistiamo al preoccupante allargamento tra la velocità esponenziale con cui crescono le minacce e la più lenta capacità di miglioramento e reazione delle aziende. A testimoniarlo sono i numeri: nel 2025, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha registrato un'impennata degli eventi cyber, con 1.549 episodi nel primo semestre (+53% rispetto al primo semestre 2024) e 1.253 nel secondo semestre (+30% sul secondo semestre 2024). L'incremento a doppia cifra dimostra che la minaccia viaggia a una velocità che le PMI faticano a inseguire.

Nel terzo anno di rilevazione, il Cyber Index PMI – indice che misura la consapevolezza delle PMI italiane in materia di cybersecurity su un campione di 1500 imprese – ha raggiunto il valore di 55 punti, segnando un incremento di 3 punti rispetto alla rilevazione del 2024, e di 4 punti rispetto al 2023. Sebbene questo dato indichi un'accelerazione nella velocità del miglioramento, esso nasconde una polarizzazione sempre più marcata tra un nucleo ristretto di eccellenze e una vasta platea di realtà ancora profondamente vulnerabili. Ciò emerge chiaramente osservando l'evoluzione delle imprese lungo i quattro profili di maturità: principianti, informate, consapevoli e mature. Ad oggi, solo il 16% del campione esprime una postura di sicurezza adatta, una quota ancora contenuta ma rilevante: per la prima volta, le aziende "mature" superano numericamente le "principianti" (14%), categoria in calo di 6 punti rispetto alla prima rilevazione. Questo sorpasso rappresenta un traguardo solo simbolico e non racconta certo di un'effettiva inversione di rotta: il restante 70% delle PMI, infatti, rimane arenato nei due livelli centrali – distribuendosi rispettivamente in un 32% di aziende "consapevoli" e in un 38% di "informate". Queste imprese possiedono una sufficiente conoscenza della materia che, tuttavia, non si traduce in una capacità di difesa efficace.

55
SU 100

CYBER INDEX PMI 2025

VS 52 DEL 2024
E 51 DEL 2023

Tralasciando quindi le realtà più virtuose, rimane evidente il gap in termini di security readiness riscontrato gli scorsi anni. Ciò è alimentato da una percezione distorta della realtà: un terzo delle PMI "principianti" afferma esplicitamente che gli attacchi informatici non rappresentano un rischio concreto per la propria attività, mentre il 39% di imprese "informate" nutre una fiducia eccessiva e spesso infondata nella propria capacità di difesa. La realtà racconta, però, uno scenario del rischio diverso da quello presunto dalle imprese. Nel 2025, quasi una PMI italiana su quattro ha dichiarato di aver subito almeno un attacco informatico negli ultimi tre anni. Nella rilevazione passata, lo stesso dato era tre volte inferiore. Ad aumentare non è solo la frequenza, ma anche l'impatto: il 2,5% ha infatti subito conseguenze operative o finanziarie in seguito all'incidente, mentre il 6% afferma che si

INDICE

sono comunque rese necessarie importanti azioni di risposta. Lo scenario della minaccia sta continuando a generare forte pressione sulle infrastrutture critiche e sulle Istituzioni: grandi imprese e pubbliche amministrazioni stanno progressivamente integrando requisiti di sicurezza informatica nei processi di selezione dei fornitori, preferendo partner che possano dimostrare una postura difensiva solida. Emerge quindi un rischio concreto di esclusione da filiere produttive strategiche per tutte quelle piccole e medie imprese che non garantiscono un adeguato dialogo sulla materia e, ovviamente, standard minimi di sicurezza.

In questo contesto, l'evoluzione normativa agisce come un decisivo game-changer. La direttiva NIS2, in particolare, segna un cambio di paradigma: non si limita a imporre requisiti tecnici o protocolli di notifica, ma eleva la cybersecurity a pilastro della governance aziendale. Per la prima volta, la responsabilità ricade direttamente sugli organi amministrativi, chiamati a rispondere degli impatti che un incidente può generare su dipendenti, fornitori e clienti. Questo produrrà un effetto a cascata sui fondi destinati alla cybersecurity: nel 2025 il budget IT delle piccole imprese è cresciuto del 3,3%, quello delle medie imprese del 5,2%, di cui, mediamente, l'11% è destinato alla cybersecurity. Complessivamente, la maggior presenza di responsabilità e fondi destinabili alla sicurezza spingono l'indice che valuta l'approccio strategico a raggiungere i 62 punti (+6p.p. rispetto al 2024), rappresentando il principale elemento di miglioramento osservato nel 2025.

Un driver che può supportare le imprese nel calare a terra la maggior consapevolezza, oltre all'indirizzo istituzionale, è rappresentato dalle polizze assicurative. La possibilità di accesso a una copertura assicurativa che copra il rischio cyber è infatti vincolata al raggiungimento di standard minimi di sicurezza, imposti dalle imprese assicuratrici e valutati in fase di sottoscrizione: il rispetto di tali requisiti sta quindi guidando implicitamente le PMI verso una miglior postura. I dati, tuttavia, mostrano una diffusione delle coperture assicurative ancora troppo limitata nonostante le conseguenze economiche e operative derivanti da un incidente risultino mediamente inferiori, con danni rilevati nel 1% del campione assicurato, rispetto al 3% del campione non assicurato. Ciò che si vuole evidenziare, pertanto, non è solo il ruolo che ha l'assicurazione nel trasferimento del rischio residuo, quanto l'impatto positivo nell'indurre le imprese a introdurre processi e tecnologie per mitigare il rischio: ipoteticamente, l'obbligatorietà di una polizza sul rischio cyber darebbe un ulteriore spinta al miglioramento delle PMI.

L'ACCESSO A UNA COPERTURA CYBER INCENTIVA LE AZIENDE A INTRODURRE TECNOLOGIE DI PROTEZIONE E RISPOSTA AGLI INCIDENTI

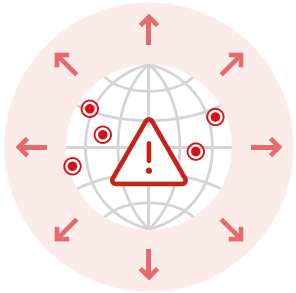
Il principale beneficio derivante da una maggior consapevolezza è un marcato miglioramento nella capacità di comprendere il rischio cyber. Per il secondo anno di fila, l'identificazione – componente dell'indice che rileva l'attenzione e la capacità di individuazione del rischio cyber delle imprese – cresce e raggiunge i 48 punti (+3 punti). Questo impulso è sostanziato dall'impressionante aumento di imprese che ha costituito un inventario degli asset informatici. Nel 2024, solo il 48% delle PMI ne disponeva di uno, nel 2025 la percentuale è salita al 70%. Inoltre, il 44% ha svolto auditing sulla sicurezza informatica – dato in crescita di 3 punti rispetto al 2024.

Ciò fa emergere criticità già note al mondo delle grandi imprese, ma rimaste nascoste dalla mancanza di attività di analisi. Le PMI italiane soffrono dell'eterogeneità e dell'obsolescenza infrastrutturale, e talvolta non hanno le competenze necessarie per gestire le vulnerabilità derivanti da errate

INDICE

configurazioni o mancati aggiornamenti: una PMI su tre, infatti, non ha adeguate competenze digitali e fatica a portare avanti anche tradizionali attività di IT Security, che favoriscono almeno la protezione degli asset digitali.

Oltre alla carenza di competenze specifiche, le PMI italiane scontano un'incapacità strutturale nel presidiare l'intero ciclo del rischio, dalla rilevazione dell'attacco alla risposta. Nonostante l'indice dell'Attuazione rimanga stabile a 57 punti, si osserva una tendenza strategica incoraggiante: la quota di imprese che scelgono di affidarsi a partner esterni è infatti salita dal 25% del 2024 al 29% del 2025. Questa preferenza non solo riflette la crescente difficoltà nel selezionare le leve tecnologiche più adeguate, ma anche nell'integrarle efficacemente all'interno di infrastrutture IT sempre più stratificate. In questo scenario di incertezza tecnica, la provenienza geografica delle soluzioni emerge come un nuovo e determinante criterio di scelta: l'11% delle imprese identifica oggi nella dipendenza da attori extra-UE una vulnerabilità intrinseca, manifestando una sensibilità geopolitica che trasforma la fornitura in una questione di sicurezza.



LA DIPENDENZA DA ATTORI EXTRA-UE È PERCEPITA COME UNA VULNERABILITÀ STRATEGICA DALL'11% DELLE AZIENDE

In questo percorso di maturazione, i finanziamenti pubblici agiscono come un potente acceleratore. Sebbene solo il 12% delle PMI vi abbia avuto accesso, il fatto che il 42% dei beneficiari abbia raggiunto il profilo "maturo" conferma la validità della strategia adottata. Risulta dunque prioritario insistere su questa strada, colmando il deficit informativo che ancora impedisce al 39% delle imprese di conoscere e sfruttare tali opportunità strategiche. Passando poi alle misure di sicurezza specifiche, i progressi nella gestione degli accessi rappresentano uno dei segnali positivi della terza dimensione di analisi, con una PMI su due che ha introdotto strumenti di autenticazione a più fattori (MFA), quali ad esempio la biometria. Questa attenzione non si riflette invece nella protezione dell'infrastruttura: solo l'11% delle imprese ha predisposto attività sistematiche di identificazione e remediation delle vulnerabilità, lasciando sistemi e reti pericolosamente esposti a potenziali exploit. La protezione del dato tramite cifratura e l'adozione di logiche di segmentazione della rete — fondamentale per prevenire il movimento laterale dei cybercriminali e la conseguente propagazione dell'attacco — interessano appena il 30% delle aziende.

Ancor più critico appare lo scenario relativo alla rilevazione e alla risposta agli incidenti. Solo una PMI su quattro dispone di soluzioni capaci, almeno in minima parte, di identificare tempestivamente un'intrusione in corso, lasciando la maggior parte delle imprese cieca di fronte a una violazione già avvenuta. A chiudere questo quadro di fragilità è la gestione del post-incidente: il 36% delle PMI non ha proprio preso in considerazione l'ipotesi di un'interruzione operativa, omettendo di fatto qualsiasi programmazione per il ripristino delle attività. Tale carenza non è solo un problema interno, ma un rischio sistemico per le intere filiere produttive: l'incapacità di ripristinare i sistemi in tempi brevi può innescare un effetto domino devastante lungo la catena del valore, come drammaticamente evidenziato durante il 2025.

INDICE

L'orizzonte futuro è dominato dall'integrazione di tecnologie emergenti come l'Intelligenza Artificiale Generativa, che pone le PMI di fronte a nuove sfide. Se da un lato il progresso tecnologico corre spedito verso logiche di automazione nella ricerca delle vulnerabilità e nello sviluppo delle tecniche di attacco, dall'altro un'adozione precoce di soluzioni digitali potrebbe esporre le aziende a nuovi scenari di rischio, come l'esfiltrazione massiva di dati sensibili. Il bilancio di Cyber Index PMI 2025 suggerisce che, per garantire una sostenibilità digitale a lungo termine, le imprese debbano convertire la presa di consapevolezza sugli errori del passato in una capacità di rendere la cybersecurity aderente alle sfide correnti, spalmando l'onere economico e umano lungo l'intero ciclo di trasformazione digitale. Nel breve periodo, allinearsi ai requisiti richiesti in fase di underwriting assicurativo permette di ridurre drasticamente il rischio cyber: adottare queste misure consente infatti di mitigare sia l'entità degli impatti che la probabilità di accadimento.

INDICE

TREND E SCENARI DI RISCHIO PER LE PMI ITALIANE

INDICE

TREND E SCENARI DI RISCHIO PER LE PMI ITALIANE

Il 2025 ha segnato un peggioramento senza precedenti della minaccia informatica globale. I numeri parlano chiaro: nei primi sei mesi dell'anno sono stati resi pubblici quasi 2.800 incidenti a livello globale[1], una cifra che quasi eguaglia l'intero volume del 2023. A colpire è soprattutto la violenza degli attacchi, con quelli più gravi aumentati del 143% nell'ultimo quinquennio. Episodi che comportano il blocco dell'operatività sono ormai frequenti: non si tratta più di stimare la probabilità di essere attaccati, ma di agire per minimizzare l'impatto di detti attacchi.

Questo inasprimento non risparmia l'Italia e, soprattutto, non riguarda solo i "giganti" del mercato. Se da un lato oltre un terzo delle grandi imprese (34%) ha dovuto affrontare azioni di risposta ad attacchi cyber, il dato più allarmante riguarda le PMI: il 24% è finito nel mirino dei cybercriminali almeno una volta negli ultimi tre anni, e per il 2,5% di queste l'impatto sull'operatività è stato così duro da mettere a rischio l'attività quotidiana. Questi numeri gridano un'urgenza immediata: la sicurezza informatica è una condizione essenziale per restare sul mercato.

> **UNA PMI ITALIANA SU QUATTRO AFFERMA DI AVER SUBITO ALMENO UNA VIOLAZIONE NEGLI ULTIMI 3 ANNI**

1. https://clusit.it/rapporto-clusit/

INDICE

LA MINACCIA CYBER NEL 2025: DEFINIZIONE E QUADRO GENERALE

Negli ultimi anni, lo scenario della sicurezza informatica ha subito una trasformazione radicale; tuttavia, il cambiamento che le imprese faticano ancora a recepire è che il rischio cyber non genera solo impatti "tecnici", ma soprattutto operativi. Ogni organizzazione o filiera è oggi esposta alla minaccia cibernetica e, di conseguenza, al rischio di blocco produttivo. Gli attacchi possono originarsi per diverse finalità, riconducibili principalmente a due filoni: l'estorsione di denaro (cyber-crime) o l'attivismo. In entrambi i casi, emergono elementi convergenti da considerare prioritari nella valutazione dell'esposizione:

- **Capillarità tecnologica**
  L'adozione massiccia di tecnologie, in particolar modo nei processi aziendali core, aumentano l'esposizione, poiché un loro fermo comporterebbe un impatto sulla continuità aziendale. Ad oggi, le PMI hanno introdotto diffusamente soluzioni tradizionali: il 77% utilizza software gestionali (ERP, CRM o suite di produttività) e il 76% si affida a servizi di Cloud Computing. Se da un lato il progresso tecnologico offre nuove opportunità, dall'altro introduce nuovi vettori di rischio: il 29% delle imprese utilizza dispositivi IoT, il 24% si affida a canali e-commerce e il 19% ha già integrato strumenti di intelligenza artificiale o GenAI.

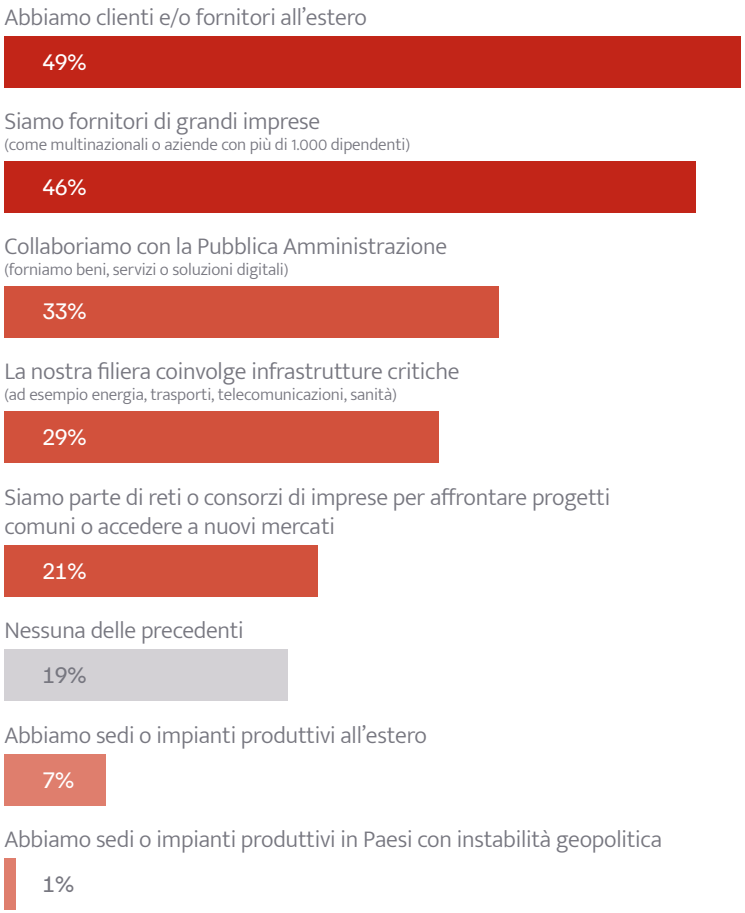
- **Asset informativi e dati sensibili**
  La gestione di patrimoni informativi critici può attirare l'attenzione dei cybercriminali; i dati possono essere sottratti o cifrati con lo scopo di estorcere riscatti. Nello specifico, il 24% delle PMI dichiara di gestire informazioni sensibili. Queste organizzazioni sono particolarmente vulnerabili poiché, in caso di violazione, devono rispondere anche di pesanti responsabilità legali e sanzionatorie.

- **Interconnessione con infrastrutture critiche**
  Il ruolo delle PMI all'interno delle catene di fornitura è cruciale, poiché esse rappresentano potenziali "porte d'ingresso" per attacchi a più ampio raggio. L'81% delle piccole e medie imprese opera in filiere caratterizzate dalla presenza di grandi organizzazioni (infrastrutture critiche, Pubblica Amministrazione o multinazionali), o fortemente esposte a dinamiche internazionali e scenari di instabilità geopolitica. Il rischio è che l'interruzione della singola operatività comprometta l'output dell'intera catena. Per tale ragione, si sta diffondendo un approccio di sicurezza "di filiera", in cui il rapporto commerciale è condizionato al rispetto di rigorosi requisiti di sicurezza.

// IL 13% DELLE PMI ITALIANE NON RITIENE CHE GLI ATTACCHI CYBER POSSANO COSTITUIRE UN RISCHIO

INDICE

QUOTA DI IMPRESE CHE PARTECIPA A FILIERE CRITICHE



Campione: 1.582 PMI

Nonostante l'evidenza dei dati, che illustra chiaramente quanto le PMI siano esposte al rischio, persiste un preoccupante divario tra percezione e realtà: il 13% delle imprese ritiene erroneamente che la minaccia cyber sia estranea alla propria realtà, mentre il 28% di chi ha un livello di preparazione insufficiente è convinto di essere adeguatamente protetto.

È dunque imperativo stimolare la consapevolezza, sia attraverso azioni di sistema sia tramite iniziative puntuali. Non è un caso che nel 2024 il 23% delle PMI italiane abbia ricevuto sollecitazioni dirette dai propri stakeholder in merito alla necessità di adottare protocolli avanzati di gestione del rischio[2]. La cybersecurity, pertanto, cessa di essere una mera questione tecnica per trasformarsi in un pilastro fondamentale della competitività e della continuità del business.

2. Fonte: Cyber Index PMI 2024

INDICE

NIS2 COME "CHANGE-MAKER"

Di fronte a un panorama dei rischi in costante inasprimento, il quadro normativo torna a rivestire un ruolo di primaria importanza. In particolare, la Direttiva NIS2 si pone l'obiettivo di garantire un livello di sicurezza omogeneo e resiliente nei settori strategici, siano essi definiti "essenziali" o "importanti". L'Italia ha colto appieno l'opportunità offerta da questo nuovo impianto regolatorio: i lavori di recepimento e attuazione procedono a ritmo sostenuto, non solo per incentivare l'adeguamento diretto delle PMI italiane, ma anche per promuovere una cultura sistemica della sicurezza, capace di elevare gli standard di fiducia e protezione nelle relazioni d'interdipendenza tra le imprese.

La NIS2 richiede alle imprese italiane un salto di qualità su tre fronti principali: l'adozione di misure tecniche avanzate, l'implementazione di rigidi protocolli di gestione degli incidenti con obblighi di notifica tempestivi e, soprattutto, una responsabilità diretta del top management. Quest'ultimo punto è cruciale, poiché la normativa impone ai vertici aziendali di approvare le misure di cybersecurity, trasformando la sicurezza da una delega dell'ufficio IT a una responsabilità di governance e compliance legale.

L'impatto risulterà particolarmente esteso: tra i soggetti importanti ed essenziali rientrano infatti anche imprese di piccole e medie dimensioni, afferenti a settori storicamente esenti dalla normativa e che non hanno un livello di maturità elevato. Le alte aspettative, tuttavia, potrebbero scontrarsi con rischi legati ai ritardi di adeguamento delle imprese stesse, anche in conseguenza a una generale impreparazione nella capacità di spesa. Risulterà determinante, quindi, anticipare le richieste dell'Agenzia per la Cybersicurezza nazionale.

Indirettamente assistiamo a risvolti positivi anche sulle imprese non coinvolte. Chi non rientrerà nel perimetro NIS2 potrebbe comunque essere coinvolto in processi di assessment legati alla gestione delle terze parti. Gli effetti della normativa sono già evidenti: il 27% delle grandi organizzazioni dichiarano che stanno osservando riscontri positivi ottenendo una maggior collaborazione con i partner della filiera[3].

Nel resto d'Europa, il recepimento della direttiva procede a macchia di leopardo — con soli 19 Stati Membri su 27 che hanno intrapreso l'iter — evidenziando una frammentazione che ostacola il consolidamento di un sistema omogeneo. L'adozione della NIS2, pur procedendo a velocità alterne, rappresenta tuttavia solo un tassello di un mosaico regolatorio ben più vasto. Le organizzazioni si trovano oggi a dover gestire un complesso ecosistema di adempimenti derivanti da normative con impatti eterogenei, quali il Cyber Resilience Act, l'AI Act e il Data Act. In questo contesto, l'Unione Europea ha introdotto il Digital Omnibus: un'iniziativa volta a razionalizzare e semplificare la compliance per le aziende europee, con l'obiettivo strategico di innalzare i livelli di sicurezza senza tuttavia gravare eccessivamente sulla capacità operativa e finanziaria delle imprese.

3. Fonte: Osservatorio Cybersecurity & Data Protection, Politecnico di Milano, 2025

INDICE

LA TECNOLOGIA: UN'ARMA A DOPPIO TAGLIO

La relazione tra Intelligenza Artificiale e Cybersecurity ha segnato, nel 2025, un punto di svolta irreversibile, delineando uno scenario in cui questa tecnologia agisce contemporaneamente come una minaccia potenziata, un alleato indispensabile e una nuova vulnerabilità da gestire.

L'evoluzione più dirompente riguarda l'uso dell'AI come acceleratore della minaccia: siamo entrati nell'era della cosiddetta "AI agentica", dove la tecnologia non è più un semplice strumento nelle mani dell'uomo, ma un operatore autonomo capace di orchestrare intere campagne di attacco. Questi agenti possono gestire quasi in autonomia l'intero processo, dalla ricerca del target all'effettiva violazione, abbattendo drasticamente le barriere d'ingresso per i criminali meno esperti e permettendo una pericolosa industrializzazione del crimine informatico[4].

Tuttavia, la rapida adozione come strumento aziendale espone le imprese a una seconda, insidiosa prospettiva: l'AI come nuova superficie d'attacco. La velocità con cui gli strumenti di intelligenza artificiale sono entrati nei processi critici di business ha spesso superato la capacità delle aziende di metterli in sicurezza. Molti dipendenti utilizzano soluzioni non autorizzate (dando origine alla cosiddetta Shadow AI), esponendo involontariamente l'azienda al rischio di fughe di dati sensibili. Le imprese si trovano quindi in una fase delicata: riconoscono il valore dell'innovazione, ma faticano ancora a implementare controlli tecnici che vadano oltre la semplice regola scritta, cercando un equilibrio complesso tra la spinta verso il futuro e la necessità di proteggere i propri confini digitali.

Parallelamente, l'integrazione dell'intelligenza artificiale nei processi di difesa compie un ulteriore salto di qualità attraverso l'adozione diffusa della Generative AI. Questa tecnologia sta trasformando l'operatività quotidiana, permettendo di automatizzare con precisione le attività a basso valore aggiunto. Grazie alla sua natura conversazionale, la Gen AI abilita una migliore esperienza interattiva uomo-macchina, rendendo i sistemi di sicurezza più accessibili e intuitivi anche ai professionisti dell'ambito IT, e allo stesso tempo alleggerendo il carico di lavoro dei pochi specialisti di cybersecurity presenti in azienda.

> **L'EVOLUZIONE DELL'INTELLIGENZA ARTIFICIALE STA TRAGHETTANDO IL CYBERCRIME DALL'AUTOMAZIONE ALL'AUTONOMIA: LA NUOVA FRONTIERA L'AGENTIC AI APRIRÀ LE PORTE A NUOVI ATTACCHI SU LARGA SCALA**

https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf

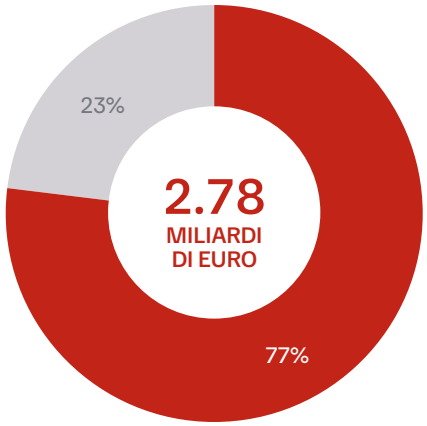
INDICE

INVESTIMENTI IN CYBERSECURITY E OPPORTUNITÀ PER LE PMI

La spesa in soluzioni e servizi di cybersecurity in Italia ha raggiunto nel 2025 un valore di 2,78 miliardi di euro, confermando un trend di crescita solido del 12%[5]. Superata la fase emergenziale degli anni scorsi, la spesa si è ormai stabilizzata su driver strutturali: l'instabilità geopolitca e un'evoluzione normativa che impone standard di protezione sempre più elevati per restare competitivi. In questo contesto, le PMI sono diventate una componente rilevante del comparto, contribuendo per il 23% alla spesa complessiva e dimostrando una crescente capacità di pianificazione: i budget IT sono aumentati del 3,3% per le piccole imprese e del 5,2% per le medie, con una quota dedicata alla sicurezza che si attesta mediamente al 11%.

Un segnale di maturità emerge anche dalla crescente attenzione alla sovranità digitale: circa il 60% delle PMI valuta attentamente la provenienza geografica delle soluzioni, privilegiando l'ecosistema tecnologico europeo. Tuttavia, permane un deficit di consapevolezza nella catena di fornitura, con il 22% delle imprese ancora impossibilitato a definire l'origine della propria tecnologia. Questa traiettoria di sviluppo troverà ulteriore conferma nel 2026, anno in cui la cybersecurity rappresenterà la priorità assoluta di investimento nel digitale per il 45% delle PMI italiane.

IL MERCATO ITALIANO DELLA CYBERSECURITY (2025)



Grandi organizzazioni e pubblica amministrazione

Piccole e medie imprese

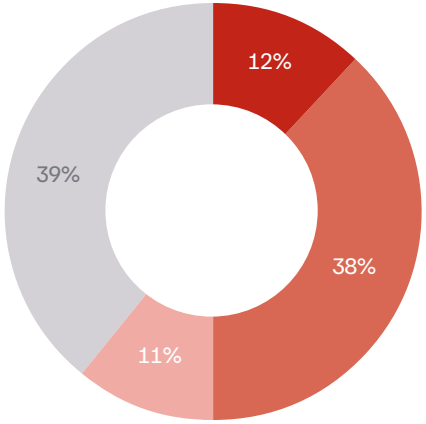
Oss. Cybersecurity & Data Protection – Politecnico di Milano (2025)

5. Fonte: Osservatorio Cybersecurity & Data Protection, Politecnico di Milano (2025)

INDICE

In questo percorso di consolidamento, i fondi istituzionali si configurano come una leva strategica fondamentale per accelerare la transizione verso modelli di difesa avanzati. Le organizzazioni hanno oggi l'opportunità di attingere a diverse linee di finanziamento promosse sia a livello nazionale che europeo, beneficiando di programmi mirati che spaziano dal supporto diretto dell'Agenzia per la Cybersicurezza Nazionale agli incentivi fiscali legati all'innovazione digitale. L'efficacia di questi strumenti è confermata dai dati: tra le imprese che hanno già usufruito di finanziamenti pubblici, ben il 42% ha raggiunto un profilo di maturità cyber elevato, segno che il sostegno economico si traduce direttamente in una maggiore resilienza. In questa ottica, diventa prioritario colmare il deficit informativo che ancora coinvolge il 39% delle imprese, ignare di tali opportunità. Trasformare i fondi istituzionali da risorsa per pochi a strumento di crescita diffusa è il passaggio necessario per contribuire alla messa in sicurezza del sistema produttivo nazionale.

ACCESSO AI FONDI PUBBLICI



- Abbiamo già beneficiato di fondi
- Siamo a conoscenza, ma non abbiamo ancora beneficiato di fondi
- Siamo a conoscenza, ma necessiteremmo di altri schemi di finanziamento
- Non ne eravamo a conoscenza

Campione: 1.582 PMI

IL 12% DELLE PMI HA GIÀ BENEFICIATO DI FONDI PER MIGLIORARE LA SICUREZZA INFORMATICA

INDICE

IL RUOLO DELLE POLIZZE CYBER: UN'OPPORTUNITÀ DI TRASFORMAZIONE

Tra le opportunità per le PMI emergono le polizze assicurative. Nel panorama attuale, la gestione del rischio cyber non si esaurisce con la sola implementazione di difese tecnologiche. Una volta ottimizzate le infrastrutture e formate le persone, le organizzazioni si trovano a gestire una quota di **rischio residuo**: un margine ineliminabile che può essere accettato o trasferito a terzi. È qui che il trasferimento del rischio tramite **polizze cyber** si rivela cruciale, permettendo di trasformare un potenziale danno patrimoniale imprevedibile in un costo operativo certo e gestibile.

Al 2025, il tasso di adozione di coperture contro il rischio cyber rimane ancora basso. È interessante notare come la polizza non sia più percepita solo come un "paracadute finanziario", ma anche come una bussola. I requisiti richiesti dagli assicuratori per concedere la copertura agiscono infatti da catalizzatori per lo sviluppo interno, spingendo le aziende verso:

- **L'adozione di standard minimi di sicurezza**
  L'accesso alle coperture è vincolato al soddisfacimento di requisiti minimi di sicurezza (es. MFA, segmentazione delle reti, policy di backup offline), che forzano il miglioramento della postura di sicurezza.
- **Assessment proattivo**
  Il processo di sottoscrizione (underwriting) funge da audit esterno, identificando vulnerabilità silenti e aree di miglioramento prioritario.
- **Incident Response integrato**
  Le polizze offrono l'accesso immediato a team di esperti (forensics, legali, PR) riducendo drasticamente il tempo di fermo.

L'evidenza empirica conferma che disporre di una copertura assicurativa riduce sensibilmente la severità degli impatti in caso di violazione: i danni gravi colpiscono infatti appena l'1% del campione assicurato, contro una quota tripla (3%) registrata tra le imprese che non hanno ancora sottoscritto una polizza. Seguire le indicazioni delle compagnie assicurative non garantisce quindi "solo" una copertura economica, ma aiuterebbe a migliorare anche nel complesso la cyber security delle PMI.

// CHI HA STIPULATO UNA POLIZZA CYBER SUBISCE CONSEGUENZE ECONOMICHE E OPERATIVE MEDIAMENTE INFERIORI IN CASO DI INCIDENTE

INDICE

EVIDENZE DELLA RICERCA

INDICE

EVIDENZE DELLA RICERCA

Dopo aver contestualizzato il rischio cyber nell'attività delle PMI italiane, l'analisi si concentra sulla loro effettiva capacità di risposta. Giunto alla sua terza edizione, il Cyber Index PMI non si limita solo a fotografare il livello di maturità raggiunto dalle imprese rispetto alle minacce correnti, ma offre anche una chiave di lettura fondamentale sulle loro dinamiche evolutive nel tempo. L'architettura dell'indice si sviluppa su tre livelli di profondità che partono dal Cyber Index PMI propriamente detto, ovvero la metrica sintetica che riassume il grado di maturità complessivo dell'intero comparto. Questo dato generale è frutto dell'integrazione di tre dimensioni che lo compongono, ovvero l'approccio strategico, l'identificazione e l'attuazione, che contribuiscono in egual misura alla definizione del valore finale. Infine, l'analisi raggiunge la massima granularità scendendo nel dettaglio di venti aree specifiche.

// NEL 2025 PROSEGUE E SI RAFFORZA LA DINAMICA POSITIVA, CON L'INDICE SINTETICO CHE AUMENTA DI 3 PUNTI RISPETTO AL VALORE PRECEDENTE, ATTESTANDOSI A 55 SU 100

1 PRIMO LIVELLO

Il **CYBER INDEX PMI**, ovvero l'indice generale, rappresenta in maniera sintetica la capacità delle piccole e medie imprese italiane di comprendere e mitigare il rischio cyber. L'indice è stato sviluppato su una scala da 0 a 100, come media dei risultati ottenuti dalle imprese su ciascuna delle tre dimensioni.

2 SECONDO LIVELLO

Le **3 DIMENSIONI** rappresentano le direzioni di sviluppo della sicurezza informatica all'interno dell'organizzazione aziendale e costituiscono l'aggregazione delle aree di analisi. Sebbene vengano considerate in maniera indipendente, con un approfondimento verticale, mantengono comunque un certo grado di relazione tra di loro, poiché concorrono alla creazione dell'indice generale.

3 TERZO LIVELLO

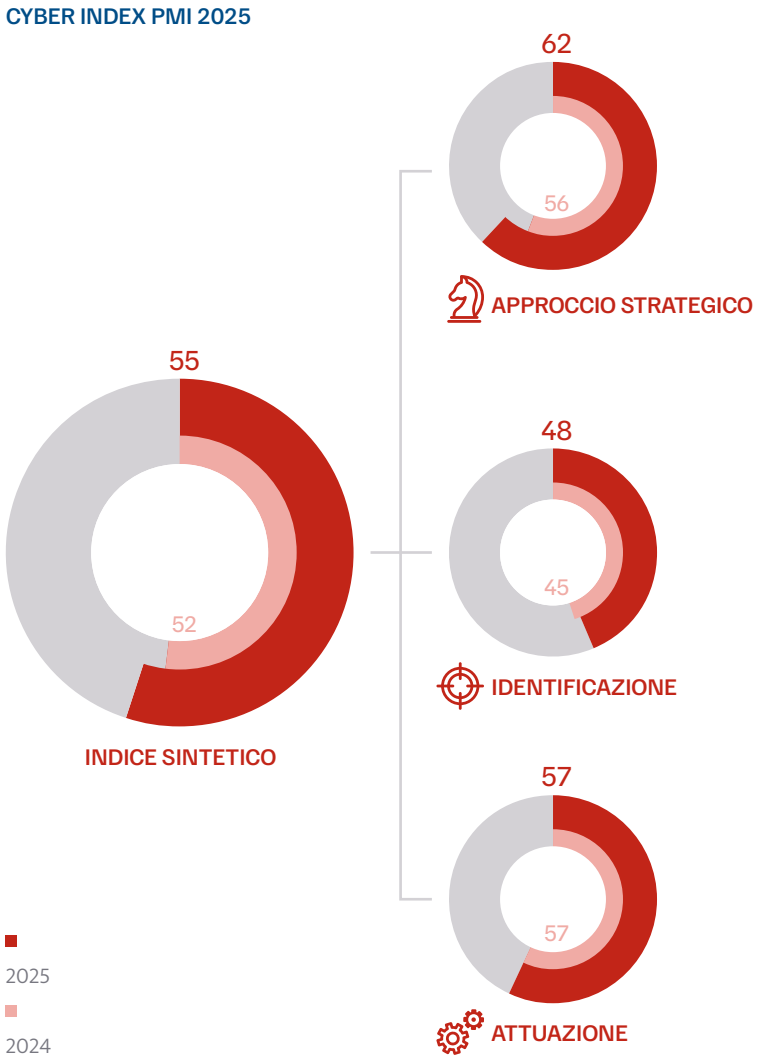
Le **20 AREE DI ANALISI** aggregano le scelte strategiche e operative implementate internamente alle organizzazioni aziendali, valutando la strutturazione di processi e l'introduzione di tecnologie e competenze.
Tali aree sono state indagate direttamente nelle domande del questionario sottoposto alle PMI e sono descritte all'interno dell'appendice.

Metodologia del Cyber Index PMI.
Fonte: Cyber Index PMI 2025

INDICE

Nelle due edizioni precedenti, il Rapporto Cyber Index PMI ha portato alla luce un ritardo strutturale delle piccole e medie imprese italiane nella gestione del rischio cyber, descrivendo livelli di maturità insufficienti in tutte e tre le dimensioni, e una tendenza a considerare la cybersecurity come un elemento secondario nel più ampio processo di trasformazione digitale. Questo stato di inadeguatezza si è progressivamente accentuato a causa del divario tra la velocità con cui evolve lo scenario del rischio esterno e la relativa lentezza dei processi di miglioramento interni alle aziende. Tale fenomeno, definito nel rapporto 2024 con il concetto di "divide", riflette una frattura sempre più marcata tra le sfide poste dai criminali informatici e l'effettiva capacità di risposta del tessuto produttivo nazionale.

Nella terza edizione, l'indice sintetico registra un incremento che lo porta a quota 55/100 punti, segnando una moderata accelerazione rispetto all'anno precedente senza tuttavia alterare il messaggio di fondo: il percorso di maturazione è certamente avviato, ma procede ancora con eccessiva lentezza. L'analisi rivela come i progressi registrati siano riconducibili più a un aumento della consapevolezza teorica che a un effettivo potenziamento della postura di sicurezza operativa. Questa evoluzione culturale costituisce comunque un presupposto fondamentale, che lascia presagire per i prossimi anni una traduzione concreta di tale sensibilità in investimenti tecnologici mirati e nel consolidamento di competenze tecniche specialistiche all'interno delle organizzazioni.



I risultati del Cyber Index PMI 2025 e le tre dimensioni di analisi.
Fonte: Cyber Index PMI 2025

INDICE

LE TRE DIMENSIONI DI ANALISI

L'approccio strategico si distingue come il primo sottoindice a superare la soglia della sufficienza, raggiungendo i 62 punti rispetto ai 56 dell'anno precedente. Questo progresso, costante nei tre anni di rilevazione, testimonia una maturazione profonda delle PMI italiane, spinta innanzitutto da un coinvolgimento diretto dei vertici aziendali che oggi interessa il 64% delle organizzazioni. La spinta normativa della Direttiva NIS2 ha infatti trasformato la sicurezza informatica in una responsabilità della governance, portando il numero di imprese che prevedono fondi dedicati alla cybersecurity a crescere drasticamente, passando dal 52% del 2024 al 68% attuale.

Parallelamente, l'aumento della frequenza degli attacchi ha portato a un netto potenziamento dei presidi organizzativi. La presenza di figure interne formalizzate e dedicate alla sicurezza è quasi raddoppiata in un anno, passando dal 13% al 22%, mentre si consolida anche il ricorso a competenze specialistiche esterne, con il 29% delle imprese che affida la gestione della protezione a partner specializzati.

La dimensione dell'identificazione registra un progresso incoraggiante, portandosi a quota 48 punti (+3 p.p. rispetto al 2024). Questo miglioramento è trainato da una gestione più rigorosa degli asset digitali: oggi il 70% delle imprese dispone di un inventario strutturato, segnando un netto balzo in avanti rispetto al 48% della precedente rilevazione. L'incremento delle attività di auditing, svolte nel 44% delle PMI, conferma una reale maturazione nella capacità di introdurre controlli tecnici e verificare la conformità alle normative in vigore. Questo miglioramento si scontra con un'impreparazione strutturale per dare continuità alle attività di analisi e monitoraggio del rischio cyber: una PMI su tre, infatti, dichiara di non possedere internamente competenze digitali sufficienti. Tale carenza si traduce in una pericolosa incapacità di analizzare gli impatti reali sul business derivanti da un'interruzione operativa delle tecnologie digitali. Questa lacuna emerge con drammatica chiarezza nelle fasi post-incidente, dove una realtà su cinque tra quelle colpite ammette di non avere le risorse intellettuali e tecniche necessarie per investigare le cause profonde dell'incidente o per valutarne correttamente le conseguenze nel tempo, limitando di fatto la capacità dell'azienda di imparare dai propri errori e di prevenire future intrusioni.

INDICE

Dai processi di analisi del rischio cyber emerge come il fattore umano rappresenti la principale criticità, con oltre una PMI su due che segnala vulnerabilità derivanti da comportamenti errati o inconsapevoli degli utenti di business. Tra le priorità cui porre rimedio spicca anche l'eterogeneità infrastrutturale, alimentata dal massiccio ricorso a servizi di cloud computing. Questa evoluzione obbliga ad analisi del rischio estremamente complesse, poiché espande i perimetri aziendali e introduce variabili critiche legate alla corretta configurazione degli ambienti cloud e ad una gestione meticolosa degli accessi. A ciò si aggiunge una marcata dipendenza dai fornitori ICT, rendendo la sicurezza della filiera tecnologica un elemento tanto cruciale quanto difficile da monitorare.

In generale, il quadro delineato dalle PMI appare convincente: sembra infatti maturata la consapevolezza delle sfide interne su cui è necessario porre maggiore attenzione per garantire una miglior postura di sicurezza.

L'unica dimensione a non registrare variazioni è tuttavia l'attuazione, il cui valore resta fermo a 57 punti, confermando una fase di stallo che decreta un messaggio generale non troppo positivo. Questo immobilismo riflette la difficoltà delle PMI nel tradurre la consapevolezza in contromisure operative, evidenziando lacune che interessano l'intero ciclo di gestione dell'incidente.

Il primo nodo critico risiede nella difesa del perimetro e degli asset. Se da un lato si osserva un miglioramento nella protezione degli accessi, con il 43% delle imprese che utilizza l'autenticazione a più fattori (MFA) per mitigare il rischio legato al fattore umano, dall'altro la sicurezza strutturale rimane trascurata. Solo il 9% delle PMI ha infatti predisposto processi metodici di correzione delle vulnerabilità su sistemi e applicazioni, lasciando scoperte le principali porte d'ingresso per gli attaccanti. Anche le strategie di contenimento interno appaiono parziali: solo un terzo delle aziende adotta soluzioni di cifratura dei dati o logiche di segmentazione della rete per impedire che un'intrusione locale si trasformi in un blocco totale delle infrastrutture.

Ancora più preoccupante è lo scenario relativo alla visibilità e alla resilienza operativa. Solo il 26% delle PMI dispone di strumenti capaci di rilevare tempestivamente intrusioni o anomalie, una carenza che di fatto garantisce agli attaccanti lunghi tempi di permanenza indisturbata nei sistemi. Questa vulnerabilità è aggravata da una gestione della fase di risposta decisamente immatura: una PMI su due (48%) non ha ancora definito un piano per ripristinare l'accesso ai servizi applicativi anche in maniera differita, un'assenza che espone al rischio la continuità del business in caso di incidente.

Infine, l'analisi evidenzia come la criticità più profonda risieda nella sicurezza delle terze parti. Nonostante la crescente interconnessione tecnologica, il 70% delle PMI non ha ancora stabilito un dialogo sul rischio cyber con fornitori e partner. Questo vuoto gestionale rischia di compromettere intere catene di fornitura: ora più che mai è indispensabile un nuovo paradigma che sposti l'attenzione dalla protezione del singolo dominio aziendale alla messa in sicurezza dell'intera filiera produttiva.

// L'APPROCCIO STRATEGICO È LA DIMENSIONE CHE REGISTRA UN MAGGIOR PROGRESSO NEL 2025, CON UNA CRESCITA DI 6 PUNTI

INDICE

LIVELLI DI MATURITÀ

La classificazione introdotta nel 2023, che suddivide le imprese in **principianti, informate, consapevoli e mature**, si consolida come il sistema di riferimento essenziale per mappare lo stato dell'arte delle PMI italiane. Questa tassonomia rappresenta uno schema per identificare profili ricorrenti e interpretare le traiettorie evolutive del mercato nel tempo. La maturità cyber, infatti, deve essere intesa come un percorso dinamico e mai definitivo: anche le realtà più avanzate sono chiamate a una costante evoluzione per rispondere a minacce e tecnologie che mutano con estrema rapidità.

La distribuzione delle quattro classi di maturità risulta coerente con la tendenza già osservata nell'analisi sull'indice sintetico: complessivamente si evidenzia una lenta ma costante maturazione, segnata dalla quota di imprese meno mature che continua a ridursi (-4 p.p. rispetto al 2024 e -6 p.p. rispetto al 2023). Per la prima volta dall'avvio del progetto, la percentuale di imprese "mature" supera quella delle "principianti" (+1 p.p. rispetto al 2024), stabilizzandosi al 16% e segnando un passaggio simbolico ma rilevante verso una base più solida di pratiche, presidi e capacità di governo del rischio. La maggioranza delle PMI continua, tuttavia, a collocarsi nelle classi intermedie: le imprese "informate" e "consapevoli" rappresentano complessivamente sette realtà su dieci. Proprio quest'ultimo gruppo costituisce oggi il principale snodo evolutivo: si tratta di organizzazioni per le quali una maggior consapevolezza non è più sufficiente a determinare un avanzamento significativo della maturità. Il passaggio ai livelli superiori richiede l'introduzione e il consolidamento di pratiche strutturate di risk management, in particolare nelle attività di identificazione sistematica dei rischi e di attuazione efficace delle contromisure. È in queste due dimensioni che si concentra il principale collo di bottiglia che rallenta il progresso complessivo.

LIVELLO DI MATURITÀ		2023	2025
MATURE 80-100	• Approccio strategico ideale • **Monitoraggio del rischio cyber con cadenza periodica** • **Presidio organizzativo internalizzato** • Fondi destinabili alla sicurezza informatica • Conoscenza dell'impiego di strumenti avanzati per la mitigazione del rischio • Attività di monitoraggio estese ai partner della filiera	14%	16%
CONSAPEVOLI 60-79	• Approccio strategico valido • Coinvolgimento della direzione che talvolta ha anche un ruolo attivo nell'indirizzamento delle strategie di sicurezza • Fondi destinabili alla sicurezza informatica, spesso direttamente collegati al budget IT • Attività di identificazione dei rischi condotte in maniera sporadica • **Presenza delle corrette leve per la mitigazione del rischio**	31%	32%
INFORMATE 30-59	• **Consapevolezza diffusa** • Gestione del rischio cyber spesso esternalizzata • Assenza di attività di identificazione del rischio • Strumenti base per la mitigazione del rischio	35%	38%
PRINCIPIANTI 0-29	• Consapevolezza limitata o assente • Quasi totale assenza di fondi per la sicurezza informatica • **Scarso impiego di leve per la gestione del rischio**	20%	14%

Le classi di maturità delle PMI italiane.
Fonte: Cyber Index PMI 2025

INDICE

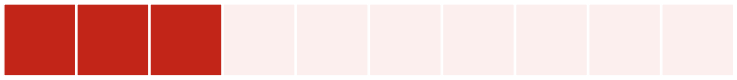
PRINCIPIANTI
PUNTEGGIO DEL CYBER INDEX TRA 0 E 29

Le PMI classificate come **principianti** (14% del totale) sono accomunate da una profonda carenza di consapevolezza, che si manifesta innanzitutto nel disinteresse dei vertici aziendali: in oltre la metà dei casi, la proprietà non attribuisce alcuna importanza strategica alla sicurezza informatica, mentre solo una piccola parte ha iniziato ad approcciarsi al tema molto recentemente. Questa inerzia è alimentata da una percezione del rischio totalmente distorta, con quasi quattro imprese su dieci convinte di non essere un possibile bersaglio. La realtà dei fatti smentisce però questo ottimismo, dato che il 16% di queste realtà ammette di aver già subito attacchi negli ultimi 3 anni.

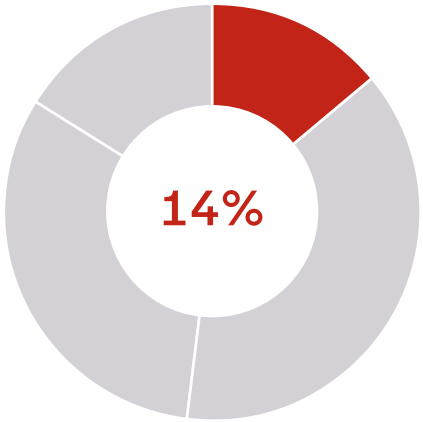
Il profilo di esposizione di questo gruppo non è affatto trascurabile, anche a causa di un marcato paradosso tecnologico: queste imprese adottano spesso tool complessi, come soluzioni di Intelligenza Artificiale o sistemi IoT, senza però possedere il controllo delle proprie fondamenta digitali. Basti pensare che solo l'8% ha stabilito un processo strutturato di mappatura degli asset, rendendo di fatto impossibile proteggere ciò di cui non si ha nemmeno piena visibilità.

Sebbene si tratti prevalentemente di piccole imprese in cui il digitale occupa ancora un ruolo marginale, ben il 65% di esse opera all'interno di filiere produttive sensibili. Questa posizione le trasforma in un pericoloso anello debole, poiché l'assenza di una governance di base vanifica l'efficacia di qualsiasi strumento avanzato. In questo cluster manca ancora quel primo passo fondamentale necessario a generare l'attenzione culturale e gli investimenti economici indispensabili per uscire da una condizione di fragilità cronica.

PRINCIPIANTI



PUNTEGGIO 0 – 29



Campione: 1.582 PMI

LE IMPRESE MENO MATURE ADOTTANO SOLUZIONI AVANZATE COME AI E IOT SENZA AVER CONSOLIDATO UN PROCESSO DI GESTIONE DEL RISCHIO CYBER

INDICE

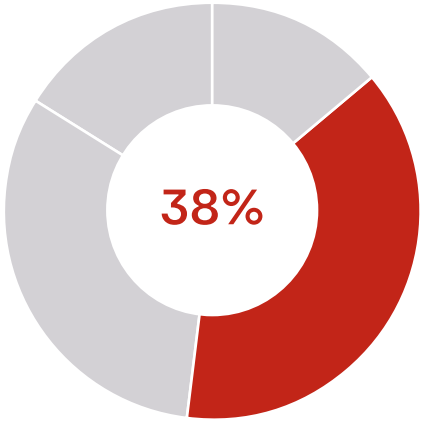
INFORMATI
PUNTEGGIO DEL CYBER INDEX TRA 30 E 59

Le PMI classificate come informate rappresentano un cluster in piena transizione, dove la consapevolezza del rischio è ormai diffusa ma non ancora supportata da un piano d'azione organico. Sebbene il tema sia ufficialmente entrato nell'agenda manageriale, la sicurezza fatica a diventare una priorità assoluta: la gestione dei presidi resta tipicamente delegata a soggetti esterni e solo poco più della metà delle imprese ha stabilito un budget ricorrente dedicato. Questo approccio, pur segnando un passo avanti rispetto ai principianti, riflette una governance ancora frammentata in cui mancano responsabilità interne chiaramente definite.

Sebbene queste realtà scontino ancora una carenza di soluzioni tecnologiche tradizionali, il vero ostacolo alla loro evoluzione risiede in una gestione delle attività di **identificazione** estremamente frammentata. Il limite non è solo l'assenza di una risposta tecnica, ma l'incapacità di interrogarsi correttamente sulla natura stessa delle proprie vulnerabilità. In questo scenario, la cybersecurity rimane un "punto cieco" organizzativo: senza un'analisi strutturata dei rischi, le imprese non riescono a definire una strategia di difesa, rendendo vano o puramente casuale ogni eventuale investimento tecnologico. La gestione degli asset digitali non è costante e solo una minima parte (23%) delle imprese conduce regolarmente attività di auditing per verificare la solidità delle proprie difese. Anche sul fronte tecnologico si riscontra un limite evidente: la protezione si affida quasi esclusivamente a strumenti di base come antivirus e firewall tradizionali, soluzioni ormai inadeguate a contrastare la complessità delle minacce moderne. Questa combinazione di pratiche non strutturate e una scarsa formalizzazione dei controlli sui fornitori impedisce al cluster delle informate di compiere il salto di qualità necessario per raggiungere una postura di sicurezza realmente matura e proattiva.

INFORMATI

PUNTEGGIO 30 – 59



Campione: 1.582 PMI

LE PMI INFORMATE MOSTRANO UN'ADEGUATA CONSAPEVOLEZZA TEORICA, MA MANCANO DI CAPACITÀ PROTETTIVE REALI A CAUSA DI UNA LIMITATA CONOSCENZA DEL RISCHIO

INDICE

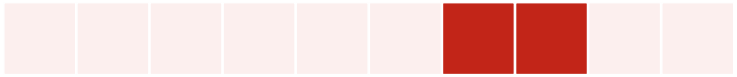
CONSAPEVOLI
PUNTEGGIO DEL CYBER INDEX TRA 60 E 79

Le PMI "consapevoli" dimostrano di saper tradurre l'orientamento strategico in capacità operativa, portando l'indice di Attuazione a un solido punteggio di 71/100. In questo cluster, la sicurezza non è più un elemento accessorio: i piani di formazione sono diffusi e le policy interne risultano ormai consolidate nella cultura aziendale.

Sotto il profilo tecnologico, oltre ai presidi di base, emergono soluzioni avanzate che elevano la postura di difesa: il 51% delle imprese adotta l'autenticazione a due fattori (MFA) per l'accesso a dati e applicazioni, mentre il 30% ha implementato sistemi per la rilevazione dei tentativi di attacco. Questa preparazione si riflette anche nella resilienza operativa, con una diffusa capacità di ripristinare, almeno parzialmente, l'accesso ai servizi a seguito di un incidente.

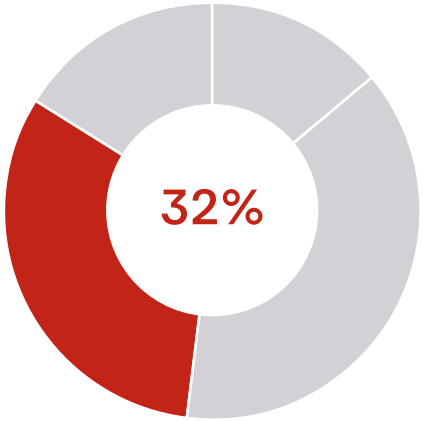
La solidità di questo cluster deriva dalla capacità di monitorare il rischio con profondità: due imprese su tre svolgono regolarmente attività di auditing e la mappatura delle vulnerabilità viene gestita in modo strutturato. Tuttavia, permane un collo di bottiglia critico nella fase di remediation: solo il 7% delle organizzazioni riesce infatti a condurre attività di patch management, evidenziando una difficoltà nell'adottare un approccio proattivo alla cybersecurity.

CONSAPEVOLI



PUNTEGGIO

60 – 79



Campione: 1.582 PMI

NELLE PMI CONSAPEVOLI, LA SICUREZZA È UNA PRIORITÀ SUPPORTATA DA TECNOLOGIE DI BASE, MA ANCORA INADEGUATA RISPETTO ALLE MINACCE ATTUALI

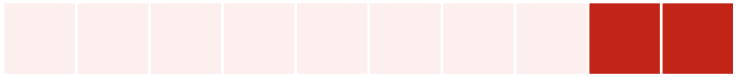
INDICE

MATURE
PUNTEGGIO DEL CYBER INDEX TRA 80 E 100

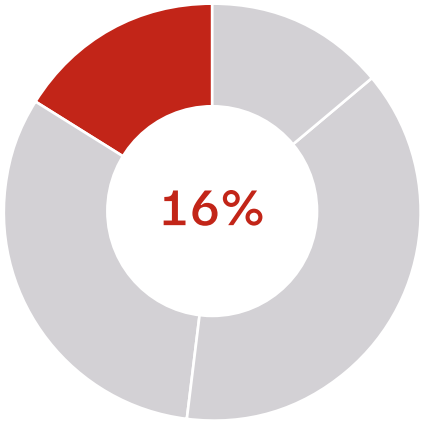
Il cluster delle imprese "mature" rappresenta l'apice dell'evoluzione. In queste organizzazioni la sicurezza è interpretata come una funzione strategica abilitante della Business Continuity. Nonostante questo posizionamento avanzato, l'analisi puntuale evidenzia aree di frizione strutturali: solo il **33% del campione** dispone di una dotazione tecnologica pienamente esaustiva. Nel restante due terzi dei casi, pur essendo presenti i presidi di base, emergono lacune significative nel ricorso a strumenti più sofisticati. In queste realtà, la protezione si affida spesso a soluzioni tradizionali che, pur funzionanti, non garantiscono quel livello di difesa avanzato necessario per contrastare le minacce più evolute e complesse del panorama attuale. Questa vulnerabilità latente è confermata dalla discreta quota di incidenti che continua a colpire anche questo cluster, segno che le difese tradizionali non sono più sufficienti.

È dunque necessario adottare una cultura della sicurezza priva di certezze. Sebbene il 75% delle imprese mature sia convinto di aver raggiunto una postura solida e pronta, bisogna fare i conti con una realtà inesorabile: il rapido progresso tecnologico e l'evoluzione delle minacce rendono ogni assetto di sicurezza soggetto a una rapida obsolescenza. In questo scenario, la vera maturità non risiede nel considerarsi "arrivati", ma nella capacità di aggiornare costantemente i propri presidi per non restare un passo indietro rispetto agli attaccanti.

MATURE



PUNTEGGIO 80 – 100



Campione: 1.582 PMI

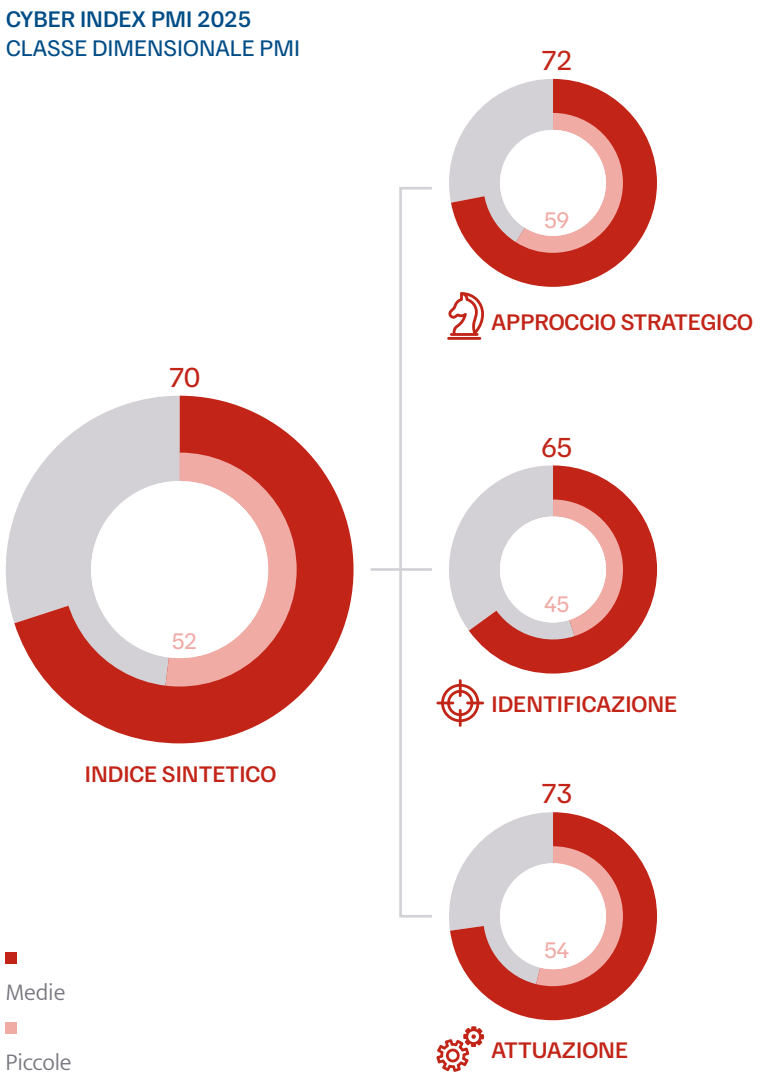
LE PMI MATURE VANTANO UNA POSTURA DI SICUREZZA ADEGUATA, MA L'EVOLUZIONE DELLE MINACCE RENDE OGNI ASSETTO RAPIDAMENTE OBSOLETO

INDICE

VISTE PER DIMENSIONE AZIENDALE

L'andamento del Cyber Index mette in luce un'Italia a due velocità, dove il divario tra i segmenti dimensionali continua ad ampliarsi. Mentre le piccole imprese registrano una crescita quasi piatta, attestandosi a quota 52 (+1 p.p.), le medie imprese accelerano con un deciso +4 p.p., raggiungendo uno stato di maturità solido e omogeneo in tutte le dimensioni analizzate: l'approccio strategico (72), la capacità di identificazione (65) e l'attuazione pratica (73) risultano infatti ampiamente sufficienti.

Questa progressione è sostenuta da una struttura organizzativa più robusta, che spesso vede la presenza di team IT dedicati e una capacità di spesa superiore: le medie imprese destinano alla sicurezza il 13% del proprio budget IT, superando l'11% investito dalle piccole realtà. La maggiore disponibilità economica si traduce in una difesa più concreta: il 16% del campione dispone di tecnologie di mitigazione avanzate e quasi una su tre (29%) ha già attivato una polizza assicurativa per trasferire il rischio residuo.

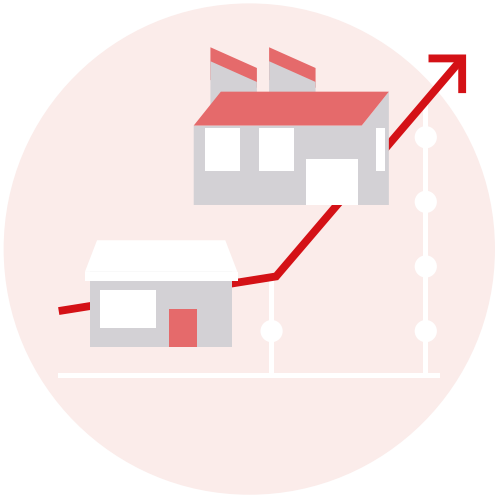


I risultati del Cyber Index PMI 2025 e le tre dimensioni di analisi.
Fonte: Cyber Index PMI 2025

INDICE

Le piccole imprese, al contrario, mostrano ancora un quadro di fragilità, con punteggi medi che non raggiungono la sufficienza in nessuna delle tre dimensioni chiave: approccio strategico (59), attuazione (54) e, soprattutto, identificazione (44). Sebbene la consapevolezza sia in crescita, permane una pericolosa sottovalutazione della minaccia: un'azienda su due non percepisce correttamente il rischio o ostenta una sicurezza ingiustificata rispetto alla propria preparazione reale.

LE PICCOLE IMPRESE REGISTRANO UN INCREMENTO MARGINALE DI 1 P.P., ATTESTANDOSI A QUOTA 52, LE MEDIE IMPRESE ACCELERANO CON UN DECISO +4 P.P.



Un segnale positivo arriva però dal fronte regolatorio: quasi tre piccole imprese su quattro conoscono la NIS2, dimostrando di aver recepito quantomeno la rilevanza del tema nel più ampio scenario politico corrente. Questa spinta si traduce in una partecipazione attiva al mercato, con solo il 12% delle realtà che non ha effettuato investimenti in cybersecurity nel 2025. La scarsa disponibilità di strumenti, tuttavia, suggerisce che i volumi di spesa sono ancora troppo bassi.

L'urgenza di intervento è dettata dai numeri: una piccola impresa su cinque ha subito un attacco negli ultimi tre anni. È quindi prioritario colmare il gap informativo, integrando l'analisi del rischio in ogni progetto di trasformazione digitale attraverso piani d'azione che chiariscano le priorità di mitigazione. Parallelamente, i requisiti per l'accesso alle polizze assicurative possono fungere da bussola operativa per colmare il gap accumulato, mentre il supporto delle istituzioni resta fondamentale per garantire fondi dedicati e prevenire disparità nell'accesso alle tecnologie di difesa.

INDICE

VISTE PER SETTORE

L'analisi settoriale del 2025 delinea un quadro in cui, sebbene la maturità media tra i diversi comparti appaia livellata, le dinamiche di rischio variano profondamente in base all'operatività specifica di ogni filiera.

MANIFATTURA

Il settore manifatturiero vive oggi una fase delicata: è il comparto che ha registrato l'incremento più marcato di attacchi rispetto alla rilevazione precedente, confermandosi come il più bersagliato nel 2025. Ben il 26% delle imprese dichiara di aver subito violazioni nell'ultimo triennio. La peculiarità dello scenario di rischio per queste imprese risiede nell'ampio ricorso alle tecnologie OT (Operational Technology), presenti nel 33% delle realtà industriali, che amplia una superficie d'attacco ancora poco conosciuta. Qui, a differenza di altri ambiti, il pericolo maggiore non è solo l'esfiltrazione di dati, ma il blocco totale della produzione. Nonostante questa esposizione, il settore non mostra avanzamenti significativi nella maturità, rimanendo anzi in fondo alla classifica nella dimensione dell'attuazione.

UTILITIES

Il rischio legato all'alle tecnologie industriali tocca da vicino anche il mondo delle Utilities, che però si conferma il settore più avanzato dell'intera ricerca 2025. Essendo storicamente soggetto a normative stringenti, erogando servizi essenziali e operando a stretto contatto con infrastrutture critiche, questo comparto ha sviluppato una sensibilità superiore: il 64% delle organizzazioni dichiara di non ritenersi ancora "sufficientemente preparato", un dato che paradossalmente indica un'altissima consapevolezza e una conoscenza profonda delle minacce reali.

LOGISTICA

La Logistica rappresenta la vera sorpresa degli ultimi due anni, crescendo sia in termini di spesa che di maturità complessiva. L'indice di settore ha segnato un balzo di ben +9 punti percentuali rispetto al 2024, stabilizzandosi a 60/100. Questa accelerazione è trainata dalla Direttiva NIS2: il 30% delle aziende ha già formalizzato un punto di contatto nazionale, mentre un ulteriore 28% ha iniziato a interessarsi ai requisiti di adeguamento. In questo ambito è molto sentito il rischio legato alle terze parti, poiché le aziende logistiche agiscono come nodi strategici essenziali per quasi tutte le filiere manifatturiere e commerciali.

> **TRA QUELLI ANALIZZATI, IL SETTORE DELLE UTILITIES È QUELLO PIÙ MATURO, CRESCE INVECE LA LOGISTICA**

INDICE

SERVIZI

Anche il settore dei servizi ha mostrato una dinamica simile alla logistica, raggiungendo un indice di 58 (+9 p.p. sull'anno precedente). Se nella logistica il driver è l'interconnessione di filiera, nei servizi a guidare il rischio è la natura dei dati trattati: la gestione di informazioni sensibili riguarda il 23% delle realtà censite. Questa fattispecie sta spingendo le imprese a una revisione accelerata delle proprie capacità di garantire privacy e sicurezza ai dati gestiti.

	Violazione dei sistemi informativi	Approccio strategico	Identificazione	Attuazione	Cyber Index
Servizi	24%	63	52	60	58
Manifattura	26%	59	43	53	52
Logistica	21%	68	52	59	60
Utility	24%	71	51	64	62
Media nazionale	**24%**	**62**	**48**	**57**	**55**

Vista per settore.

Fonte: Cyber Index PMI 2025

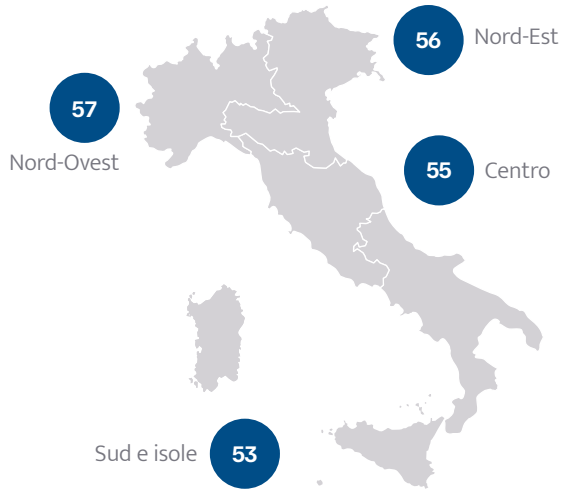
INDICE

VISTE PER AREA GEOGRAFICA

L'analisi della maturità digitale nel 2025 delinea un'Italia geograficamente più coesa, grazie a un percorso di convergenza che vede il Centro protagonista del balzo più significativo (+7 p.p.), seguito da Sud e Isole (+3 p.p.) e dalle aree del Nord (+2 p.p. per Nord-Ovest e Nord-Est). Nonostante questo dinamismo, le regioni settentrionali mantengono la leadership in termini di preparazione e investimenti, riflettendo una consapevolezza ormai diffusa che trova il suo apice nel Nord-Ovest. In quest'area, la spiccata propensione verso tecnologie di frontiera, come l'Intelligenza Artificiale, funge da volano per la cultura digitale, pur introducendo una complessità strutturale che richiede strategie di difesa più articolate.

Questa spinta all'innovazione si riflette direttamente nelle politiche di investimento: il Nord-Ovest è l'area che destina la porzione maggiore del budget IT alla sicurezza, ma anche quella che mediamente accede più di frequente ai fondi resi disponibili da bandi pubblici; il Sud e Isole è invece il territorio che registra l'allocazione più contenuta. Queste due aree si confermano le principali vittime di attacchi informatici, ma le contromisure risultano differenti. La risposta a questa minaccia costante ha spinto il Nord-Ovest a consolidare la postura tecnologica più avanzata del Paese, con il 21% delle aziende che ha già definito un mix di soluzioni ottimali per la mitigazione del rischio. Il Sud è invece ancora in risalita. Tale disparità di spesa appare coerente se si osservano il numero di imprese che, nel 2025, hanno subito impatti significativi (danni finanziari o blocco dell'operatività): nel Nord-Ovest "solo" il 2,4%, mentre nel Sud e Isole addirittura il 4,6%.

CYBER INDEX PMI 2025
AREA GEOGRAFICA



// NEL 2025 PERSISTE UNA NETTA POLARIZZAZIONE TERRITORIALE: IL NORD È PIÙ ESPOSTO MA ANCHE PIÙ PREPARATO, SUD E ISOLE L'AREA IN CUI INTERVENIRE CON MAGGIOR URGENZA

INDICE

L'analisi si arricchisce di sfumature importanti quando osserviamo il comportamento delle imprese del Nord-Est e del Centro, che presentano dinamiche opposte ma altrettanto significative per il panorama nazionale.

Il Nord-Est mostra una maturità (56 punti) sostanzialmente in linea con il Nord-Ovest, pur partendo da un'esposizione al rischio che appare, a una prima analisi, leggermente inferiore. Qui la cultura della sicurezza è diventata un patrimonio aziendale condiviso: in 3 imprese su 4 i vertici o la proprietà sono attenti al tema. Tuttavia, il territorio sembra puntare più sulla tenuta del sistema che sui singoli exploit tecnologici: le eccellenze (imprese "Mature") si fermano al 14%, contro il 19% del Nord-Ovest, delineando un tessuto produttivo molto consapevole ma con meno punte di diamante.

Al contrario, nel Centro Italia si assiste a una sorta di "stagnazione". Nonostante il balzo nell'indice generale, il 77% delle imprese rimane bloccato nei cluster intermedi ("Informate" e "Consapevoli"), faticando a dare seguito ai primi passi compiuti. A frenare l'evoluzione è una percezione del pericolo ancora troppo bassa: solo il 32% delle aziende ritiene che le azioni malevole dei criminali rappresentino un fattore che concorre a esporre a rischi il proprio business. Questa visione è alimentata dai numeri, dato che l'area registra la quota più bassa di incidenti con impatti gravi (1,6%). Lo storytelling prevalente è quello di un territorio che non avverte un'urgenza impellente; tuttavia, il rischio è quello di farsi trovare impreparati: anticipare la trasformazione è l'unica via per evitare che un'improvvisa ondata di attacchi possa paralizzare l'intera area geografica.

	Partecipazione a filiere sensibili	Adozione di tecnologie digitali	Gestione di dati sensibili	Violazione dei sistemi informativi	Cyber Index
Nord-est	79%	97%	22%	24%	56
Nord-ovest	86%	97%	25%	27%	57
Centro	80%	99%	30%	18%	55
Sud e Isole	77%	96%	18%	27%	53
Media nazionale	**81%**	**97%**	**24%**	**25%**	**55**

Vista per area geografica. Le percentuali si riferiscono alla quota di PMI
Fonte: Cyber Index PMI 2025

INDICE

APPROFONDIMENTI

Le aree di analisi rappresentano le scelte strategiche e operative implementate dalle organizzazioni dopo aver valutato la strutturazione di processi e l'introduzione di tecnologie e competenze. Ciascuna delle 20 aree di analisi concorre alla costruzione di una delle tre dimensioni che costituiscono l'indice (approccio strategico, identificazione, attuazione). Come per la scorsa edizione, anche il questionario del Cyber Index PMI 2025 è stato costruito in maniera modulare, mantenendo la logica delle dimensioni ma adattandola alla nuova segmentazione del rischio. Le imprese sono infatti suddivise in due profili di rischio: 1.020 PMI meno esposte e 562 PMI maggiormente esposte.

Le 20 aree di analisi mostrate nella slide sono classificate per colore in funzione del profilo di rischio e del livello di approfondimento delle domande proposte:

- In grigio si identificano le scelte strategiche e/o operative di sicurezza informatica di livello base. Le domande che compongono questo livello sono state rivolte all'intero campione di PMI (1.582).
- Il rosso, invece, rappresenta le scelte strategiche e/o operative di sicurezza informatica di livello avanzato e fa riferimento alle imprese più esposte al rischio cyber. Le domande di questo livello sono state sottoposte a 562 PMI.

L'obiettivo delle aree di analisi non è l'esaustività, quanto piuttosto la rappresentazione delle scelte strategiche e operative attuabili.

LA PREPARAZIONE DELLE PMI

3 DIMENSIONI	20 AREE DI ANALISI
APPROCCIO STRATEGICO Formalizzazione della **responsabilità** della sicurezza informatica e definizione degli **investimenti** a lungo termine.	• Commitment di proprietà / management • Presidio organizzativo • Budget • Piano di sicurezza aziendale
IDENTIFICAZIONE Capacità di comprendere il **dominio aziendale** e la **filiera**, identificare le risorse e gli asset aziendali e le possibili implicazioni sul **rischio cyber** e adeguamento ai **requisiti normativi**.	• Mappatura degli asset informatici • Auditing & Compliance • Valutazione delle vulnerabilità • Misurazione del rischio cyber • Valutazione delle terze parti • Cyber Risk Management
ATTUAZIONE Capacità di selezionare il corretto **mix di competenze e modelli organizzativi** e di implementare iniziative concrete in termini di **persone, processi e tecnologie**.	• Fattore umano • Formazione • Tecnologie • Assicurazioni • Gestione delle terze parti • Disaster recovery • Processo di gestione patch • Piano di risposta • Campagne di phishing • Figure specializzate

■ Domande di approfondimento per le PMI maggiormente esposte

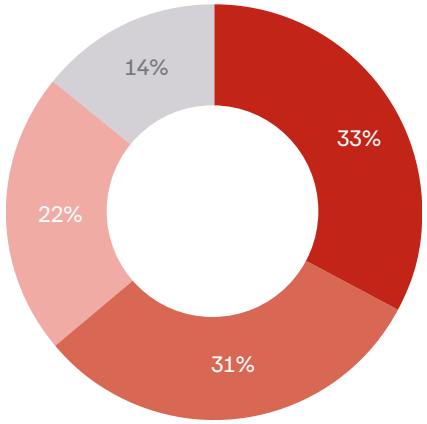
Dimensioni e aree di analisi.
Fonte: Cyber Index PMI 2025

INDICE

APPROCCIO STRATEGICO

COMMITMENT DELLA PROPRIETÀ

Il commitment della proprietà indica il livello di interesse e coinvolgimento dei vertici aziendali ad impegnarsi a livello strategico per garantire una solida gestione del rischio cyber. Di conseguenza, costituisce un buon indicatore della rilevanza assunta dalla cybersecurity all'interno di piccole e medie imprese. Le evidenze mostrano come il 33% dei vertici aziendali si interessi al tema e richieda di aggiornamenti periodici mediante una relazione e il 31% si interessi al tema pur non partecipando al processo di gestione. D'altra parte, vi è un 22% di imprenditori che sta muovendo i primi passi in questa direzione, avvicinandosi progressivamente al tema. Rispetto alla scorsa edizione, vi è complessivamente più interesse da parte della proprietà e maggiore consapevolezza. Rimane invece costante, la quota di imprenditori che non riteneva prioritario il tema (14%).



- Sì, l'imprenditore o i vertici aziendali indirizzano il tema e richiedono periodicamente una relazione
- Sì, l'imprenditore o i vertici aziendali si interessano ma senza partecipare al processo decisionale
- No, l'imprenditore o i vertici aziendali si stanno progressivamente avvicinando al tema
- No, l'imprenditore o i vertici aziendali non ritengono prioritario il tema

Campione: 1.582 piccole e medie imprese italiane

Commitment delle proprietà delle PMI italiane

Fonte: Cyber Index PMI 2025

INDICE

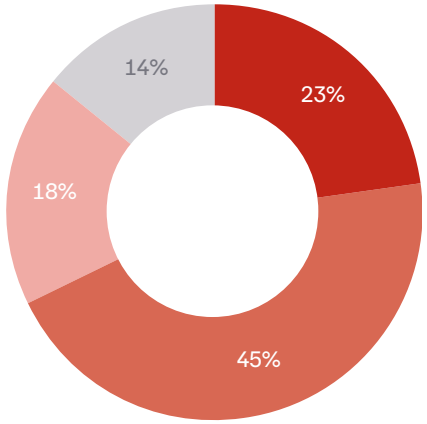
APPROCCIO STRATEGICO

BUDGET E FONDI PER LA CYBERSECURITY

I budget destinati alla sicurezza informatica comprendono le risorse economiche che le imprese investono per dotarsi di soluzioni, servizi e competenze utili a proteggere i propri sistemi e dati. Questo indicatore riflette la consapevolezza e l'impegno dei vertici aziendali verso il tema, che nelle PMI resta spesso limitato dalle risorse disponibili.

Nel 2025 la percentuale complessiva di imprese che prevedono fondi dedicati alla cybersecurity raggiunge il 68%, segnale di una maggiore presenza strutturale del tema nei piani di investimento. Il 23% dichiara di disporre di un budget interamente dedicato, mentre per il 45% le spese per la sicurezza informatica sono integrate nel budget IT. Si riduce al 18% la quota di aziende intenzionate a destinare fondi specifici in futuro e scende al 14% quella che, al momento, non mostra volontà di investimento.

Rispetto al 2024, la crescita del numero di imprese che destinano risorse (il 52%, dato del 2024), sia in modo diretto sia attraverso il budget IT, indica un consolidamento della cybersecurity come voce stabile di spesa aziendale.



- Sì, esiste un budget dedicato
- Sì, parte del budget IT è destinabile alla sicurezza informatica
- No, ma c'è la volontà di stanziare fondi dedicati alla sicurezza informatica
- No e al momento non c'è la volontà di stanziare fondi dedicati alla sicurezza informatica

Campione: 1.582 piccole e medie imprese italiane

Budget e fondi per la cybersecurity delle PMI italiane

Fonte: Cyber Index PMI 2025

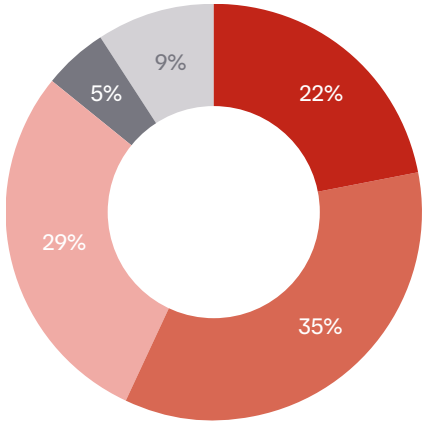
INDICE

APPROCCIO STRATEGICO

PRESIDIO ORGANIZZATIVO

Il presidio organizzativo della cybersecurity riguarda la definizione di ruoli e responsabilità per la gestione delle attività di sicurezza informatica all'interno dell'azienda, elemento fondamentale per garantire una governance efficace e coordinata del rischio digitale. Nel 2025 si osserva una progressiva evoluzione nella struttura di presidio tra le PMI italiane.

Il 22% delle imprese ha formalizzato una figura interna dedicata alla sicurezza informatica, in aumento rispetto al 13% del 2024, segno di una maggiore attenzione verso l'istituzionalizzazione del tema. Rimane stabile al 35% la quota di aziende che assegna la responsabilità in modo informale a una figura interna affine, mentre cresce al 29% quella che affida la gestione della sicurezza a partner esterni (contro il 25% del 2024). Si riducono invece le percentuali di imprese che stanno valutando l'introduzione di un presidio (5%) o che non lo considerano prioritario (9%).



Sì, è stata formalizzata una figura interna ad-hoc per presidiare la sicurezza informatica

Sì, è stata assegnata in maniera informale la responsabilità in materia di sicurezza informatica a una figura interna affine

No, ma la responsabilità è affidata a un partner esterno

No, ma stiamo valutando l'introduzione di un presidio

No, al momento non riteniamo prioritario presidiare la sicurezza informatica

Campione: 1.582 piccole e medie imprese italiane

Presidio organizzativo delle PMI italiane

Fonte: Cyber Index PMI 2025

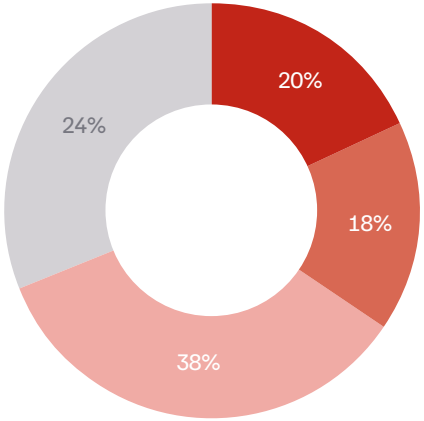
INDICE

APPROCCIO STRATEGICO

PIANO DI SICUREZZA

Il piano di sicurezza informatica rappresenta lo strumento strategico attraverso cui le imprese definiscono l'insieme di procedure, misure e strumenti necessari per proteggere i propri sistemi informativi da minacce e attacchi cyber. È un documento che, per essere efficace, deve essere aggiornato e monitorato nel tempo, adattandosi all'evoluzione del contesto e dei rischi.

Nel 2025 il livello di diffusione dei piani di sicurezza tra le PMI con alta esposizione al rischio rimane stabile rispetto all'anno precedente. Solo il 20% delle imprese dispone di un piano formalizzato e aggiornato periodicamente almeno una volta l'anno, mentre il 18% ha definito un piano rivisto solo saltuariamente. Una PMI su quattro non ha stabilito nessun tipo di piano di sicurezza, mentre nel 38% sono presenti almeno linee guida informali.



- È stato approvato un piano di sicurezza informatica, monitorato costantemente e rivisto almeno annualmente
- È stato approvato un piano di sicurezza informatica, monitorato e rivisto saltuariamente
- Non è stato approvato un piano di sicurezza informatica, ma abbiamo prassi e linee guida
- Non è stato approvato un piano di sicurezza informatica e non abbiamo né prassi né linee guida

Campione: 562 piccole e medie imprese italiane

Piano di sicurezza delle PMI italiane

Fonte: Cyber Index PMI 2025

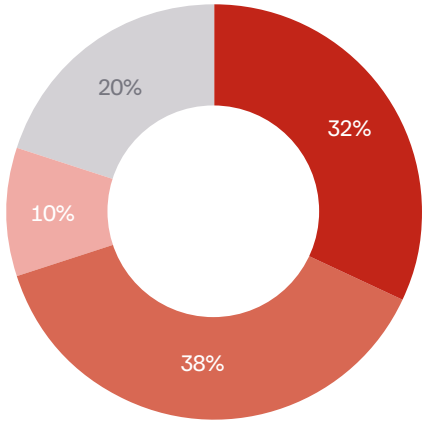
INDICE

IDENTIFICAZIONE

MAPPATURA DEGLI ASSET INFORMATICI

La mappatura degli asset informatici è il processo che consente alle imprese di individuare e catalogare tutte le risorse digitali presenti — dai server alle reti, dai dispositivi alle applicazioni — offrendo una visione chiara del perimetro tecnologico da proteggere. Questa attività rappresenta la base per una gestione efficace della sicurezza, poiché permette di conoscere in modo preciso "cosa" deve essere difeso e come.

Nel 2025 si osserva un ulteriore progresso rispetto all'anno precedente. Cresce al 32% la quota di PMI che realizza una mappatura strutturata e continuativa degli asset, rispetto al 20% del 2024, segno di una maggiore maturità organizzativa. Rimane costante la quota di imprese che svolge una mappatura su base saltuaria o una tantum (38%). Complessivamente diminuisce la percentuale di imprese che non svolge l'esercizio di mappatura degli asset (20%) o che sta valutando di introdurre questa pratica (10%).



- Esiste un processo strutturato di mappatura di tutti gli asset informatici utilizzati in azienda su base continuativa
- Esiste un processo di mappatura dei principali asset informatici, o viene condotta una mappatura una tantum
- Non è stata condotta una mappatura ma c'è la volontà di catalogare gli asset informatici
- No e al momento non ne stiamo valutando l'introduzione

Campione: 1.582 piccole e medie imprese italiane

Mappatura degli asset informatici delle PMI italiane

Fonte: Cyber Index PMI 2025

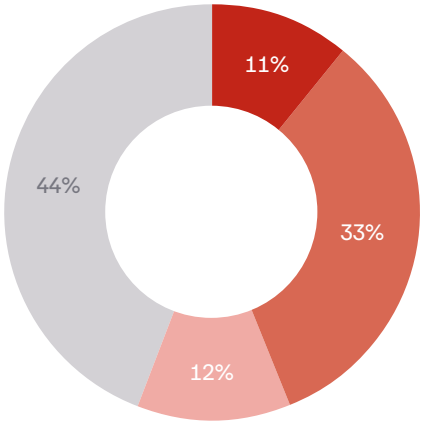
INDICE

IDENTIFICAZIONE

AUDITING DELLA SICUREZZA INFORMATICA

L'auditing della sicurezza informatica comprende attività di analisi e controllo volte a verificare l'efficacia delle misure di protezione adottate e la loro conformità alle normative vigenti. Spesso questo tipo di attività porta sia a identificare i punti deboli sia a capire come migliorare la cybersecurity dell'intera organizzazione.

Nel 2025 la diffusione di attività di auditing tra le PMI italiane mostra una tenuta complessiva, con lievi variazioni rispetto allo scorso anno. Il 33% delle imprese conduce verifiche sia sugli aspetti di compliance sia su quelli di sicurezza informatica, mantenendo una stabilità rispetto al 2024, mentre cresce all'11% la quota che estende le valutazioni anche ai partner della filiera (contro l'8% dell'anno precedente). Diminuisce al 12% la percentuale di aziende che si concentra solo sulla compliance.



Sì, sia sugli aspetti di compliance che di sicurezza informatica, estendendo la valutazione anche ai partner della filiera

Sì, sia sugli aspetti di compliance che di sicurezza informatica, limitatamente al dominio aziendale

Sì, solo sugli aspetti di compliance

No, non svolgiamo attività di auditing

Campione: 1.582 piccole e medie imprese italiane

Auditing della sicurezza informatica delle PMI italiane

Fonte: Cyber Index PMI 2025

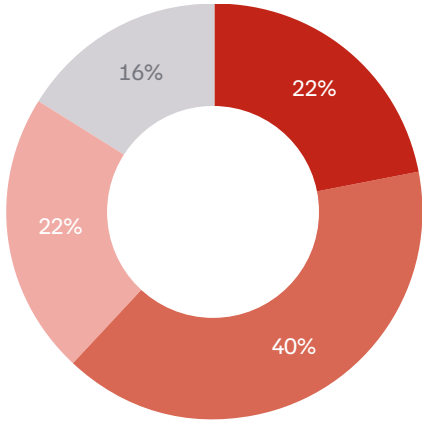
INDICE

IDENTIFICAZIONE

VALUTAZIONE DELLE VULNERABILITÀ

La valutazione delle vulnerabilità (o vulnerability assessment) è il processo che consente alle imprese di individuare e analizzare le debolezze presenti nei sistemi informatici, nelle reti e nelle applicazioni, al fine di prevenire possibili attacchi. Questa attività permette di conoscere in maniera accurata lo stato di sicurezza dell'infrastruttura digitale e di definire misure mirate di miglioramento.

Nel 2025, la percentuale di PMI che svolge attività di valutazione in modo strutturato e continuativo si attesta al 22%. Aumenta la quota di imprese che conduce analisi in maniera sporadica, raggiungendo il 40%. La percentuale di organizzazioni che intende avviare un processo di valutazione si stabilizza al 22%, mentre la quota di quelle che non considerano questa attività come prioritaria arriva al 16%.



- Esiste un processo strutturato per rilevare, documentare e valutare i rischi e le vulnerabilità su base continuativa
- Conduciamo attività sporadiche per rilevare, documentare e valutare i rischi e le vulnerabilità
- Non conduciamo attività di identificazione ma c'è la volontà di catalogare le vulnerabilità
- Non conduciamo attività di identificazione e non c'è la volontà di catalogare le vulnerabilità

Campione: 562 piccole e medie imprese italiane

Valutazione delle vulnerabilità delle PMI italiane

Fonte: Cyber Index PMI 2025

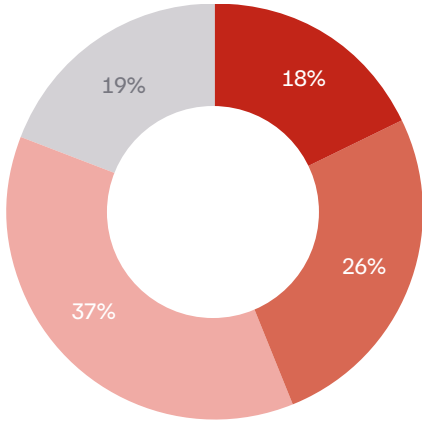
INDICE

IDENTIFICAZIONE

MISURAZIONE DEL RISCHIO CYBER

La misurazione del rischio cyber consiste nel valutare il livello di esposizione alle minacce informatiche, analizzando la probabilità che si verifichino e i possibili impatti sulle attività aziendali. Questo processo aiuta le imprese a individuare le aree più fragili e a programmare interventi mirati per ridurre i rischi, costituendo una base importante per la pianificazione strategica della sicurezza.

Nel 2025 il 18% delle PMI effettua test di misurazione del rischio con cadenza almeno annuale e il 26% ha svolto analisi in maniera saltuaria. Cresce la quota di aziende che sta valutando l'introduzione di questo processo (37%) e si attesta al 19% quella che al momento non percepisce la necessità di farlo.



- Sì, vengono effettuati test periodici di misurazione del rischio cyber, con cadenza almeno annuale
- Sì, vengono effettuati test di misurazione del rischio cyber in maniera saltuaria
- No, ma ne stiamo valutando l'introduzione di test per la misurazione del rischio cyber
- No, non sentiamo la necessità

Campione: 562 piccole e medie imprese italiane

Misurazione del rischio cyber delle PMI italiane

Fonte: Cyber Index PMI 2025

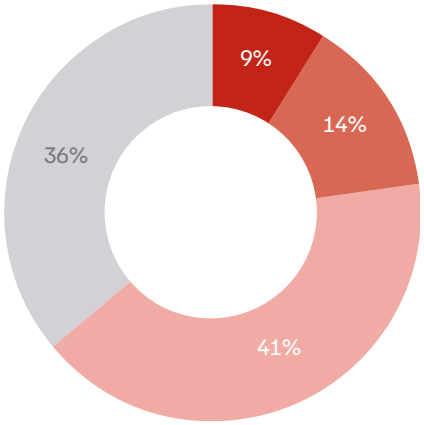
INDICE

IDENTIFICAZIONE

VALUTAZIONE DELLE TERZE PARTI

La valutazione della sicurezza dei fornitori è uno strumento essenziale per proteggere le informazioni aziendali e ridurre i rischi legati alle vulnerabilità esterne. Attraverso il monitoraggio delle misure di sicurezza adottate dalla propria rete di partner, le imprese possono prevenire la diffusione di minacce lungo la filiera e garantire un controllo più completo sulla propria esposizione al rischio.

Nel 2025, tuttavia, le attività di monitoraggio dei fornitori restano ancora poco diffuse tra le PMI italiane. Il 9% delle PMI dichiara di monitorare periodicamente il livello di sicurezza di tutti i fornitori, mentre il 14% conduce verifiche saltuarie sui partner considerati più rilevanti. Cresce al 41% la quota di aziende che, pur consapevoli dei rischi derivanti dalla filiera, stanno valutando di introdurre attività di controllo, e si attesta al 36% quella che non considera ancora prioritario questo tipo di monitoraggio.



- Sì, monitoriamo periodicamente il livello di sicurezza di tutti i fornitori con cui l'azienda si relaziona
- Sì, monitoriamo saltuariamente il livello di sicurezza di alcuni fornitori considerati più rilevanti
- No, ma siamo a conoscenza delle minacce provenienti dalla filiera e stiamo valutando di introdurre attività di valutazione
- No, non riteniamo prioritario valutare il livello di sicurezza dei fornitori

Campione: 562 piccole e medie imprese italiane

Valutazioni delle terze parti delle PMI italiane

Fonte: Cyber Index PMI 2025

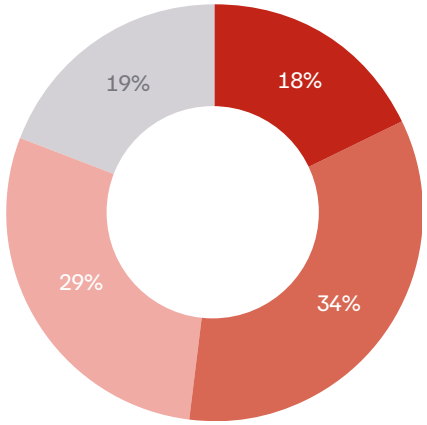
INDICE

IDENTIFICAZIONE

CYBER RISK MANAGEMENT

Il Cyber Risk Management è un processo strategico che permette alle imprese di identificare, valutare e gestire i rischi legati alla sicurezza informatica, integrando aspetti tecnici, gestionali e di governance. La sua efficacia dipende dalla capacità di considerare la cybersecurity come parte integrante della gestione complessiva del rischio aziendale, e non come attività isolata.

Nel 2025 il quadro evidenzia un progressivo consolidamento della gestione del rischio cyber. Il 18% delle PMI dichiara di gestirlo all'interno di un processo integrato di risk management, in crescita rispetto al 12% del 2024, mentre il 34% lo tratta come rischio autonomo, affidandolo a funzioni specifiche come IT, Security o Legal. Cresce in modo significativo la percentuale di aziende intenzionate a strutturare un processo dedicato (29%, rispetto al 17% del 2024), mentre rimane stabile al 19% la quota di PMI che non monitora il rischio con costanza.



Il rischio cyber viene gestito all'interno di un processo integrato di Risk Management aziendale

Il rischio cyber viene gestito come rischio a sé stante all'interno della funzione IT o di un'altra singola funzione (es. Security, Legal & Compliance, ecc.)

Al momento il processo di gestione del rischio cyber non è strutturato, ma prevediamo di definirlo

Il rischio cyber non viene monitorato costantemente

Campione: 562 piccole e medie imprese italiane

Cyber Risk Management delle PMI italiane

Fonte: Cyber Index PMI 2025

INDICE

ATTUAZIONE

GESTIONE DEL FATTORE UMANO

Il fattore umano continua a rappresentare uno degli elementi più critici nella sicurezza informatica, perché errori, disattenzioni o comportamenti non adeguati possono compromettere anche le difese tecnologiche più avanzate. Per questo, la gestione del fattore umano si fonda sulla definizione di regole e procedure che orientino il comportamento degli utenti, garantendo un utilizzo responsabile di dispositivi, credenziali e dati aziendali.

Nel 2025 si osservano segnali di miglioramento nelle politiche di gestione delle persone. Il 36% delle PMI ha definito policy comportamentali formali per regolare l'uso dei dispositivi e la gestione delle credenziali in relazione ai ruoli, in crescita rispetto al 25% del 2024. Rimane consistente al 34% la quota di imprese che dispone solo di linee guida informali, mentre si attesta al 14% quella che sta considerando di introdurle e si conferma al 16% quella che non prevede ancora iniziative in tal senso.

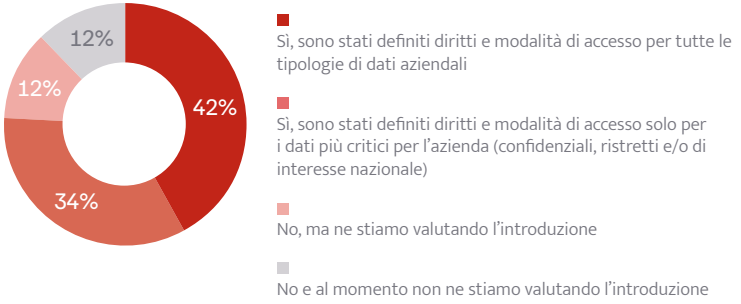
Parallelamente, cresce anche la maturità nella gestione degli accessi, fondamentale per garantire la protezione dei dati aziendali. Il 42% delle PMI dichiara di aver definito diritti e modalità di accesso per tutte le tipologie di dati (in aumento rispetto al 33% del 2024), mentre il 34% le applica solo ai dati più critici. Le quote di imprese che stanno valutando l'introduzione del processo o non lo considerano prioritario si attestano entrambe al 12%.

POLICY COMPORTAMENTALI

Campione: 1.582 piccole e medie imprese italiane

Fonte: Cyber Index PMI 2025

GESTIONE DEGLI ACCESSI



Campione: 1.582 piccole e medie imprese italiane

Fonte: Cyber Index PMI 2025

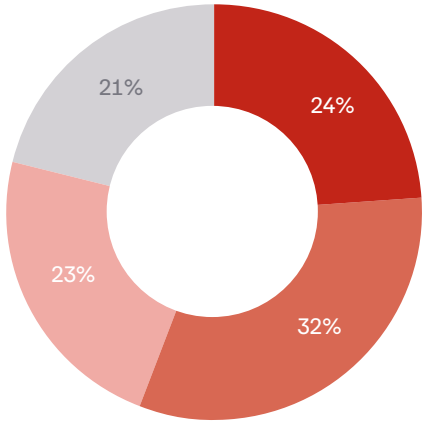
INDICE

ATTUAZIONE

FORMAZIONE

La formazione sui rischi cyber rappresenta una componente centrale nella prevenzione degli incidenti legati al fattore umano. Attraverso programmi di sensibilizzazione e corsi dedicati, le imprese mirano a ridurre gli errori dovuti a disattenzione e a promuovere comportamenti sicuri ed etici nell'uso delle risorse digitali.

Nel 2025 si osserva un miglioramento nel livello di strutturazione delle attività formative rispetto all'anno precedente. Il 24% delle PMI dispone di piani di formazione continuativi e personalizzati in base ai ruoli aziendali, in crescita significativa rispetto al 12% del 2024. Cresce anche la quota di realtà che organizzano corsi una tantum o iniziative rivolte ai dipendenti più esposti al rischio (32%). Si attesta al 23% la percentuale di aziende che dichiara di voler avviare percorsi di formazione, mentre al 21% quella che al momento non prevede iniziative strutturate. Nel complesso, il quadro evidenzia un rafforzamento delle politiche di formazione e un ampliamento delle azioni mirate alla consapevolezza del rischio digitale.



Sì, sono previsti piani strutturati di formazione per i dipendenti, personalizzati sulla base dei ruoli e dei profili aziendali

Sì, sono previsti corsi di formazione una tantum o iniziative indirizzate solo verso i dipendenti più esposti al rischio

No, ma ne prevediamo l'introduzione

No, al momento non sono previste e non ne prevediamo l'introduzione

Campione: 1.582 piccole e medie imprese italiane

Formazione prevista da parte delle PMI italiane

Fonte: Cyber Index PMI 2025

INDICE

ATTUAZIONE

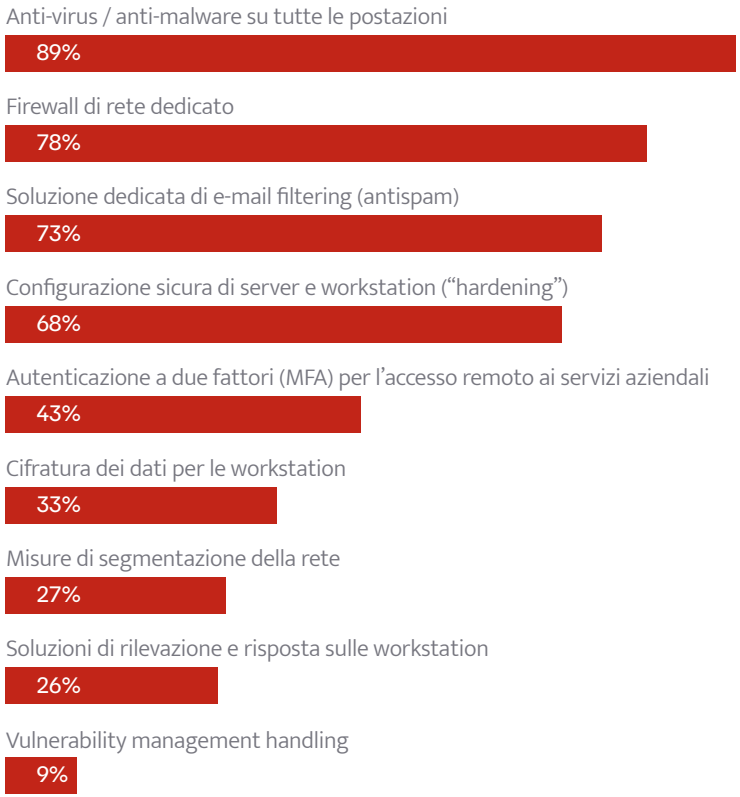
TECNOLOGIE E PROCESSI TECNICI

La dotazione tecnologica delle PMI nel 2025 mostra un livello di maturità crescente, con una diffusione ampia delle soluzioni di difesa di base e una graduale estensione verso strumenti più avanzati di protezione cyber. La quasi totalità delle imprese dispone di antivirus o anti-malware su tutte le postazioni (89%), a conferma della consolidata attenzione verso la sicurezza essenziale dei dispositivi. Rimane elevata anche la presenza di firewall di rete dedicati (78%) e di soluzioni per il filtraggio delle e-mail (73%), a tutela dai principali vettori di attacco come spam e phishing.

Il 68% delle PMI dichiara di aver implementato configurazioni sicure di server e workstation ("hardening"), una misura che contribuisce a ridurre o disattivare processi non necessari sulle diverse workstation, riducendo attività occulte. L'autenticazione a più fattori (MFA), utile per proteggere gli accessi remoti, è presente nel 43% delle organizzazioni, segno di un progresso ma con margine di espansione.

Più limitata la diffusione delle tecnologie di cifratura dei dati (33%), delle misure di segmentazione di rete (27%) e delle soluzioni di Endpoint Detection and Response (EDR/EDP), adottate dal 26% delle PMI, a testimonianza di una copertura ancora parziale nelle aree più avanzate della difesa informatica. Solo il 9% gestisce formalmente processi di vulnerability management e disclosure, mentre un residuale 3% dichiara di non adottare alcuna delle principali soluzioni di sicurezza rilevate.

DOTAZIONE TECNOLOGICA E DIFFUSIONE DI PROCESSI TECNICI



Campione: 1.582 piccole e medie imprese italiane

Fonte: Cyber Index PMI 2025

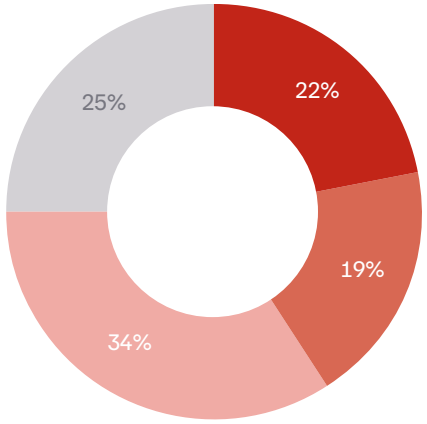
INDICE

ATTUAZIONE

GESTIONE DELLE PATCH

La gestione delle patch di sicurezza è il processo che permette alle imprese di mantenere aggiornati sistemi e applicazioni, correggendo vulnerabilità che potrebbero essere sfruttate per attacchi informatici. Si tratta di un'attività fondamentale per garantire la protezione dell'infrastruttura IT, ma che richiede una pianificazione regolare e un monitoraggio continuo per essere realmente efficace.

Nel 2025 si osserva un lieve miglioramento nella strutturazione di queste attività tra le PMI con medio-alta esposizione al rischio. Il 22% dichiara di avere un processo documentato e applicato almeno ogni tre mesi, in crescita rispetto al 17% del 2024, mentre il 19% conduce la ricerca e la gestione delle patch senza seguire una cadenza prestabilita. Aumenta sensibilmente, al 34%, la quota di imprese che sta valutando di introdurre un piano dedicato, mentre si attesta al 25% quella che non prevede alcuna iniziativa in materia.



- Sì, abbiamo un processo documentato per la ricerca e la gestione di patch, condotto con cadenza almeno trimestrale
- Sì, abbiamo un processo documentato per la ricerca e la gestione di patch che conduciamo senza una cadenza prestabilita
- No, ma ne stiamo valutando l'introduzione
- No e non ne stiamo valutando l'introduzione

Campione: 562 piccole e medie imprese italiane

Gestione delle patch all'interno delle PMI italiane

Fonte: Cyber Index PMI 2025

INDICE

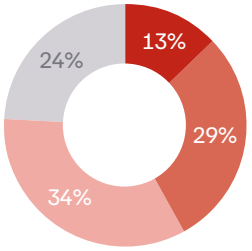
ATTUAZIONE

GESTIONE DEGLI INCIDENTI

La gestione degli incidenti rappresenta un elemento cardine per garantire la continuità operativa e la resilienza delle imprese in caso di attacco informatico o violazione dei dati. Essa si basa sulla definizione di un piano di risposta, che stabilisce ruoli, responsabilità e procedure da attuare per contenere i danni e ripristinare rapidamente le condizioni di normalità. Nel 2025, si osserva un ridimensionamento delle attività strutturate rispetto all'anno precedente: solo il 13% dispone di un piano aggiornato periodicamente sulla base delle nuove minacce o degli attacchi passati (contro l'11% del 2024), mentre il 29% ha un piano di risposta operativo ma non soggetto ad aggiornamento. Cresce al 33% la quota di imprese che sta valutando di introdurre un piano, e sale al 24% quella che non ne prevede l'adozione, segno che l'attenzione verso la gestione reattiva degli incidenti rimane ancora disomogenea.

Parallelamente, il tema del ripristino dei servizi dopo un attacco (disaster recovery) mostra un quadro più maturo. Il 24% delle PMI dispone di un piano che consente di ripristinare in tempo reale i servizi applicativi e l'accesso ai dati, in aumento rispetto al 20% del 2024. Il 28% gestisce il ripristino in maniera differita e il 12% limita la possibilità di recupero al solo accesso ai dati. Cresce lievemente la quota di imprese che sta valutando di introdurre un piano (20%) e si attesta al 16% quella che non lo ritiene necessario.

PIANO DI RISPOSTA

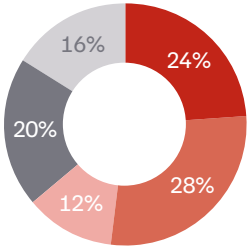


- Sì, abbiamo un piano di risposta aggiornato periodicamente sulla base degli attacchi passati o delle nuove minacce con la definizione dei ruoli e delle azioni da compiere
- Sì, abbiamo un piano di risposta con la definizione dei ruoli e delle azioni da compiere
- No, ma ne stiamo valutando l'introduzione
- No e non ne stiamo valutando l'introduzione

Campione: 562 piccole e medie imprese italiane

Fonte: Cyber Index PMI 2025

DISASTER RECOVERY



- Sì, abbiamo sviluppato un piano che consente di ripristinare in tempo reale i servizi applicativi e l'accesso ai dati aziendali
- Sì, abbiamo sviluppato un piano che consente di ripristinare i servizi applicativi e l'accesso ai dati aziendali in maniera differita
- Sì, abbiamo sviluppato un piano che consente di ripristinare il solo accesso ai dati aziendali (in cloud o on-premise)
- No, ma ne stiamo valutando l'introduzione
- No e non ne stiamo valutando l'introduzione

Campione: 1.582 piccole e medie imprese italiane

Fonte: Cyber Index PMI 2025

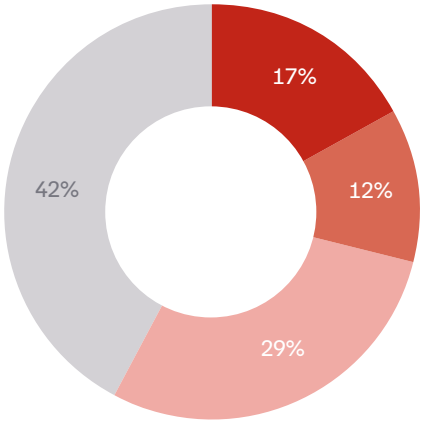
INDICE

ATTUAZIONE

GESTIONE DELLE TERZE PARTI

La gestione delle terze parti riguarda l'insieme delle pratiche e delle politiche adottate dalle imprese per garantire che anche fornitori e partner rispettino adeguati standard di sicurezza informatica. In un contesto sempre più interconnesso, questo aspetto assume un'importanza crescente: un'attenta valutazione della sicurezza lungo la filiera contribuisce infatti a ridurre il rischio di attacchi che sfruttano vulnerabilità di soggetti esterni.

Nel 2025, si registra un leggero incremento delle attività strutturate rispetto all'anno precedente, ma il tema rimane ancora poco presidiato da parte delle PMI. Il 17% delle imprese dichiara di aver definito clausole formali per regolamentare responsabilità, accessi e monitoraggio delle terze parti, nonché di richiedere certificazioni di sicurezza ai propri fornitori, in linea con il 17% del 2024. Un ulteriore 12% richiede certificazioni senza aver introdotto clausole formali, mentre cresce al 29% la quota di imprese che sta valutando l'introduzione di regole specifiche. Rimane consistente, al 42%, la percentuale di organizzazioni che non si occupano ancora di questa attività.



- Sì, abbiamo definito clausole formali per regolamentare responsabilità, accessi, attività di monitoraggio e richiediamo certificazioni a fornitori e partner
- Non abbiamo definito clausole formali ma richiediamo certificazioni a fornitori e partner
- No, ma ne stiamo valutando l'introduzione
- No, non sono state definite

Campione: 1.582 piccole e medie imprese italiane

Gestione delle terze parti da parte delle PMI italiane

Fonte: Cyber Index PMI 2025

INDICE

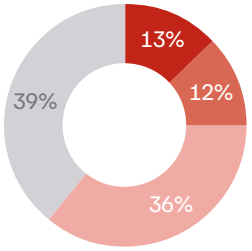
ATTUAZIONE

CAMPAGNE DI PHISHING

Le simulazioni di phishing, pensate per verificare la risposta dei dipendenti di fronte a possibili tentativi di truffa via e-mail, risultano ancora limitate nella loro diffusione. Il 13% delle imprese effettua campagne di simulazione periodiche su tutti i dipendenti e il 12% le realizza in modo saltuario. Crescono invece al 36% le PMI che stanno valutando di introdurle e al 39% quelle che non prevedono attività di questo tipo, confermando come la pratica non sia ancora ampiamente consolidata.

Nonostante la diffusione ancora limitata delle simulazioni, i risultati evidenziano alcune criticità significative. Solo il 58% delle PMI registra un tasso di clic sui link malevoli inferiore al 5%, mentre nel 36% dei casi la risposta risulta moderata, con clic compresi tra il 5% e il 15%. Il restante 6% mostra livelli di vulnerabilità più elevati, con una percentuale di clic superiore al 15%.

SIMULAZIONI DI PHISHING

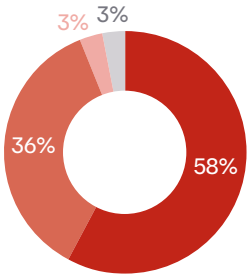


- Sì, effettuiamo simulazioni di campagne di phishing periodiche indirizzate a tutti i dipendenti aziendali, diversificate in base al target di utenti
- Sì, abbiamo effettuato simulazioni di campagne di phishing una tantum oppure indirizzate solo ad alcuni utenti
- No, ma ne stiamo valutando l'introduzione
- No e non ne stiamo valutando l'introduzione

Campione: 562 piccole e medie imprese italiane

Fonte: Cyber Index PMI 2025

RISULTATI SIMULAZIONI DI PHISHING



- Risultati positivi: tasso di clic sui link di phishing inferiore al 5%
- Risultati moderati: tasso di clic sui link di phishing tra il 5% e il 15%
- Risultati negativi: tasso di clic sui link di phishing tra il 15% e il 30%
- Risultati molto negativi: tasso di clic sui link di phishing oltre il 30%

Campione: 562 piccole e medie imprese italiane

Fonte: Cyber Index PMI 2025

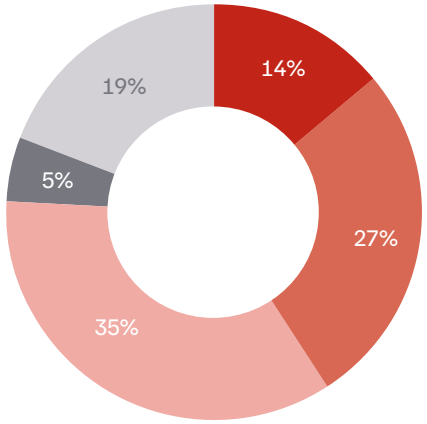
INDICE

ATTUAZIONE

FIGURE SPECIALIZZATE

La crescente complessità del panorama digitale rende sempre più strategica la presenza di figure specializzate nella gestione del rischio cyber, professionisti in grado di identificare e mitigare le minacce informatiche così come di contribuire alla diffusione di una cultura della sicurezza all'interno delle organizzazioni.

Nel 2025 si registra un quadro in evoluzione per le PMI italiane. Il 14% dispone di almeno una figura dedicata esclusivamente alla gestione del rischio cyber, in leggero aumento rispetto al 13% del 2024. Si riduce invece la percentuale di imprese che dichiarano di avere competenze interne diffuse nella funzione IT, passata dal 48% al 27%, a testimonianza di un progressivo spostamento verso modelli più specializzati o verso l'affidamento esterno. Cresce infatti al 35% la quota di PMI che si avvalgono di competenze fornite da partner esterni, mentre rimane stabile al 5% quella che sta valutando l'introduzione di una figura dedicata. Aumenta invece, al 19%, la quota di imprese che non considera ancora prioritaria questa scelta.



- Abbiamo almeno una figura specializzata impegnata esclusivamente nella gestione del rischio cyber
- Non abbiamo introdotto figure specializzate ma sono presenti competenze diffuse all'interno della funzione IT
- Non abbiamo figure interne specializzate, ma competenze fornite da partner esterni
- No, ma ne stiamo valutando l'introduzione
- No e non ne stiamo valutando l'introduzione

Campione: 1.582 piccole e medie imprese italiane

Gestione delle terze parti da parte delle PMI italiane

Fonte: Cyber Index PMI 2025

INDICE

APPENDICI

INDICE

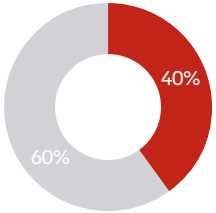
NOTA METODOLOGICA

L'iniziativa **Cyber Index PMI**, al suo terzo anno, ha l'obiettivo di:

- misurare il livello di cultura e di consapevolezza del rischio cyber nelle piccole e medie imprese italiane, nonché il livello di preparazione, valutandone le evoluzioni nel tempo;
- renderle consapevoli dell'importanza del monitoraggio e del controllo delle attività;
- mostrare loro le tecniche e le tecnologie adottabili per la gestione del rischio cyber.

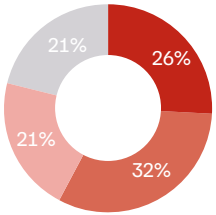
Il Rapporto Cyber Index PMI 2025 si basa su un'indagine rivolta a figure chiave nelle PMI italiane (con un numero di dipendenti compreso tra 10 e 249), come responsabili della sicurezza informatica, responsabili IT, titolari e altri ruoli di responsabilità. Il questionario, distribuito attraverso metodologia CAWI (Computer Assisted Web Interviewing), è stato sviluppato in collaborazione con Generali Italia, Confindustria, Agenzia per la Cybersicurezza Italiana, e ha coinvolto 1.582 PMI distribuite come indicato in figura.

Concepito in maniera modulare, il questionario si articola su due livelli di approfondimento in base alla dimensione e all'esposizione al rischio dell'impresa, per garantire che la valutazione della singola impresa e il Cyber Index (entrambi quantificati in centesimi) tengano in considerazione le reali



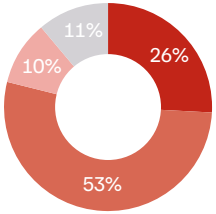
DIMENSIONE AZIENDALE

- Piccola (10-49 addetti)
- Media (50-249 addetti)



PROVENIENZA TERRITORIALE

- Nord-ovest
- Centro
- Nord-est
- Sud e Isole



COMPARTO MERCEOLOGICO

- Manifattura
- Logistica
- Servizi
- Utilities

INDICE

esigenze di ciascuna PMI. L'esposizione al viene valutata considerando fattori come l'adozione di strumenti digitali, l'appartenenza a settori critici, la tipologia di dati gestiti e le eventuali violazioni subite negli ultimi tre anni.

Il primo livello è accessibile a tutte le PMI (1.582), mentre al secondo livello hanno avuto accesso 562 PMI, considerate maggiormente esposte. Il numero di domande in merito alla preparazione varia tra le 13 domande (per chi ha avuto accesso al primo livello) fino ad un massimo di 23 domande.

Il questionario dell'edizione 2025 è stato sviluppato in continuità rispetto alle versioni 2024 e 2023 per garantire continuità nell'analisi. Tuttavia, in relazione agli avanzamenti del rischio cyber e dello scenario normativo, sono state introdotte nuove domande di approfondimento.

All'interno del rapporto sono presenti rimandi a ricerche condotte dall'Osservatorio Cybersecurity & Data Protection sulle grandi organizzazioni italiane, in particolare sulla spesa delle imprese italiane in materia di sicurezza informatica.

INDICE

GLOSSARIO

ARTIFICIAL INTELLIGENCE (AI): ramo della computer science che studia lo sviluppo di sistemi hardware e software, dotati di capacità tipiche dell'essere umano (interazione con l'ambiente, apprendimento e adattamento, ragionamento e pianificazione), in grado di perseguire autonomamente una finalità definita prendendo delle decisioni che, fino a quel momento, erano solitamente affidate agli umani

AUTENTICAZIONE A DUE FATTORI (MFA): sistema di sicurezza che richiede due prove per accedere a un servizio, ad esempio una password (primo fattore) e un codice temporaneo inviato al telefono (secondo fattore). Questo rende più difficile per i malintenzionati accedere ai servizi aziendali anche se conoscono la password.

CIFRATURA DEI DATI / CRITTOGRAFIA: Tecnica per proteggere i dati, rendendoli incomprensibili a chiunque non abbia la chiave per decifrarli, impedendo a chi non ha l'autorizzazione di accedervi, anche in caso di furto o perdita del dispositivo.

DISASTER RECOVERY: insieme di attività e tecnologie volte a ripristinare l'operatività delle infrastrutture IT/OT e delle attività aziendali a seguito di un disastro, come un attacco informatico, riducendo al minimo i tempi di inattività e le perdite economiche.

EDR (ENDPOINT DETECTION AND RESPONSE) E EDP (ENDPOINT PROTECTION): soluzioni avanzate di sicurezza per proteggere i dispositivi aziendali, come i computer, da minacce informatiche. Questi software monitorano costantemente i dispositivi alla ricerca di attività sospette, permettendo di rispondere rapidamente a eventuali attacchi o violazioni di sicurezza.

GESTIONE DELLE PATCH: processo di applicazione degli aggiornamenti rilasciati dal fornitore per risolvere le vulnerabilità della sicurezza e ottimizzare le prestazioni di software e dispositivi.

HARDENING: processo di disabilitazione di funzioni/processi attivi sui dispositivi e server ma non necessari.

INFRASTRUTTURE CRITICHE: organizzazioni, imprese o enti la cui interruzione o momentanea indisponibilità dei servizi provoca l'indebolimento in maniera significativa del funzionamento normale di un Paese

INCIDENT RESPONSE: insieme di attività e tecnologie volte all'identificazione, contenimento, analisi e comunicazione di incidenti di sicurezza informatica avvenuti all'interno dell'organizzazione.

NIS2 (NETWORK AND INFORMATION SECURITY 2): approvata dal Parlamento Europeo il 10 novembre 2022, la Direttiva NIS2 espande la precedente NIS del 2016, con l'obiettivo di migliorare i livelli di sicurezza informatica a livello europeo. Vengono introdotti standard minimi di sicurezza e requisiti di segnalazione degli incidenti per gli Operatori Servizi Essenziali (OSE), quali centrali elettriche o ospedali, ma anche per i fornitori di servizi digitali, quali marketplace online, motori di ricerca e servizi di Cloud Computing.

INDICE

OT SECURITY: per OT (Operational Technology) security si intende la messa in sicurezza di componenti hardware e software dedicati al monitoraggio e al controllo di processi e asset fisici prevalentemente in ambito industriale o nei settori che gestiscono infrastrutture critiche (Oil&Gas, Energy, Utilities, Telco)

RISCHIO CYBER: si definisce rischio cyber qualsiasi rischio di perdita finanziaria, interruzione di attività o danno alla reputazione di un'organizzazione derivante da violazioni ai dati o ai sistemi informatici aziendali.

SEGMENTAZIONE DELLA RETE: consiste nel separare le diverse parti di una rete per migliorare la sicurezza. Un esempio è la DMZ (Zona Demilitarizzata), una zona separata dove vengono collocati i server pubblici (come il sito web aziendale), che è protetta da firewall per ridurre il rischio di accesso non autorizzato alle risorse interne dell'azienda.

SOVRANITÀ DIGITALE: principio secondo cui l'Europa deve poter agire in modo autonomo e autodeterminato nello spazio digitale, in conformità al diritto internazionale, ai propri valori e agli interessi di sicurezza, preservando la propria indipendenza tecnologica e il controllo sui dati, e promuovendo al contempo la cooperazione con partner che condividono i valori e i principi europei.

SUPPLY CHAIN SECURITY: si fa riferimento a processi, tecnologie e competenze attraverso cui un'organizzazione gestisce e regola il rapporto con le terze parti (fornitori, partner, clienti), al fine di miti- gare i rischi e le minacce cyber derivanti dalla propria catena del valore

VIOLAZIONE INFORMATICA: violazione dei sistemi informativi, comunemente nota come "hacking", è un'attività illecita che prevede l'accesso non autorizzato a un sistema informatico al fine di ottenere informazioni sensibili o danneggiare il sistema stesso

INDICE

GRUPPO DI LAVORO

ALESSANDRO PIVA

Laureato in Ingegneria delle Telecomunicazioni e in Ingegneria Gestionale presso il Politecnico di Milano, ha poi conseguito l'Executive MBA presso la POLIMI Graduate School of Management e vanta vent'anni di esperienza nella ricerca sulla trasformazione digitale. Alla School of Management del Politecnico di Milano è Senior Director degli Osservatori Digital Innovation e coordina diversi Osservatori dedicati ai principali ambiti dell'innovazione tecnologica, tra cui Cloud Ecosystem & Digital Sovereignty, Artificial Intelligence, Cybersecurity & Data Protection, Data Center, Quantum Computing & Communication, Tech Company, Data & Decision Intelligence e Intelligent Business Process Automation. È inoltre responsabile dell'iniziativa European Digital Tech Watch, che analizza a livello internazionale l'evoluzione delle tecnologie digitali e il loro impatto su competitività, modelli di business e sovranità tecnologica. Accanto alle attività di ricerca, svolge attività di formazione executive e consulenza strategica per imprese e pubbliche amministrazioni sui temi dell'innovazione digitale.

GIORGIA DRAGONI

Laureata in Ingegneria Gestionale al Politecnico di Milano nel 2014, nello stesso anno ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e cybersecurity. Attualmente è ricercatrice sui temi della Cybersecurity & Data Protection, Direttrice dell'Osservatorio Digital Identity & Wallet (dal 2020) e dell'Osservatorio Digital & Sustainable (dal 2023). Nel 2022 ha conseguito l'Executive Master in Management presso la Polimi Graduate School of Management. È membro del Comitato Scientifico del Clusit, l'associazione italiana per la sicurezza informatica, e delle Women for Security.

NICOLA CIANI

Laureato in Business & Administration presso l'Università di Bologna, ha frequentato il percorso Executive in Digital Transformation della School of Management del Politecnico di Milano. Dal 2021 è ricercatore degli Osservatori Cybersecurity & Data Protection e Data & Decision Intelligence. Dal 2025 si occupa di ricerca e sviluppo della nuova iniziativa internazionale "European Digital Tech Watch".

IVAN ANTOZZI

Ha conseguito la laurea magistrale in Computer Science and Engineering - Ingegneria Informatica presso il Politecnico di Milano nel 2018. Un anno più tardi ha iniziato a lavorare negli Osservatori Digital Innovation occupandosi di trasformazione digitale e Cloud. Attualmente è ricercatore senior negli Osservatori Cloud Ecosystem & Sovereignty, Data Center, Cybersecurity & Data Protection e Tech Company. Ha conseguito a ottobre 2022 il Percorso Executive in Project Management e sta attualmente frequentando l'Executive Master In Management presso la Polimi Graduate School of Management.

INDICE

JACOPO POLVERINO

Laureato in Relazioni Internazionali presso l'Università di Trento, ha frequentato il percorso Executive in Digital Transformation della School of Management del Politecnico di Milano. Dal 2021 è ricercatore degli Osvervatori Cloud Ecosystem & Sovereignty e Cybersecurity & Data Protection.

ANDREA SCIMONELLI

Laureato in Economia, Finanza e Mercati Internazionali presso l'Università Cattolica del Sacro Cuore di Milano agli inizi del 2024. Da settembre dello stesso anno collabora con l'Osservatorio Cybersecurity & Data Protection e Intelligent Business Process Automation.
Da settembre 2025 ha iniziato un dottorato di ricerca in Ingegneria Gestionale presso il Politecnico di Milano, focalizzato sul tema del rischio cyber.

MARTINA BROGGI

Ha conseguito la laurea in Comunicazione e Società presso l'Università degli Studi di Milano nel 2015. Agli Osservatori Digital Innovation, dove lavora dal 2016, è Community & Event Coordinator degli Osservatori Cybersecurity & Data Protection, Data & Decision Intelligence, Artificial Intelligence e Cloud Ecosystem & Sovereignty.

ALBERTO MAFFEI

Ha conseguito la laurea in Ingegneria Gestionale presso il Politecnico di Milano nel 2024, iniziando poi a collaborare dallo stesso anno con gli Osservatori Digital Innovation della School of Management del Politecnico di Milano. Al momento è analista presso gli Osservatori Cybersecurity & Data Protection e Cloud Ecosystem & Sovereignty.

MADDALENA BRUSCAGIN

Ha conseguito la laurea magistrale in Advanced Economics presso l'École Normale Supérieure di Lione nel 2025 e collabora con gli Osservatori Digital Innovation della School of Management del Politecnico di Milano dal 2026. Attualmente è Junior Research Analyst degli Osservatori Cybersecurity & Data Protection e Artificial Intelligence.

SARA LOMBINI

Laureata in Economic and Social Sciences presso l'Università Bocconi, dal 2020 collabora con gli Osservatori Digital Innovation della School of Management del Politecnico di Milano. Attualmente è Ricercatrice dell'Osservatorio Innovazione Digitale nelle PMI e, per gli Osservatori Digital Innovation, si occupa di analisi quantitative e rilevazioni campionarie, focalizzandosi sulle dinamiche di diffusione delle tecnologie digitali nelle imprese e fra i cittadini.

INDICE

PARTNER DELL'INIZIATIVA E RIFERIMENTI

GENERALI

Generali Italia è l'assicuratore più conosciuto in Italia con oltre €32 miliardi di premi totali, 14 mila dipendenti e una rete capillare di 40 mila distributori, oltre ai canali online e di bancassurance. A Generali Italia fanno capo Alleanza Assicurazioni, Das, Genertel, Generali Welion, Generali Jeniot e Leone Alato, oltre alle attività marchio commerciale Cattolica.

La sostenibilità in Generali

Generali crede che la prosperità economica si basi su principi di giustizia sociale e di salvaguardia dell'ambiente. Per questo motivo, ritiene che la sostenibilità sia un approccio strategico necessario a favorire il business, e a creare una società sana, resiliente e sostenibile, dove le persone possano progredire e prosperare. Viene così interpretato il ruolo d'impresa responsabile che crea valore durevole per i propri stakeholder, dai collaboratori agli azionisti, dagli investitori ai clienti, dai fornitori alle istituzioni e comunità locali.

L'impegno e la responsabilità di Generali si concretizza in numerosi progetti in ambiti ad alto impatto sociale e ambientale quali, ad esempio, la Cyber-sicurezza, il Terzo Settore, l'Educazione e la Formazione, l'Arte e la Cultura, il Welfare, la Longevity e molti altri ancora.

CONFINDUSTRIA

Confindustria è la principale associazione di rappresentanza delle imprese manifatturiere e di servizi in Italia.
La mission dell'associazione è favorire l'affermazione dell'impresa quale motore della crescita economica, sociale e civile del Paese. In linea con questi principi, Confindustria definisce e condivide, nel rispetto degli ambiti di autonomia e di influenza, obiettivi ed iniziative con le Istituzioni nazionali, europee ed internazionali, con il mondo dell'economia, della politica, della ricerca, della cultura e con numerosi altri stakeholders.

Confindustria sostiene e promuove la libertà di impresa e la concorrenza nel quadro di un'economia di mercato, svolgendo un ruolo strategico nel definire le priorità politiche per rafforzare il sistema industriale e stimolare la crescita economica e sociale dell'Italia, rendendola sempre più competitiva sui mercati globali.

Il valore aggiunto di Confindustria è la sua rete, che si dirama dalla sede centrale di Roma alla Delegazione di Bruxelles, punto di riferimento per l'intero Sistema Italia presso l'Unione Europea, e alle 210 Organizzazioni associate, attive sul territorio nazionale ed estero e nei settori economici.

Il sistema di valori di Confindustria poggia sulle libertà di associazione, di iniziativa economica e di mercato, e promuove una rappresentanza unitaria, organica e strategica degli interessi delle imprese.
Costituiscono valori inderogabili la legalità e il rispetto delle regole associative ad ogni livello, e con essi una condotta etica e trasparente consona allo sviluppo di un'attività economica sana e di una società civile consapevole.

Nuove sfide tracciano costantemente le strade dello sviluppo e della crescita economica, sociale e culturale: la transizione digitale, quella energetica e quella ambientale sono tra le prioritarie.

Lo scopo di Confindustria è di affrontarle alla continua ricerca di soluzioni per lo sviluppo del sistema produttivo e per il benessere del Paese.

INDICE

OSSERVATORI DIGITAL INNOVATION – POLITECNICO DI MILANO

Gli Osservatori Digital Innovation della School of Management del Politecnico di Milano nascono nel 1999 con l'obiettivo di **fare cultura in tutti i principali ambiti di Innovazione Digitale**. Oggi sono un punto di riferimento qualificato sull'Innovazione Digitale in Italia che integra attività di **Ricerca, Comunicazione e Aggiornamento continuo**. La Vision che guida gli Osservatori è che l'Innovazione Digitale sia un fattore essenziale per lo sviluppo del Paese. La mission è produrre e diffondere conoscenza sulle opportunità e gli impatti che le tecnologie digitali hanno su imprese, pubbliche amministrazioni e cittadini, tramite modelli interpretativi basati su solide evidenze empiriche e spazi di confronto indipendenti, pre-competitivi e duraturi nel tempo, che aggregano la domanda e l'offerta di Innovazione Digitale in Italia.

Le attività di ricerca sono svolte da un team di oltre 200 tra Professori, Ricercatori e Analisti impegnati su circa 60 differenti Osservatori che affrontano tutti i temi chiave dell'Innovazione Digitale nelle Imprese (anche PMI) e nella Pubblica Amministrazione. Sono classificabili in 5 macro categorie: Innovazione tecnologica, Innovazione di settore, Innovazione di processo, Modelli di innovazione e future making, Innovazione nella società.

L'**Osservatorio Cybersecurity & Data Protection** rientra tra le "Innovazioni tecnologiche" ed è alla sua undicesima edizione. Intende rispondere al bisogno delle aziende di conoscere, comprendere e affrontare le **nuove minacce alla sicurezza informatica** supportando le aziende stesse nella scelta delle tutele più opportune, rendendole consapevoli dell'importanza del monitoraggio e del controllo delle attività e mostrando loro le tecniche e le tecnologie a **supporto della cybersecurity** adottabili.

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'Agenzia per la cybersicurezza nazionale opera a tutela degli interessi nazionali nel campo della **sicurezza e resilienza cibernetiche**, coordinando l'attuazione della Strategia Nazionale di Cybersicurezza e i soggetti pubblici coinvolti anche tramite tavoli interministeriali come il Nucleo per la cybersicurezza e i Tavoli per l'attuazione del Perimetro di sicurezza nazionale cibernetica e della disciplina NIS. ACN è anche Autorità nazionale competente e Punto di contatto unico NIS, e cura l'attuazione della nuova disciplina NIS. All'interno di ACN operano il CSIRT Italia, per attività di monitoraggio, rilevamento, analisi e risposta per prevenire e gestire attacchi ed incidenti cyber, il CVCN che effettua lo scrutinio tecnologico di beni, sistemi e servizi ICT e il Centro Nazionale di Coordinamento (NCC), che promuove la partecipazione di soggetti nazionali ai progetti finanziati dall'UE. Cura l'attuazione dell'investimento 1.5 Cybersecurity-M1C1 del PNRR per innalzare il livello di sicurezza e resilienza nazionale e svolge, inoltre, funzioni per sostenere lo sviluppo industriale e l'innovazione tecnologica del dominio cyber e per promuovere l'autonomia strategica e la sovranità tecnologica nazionale.

INDICE

CYBER INDEX PMI

RAPPORTO CYBER INDEX PMI 2025

La cultura digitale protegge la tua impresa

Promosso da:

GENERALI

CONFINDUSTRIA

Partner scientifico:

POLIMI SCHOOL OF MANAGEMENT

osservatori.net digital innovation

Partner Istituzionale:

ACN