



Allianz

THE
Ardonagh
GROUP

CHUBB®

REALE
MUTUA

ZURICH®



Charles
Taylor

Adjusting

GA
GRUPPO
AGENTI
SARA

VHV
ASSICURAZIONI

IL GOVERNO DEI RISCHI DELL'INNOVAZIONE

XIII OSSERVATORIO SULLA DIFFUSIONE DEL RISK MANAGEMENT NELLE MEDIE IMPRESE ITALIANE

Osservatorio CINEAS 2026

Sommario

PROFILO DEL CONSORZIO CINEAS	3
INTRODUZIONE DEL PRESIDENTE	5
CONTRIBUTI DEGLI SPONSOR DELL'OSSERVATORIO	8
INTRODUZIONE ALLA LETTURA.....	18
CAPITOLO 1. ELEMENTI DI SCENARIO	20
1.1 Una mappa globale dei rischi: geopolitica, mercati, cyber e clima	20
1.2 Il rischio geopolitico	21
1.3 Il rischio finanziario e di mercato	22
1.4 Il rischio cyber	23
1.5 Il rischio fisico	24
1.6 Conclusione	25
1.7 Un caso di studio: lo stretto di Hormuz	26
CAPITOLO 2. RISCHIO DI CALAMITÀ NATURALE.....	33
2.1 Principali eventi in Italia e rilevanza per le imprese	33
2.2 Sistemi di monitoraggio e rendicontazione degli obiettivi di sostenibilità.....	34
2.3 Misure di prevenzione introdotte.....	35
2.4 Efficacia percepita delle misure di prevenzione.....	37
2.5 Eventi subiti, danni e gestione del danno	37
CAPITOLO 3. INTELLIGENZA ARTIFICIALE E RISCHIO TECNOLOGICO	40
3.1 Intelligenza artificiale, rischio tecnologico e rilevanza per le imprese.....	40
3.2 Adozione dell'IA e ambiti di utilizzo.....	41
3.3 Rischi e opportunità percepiti	42
3.4 Sperimentazione e percezione di rischi e opportunità	43
3.5 Focus sulle aziende potenzialmente utilizzatrici di IA.....	44
3.6 Competenze interne in azienda	46
3.7 Formazione e sicurezza aziendale	47
CAPITOLO 4. SISTEMI DI GESTIONE DEL RISCHIO	50
4.1 Dalla consapevolezza alla gestione strutturata del rischio	50
4.2 Importanza percepita e comitati presenti in azienda	51
4.3 Bisogni a cui risponde la gestione del rischio	52
4.4 Modelli di mappatura dei rischi	52
4.5 Metodi di gestione: integrato, segmentato, in valutazione	54
4.6 Supervisione del sistema di gestione dei rischi	54
4.7 Fattori di efficacia e prospettive di investimento	55

4.8 Coperture assicurative	57
4.9 Sinistri subiti dalle aziende	59
CAPITOLO 5. FORMAZIONE AZIENDALE	61
5.1 La formazione aziendale	61
5.2 La formazione in materia di rischio	62
5.3 Tipologie di corso e temi prioritari	62
5.4 Prospettive per il prossimo anno	63

Osservatorio CINEAS 2026

PROFILO DEL CONSORZIO CINEAS

Cineas è il primo Consorzio fondato dal Politecnico di Milano nel 1987.

È un ente senza fini di lucro che si occupa di contribuire a diffondere la cultura del rischio sia attraverso **master e corsi specialistici** sui temi del risk e del claims management.

Oggi il Consorzio annovera **64 Soci** tra i quali: 6 Atenei (oltre al Polimi, l'Università degli Studi di Parma, di Pavia, di Trieste, di Torino e di Napoli Federico II), primarie compagnie assicurative a livello nazionale e internazionale, società di brokeraggio, associazioni di categoria, società di bonifica, studi professionali d'ingegneria e di loss adjusting.

Cineas ha sviluppato **partnership** strategiche con aziende leader nella gestione del rischio e della sostenibilità, tra cui **Generali Italia, Charles Taylor Adjusting, Gruppo Agenti Sara Assicurazioni e VHV assicurazioni**.

Il Consorzio collabora inoltre con numerose realtà per progettare e offrire percorsi di formazione mirati alle esigenze emergenti del mercato, tra cui **Alma Impact, Asnacodi, Borsa Italiana – Euronext, Consorzio CISE, Dipartimento della Protezione Civile e Pool Ambiente**.

Queste collaborazioni permettono a Cineas di coniugare competenze tecniche, innovazione e aggiornamento continuo, offrendo ai professionisti strumenti concreti per la gestione efficace dei rischi.

La formazione

Nel corso dell'a.a. 2025/2026 Cineas ha erogato 7 Master e 25 corsi specialistici, rivolti a professionisti già inseriti nel mondo lavoro a livello di middle e di top management e organizzati in 6 aree:

1. Risk Governance e competenze trasversali
2. Risk Management
3. Claims Management
4. Rischio in Sanità
5. Sicurezza, rischi innovazione & cyber protection
6. Rischio Climatico, Ambientale e Sostenibilità

In aggiunta ai corsi a catalogo, il consorzio è ampiamente coinvolto nella progettazione ed erogazione di iniziative formative "su misura" per le aziende, in linea con le esigenze emergenti del mondo professionale e finanziabili attraverso i fondi interprofessionali (FBA, Fondimpresa, Fondirigenti).

I percorsi di formazione di Cineas sono accreditati da molteplici Ordini e per diverse figure professionali: Avvocati, Assicuratori (**IVASS**), Ingegneri (**CNI**), Medici (**ECM**), Agronomi (**Conaf**), Periti agrari (**CNPA**), Architetti (**CNAPPC**), Periti liquidatori assicurativi (**ICMQ BU-CERSA**).

Il metodo didattico Cineas è:

- **Attivo**, basato su casi ed esempi pratici da cui ricavare i modelli teorici;
- **Esperienziale**, grazie a lezioni laboratoriali e project work sul campo, per un apprendimento pratico e per l'applicazione immediata delle competenze acquisite;
- **Innovativo**, attento ai trend emergenti di tecnologia e didattica.

La ricerca

Oltre alle attività di formazione, il Consorzio promuove la diffusione del rischio attraverso studi, pubblicazioni, white paper e protocolli operativi, in ambito ambientale, assicurativo, sanitario, industriale.

Con l'**Osservatorio sulla diffusione del risk management nelle medie imprese italiane**, Cineas monitora ogni anno la maturità delle PMI nella gestione dei rischi, producendo report dettagliati e strumenti di analisi utilizzabili da aziende e operatori del settore.

Tra gli studi e le pubblicazioni più recenti, si ricordano:

- Il manuale **ISPRA CINEAS per la prevenzione e la gestione del danno ambientale in casi di incendio presso gli impianti di gestione dei rifiuti** (2022), coordinato dall'ing. Aldo Rebuffi;
- White Paper: **L'assicurazione delle calamità naturali e delle pandemie** (2023), coordinato dall'Ing Ginocchietti;
- **'Il rischio delle calamità naturali in Italia: conoscere, stimare e gestire'** (2025), coordinato da Ing. Massimo Fedeli;
- Protocollo d'intervento: **Coordinamento Interventi Grandi Eventi da calamità naturali** (2025), coordinato dal dott. Omar El Idrissi;
- Atti del convegno sulla **Gestione dei rischi in sanità** (2025), consistente in uno studio dedicato al tema della Sicurezza degli ospedali e delle Assicurazioni, coordinato dal prof. Gustavo Galmozzi.

Il Consorzio partecipa inoltre a **progetti nazionali e internazionali** ad alto contenuto innovativo, integrando il risk management in tematiche come sviluppo sostenibile, economia circolare e adattamento ai cambiamenti climatici.

A livello nazionale, Cineas è tra i soci fondatori di **ASVIS – Alleanza Italiana per lo sviluppo sostenibile**, in base agli obiettivi ONU 2030.

Cineas mette a disposizione dei professionisti anche strumenti tecnici di supporto operativo. Tra questi rientra il software **CINEAS-CRESME**, una soluzione aggiornata e affidabile per la determinazione delle somme assicurate e la stima dei costi di costruzione degli edifici civili e industriali.

Il **Sistema di Gestione della Qualità** di Cineas è conforme a quanto previsto dalla norma UNI EN ISO 9001-2015 per l'organizzazione di corsi in risk e claims management e per l'accreditamento alle figure professionali di riferimento (settore IAF 37).

Gli eventi

Cineas si distingue non solo per la formazione accademica ma anche per il suo impegno attivo nella diffusione della cultura del rischio attraverso eventi, convegni e webinar aperti a professionisti, imprese e istituzioni.

Tra gli eventi recenti:

- Webinar: **Catastrofi naturali: quando la natura colpisce, il perito decide** — maggio 2026;
- Convegno: **Governance d'impresa e rischi esistenziali: il ruolo del CdA nelle imprese medie italiane** — maggio 2026;
- Evento formativo: **CdA sotto esame: i nuovi rischi della governance** — marzo 2026;
- Evento formativo: **Governare il rischio in sanità: modelli, errori, soluzioni** — marzo 2026;
- Webinar: **Contaminanti emergenti e responsabilità ambientale** — gennaio 2026;
- **Convegno sulla gestione dei rischi in sanità** — maggio 2025;
- **XII Osservatorio sulla diffusione del Risk Management nelle medie imprese italiane** — maggio 2025.

INTRODUZIONE DEL PRESIDENTE



Massimo Michaud

Presidente di CINEAS

Anche quest'anno l'Osservatorio sul Risk Management del CINEAS presenta l'evoluzione della gestione dei rischi da parte delle imprese del nostro Paese. L'indagine, realizzata su un campione rappresentativo di 380 medie imprese italiane, consente di osservare come stiano evolvendo la percezione, la governance e gli strumenti di gestione dei principali rischi che incidono sulla continuità e sulla competitività delle aziende.

Dopo aver dedicato nell'edizione precedente un'attenzione particolare ai rischi da catastrofi naturali, per i quali la normativa ha introdotto l'obbligo di assicurazione per le imprese, l'edizione di quest'anno è stata dedicata ai rischi tecnologici e, in particolare, a quelli connessi alla diffusione dell'intelligenza artificiale nei processi aziendali.

Il CINEAS ha dedicato negli ultimi anni una particolare attenzione alla categoria dei "rischi esistenziali", ovvero di quei rischi che debbono essere evitati o disinnescati nella maniera più assoluta dalle imprese in quanto possono mettere a repentaglio la loro sopravvivenza, l'incolumità dei loro collaboratori o delle comunità dove operano. Si tratta di un tipo di rischio talmente rilevante che deve essere conosciuto e trattato dagli organi di governo dell'impresa, primo fra tutti il Consiglio di Amministrazione.

La ricerca di quest'anno evidenzia **come questi rischi non agiscano più come fenomeni indipendenti. Instabilità geopolitica, tensioni commerciali, cyber risk, cambiamento climatico e trasformazione tecnologica tendono sempre più a rafforzarsi reciprocamente**, generando effetti simultanei sulle catene di fornitura, sui costi, sulla continuità operativa e sulla capacità di pianificazione delle imprese. In questo contesto, il tema centrale non è soltanto l'aumento dei rischi, ma la loro crescente interdipendenza.

Alcune recenti pronunce della magistratura hanno riportato in primo piano il tema della responsabilità dei vertici aziendali nel caso di gravi eventi. Difficilmente nei grandi gruppi i principali dirigenti possono prevedere ogni possibile evento dannoso; tuttavia, essi sono chiamati a creare e presidiare il sistema di prevenzione dei rischi dimostrando una capacità di reazione immediata ove emergano nuovi rischi e potenziali pericoli. Questo vale in particolare in un contesto nel quale i rischi tendono a propagarsi attraverso filiere, mercati, infrastrutture tecnologiche e sistemi informativi.

La nostra ricerca segue da molti anni il coinvolgimento del Consiglio di Amministrazione nella gestione dei rischi e la sua attività volta a prevenire i rischi esistenziali. L'atteggiamento è ancora per lo più reattivo, anche se si colgono segnali di miglioramento. A fronte di un utilizzo della mappatura dei rischi piuttosto diffuso, che interessa quasi due terzi del campione e tre quarti delle imprese più grandi, l'esame e la discussione sui rischi in Consiglio è relegata, secondo quanto dichiarato, a meno di un terzo delle imprese. Conforta, invece, che oltre la metà

delle imprese intervistate abbiano costituito un Comitato endoconsiliare Controlli e Rischi. La sfida non consiste quindi soltanto nell'identificare i rischi, ma nel portarli stabilmente all'attenzione degli organi di governo affinché influenzino decisioni, investimenti e priorità aziendali.

In ogni caso, a fronte delle vicende più recenti, la consapevolezza su rischi che possono assumere un carattere "esistenziale" è sempre più diffusa: interruzione delle catene di fornitura, dazi e aumento dei costi delle merci, catastrofi naturali e rischi cibernetici sono considerati sempre più importanti e ricevono un'attenzione crescente.

La ricerca mostra tuttavia che la crescita della consapevolezza procede spesso più rapidamente della piena integrazione dei rischi nei sistemi di governo, nei programmi di prevenzione, nelle coperture assicurative e nei processi decisionali. Permane quindi un divario tra la rilevanza attribuita a molti rischi emergenti e la capacità delle organizzazioni di tradurre tale consapevolezza in strumenti effettivi di protezione.

Lo sviluppo delle tecnologie e, in particolare, l'adozione crescente dell'intelligenza artificiale, che è stata introdotta da due terzi del campione, si accompagna con alcuni fenomeni particolari:

- l'emergere di una sensibilità crescente verso i rischi legali e normativi, la protezione dei dati e la sicurezza delle informazioni;
- la classificazione dei rischi tecnologici nell'ambito dei rischi "strategici" e non più soltanto operativi;
- l'ampliamento delle funzioni coinvolte nella prevenzione, precedentemente confinata alla funzione ICT, e il presidio della governance, della proprietà intellettuale dei dati e delle informazioni, delle forme di protezione possibili, tra cui quella assicurativa, e dell'impatto sulla conformità normativa, che richiedono il coinvolgimento di molte funzioni aziendali;
- il riconoscimento del gap esistente tra la diffusa adozione delle tecnologie e la limitata disponibilità di competenze interne per poterle gestire, con il corollario della necessità di valutare la qualità dei fornitori esterni di tecnologia;
- la crescente attenzione alla definizione di regole interne, alla supervisione umana dei processi automatizzati e alla responsabilità finale delle decisioni supportate dall'intelligenza artificiale.

L'esperienza delle imprese che hanno già adottato l'intelligenza artificiale dimostra che le principali preoccupazioni riguardano sia la sostituzione del lavoro umano sia, e sempre di più, la governance, la protezione dei dati, le responsabilità legali, qualità dei partner tecnologici e la capacità di integrazione organizzativa.

Proprio in virtù di questa ultima constatazione **emerge la domanda di una formazione adeguata.** Presente in circa tre quarti delle imprese, **essa viene sempre più percepita non come una semplice attività di aggiornamento professionale, ma come una componente essenziale del sistema di prevenzione e della capacità di gestione dei rischi dell'organizzazione.** La diffusione di nuove tecnologie, l'evoluzione normativa e la crescente complessità dei rischi richiedono infatti competenze trasversali in materia di governance, compliance, cybersecurity, gestione del rischio e continuità operativa.

Per affrontare questa esigenza, CINEAS ha sviluppato da alcuni anni l'area didattica "Rischi della Tecnologia" ed ha inserito nella maggior parte dei suoi insegnamenti lezioni su questa categoria di rischio. Questa scelta è coerente con la sua missione di diffusione della cultura del rischio e con l'obiettivo di supportare lo sviluppo delle competenze necessarie per governare fenomeni sempre più rilevanti per la continuità e la competitività delle imprese.

Dalla ricerca emerge, in conclusione, che in un mondo nel quale il livello dei rischi è in crescita e le imprese sono sottoposte a rischi sempre nuovi, quindi caratterizzato da incertezza crescente, **la competenza di gestione del rischio – di prevenzione, mitigazione e gestione delle crisi – diventa sempre più importante e la gestione dei rischi non può essere delegata solo alle strutture tecniche,** ma rappresenta una delle attività fondamentali di governo dell'impresa e deve poter contare su competenze adeguate in materia.

La trasformazione più significativa che emerge dall'Osservatorio è il progressivo passaggio del rischio da tema prevalentemente operativo a tema di governance. Questo cambiamento appare particolarmente evidente per i rischi tecnologici e per l'intelligenza artificiale, ma riguarda più in generale tutti quei rischi che possono assumere una dimensione esistenziale per l'impresa. In un contesto caratterizzato da rischi sempre

più interconnessi, la responsabilità degli organi di amministrazione non consiste soltanto nel reagire agli eventi avversi, ma nel promuovere una capacità diffusa di anticipazione, prevenzione e resilienza. La gestione dei rischi esistenziali diventa così una componente essenziale del governo dell'impresa e una condizione sempre più importante per garantirne la continuità, la competitività e la sostenibilità nel tempo.

CONTRIBUTI DEGLI SPONSOR DELL'OSSERVATORIO



Valentina Di Marco

Head of Property -Mid Corporate -Brokers & Multinational

Allianz Italia

www.allianz.it



Gennaro Petito

Responsabile Commercial Line Property & Engineering

Allianz Italia

www.allianz.it

La XIII edizione dell'Osservatorio sul Risk Management nelle Medie Imprese Italiane, curata da CINEAS e Prometeia per il 2026, ci restituisce una fotografia nitida e dettagliata di come il tessuto produttivo del nostro Paese stia imparando a muoversi all'interno di un panorama globale dominato da quella che ormai viene definita una vera e propria "policrisi".

Oggi le imprese non si trovano più a fronteggiare minacce isolate, ma un intreccio continuo e simultaneo di shock geopolitici, fluttuazioni finanziarie, attacchi cibernetici ed eventi climatici estremi che mettono a dura prova la stabilità delle filiere e i costi operativi.

In questo scenario di forte volatilità, l'instabilità geopolitica e il ritorno delle barriere commerciali, a partire dalle recenti politiche sui dazi, rappresentano la preoccupazione principale per un'azienda su quattro.

Per rispondere a queste sfide, la priorità strategica delle medie imprese si è concentrata sulla tutela della continuità operativa.

Questo si traduce in un impegno diffuso per diversificare i mercati di sbocco, rendere le catene di fornitura più flessibili e resilienti, e proteggere l'infrastruttura aziendale dai rischi informatici e ambientali.

Sul fronte della sostenibilità, il report evidenzia un salto di qualità importante nella maturità organizzativa.

Quasi sette imprese su dieci hanno già integrato sistemi di monitoraggio ESG, spinte sia dall'adeguamento normativo sia dalla necessità di proteggersi dai rischi fisici e di transizione energetica.

Tuttavia, la gestione del rischio climatico mostra ancora qualche ombra: sebbene circa tre quarti delle aziende adottino misure preventive o coperture assicurative, tra quel 21% di imprese che ha subito danni da eventi meteo estremi, un terzo è risultato del tutto privo di tutele al momento dell'impatto, evidenziando come la cultura della protezione vada ulteriormente rafforzata.

Una delle trasformazioni più profonde riguarda l'introduzione dell'Intelligenza Artificiale, che coinvolge ormai due terzi delle imprese analizzate, con punte che sfiorano il 70% tra le realtà di maggiori dimensioni.

L'IA si sta integrando rapidamente nella produzione, nella progettazione e nella gestione dei clienti. Curiosamente, chi ha già avviato l'uso pratico di queste tecnologie tende a percepirne soprattutto i benefici operativi, mentre i timori sfumano.

Il vero nodo critico resta però il fattore umano: soltanto il 14% delle aziende ritiene di possedere competenze interne sufficienti a gestire i rischi connessi all'IA.

La privacy, la protezione dei dati e la sicurezza informatica emergono così come i campi in cui serve il maggiore sforzo di aggiornamento.

Per affrontare questa complessità, la gestione del rischio sta smettendo di essere un semplice adempimento formale per trasformarsi in una vera leva strategica guidata dal vertice aziendale.

Aumentano le imprese che formalizzano la mappatura dei rischi a livello di Consiglio di Amministrazione e si consolida il ruolo del Risk Manager.

A fare da collante in questo percorso di crescita è la formazione: la grande maggioranza delle aziende promuove corsi interni e ha intenzione di confermare o aumentare gli investimenti nelle competenze.

In definitiva, l'Osservatorio 2026 ci mostra un'imprenditoria italiana dinamica che, di fronte all'incertezza globale, sceglie di investire sulla preparazione e sulla governance per trasformare la prevenzione in un fattore chiave di competitività.



Gianluca Iulianello

Sales Manager, Direzione commerciale

Ardonagh Italia

www.ardonagh.com

L'intelligenza artificiale corre. Il governo del rischio deve tenere il passo

I risultati della XIII Edizione dell'Osservatorio restituiscono un'immagine nitida: nelle medie imprese italiane l'intelligenza artificiale non è più una promessa, ma una componente dell'operatività. Nel 2026 il 66% delle aziende dichiara di averla già utilizzata, sei punti in più rispetto all'anno precedente. Produzione, progettazione, controllo qualità e customer care sono i primi terreni di applicazione. La domanda decisiva è: la capacità di governo cresce alla stessa velocità dell'adozione?

La risposta suggerita dai dati è prudente. Nel focus sulle imprese più vicine all'IA, il 69% ne dichiara un uso concreto, mentre il 61% si considera preparato. Solo 7 aziende su 52 ritengono pienamente adeguate le proprie competenze. È il tratto delle tecnologie che entrano in azienda attraverso singole funzioni, fornitori o strumenti online, prima che policy, ruoli e controlli siano definiti.

Anche la natura dei timori sta cambiando. La sicurezza dei dati, indicata dal 31%, supera la sostituzione del lavoro umano; seguono le questioni legali. E chi ha già sperimentato l'IA teme più degli altri responsabilità, capacità di adattamento, cultura manageriale e inadeguatezza dei partner tecnologici. L'esperienza, quindi, non riduce la percezione del rischio: la rende più concreta. Sposta l'attenzione dall'algoritmo alla qualità delle decisioni, dalla tecnologia alla governance.

È qui che l'Osservatorio offre l'indicazione più utile. Il 62% delle imprese dispone di una mappatura dei rischi a livello di CdA e il 75% ha un metodo di gestione; tuttavia, nel 41% dei casi il modello resta segmentato e solo nel 35% è integrato. Per rischi interdipendenti questo divario pesa: un errore dell'IA può diventare violazione di dati, fermo operativo, danno reputazionale e responsabilità verso terzi. Non basta affidarlo all'IT o alla sola compliance.

Governare l'IA significa stabilire quali strumenti siano ammessi, quali dati possano essere utilizzati, come verificare gli output, chi conservi la supervisione umana e come selezionare i fornitori. Significa anche prepararsi all'incidente: continuità operativa, risposta cyber, gestione della crisi e trasferimento assicurativo devono essere progettati insieme. La copertura cyber, presente nel 42% delle imprese nonostante il 15% abbia subito un sinistro negli ultimi 24 mesi, segnala uno spazio di protezione ancora rilevante. Ma una polizza efficace nasce da un rischio conosciuto, misurato e presidiato, non sostituisce la prevenzione.

Per Ardonagh Italia, il messaggio è chiaro: l'intermediario evoluto deve affiancare l'impresa prima del contratto, traducendo innovazione e vulnerabilità in scenari, priorità e soluzioni sostenibili. L'IA crea valore quando accelera i processi senza rendere invisibile la responsabilità. La vera maturità digitale non consiste nell'adottarla per primi, ma nel saperla governare prima che sia il rischio a dettare le regole.



Orazio Rossi

Country President Italy

Chubb

www.chubb.com

Dalla consapevolezza all'azione: colmare il gap tra percezione del rischio e protezione.

Leggere i risultati della XIII edizione dell'Osservatorio sul risk management nelle medie imprese italiane è un esercizio che va ben oltre l'analisi di dati e percentuali. È uno specchio fedele di un sistema imprenditoriale che attraversa una delle stagioni più complesse della storia recente.

Il contesto globale non lascia spazio all'indifferenza: il costo degli attacchi Cyber ha raggiunto i 10,5 trilioni di dollari; le perdite da eventi meteo climatici estremi si attestano a 2,3 trilioni; la spesa militare globale raggiunge i 2,9 trilioni; mentre i dazi USA di aprile 2025 hanno bruciato 2,5 trilioni di capitalizzazione. Le interconnessioni tra rischi geopolitici, fisici, tecnologici e finanziari non sono più eccezionali: sono strutturali.

Le medie imprese italiane lo percepiscono. Il 62% ha introdotto un modello di mappatura dei rischi a livello di CdA (vs 59% nel 2025), il 75% si avvale di figure dedicate e il 72% ha già in programma attività di formazione, con normative di settore e cybersecurity in cima ai temi trattati. Segnali che confermano come la cultura del rischio stia diventando parte del DNA aziendale.

Un capitolo merita attenzione particolare: le calamità naturali. Il 74% delle imprese ha adottato misure di prevenzione (vs 69% nel 2025) e le catastrofi naturali rappresentano la terza voce di budget assicurativo (18,4%). Tuttavia, un'azienda su cinque ha già subito un danno e tra queste un terzo non aveva alcuna copertura. I danni riguardano strutture e attrezzature (41%), interruzione dell'attività (28%) e pericoli per il personale (28%): conseguenze che minacciano direttamente la continuità operativa.

Analogo gap tra percezione e copertura si registra sul Cyber: solo il 42% è assicurato, nonostante il rischio sia amplificato dall'Intelligenza Artificiale, che ha moltiplicato scala e sofisticazione degli attacchi (come documentato anche nel Chubb Cyber Claims Report 2026) e il 58% abbia già subito almeno un sinistro. Sul fronte IA, il 66% ne ha sperimentato l'utilizzo; le opportunità prevalgono sui timori, ma protezione dei dati, formazione del personale e difesa da attacchi Cyber guidano le preoccupazioni. Ignorare l'IA non è un'opzione; governarla è una necessità.

Il valore di una compagnia assicurativa si misura sempre più sulla capacità di affiancare il cliente prima che il danno accada, mettendo al centro la continuità operativa, non solo la liquidazione del sinistro. Le imprese italiane stanno investendo con stabilità nella gestione strutturata del rischio: il nostro compito è essere degni di questa fiducia, traducendo scenari complessi in soluzioni assicurative accessibili a imprese di ogni dimensione. Il rischio è la condizione naturale di ogni impresa che cresce; la vera differenza la fanno la capacità di gestirlo con visione, metodo e i partner giusti al proprio fianco.



Andrea Paoli

Funzionario ufficio assunzioni Corporate e Multirischio, Direzione Beni e Patrimonio

Italiana Assicurazioni

Gruppo Reale Mutua

www.realemutua.it

Risk management, dall'emergenza alla strategia: cosa ci dice l'Osservatorio Cineas 2026

L'Osservatorio Cineas 2026 sul risk management nelle medie imprese italiane racconta un Paese imprenditoriale che sta prendendo coscienza di una realtà ormai evidente: il rischio non è più un'eccezione da gestire quando si manifesta, ma una dimensione permanente del fare impresa. Dalle tensioni geopolitiche alle calamità naturali, dalla cybersecurity all'intelligenza artificiale, il panorama competitivo è diventato più complesso, volatile e interconnesso.

Non sorprende quindi che, tra le principali sfide percepite dalle imprese per i prossimi dodici mesi, figurino la diversificazione dei mercati, la continuità delle forniture, la riduzione dell'impatto ambientale e la protezione informatica. I rischi emergenti non sono più considerati fenomeni separati, ma fattori che influenzano direttamente la capacità di generare ricavi, preservare margini e mantenere la competitività. Il tutto però nella speranza che tutte queste consapevolezze si concretizzino in assicurazioni mirate e non solo di mera consapevolezza in assenza di concretezza assicurativa.

Geopolitica: il rischio che entra nei conti economici

Il rischio geopolitico è percepito come una delle principali minacce per il sistema produttivo. Le guerre in corso, la frammentazione delle relazioni commerciali internazionali e l'incertezza legata alle politiche economiche delle grandi potenze stanno modificando le strategie aziendali.

Le imprese italiane associano all'evoluzione della politica commerciale degli Stati Uniti conseguenze molto concrete: aumento dei costi delle importazioni, volatilità dei mercati, riduzione delle esportazioni e necessità di diversificare gli sbocchi commerciali. Un'azienda su quattro considera già le politiche tariffarie statunitensi un rischio significativo per il proprio business.

Si tratta di un cambio di prospettiva importante. Fino a pochi anni fa la geopolitica era percepita come una variabile distante; oggi entra direttamente nella gestione della supply chain, delle materie prime, dell'energia e degli investimenti.

Cambiamento climatico: dalla sostenibilità alla resilienza

Un altro dato particolarmente rilevante riguarda il rischio climatico. Il 68% delle imprese dispone di sistemi di monitoraggio e rendicontazione degli obiettivi di sostenibilità, mentre circa il 18% ha introdotto strumenti specifici per monitorare i rischi derivanti dai cambiamenti climatici.

L'aspetto più significativo è però legato all'esperienza diretta: un'impresa su cinque dichiara di aver subito danni causati da eventi naturali estremi. Tra i danni più frequenti emergono quelli alle strutture e alle attrezzature, le interruzioni produttive e i rischi per il personale.

La risposta delle aziende appare sempre più orientata alla prevenzione. Il 74% ha adottato misure specifiche di mitigazione, dalle coperture assicurative agli interventi strutturali, dai piani di continuità operativa alla formazione

del personale. Inoltre, oltre tre quarti delle imprese che hanno implementato tali misure ne riconoscono l'efficacia.

Il messaggio è chiaro: la gestione del rischio climatico non può limitarsi alla compensazione dei danni. Diventa fondamentale costruire resilienza organizzativa prima che l'evento si verifichi.

L'intelligenza artificiale non è più un esperimento

Molto interessante è il rapporto che riguarda l'adozione dell'intelligenza artificiale. Il 66% delle medie imprese italiane ha già utilizzato applicazioni di IA nei propri processi aziendali, con un aumento rispetto all'anno precedente. Gli utilizzi più diffusi riguardano l'automazione dei processi produttivi, la progettazione, il monitoraggio delle performance e il customer care.

L'Osservatorio mostra che la diffusione dell'IA modifica profondamente la percezione del rischio. Le aziende che hanno sperimentato queste tecnologie tendono a essere meno diffidenti e più consapevoli delle opportunità offerte. Tra i principali vantaggi vengono citati l'efficienza organizzativa, la velocità nell'elaborazione dei dati e il miglioramento dei processi produttivi.

L'altra faccia della medaglia riguarda però la gestione dei nuovi rischi. La protezione dei dati, la cybersecurity, le questioni normative e la necessità di nuove competenze figurano tra le principali preoccupazioni. Non a caso, nel focus dedicato alle aziende più strutturate emerge che solo una minoranza ritiene di possedere competenze pienamente adeguate per governare l'IA, mentre molte imprese stanno investendo in programmi di formazione per colmare il gap.

La lezione è evidente: l'intelligenza artificiale non è soltanto una tecnologia da adottare, ma un cambiamento organizzativo da governare.

Risk management: cresce la maturità delle imprese

L'indagine registra un'evoluzione positiva nella diffusione dei sistemi di gestione del rischio. Il 62% delle aziende dispone oggi di un modello di mappatura dei rischi a livello di Consiglio di amministrazione, mentre il 75% ha implementato un metodo strutturato di gestione dei rischi.

Anche il ruolo del Risk Manager si consolida, diventando la figura più frequentemente incaricata della supervisione del sistema di gestione dei rischi. Parallelamente aumenta la consapevolezza che l'efficacia del risk management dipenda dall'integrazione con le altre funzioni aziendali, dalla disponibilità di dati e dalla presenza di personale specializzato.

Permane tuttavia una contraddizione. Oltre la metà delle imprese continua a considerare il risk management meno importante rispetto allo sviluppo del business. È una visione che riflette una cultura ancora in transizione, nella quale la gestione del rischio viene talvolta percepita come un costo piuttosto che come un fattore di creazione del valore.

Eppure il rapporto dimostra l'esatto contrario: le imprese che identificano tempestivamente i rischi, investono in prevenzione e integrano la gestione dell'incertezza nei processi decisionali sono quelle più preparate ad affrontare scenari complessi.

Assicurazioni: nuove priorità per nuovi rischi

Sul fronte assicurativo emerge un progressivo adeguamento delle coperture ai rischi contemporanei. Le imprese detengono in media quasi sette coperture assicurative e destinano quote crescenti di budget alle catastrofi naturali e al cyber risk.

Accanto alle tradizionali coperture per incendio e infortuni sul lavoro, aumentano l'attenzione verso i rischi digitali, ambientali e geopolitici. Non si tratta di una semplice evoluzione del mercato assicurativo, ma della presa d'atto che i danni più significativi del futuro potrebbero derivare da eventi diversi da quelli storicamente considerati prioritari.

Formazione: la prima linea di difesa

Un elemento trasversale a tutto il report è il ruolo della formazione. Il 72% delle imprese ha in programma attività formative dedicate ai rischi aziendali e il 75% intende mantenere o rafforzare questi programmi nel prossimo anno. I temi più trattati riguardano la normativa di settore, la cybersecurity, le nuove tecnologie e la sostenibilità.

È forse questo il segnale più incoraggiante dell'indagine. In un contesto caratterizzato da trasformazioni rapide e spesso imprevedibili, la competenza diventa il primo strumento di mitigazione del rischio. L'innovazione tecnologica, la conformità normativa e la sicurezza non possono essere delegate esclusivamente a procedure o polizze assicurative: richiedono persone preparate e organizzazioni capaci di apprendere.

Una nuova cultura dell'impresa

L'Osservatorio Cineas 2026 fotografa quindi un sistema imprenditoriale che sta maturando. Le imprese italiane non ignorano più l'incertezza: la studiano, la monitorano e iniziano a integrarla nelle proprie strategie.

La sfida dei prossimi anni sarà trasformare definitivamente il risk management da funzione specialistica a leva strategica. In un mondo in cui shock geopolitici, crisi climatiche, attacchi cyber e rivoluzioni tecnologiche possono modificare in pochi giorni gli equilibri di mercato, la capacità di anticipare i rischi diventa un vantaggio competitivo tanto importante quanto l'innovazione o la crescita commerciale.

Le imprese che sapranno comprendere questa trasformazione non si limiteranno a sopravvivere all'incertezza; saranno quelle che riusciranno a prosperare proprio grazie alla loro capacità di governarla.



Francesco Semprini

Direttore Generale

VHV assicurazioni

www.vhv.it

Il rischio è da sempre parte integrante dell'esistenza dell'uomo. Valutarlo in modo corretto e decidere se ed in che misura accettarlo può determinare l'esito più o meno favorevole di qualsiasi azione. Si può obiettare che per quanto accurata sia la stima di un rischio esistono fatti imponderabili nei confronti dei quali qualsiasi decisione o azione dell'uomo sia vana. In realtà anche nei confronti dei così detti Atti di Dio è possibile agire in modo preventivo limitando le conseguenze di un evento avverso.

Fatta questa premessa, che pone le basi per affrontare i rischi non con un approccio fatalista ma con metodologie razionali, dallo studio condotto dall'Osservatorio ed in particolare riferendosi ai capitoli relativi ai sinistri si può notare come la tipologia degli stessi sia in gran parte riconducibile agli stessi eventi quali incendio, calamità naturali, danni di varia natura causati a terzi quindi a fatti sia causati dell'uomo sia da catastrofi naturali. Fatti garantiti da più o meno adeguate coperture assicurative in misura più o meno ampia a seconda della sofisticazione delle analisi svolte in fase di prevenzione. In questi casi le garanzie prestate dagli assicuratori e riassicuratori hanno operato in base ai così detti termini, condizioni e franchigie e limiti in base ai quali è stato trasferito il rischio al mercato assicurativo a fronte di un premio. L'analisi costi benefici dirà poi se questo processo sia stato fatto in modo corretto.

Queste procedure, i cui fondamenti hanno contrassegnato l'industria assicurativa per decenni, sono nella loro essenza ancora valide ma devono essere adeguate di fatto all'evoluzione tecnologica, industriale, finanziaria e nella sostanza alla globalizzazione che sta imponendosi con un'avanzata inarrestabile in tutti i settori produttivi, del commercio ed in generale nella vita umana nel suo più ampio spettro.

I risultati dell'osservatorio, che confermano quanto già riscontrato da indagini svolte da alcuni dei più noti istituti di ricerca quale ad esempio il Swiss Re Institute, confermano che i rappresentanti dell'industria temono i così detti rischi emergenti, che è ridondante elencare in quanto ben illustri nella ricerca, pur esprimendo attenzione nei confronti dei rischi classici (che sono per altro come già detto causa della stragrande maggioranza dei sinistri sia di frequenza che di magnitudo).

Ora a mio giudizio l'individuazione e valutazione della magnitudo dei rischi emergenti è solo il primo passo di un percorso evolutivo che l'industria, intesa nel termine più ampio, deve avviare in stretta collaborazione con il mercato assicurativo per definire quanto è già stato fatto in passato: delimitare le adeguate protezioni finanziarie (coperture assicurative) in un giusto equilibrio tra costo e beneficio. Facile a dirsi molto più difficile da farsi.

Uno strumento importantissimo, se utilizzato in modo adeguato, sarà la AI di cui tanto si parla in ogni contesto appena ce ne sia anche solo la minima occasione. Si tratta però di usare lo strumento e non di farsi usare.



Lucio Silvio Casati

Head ZRS Zurich Resilience Solutions Italy

Zurich Insurance Group in Italia

www.zurich.it

Risk management e sostenibilità: una tensione virtuosa da trasformare in vantaggio competitivo

Risk management e sostenibilità sono a volte descritti come mondi separati: il primo focalizzato sulla protezione del valore nel breve periodo, la seconda orientata alla creazione di impatti positivi nel lungo termine.

Dall'Osservatorio sulle dinamiche del risk management nelle Medie Imprese italiane emerge che il 32% delle imprese non ha ancora compiuto il passaggio verso la sostenibilità, segno che la prevenzione viene spesso penalizzata quando i suoi benefici non sono immediatamente visibili o misurabili.

In realtà, sono due facce della stessa medaglia e, se ben integrate, diventano un potente fattore abilitante per il successo futuro delle aziende.

La difficoltà sta nel gestire la tensione tra orizzonti temporali diversi, approcci culturali differenti e priorità che cambiano nel tempo.

La ricerca condotta per conto di CINEAS fotografa bene questa tensione di orizzonte temporale: se nel medio e lungo termine i rischi più temuti riguardano soprattutto il cambiamento climatico (monitorati dal 18% delle imprese, ma i rischi fisici correlati, dal 52% delle imprese), nel breve dominano, tra gli altri, guerre, instabilità geopolitica, oscillazioni finanziarie e la loro simultaneità.

Il fatto che nel breve si temano soprattutto rischi geopolitici non significa che clima e ambiente siano meno importanti, ma evidenzia che, per concentrarsi su questi, occorre prima gestire le minacce più impellenti.

Il risk management nasce per ridurre i rischi e salvaguardare il valore aziendale nel breve e medio periodo: in pratica significa contenere costi, evitare interruzioni operative, proteggere asset e stabilità finanziaria.

La sostenibilità, invece, richiede investimenti di lungo termine, che spesso appaiono rischiosi o poco redditizi nell'immediato: nuovi materiali, tecnologie innovative, trasformazioni organizzative.

Le risorse – finanziarie, di tempo, di competenze – sono spesso non infinite, e la tensione si manifesta quando obiettivi ambiziosi di sostenibilità sembrano aumentare il rischio operativo o finanziario nel breve.

A questa differenza di prospettiva si aggiunge un diverso rapporto con l'innovazione: il risk management tende a privilegiare soluzioni collaudate, riducendo il ricorso a tecnologie non pienamente testate. La sostenibilità, al contrario, spinge verso innovazioni a volte più radicali, necessarie per ridurre l'impatto ambientale o sociale.

Il risultato è un apparente conflitto: ciò che è innovativo e sostenibile può essere percepito come "rischioso" dal punto di vista tradizionale.

Questa distanza di prospettiva genera spesso incomprensioni quasi “semantiche”: è come pensare di ridurre il rischio di allagamenti intervenendo solo sulle cause climatiche, a lungo termine, ma dimenticando le azioni di protezione immediata, come la costruzione di argini e difese strutturali.

Il punto non è scegliere tra breve e lungo periodo, ma comprendere che servono entrambi: misure di mitigazione immediata e strategie strutturali di trasformazione.

Il collegamento tra risk management e sostenibilità è però oggi riconosciuto come centrale per il successo futuro delle aziende poiché il successo attuale non garantisce automaticamente il successo futuro.

L'equilibrio tra i due approcci passa però dalla consapevolezza che ogni decisione strategica – anche in ambito sostenibilità – può generare rischi collaterali che vanno conosciuti, ponderati e gestiti.

Se ad esempio un'azienda decidesse di ridurre l'impatto ambientale puntando sul risparmio energetico, potrebbe pensare ad un isolamento a cappotto in polistirolo sul building più strategico, pannelli fotovoltaici in copertura, conversione dell'intero parco auto alla trazione elettrica con colonnine di ricarica in autorimessa interrata.

L'intento è corretto, l'obiettivo nobile, ma la soluzione è potenzialmente pericolosa: il polistirolo è un materiale “fast burning”, i pannelli fotovoltaici sul tetto possono diventare fonti di innesco, le colonnine di ricarica in spazi chiusi espongono al rischio di incendi di batterie al litio difficili da gestire.

La risposta non è rinunciare alla sostenibilità, ma integrarla con la consapevolezza dei rischi: nella fattispecie coibentazione in lana di roccia, pannelli fotovoltaici isolati dalla copertura o installati a terra, colonnine di ricarica all'esterno.

In altre parole, perseguire gli obiettivi ESG senza dimenticare i rischi collaterali e progettando soluzioni sicure.

Può il risk management contribuire anche allo sviluppo di prodotti e servizi sostenibili?

La risposta è sì, a condizione di creare un percorso virtuoso di mutua collaborazione tra funzioni di sostenibilità e risk management: la sostenibilità porta alla luce nuovi rischi ambientali, sociali, reputazionali e normativi, che il risk management può affrontare in modo strutturato, prevenendo crisi future.

Le aziende che integrano le due dimensioni sono più capaci di adattarsi alle evoluzioni del mercato, alle nuove normative e alle aspettative di clienti e stakeholder, diventando più resilienti: una sostenibilità integrata nella gestione del rischio non si limita a proteggere, ma apre opportunità, nuovi mercati, nuovi clienti, partnership strategiche, reputazione più forte.

La chiave è abbandonare la visione rischio vs sostenibilità, e costruire un approccio integrato, in cui ogni decisione sostenibile sia progettata con consapevolezza dei rischi, e ogni analisi di rischio tenga conto del valore che la sostenibilità può generare nel lungo periodo.

INTRODUZIONE ALLA LETTURA

L'Osservatorio sulle dinamiche del risk management nelle Medie Imprese italiane 2026 presenta alcune novità di metodo e di contenuto cui occorre dare evidenza per agevolare la lettura ed il confronto con le precedenti edizioni.

La **prima novità** riguarda un aspetto di metodo relativo alla rimodulazione del campione intervistato. Il campione è concentrato sulle imprese di media dimensione ovvero con addetti compresi fra 50 e 499. La focalizzazione delle interviste sul segmento di riferimento consente di ottenere risultati con un minore errore statistico di rilevazione.

Premessa, obiettivi e note metodologiche

Questo documento riporta le principali evidenze emerse dall'indagine condotta per conto di CINEAS e rappresenta la XIII edizione dell'**Osservatorio sul risk management nelle medie imprese italiane**.

L'obiettivo principale, in continuità con il passato, è quello di fornire un **quadro generale per analizzare la diffusione del risk management nelle medie imprese italiane** e comprendere il loro livello di consapevolezza relativamente ai profili di rischio a cui sono esposte.



TARGET

Medie aziende italiane
50-499 addetti



DIMENSIONE CAMPIONARIA

380 interviste
equidistribuite per
dimensione (addetti),
territorio, settore e
riportate all'universo



METODOLOGIA

interviste con sistema
CATI/CAWI



LUNGHEZZA DEL QUESTIONARIO

50 domande principali
in circa 20 minuti



PERIODO DI RILEVAZIONE

Marzo 2026



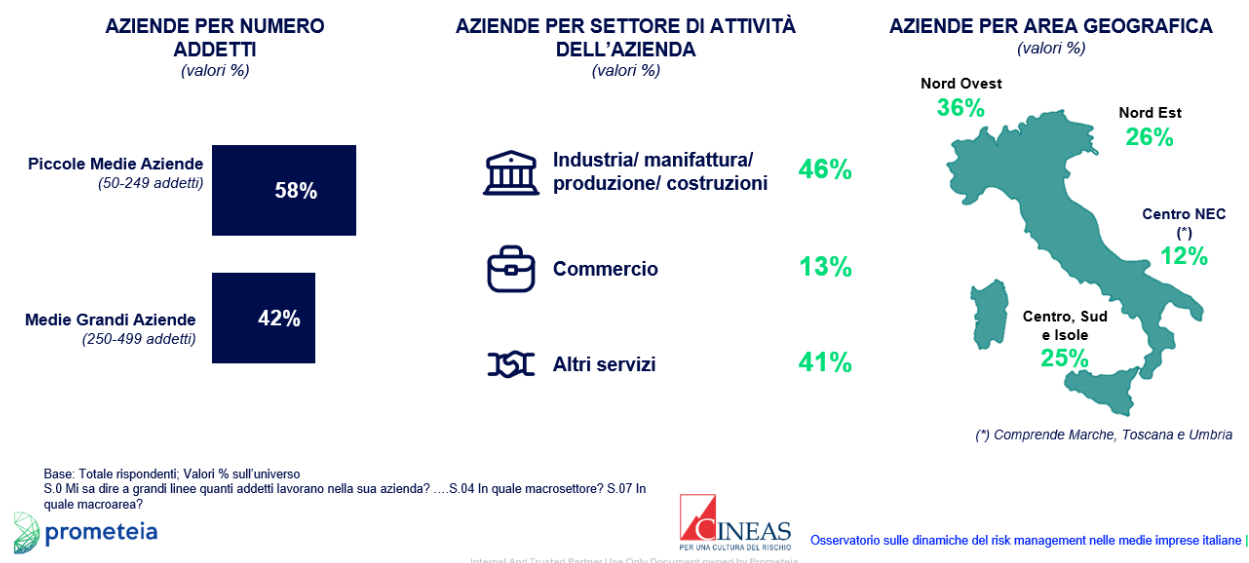
Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 2

Internal And Trusted Partner Use Only Document owned by Prometeia

La **seconda novità** sempre di metodo riguarda l'adozione di un piano di campionamento equidistribuito per classe dimensionale, settore e territorio di appartenenza in modo tale da garantire il minimo errore statistico all'interno della cella campionaria. Questa metodologia consente ove possibile la lettura dei risultati anche sulle distribuzioni marginali come, ad esempio, per le aziende medio-piccole, tra 50 e 249 addetti, e le aziende medio-grandi, 250-499 addetti contenendone l'errore statistico. Il campione che conta 380 interviste opportunamente pesato è rappresentativo dell'universo di riferimento le cui principali caratteristiche sono riportate nella diapositiva che segue.

L'universo delle aziende target

E le dimensioni di analisi



Come **terzo elemento** innovativo questa volta di contenuto è stato dato ampio spazio nel primo capitolo all'inquadramento del contesto economico e geopolitico in cui le aziende si ritrovano ad operare dando enfasi a quelli che sono i principali rischi emergenti che ne conseguono e alle nuove regole di mercato.

Questa premessa fornisce alcuni spunti di riflessione definiti sulla base di evidenze quantitative anche relative agli accadimenti più recenti come la chiusura dello stretto di Hormuz che è stato utilizzato come caso di studio per declinare i possibili impatti in chiave di gestione del rischio.

I risultati dell'indagine tramite interviste possono quindi essere letti e interpretati con una migliore consapevolezza dei riflessi indotti dal contesto economico e geopolitico più recente. Tuttavia i cambi repentini delle strategie politiche delle principali economie mondiali, il presidio dei mercati e l'espansionismo sempre più importante dei paesi dell'Oriente, l'instabilità delle relazioni tra i paesi del Medio Oriente, l'eterogeneità delle politiche ambientali adottate dalle principali economie mondiali e le asimmetrie nelle filiere dei mercati della tecnologia digitale e della produzione energetica ridisegnano gli equilibri relazionali tra i Paesi e rendono sempre più instabile e incerto l'orizzonte anche di breve termine dell'economia. Il contesto cambia quindi rapidamente e cresce di conseguenza l'importanza della gestione del rischio in azienda.

La **quarta ed ultima novità** riguarda la realizzazione di un focus sui temi emergenti dell'AI rivolto ad un campione di 52 imprese di medio-grande dimensione (250-499 dipendenti) che hanno risposto a un set di domande relative all'utilizzo, alle competenze, ai rischi e alla gestione degli stessi attraverso la formazione.

In particolare, riteniamo opportuno ricordare che la presente indagine non esamina tutti i rischi assicurabili da una azienda ma si concentra su quelli che sono i rischi emergenti (calamità naturali e tecnologici).

CAPITOLO 1. ELEMENTI DI SCENARIO

Agenda

ELEMENTI DI SCENARIO

- rischio geopolitico e conseguente diversificazione dei mercati a valle e a monte come principali sfide attuali
- la crescita del fatturato rimane il focus delle aziende in un contesto incerto e instabile, seguono ambiente e AI



RISCHIO DI
CALAMITA'
NATURALE



INTELLIGENZA
ARTIFICIALE



SISTEMI DI
GESTIONE DEL
RISCHIO



FORMAZIONE
AZIENDALE



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 5

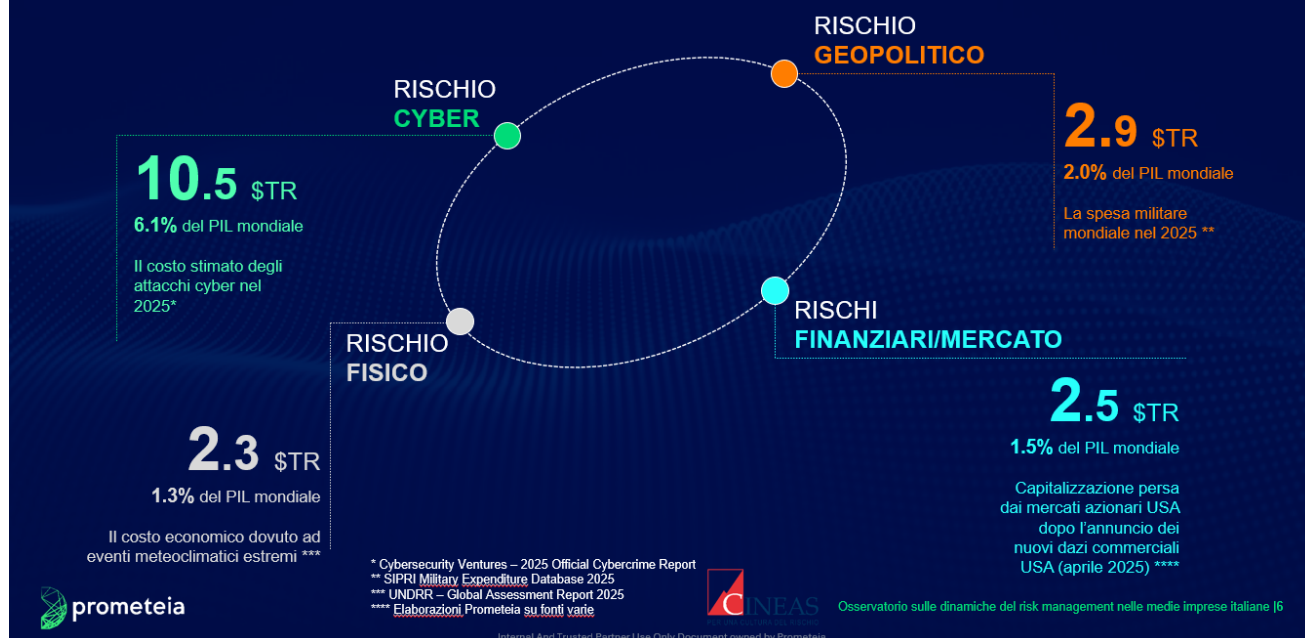
Internal And Trusted Partner Use Only Document owned by Prometeia

1.1 Una mappa globale dei rischi: geopolitica, mercati, cyber e clima

I rischi globali sono stati tradizionalmente interpretati come eventi eccezionali: shock a bassa probabilità e alto impatto, esterni al funzionamento ordinario dell'economia e gestibili attraverso strumenti specifici di copertura, mitigazione o trasferimento. Tale impostazione appare oggi sempre meno adeguata a descrivere la natura del contesto internazionale.

L'evidenza degli ultimi anni segnala infatti un cambiamento più profondo. I principali rischi che incidono sull'economia globale - geopolitici, finanziari, cyber e fisici - non si manifestano più prevalentemente come episodi isolati, ma come fenomeni ricorrenti, sistemici e tra loro interconnessi. Essi influenzano in modo diretto le decisioni di investimento, i costi di produzione, la stabilità dei mercati, la sicurezza delle infrastrutture e la sostenibilità dei bilanci pubblici e privati.

Una view globale dei rischi... e del loro potenziale economico



Il punto centrale non è soltanto l'aumento dei rischi, ma la loro crescente simultaneità. La frammentazione geopolitica alimenta l'incertezza economica; l'incertezza si trasmette ai mercati e alle scelte di investimento; la digitalizzazione accresce l'esposizione agli attacchi cyber; il cambiamento climatico introduce costi fisici sempre più frequenti e complessi da assorbire. Ne deriva una configurazione nella quale l'esposizione complessiva del sistema economico risulta superiore alla somma delle singole componenti.

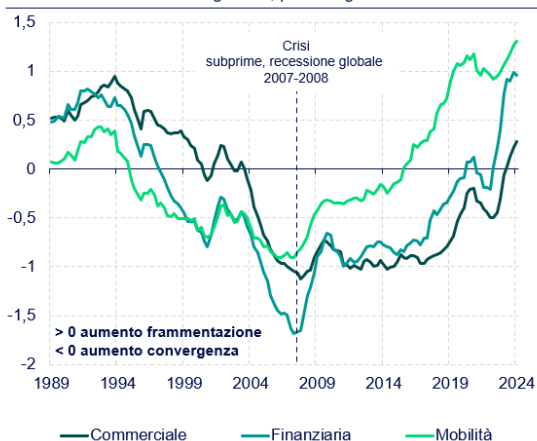
1.2 Il rischio geopolitico

La traiettoria del rischio geopolitico può essere ricondotta, in larga misura, alla crisi finanziaria del 2007-2008. La crisi dei mutui subprime e la successiva recessione globale hanno rappresentato un punto di discontinuità non solo sul piano economico, ma anche su quello politico e istituzionale. Da quel momento, l'assetto cooperativo che aveva sostenuto la fase precedente della globalizzazione ha iniziato a indebolirsi in modo progressivo.

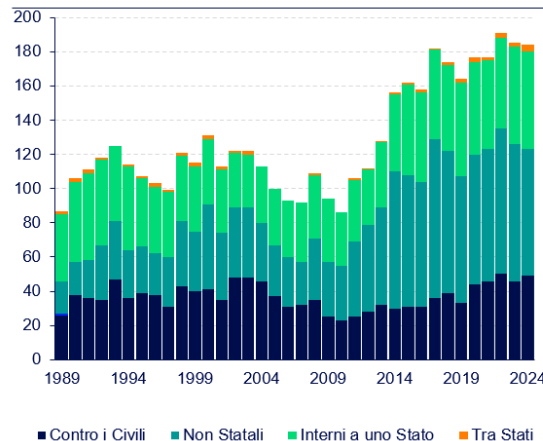
Una view globale dei rischi | Il Rischio Geopolitico

La crisi finanziaria del 2007-2008 ha segnato l'inizio di una fase di crescente frammentazione globale, ridefinendo gli equilibri economici, commerciali e geopolitici internazionali

La genesi delle crisi di oggi è da cercare nel passato
Indici di frammentazione globale, per categoria



Conflitti armati nel mondo
di conflitti con almeno 25 vittime



Fonte: Elab. Prometeia su dati Uppsala Conflict Data Program (2025) e Fernández-Villaverde, Mineyama, Song, «Geopolitical Fragmentation Index»



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 7

La crisi ha contribuito ad accelerare un riorientamento delle politiche nazionali verso obiettivi di sicurezza, autonomia strategica e tutela degli interessi domestici. L'integrazione commerciale, finanziaria e tecnologica ha gradualmente lasciato spazio a una logica più frammentata, nella quale le interdipendenze internazionali sono percepite non solo come fonte di efficienza, ma anche come potenziali fattori di vulnerabilità.

Questa dinamica non riguarda un unico ambito. La frammentazione delle relazioni internazionali si manifesta simultaneamente lungo più dimensioni: commercio, finanza, tecnologia, energia, difesa e catene globali del valore. Proprio tale natura multidimensionale ne accresce la rilevanza economica. Quando la frammentazione assume carattere strutturale, le imprese sono chiamate a rivedere fornitori, mercati di sbocco, localizzazione produttiva e gestione delle scorte; gli Stati ridefiniscono le proprie priorità industriali e strategiche; gli investitori incorporano premi al rischio più elevati.

A questa tendenza si accompagna un aumento della conflittualità internazionale. La minore interdipendenza può ridurre il costo percepito della rottura delle relazioni economiche e diplomatiche, abbassando la soglia oltre la quale il conflitto diventa sostenibile per gli attori coinvolti. Il rischio geopolitico assume così una natura strutturale: non più una deviazione temporanea rispetto a un equilibrio stabile, ma una componente permanente del contesto economico globale.

1.3 Il rischio finanziario e di mercato

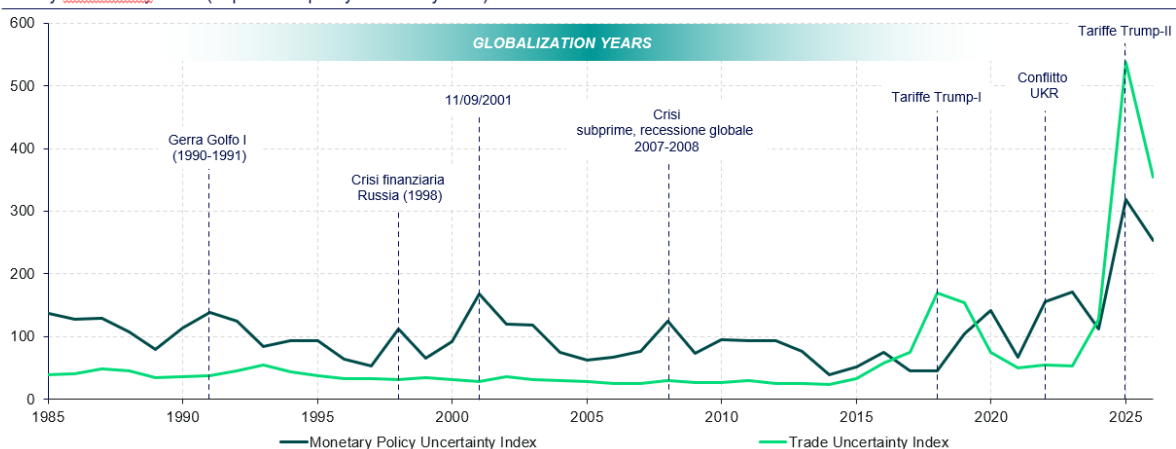
Anche il rischio finanziario ha mutato configurazione. In passato, molti shock di mercato risultavano circoscritti nel tempo e nello spazio. Crisi regionali, episodi di instabilità politica o shock terroristici potevano generare correzioni anche significative, ma erano spesso seguiti da fasi di riassorbimento e di ritorno verso condizioni di maggiore normalità.

Il contesto attuale presenta caratteristiche differenti. I mercati operano in un ambiente contraddistinto dalla sovrapposizione di molteplici fonti di incertezza: politica monetaria, tensioni commerciali, instabilità geopolitica, transizione energetica e frammentazione delle catene globali del valore. Nessuna di queste dimensioni agisce in modo isolato. Al contrario, esse tendono a sommarsi e ad amplificarsi reciprocamente, rendendo più difficile distinguere tra shock temporanei e cambiamenti strutturali di regime.

Una view globale dei rischi | Il Rischio Finanziario / di Mercato

A differenza delle crisi passate, il contesto attuale si caratterizza per shock multipli e persistenti: politica monetaria, commercio internazionale e geopolitica agiscono simultaneamente come driver di volatilità

Incertezza globale come caratteristica intrinseca della frammentazione delle relazioni internazionali
Policy Uncertainty Index (<https://www.policyuncertainty.com/>)



Fonte: Elab. Prometeia su dati EPU, aa.vv.



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |8

La conseguenza è un livello di incertezza più persistente. Le variabili finanziarie non reagiscono soltanto a singole notizie o a eventi circoscritti, ma incorporano una condizione di fondo più instabile. In tale quadro, i modelli di gestione del rischio basati sull'ipotesi di eventi indipendenti risultano meno efficaci, poiché i principali driver di volatilità tendono a muoversi simultaneamente.

Le implicazioni per l'economia reale sono rilevanti. In presenza di incertezza persistente, le imprese possono rinviare decisioni di investimento, richiedere rendimenti più elevati per impegnare capitale e privilegiare flessibilità e liquidità rispetto a progetti di lungo periodo. Da questo punto di vista, il rischio finanziario diventa un canale di trasmissione della frammentazione globale alla crescita economica.

1.4 Il rischio cyber

Il rischio cyber rappresenta una delle aree di rischio in più rapida evoluzione. La sua crescente rilevanza deriva dalla combinazione di diversi fattori: la digitalizzazione dei processi produttivi, la diffusione del cloud, l'aumento del lavoro da remoto, l'interconnessione delle infrastrutture critiche e l'abbassamento delle barriere tecniche necessarie per condurre attacchi.

L'intelligenza artificiale ha ulteriormente accelerato questa dinamica. Strumenti automatizzati consentono di aumentare scala, velocità e sofisticazione delle azioni malevole. Il phishing, il social engineering e la produzione di contenuti ingannevoli diventano più credibili, personalizzati e difficili da identificare. Parallelamente, modelli come il ransomware-as-a-service trasformano capacità offensive complesse in servizi accessibili anche ad attori con competenze tecniche limitate.

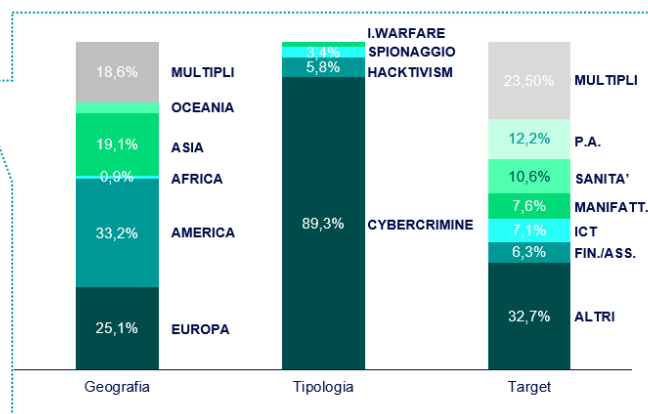
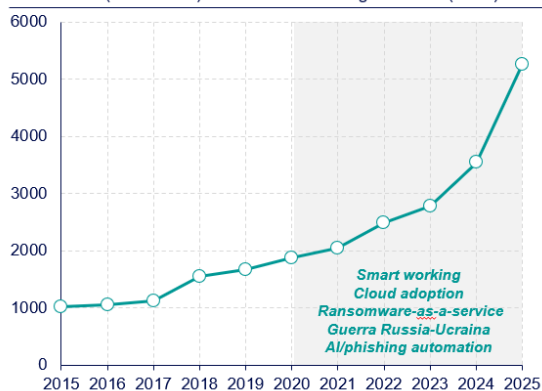
Il rischio cyber si distingue anche per la sua pervasività. Non riguarda un solo settore né una specifica area geografica. Può interessare servizi finanziari, industria, sanità, pubblica amministrazione, infrastrutture, telecomunicazioni e catene di fornitura. Anche le motivazioni degli attacchi risultano eterogenee: criminalità economica, spionaggio, hacktivism, information warfare, sabotaggio o obiettivi multipli.

Una view globale dei rischi | Il Rischio Cyber

Tra il 2025 e il 2026 le azioni malevole (cyberattacchi) sono aumentate drasticamente. L'intelligenza artificiale ha aumentato scala, velocità e sofisticazione degli attacchi cyber, in particolare nel phishing e nel social engineering

Cyberattacchi nel Mondo

di eventi (2015-2025) e caratteristiche degli attacchi (2025)



Fonte: Elab. Prometeia su dati CLUSIT, Rapporti 2020-2026

Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 9

Questa pluralità rende il rischio cyber particolarmente complesso da governare. Non esiste una singola minaccia né una singola contromisura. La superficie esposta cresce insieme alla digitalizzazione, mentre gli attaccanti beneficiano di strumenti sempre più accessibili e scalabili. Per questo, il rischio cyber non è più riconducibile alla sola dimensione tecnologica, ma assume una rilevanza operativa, finanziaria e strategica.

Un attacco informatico può compromettere la continuità dei processi aziendali, generare perdite economiche dirette, incidere sulla reputazione dell'organizzazione, esporre a responsabilità regolamentari e, nei casi più gravi, interrompere il funzionamento di infrastrutture critiche o servizi essenziali. Il rischio cyber deve quindi essere considerato parte integrante della resilienza complessiva di imprese, istituzioni e sistemi economici.

1.5 Il rischio fisico

Il rischio fisico legato al cambiamento climatico è sempre meno riconducibile a un orizzonte esclusivamente di lungo periodo. Gli eventi climatici estremi producono già oggi effetti economici rilevanti, attraverso danni diretti ad asset, infrastrutture, abitazioni, colture e attività produttive, ma anche attraverso interruzioni operative, aumento dei costi assicurativi e maggiore pressione sui bilanci pubblici.

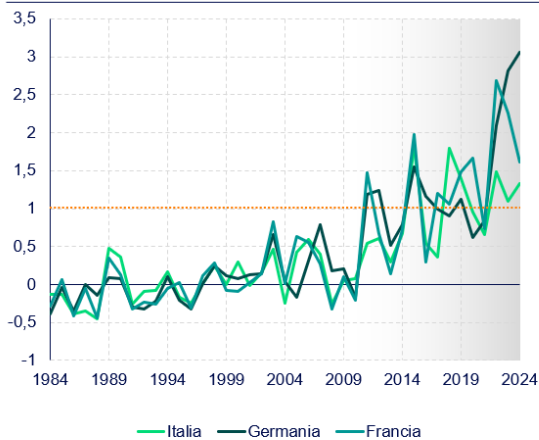
L'aspetto più rilevante è rappresentato dall'accelerazione del fenomeno. La frequenza e l'intensità degli eventi estremi mostrano una tendenza crescente, mentre le perdite economiche associate tendono a concentrarsi in archi temporali sempre più brevi. Il rischio climatico non si manifesta quindi come un deterioramento lento e lineare, ma come una successione di shock fisici con effetti cumulativi.

Una view globale dei rischi | Il Rischio Fisico

Nell'ultima decade (2014-2024) le perdite economiche causate da eventi climatici estremi in Europa hanno superato quelle cumulate dei 25 anni precedenti

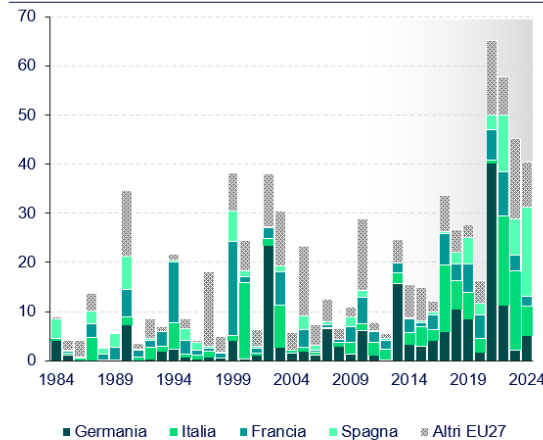
Sempre più frequenti...

Temperature: anomalia standard rispetto alla media 1981-2010



... sempre più costosi

Perdite dovute ad eventi climatici, in mld € a pz. costanti



Fonte: Elab. Prometeia su dati Eurostat, [European Climate Index](#)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |10

Internal And Trusted Partner Use Only Document owned by Prometeia

Due dimensioni agiscono congiuntamente. Da un lato, l'aumento delle anomalie climatiche segnala un progressivo allontanamento dai valori storici di riferimento. Dall'altro, i danni aumentano perché eventi climatici estremi colpiscono territori oggi più urbanizzati, infrastrutture più complesse e attività economiche di maggior valore rispetto al passato. Il risultato è un effetto moltiplicativo: eventi più frequenti colpiscono sistemi economici più esposti e, quindi, più onerosi da ripristinare.

Le implicazioni sono ampie. Il settore assicurativo deve confrontarsi con rischi più difficili da prezzare e, in alcuni casi, con aree progressivamente meno assicurabili. Le amministrazioni pubbliche sono chiamate a sostenere costi crescenti per prevenzione, emergenza e ricostruzione. Le imprese devono incorporare il rischio fisico nelle decisioni di localizzazione, investimento e continuità operativa.

Il rischio climatico diventa quindi una variabile economica centrale, non più soltanto una questione ambientale o regolatoria.

1.6 Conclusione

Le quattro categorie di rischio condividono una caratteristica comune: non agiscono più in modo separato. La frammentazione geopolitica aumenta l'instabilità del quadro internazionale; tale instabilità si riflette sui mercati, sui flussi commerciali e sugli investimenti; la digitalizzazione, pur sostenendo produttività e innovazione, amplia l'esposizione cyber; il cambiamento climatico introduce una componente fisica di costo sempre più frequente e strutturale.

La nuova mappa globale dei rischi è quindi, in misura crescente, una mappa di interdipendenze. I rischi si propagano attraverso canali diversi (prezzi, capitale, infrastrutture, supply chain, sicurezza) ma producono effetti convergenti: maggiore volatilità, aumento dei costi, riduzione della prevedibilità e indebolimento della capacità di pianificazione.

Per imprese, istituzioni finanziarie e policy maker, la conseguenza è chiara: il rischio è diventato una delle condizioni strutturali entro cui opera il sistema economico, e non può quindi più essere gestito come un evento eccezionale, ma integrato nei processi ordinari di analisi macroeconomica, pianificazione strategica, allocazione del capitale e gestione della resilienza.

1.7 Un caso di studio: lo stretto di Hormuz

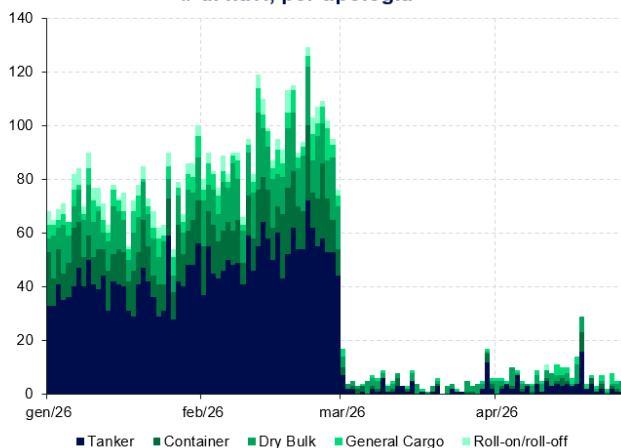
La chiusura dello stretto di Hormuz è un tipico esempio di come un singolo evento geopolitico produca oggi molteplici effetti con ricadute dirette e indirette sull'operato delle aziende.

Il primo effetto diretto riguarda la riduzione drastica del traffico navale con una interruzione di oltre il 20% del traffico marittimo mondiale di petrolio e di gas naturale.

Le quotazioni del Brent (\$/barile) si impennano nei due mesi post-shock e registrano un aumento di quasi il 60%. Un impatto che resta inferiore ma di poco a quello relativo alla guerra del golfo degli anni 90, probabilmente come conseguenza di livello dei prezzi già influenzati dal recente conflitto RUSS-UKR del 2022.

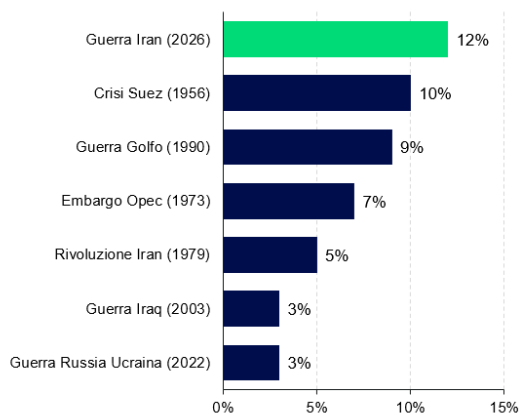
Focus sulla chiusura dello Stretto di Hormuz | Traffico navale

Navi in transito nello stretto di Hormuz, 2026
di navi, per tipologia



Shock a confronto (1974-2026)

Ammanco in % della produzione mondiale di petrolio



Elaborazioni Prometeia su dati Eikon, IMF Portwatch



Elaborazioni Prometeia su dati IMF Portwatch, Energy Institute ed altri

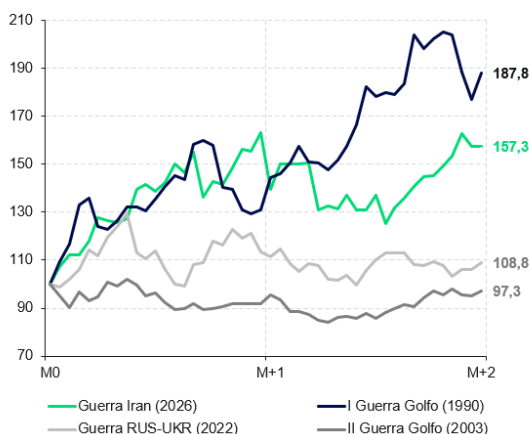
Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |11

Internal And Trusted Partner Use Only Document owned by Prometeia

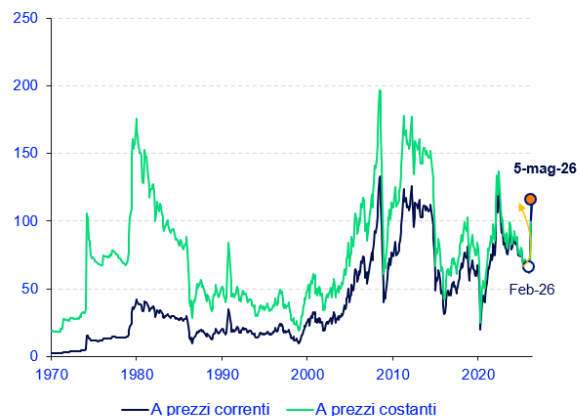
Focus sulla chiusura dello Stretto di Hormuz | Petrolio

...innescando una delle crisi più gravi nella storia del mercato del petrolio, ma impatto finora ridotto rispetto ad altri eventi del passato

Brent, dinamica delle quotazioni nei 2 mesi post-shock
\$/barile, giorno precedente allo shock = 100, dati giornalieri



Brent, quotazioni in \$/barile
a prezzi correnti e costanti*, dati mensili



* deflazionato con il CPI USA, Brent BFO Dated
Fonte: Elaborazioni Prometeia su dati EIA, Eikon, U.S. Bureau of Labor Statistics

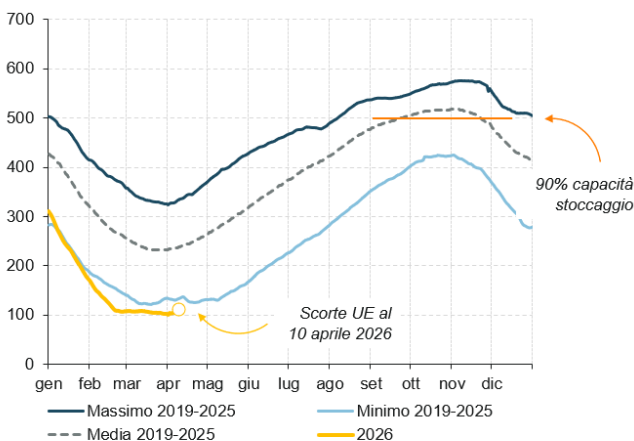
Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 12

Focus sulla chiusura dello Stretto di Hormuz | Gas

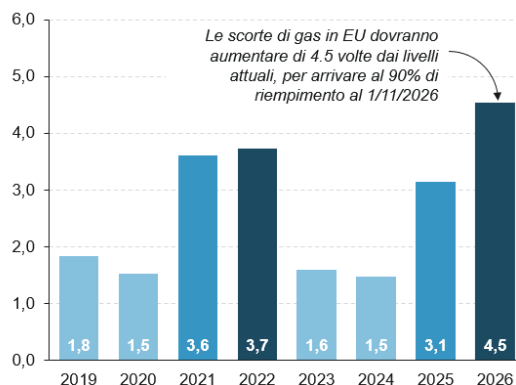
In Europa le scorte del gas sono ai minimi... per raggiungere un grado di riempimento adeguato all'inizio dell'anno termico 2026 (ottobre/novembre) occorrerà uno sforzo ancora superiore rispetto a quello del 2022

Scorte di metano, EU27

In TWh, livello al 10/4/2026 e confronto con la media di periodo



Distanza dal «target» del 90% di riempimento scorte al 1° novembre - Situazione al 10 aprile di ogni anno



Fonte: Elaborazioni Prometeia su dati ENTSG

Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 13

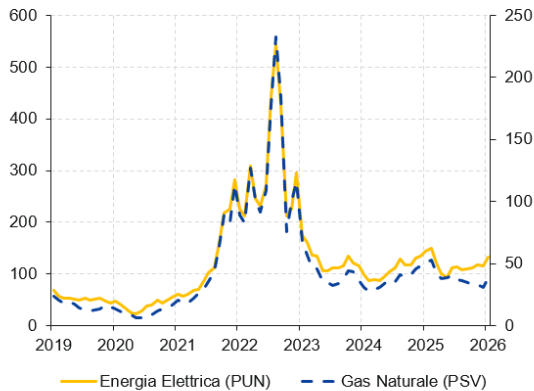
Come per il petrolio, così per il Gas. In Europa le scorte sono ai minimi. Nell'estate 2026, per raggiungere un grado di riempimento adeguato all'inizio dell'anno termico 2026 (ottobre/novembre) occorrerà uno sforzo ancora superiore rispetto a quello implementato nel 2022.

Il rialzo dei prezzi del gas metano rende inevitabile una trasmissione dei rincari anche ai prezzi di energia elettrica, soprattutto in Italia dove i prezzi (tra più elevati nel contesto UE) sono legati a doppio filo con quelli del metano, vista a struttura del parco di generazione fortemente orientata verso questo combustibile.

Focus sulla chiusura dello Stretto di Hormuz | Energia

Inevitabile trasmissione dei rincari del gas ai prezzi dell'elettricità soprattutto in Italia

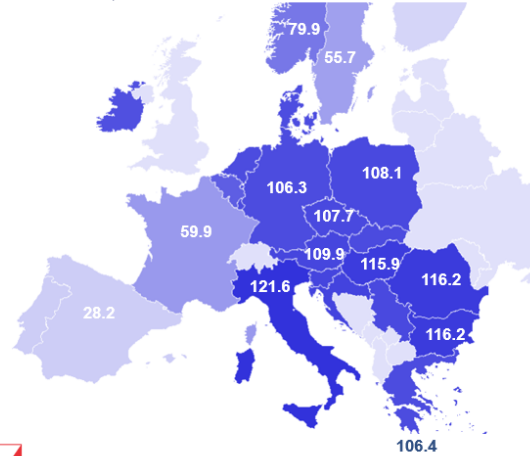
Quotazioni del metano e dell'energia elettrica in Italia
In €/MWh, dati giornalieri



Fonte: Elaborazioni Prometeia su dati ENTSOE, EEX



Quotazioni dell'energia elettrica in Europa
In €/MWh, 03/03/2026



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |14

Internal And Trusted Partner Use Only Document owned by Prometeia

Gli effetti del conflitto in Medio Oriente non si faranno sentire solo sui costi dell'energia e degli input energetici, ma avranno ripercussioni anche sulle catene globali del valore e, conseguentemente, sulla crescita mondiale e italiana.

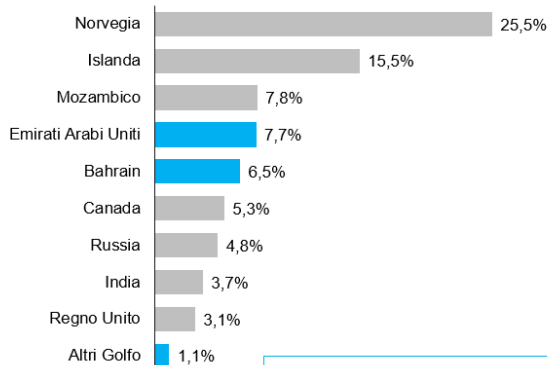
In caso di conflitto prolungato si avranno effetti diretti anche su altre materie prime. La quotazione di alcuni metalli ha già iniziato a crescere. Dal Golfo origina il 9% della produzione mondiale di alluminio e il 15% dell'import UE. Le aspettative sono di un plausibile aumento significativo dei premi in caso di conflitto prolungato, dato anche il basso livello di scorte.

Non solo i metalli ma anche il settore della chimica è fortemente condizionato dalle tensioni nel Medio Oriente. Dai paesi del golfo origina il 16% di import di plastiche (il 25-30% per quelle più rilevanti), che mostrano rialzi significativi delle quotazioni (etilene quasi triplicato, propilene raddoppiato rispetto a febbraio).

Focus sulla chiusura dello Stretto di Hormuz | Metalli

Dal Golfo origina il 9% della produzione mondiale di alluminio e il 15% dell'import UE: plausibile un aumento significativo dei premi in caso di conflitto prolungato, dato anche il basso livello di scorte LME

UE27, Importazioni di alluminio greggio
In % sul totale



GCC+Iran
Import UE ~15.2%
Produzione mondiale ~ 9%

Alluminio LME, quotazioni
In €/ton, dati giornalieri



+ premio Europa LME, 360 → 470 €/ton
Elaborazioni Prometeia su dati TDM, World Bureau of Metal Statistics (WBMS), Eikon



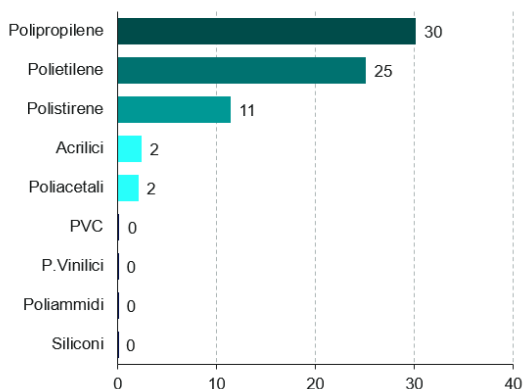
Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |15

Internal And Trusted Partner Use Only Document owned by Prometeia

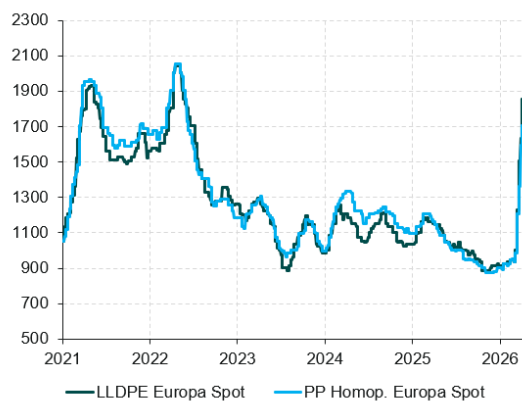
Focus sulla chiusura dello Stretto di Hormuz | Chimica

Dal Golfo origina il 16% di import di plastiche (il 25-30% per quelle più rilevanti), che mostrano rialzi significativi delle quotazioni (etilene quasi triplicato, propilene raddoppiato rispetto a febbraio)

EU27, Importazioni di plastiche dal Golfo
In % rispetto al totale delle import da extra-UE



Plastiche, quotazioni europee
Dati giornalieri in €/ton, spot



Fonte: banca dati APPIA-MP Prometeia



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |16

Internal And Trusted Partner Use Only Document owned by Prometeia

Gli United Arab Emirates (UAE) sono inoltre in 2° posizione mondiale per capacità di calcolo installata e presenza di un ecosistema AI. Si tratta di pochi hub ad altissima intensità, finanziati da fondi sovrani e «abilitati» dalla partnership privilegiata con gli USA. Il Golfo è dunque un importante driver per l'offerta di Tecnologia ed anche un nodo cruciale per il traffico internazionale di dati.

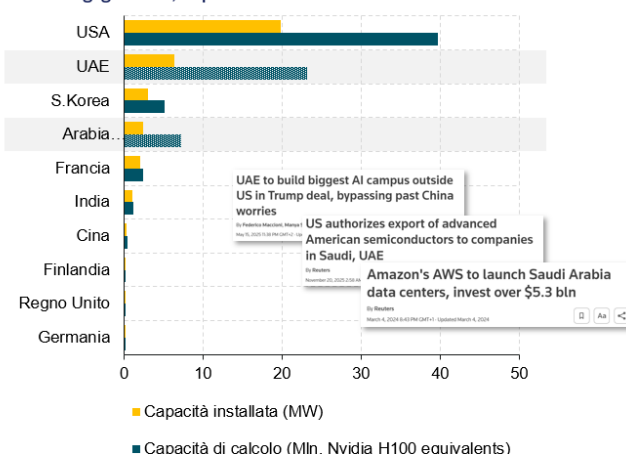
Sotto il Golfo transita il 17% del traffico dati mondiale e il 90% di quello Asia-Europa; un'importante vulnerabilità, in un contesto peraltro segnato da incidenti riconducibili a operazioni di guerra ibrida (es. Mar Baltico).

Focus sulla chiusura dello Stretto di Hormuz | IT

UAE in 2° posizione mondiale per capacità di calcolo installata e presenza di un ecosistema AI...pochi hub ad altissima intensità, finanziati da fondi sovrani e «abilitati» dalla partnership privilegiata con gli USA

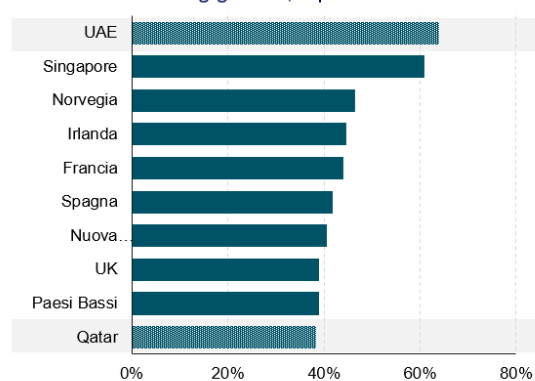
World's Top AI Superpowers 2025

Ranking globale, top-10



AI Diffusion Index 2025

Ranking globale, top-10



Elaborazioni Prometeia su dati TRG Datacenters, Microsoft

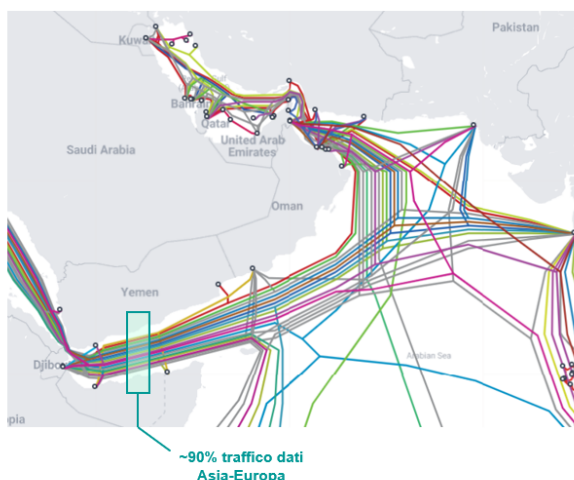


Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |17

Focus sulla chiusura dello Stretto di Hormuz | Cable Network

Sotto il Golfo transita il 17% del traffico dati mondiale e il 90% di quello Asia-Europa; un'importante vulnerabilità, in un contesto peraltro segnato da incidenti riconducibili a operazioni di guerra ibrida (es. Mar Baltico)

Cavi sottomarini nell'Oceano Indiano / Golfo / Mar Rosso



Danni intenzionali di infrastrutture sottomarine (2023-2025)

Data	Area	Evento	Valutazione
feb-23	Taiwan	Isole Matsu (Taiwan) — 2 cavi tranciati in 6 giorni	Probabile sabotaggio
ott-23	Mar Baltico	Balticconnector — gasdotto + cavo dati (Finlandia-Estonia)	Probabile sabotaggio
feb-24	Mar Rosso	Rubymar colpita dagli Houthi — ancora trascina 3 cavi (AAE-1, EIG, SEACOM)	Conflitto armato - danno collaterale
mar-24	Mar Rosso	4 cavi tranciati — AAE-1, EIG, SEACOM, TGN	Sospetto sabotaggio Houthi
nov-24	Mar Baltico	C-Lion1 (Finlandia-Germania) e BCS East-West (Lituania-Svezia) — tagli simultanei	Sospetto sabotaggio Russia
dic-24	Mar Baltico	Shadow fleet russa — 4 cavi + interconnessione elettrica EstLink 2	Sabotaggio - Russia
gen-25	Taiwan	Trans-Pacific Express tranciato — cargo con bandiera Tanzania, equipaggio cinese	Sospetto sabotaggio Cina
apr-26	S. di Hormuz	Iran minaccia i cavi di Hormuz — droni colpiscono data center AWS in BAH e UAE	Target Conflitto

Elaborazioni Prometeia su fonti varie, Submarinecablemap.com



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |18

Il Golfo è anche un provider di input strategici per la produzione di semiconduttori. Taiwan, principale produttore di semiconduttori, dipende fortemente dalle importazioni di elio e metano dal Qatar ed eventuali shock geopolitici

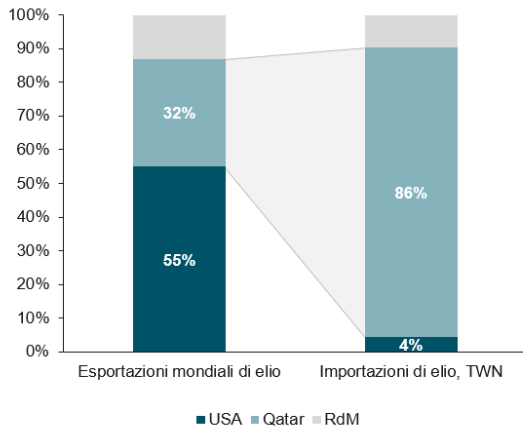
in Medio Oriente rappresentano una vulnerabilità sistemica per la produzione globale di semiconduttori e chip avanzati.

Focus sulla chiusura dello Stretto di Hormuz | Semiconduttori

Data la dipendenza di TWN dalle import di elio e metano dal Qatar, eventuali shock geopolitici in Medio Oriente rappresentano una vulnerabilità sistemica per la produzione globale di semiconduttori e chip avanzati

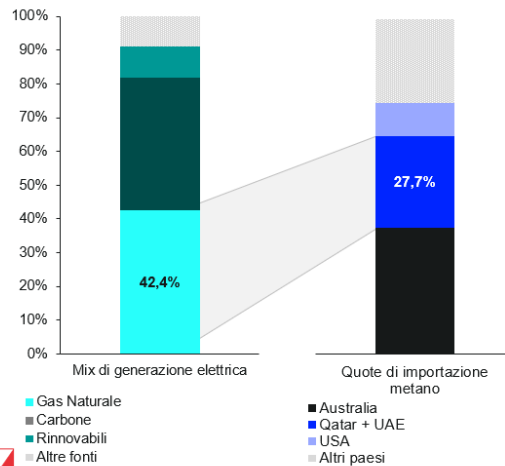
Elio: esportazioni mondiali e importazioni di Taiwan

In % sul totale, volume



Taiwan, mix di generazione elettrica e importazioni di metano - In % sul totale, volume 2024

In % sul totale, volume 2024



Elaborazioni Prometeia su dati TDM, Energy Institute



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 19

Tutte queste evidenze lasciano intendere come un singolo evento, in questo caso geopolitico come la chiusura dello stretto di Hormuz, possa scatenare una serie di effetti a cascata su molteplici direzioni quali aumento dei prezzi degli input energetici, aumenti dei costi delle materie prime, razionamento delle forniture di input strategici, cybersecurity, etc.

I rischi che gravano sugli operatori economici si moltiplicano e le aziende lo sanno bene come dimostrano le risposte date in merito al clima di tensione e incertezza derivante dalla politica USA. Le aziende rispondenti riflettono quanto effettivamente emerge dalle evidenze fin qui emerse.

Le conseguenze attese della politica USA come rischio geopolitico

Aumento dei costi delle importazioni, calo del fatturato delle export e incertezza



Base: Totale rispondenti; Valori %

Q.2 Secondo Lei quali sono le principali conseguenze a cui stanno andando incontro le aziende italiane con l'insediamento del nuovo Presidente degli USA, Donald Trump? (Max 3 risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 21

Internal And Trusted Partner Use Only Document owned by Prometeia

La principale ricaduta riguarda “l’aumento dei prezzi dei beni importati”. Seguono al secondo posto “la maggiore incertezza e volatilità dei mercati reali e finanziari” e “una riduzione del fatturato derivante dalla minori esportazioni”.

Un contesto geopolitico e di mercato che solo l’11% delle aziende vede come possibile veicolo di maggior coesione tra i Paesi dell’Unione Europea.

CAPITOLO 2. RISCHIO DI CALAMITÀ NATURALE

Agenda



2.1 Principali eventi in Italia e rilevanza per le imprese

Il rischio di calamità naturale non appare più come una variabile remota o confinata ad aree specifiche del Paese. Negli ultimi anni, la frequenza e la severità degli eventi meteoroclimatici hanno reso più visibile il legame tra vulnerabilità del territorio, continuità operativa delle imprese e capacità di prevenzione. Per le medie aziende italiane il tema riguarda sia la tutela degli asset sia la capacità di proseguire l'attività dopo l'evento. Danni a impianti, magazzini o sedi possono infatti trasformarsi rapidamente in fermo produttivo. In questa prospettiva, il rischio fisico entra stabilmente nel perimetro del risk management aziendale.

Le evidenze dell'Osservatorio confermano questa centralità. Gran parte delle aziende dichiara infatti di monitorare i rischi ambientali e di attivare coperture o iniziative di prevenzione, con una quota che si colloca intorno al 70%. Il dato segnala una sensibilità ormai diffusa, ma non ancora pienamente consolidata. Un'azienda su cinque afferma di aver subito un danno legato a eventi naturali e, tra queste, circa un terzo non aveva attivato alcuna copertura o iniziativa di prevenzione. È un elemento rilevante perché mostra come la consapevolezza del rischio non sempre si traduca in strumenti operativi di protezione. I danni riguardano principalmente le strutture aziendali, l'interruzione delle attività e i pericoli per il personale, confermando che l'impatto delle calamità naturali interessa sia la dimensione patrimoniale sia quella organizzativa e produttiva.

La sequenza recente degli eventi nel nostro Paese conferma questa centralità. L'alluvione in Emilia-Romagna del maggio 2023 ha rappresentato uno degli episodi più rilevanti per estensione territoriale e impatto produttivo, con l'esondazione di numerosi corsi d'acqua, frane e allagamenti in aree a forte densità manifatturiera, agroalimentare e logistica. A novembre 2023, gli eccezionali eventi meteorologici in Toscana hanno mostrato come i fenomeni di pioggia intensa possano colpire territori ad alta concentrazione di attività produttive e commerciali. Nel settembre e nell'ottobre 2024 l'Emilia-Romagna è stata nuovamente interessata da eventi meteorologici estremi, con il coinvolgimento di diverse province e la dichiarazione dello stato di emergenza. Accanto al rischio idrogeologico, va considerata anche la crisi bradisismica dei Campi Flegrei: il sisma del 20 maggio 2024, di magnitudo 4.4, e la successiva mobilitazione straordinaria del sistema di protezione civile hanno ricordato come anche rischi di natura geologica o vulcanica siano capaci di incidere su sicurezza, mobilità, infrastrutture e continuità dei servizi. A questi episodi si aggiunge la frana di Niscemi del gennaio 2026, che ha

richiamato ancora una volta l'attenzione sulla fragilità di alcune aree del Paese. L'evento ha avuto effetti rilevanti sulla popolazione, sulla viabilità, sugli edifici e sulla continuità dei servizi, incidendo anche sulle attività produttive e commerciali presenti nell'area interessata. Per le imprese, episodi di questo tipo possono incidere non solo sulle sedi eventualmente coinvolte, ma anche sull'accessibilità dei luoghi di lavoro, sulla continuità dei servizi e sui tempi di ripristino. Il caso di Niscemi conferma quindi la necessità di rafforzare le misure di prevenzione, affinché le aziende siano preparate non solo a reagire al danno, ma anche a contenerne gli effetti organizzativi ed economici.

Questi eventi rendono sempre più rilevante il passaggio da una gestione prevalentemente reattiva a una logica di prevenzione, monitoraggio e preparazione. Il danno economico di una calamità non coincide solo con il ripristino dei beni compromessi. Può tradursi anche in fermo operativo, ritardi, perdita di commesse e maggiori costi assicurativi. Per questo motivo, il tema va letto come parte della capacità complessiva dell'impresa di prevenire e gestire le interruzioni.

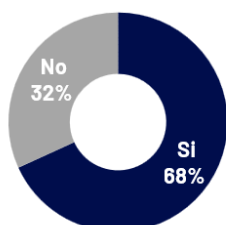
2.2 Sistemi di monitoraggio e rendicontazione degli obiettivi di sostenibilità

L'analisi del rischio climatico parte dagli strumenti con cui le imprese monitorano e misurano i propri obiettivi di sostenibilità. Si tratta, in particolare, di sistemi di monitoraggio, rendicontazione e misurazione delle performance ambientali, sociali e di governance. Il 68% delle imprese dichiara di disporre di strumenti e metodologie per misurare, gestire e comunicare le performance ambientali, sociali e di governance. I risultati del questionario mostrano una diffusione più elevata tra le imprese di dimensione maggiore: il 72% delle aziende con 250-500 addetti dichiara di aver introdotto sistemi di monitoraggio e rendicontazione degli obiettivi di sostenibilità, a fronte del 65% rilevato tra le imprese con 50-250 addetti. Il divario non è sorprendente, perché la rendicontazione ESG e il monitoraggio climatico richiedono competenze, flussi informativi e capacità organizzative più facilmente disponibili nelle strutture di dimensione superiore. Tuttavia, il fatto che quasi due imprese su tre anche nella fascia medio-piccola abbiano avviato questi sistemi indica che il tema non è più limitato alle realtà più strutturate.

Sistemi di monitoraggio degli obiettivi di sostenibilità in azienda

Il 68% delle aziende ha introdotto sistemi di monitoraggio degli obiettivi di sostenibilità soprattutto per garantire il rispetto delle nuove normative ...

INTRODUZIONE DI SISTEMI DI MONITORAGGIO / RENDICONTAZIONE DEGLI OBIETTIVI DI SOSTENIBILITA'

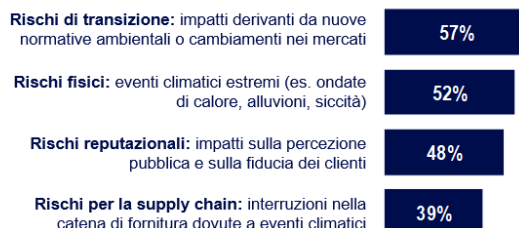


Medie Piccole aziende (50-249 addetti) 65%
Medie Grandi aziende (250-499 addetti) 72%

Base: Totale rispondenti Valori %
Q.7 La sua azienda ha in essere un sistema di monitoraggio e rendicontazione degli obiettivi di sostenibilità, ossia strumenti e metodologie volte a misurare, gestire e comunicare le performance ambientali, sociali e di governance aziendali? (Solo una risposta)



FOCUS RISCHI LEGATI AI CAMBIAMENTI CLIMATICI IN MONITORAGGIO (18% le aziende che hanno introdotto un sistema di monitoraggio dei rischi derivanti dai cambiamenti climatici)



Base: Aziende che hanno introdotto un sistema di monitoraggio dei rischi derivanti dai cambiamenti climatici (valori%)
Q.10 E quali rischi derivanti dai cambiamenti climatici e le loro conseguenze la sua azienda ha iniziato a monitorare? (Possibili più risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane [24]

Internal And Trusted Partner Use Only Document owned by Prometeia

Tra le aziende che hanno adottato sistemi di monitoraggio dei rischi derivanti dai cambiamenti climatici (circa il 18% dell'universo imprese), i rischi più osservati sono quelli di transizione, citati dal 57% delle imprese derivati da nuove normative ambientali, cambiamenti nei mercati o nuove aspettative dei clienti. È un risultato importante perché mostra che le imprese leggono la sostenibilità non solo come esposizione agli eventi fisici, ma anche come trasformazione del contesto competitivo. I rischi fisici derivati da eventi climatici estremi come ondate di

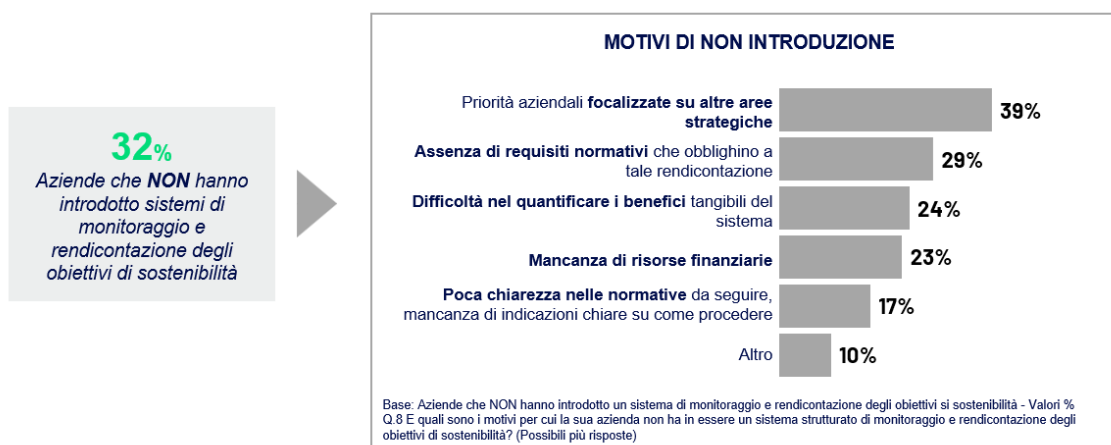
calore, alluvioni e siccità, sono monitorati dal 52% delle imprese; seguono i rischi reputazionali, indicati dal 48%, e quelli per la supply chain, al 39%. La scala dei risultati suggerisce una consapevolezza abbastanza articolata. Il cambiamento climatico viene infatti percepito come un rischio trasversale, che può incidere su più aspetti dell'impresa.

È utile sottolineare che il monitoraggio costituisce solo il primo livello della gestione del rischio. Misurare l'esposizione, raccogliere dati e produrre report non equivale necessariamente a ridurre il rischio; rappresenta però la condizione preliminare per prendere decisioni migliori. Il passaggio successivo è trasformare il monitoraggio in decisioni operative, ad esempio aggiornando piani di emergenza, valutazione della vulnerabilità degli impianti e coperture assicurative. In questo senso, il dato del 68% è positivo, ma non dice ancora quanto questi strumenti incidano davvero sulle scelte aziendali.

Accanto alle imprese che hanno già adottato strumenti di monitoraggio e rendicontazione, è importante osservare anche il gruppo di aziende che non ha ancora compiuto questo passaggio. Queste risposte aiutano a capire quali ostacoli frenano una maggiore diffusione dei sistemi di presidio della sostenibilità e dei rischi climatici. Il 32% delle aziende che non ha ancora introdotto sistemi strutturati fornisce infatti indicazioni utili sulle barriere all'adozione. La motivazione più frequente è la scelta di concentrare le risorse su altre aree strategiche, citata dal 39%. Seguono l'assenza di requisiti normativi obbligatori, al 29%, la difficoltà nel quantificare i benefici tangibili del sistema, al 24%, e la mancanza di risorse finanziarie, al 23%. Queste motivazioni mostrano che la prevenzione viene spesso penalizzata quando i suoi benefici non sono immediatamente visibili o misurabili. In questi casi, le imprese tendono a dare priorità ad altri investimenti, percepiti come più urgenti o più direttamente collegati all'attività aziendale.

Sistemi di monitoraggio degli obiettivi di sostenibilità in azienda

....Le aziende non attivano un sistema di monitoraggio perché scelgono di focalizzare le risorse su altre aree strategiche o per assenza di requisiti normativi



La difficoltà nel quantificare i benefici è particolarmente rilevante. Le misure di prevenzione producono valore soprattutto quando impediscono un danno che, proprio perché evitato, non si manifesta. La sfida del risk management consiste anche nel rendere più leggibile questo valore, collegando la prevenzione a indicatori operativi e non solo a obiettivi generali di sostenibilità. In questo modo il monitoraggio climatico può essere trattato come componente del business, e non come capitolo separato della sostenibilità.

2.3 Misure di prevenzione introdotte

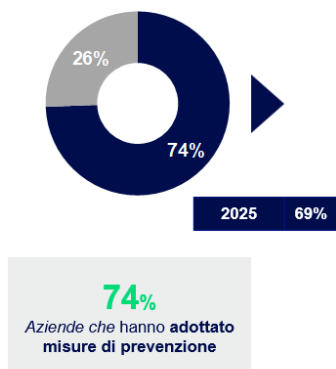
La sezione sulle misure di prevenzione mostra che tra le aziende che hanno subito un danno derivante da un evento naturale, il 74% ha introdotto misure di prevenzione. Questo risultato va però letto distinguendo tra prevenzione già presente prima dell'evento e interventi successivi di rafforzamento. L'esperienza diretta del

danno può certamente accelerare la consapevolezza, perché rende tangibile un rischio che in precedenza poteva apparire remoto o difficilmente governabile; allo stesso tempo, il fatto che molte imprese fossero già intervenute prima del danno mostra che la prevenzione non nasce sempre solo come reazione all'emergenza.

Misure di prevenzione introdotte per rispondere alle calamità naturali

Il 74% delle aziende introduce misure di prevenzione : scelgono prevalentemente una copertura assicurativa ma anche misure preventive dirette sulle attività e i processi interni

AZIENDE CHE HANNO ADOTTATO MISURE DI PREVENZIONE



TIPOLOGIA DI MISURE ADOTTATE



Base: Aziende che hanno adottato misure di prevenzione; Valori %

Q.32 Quali misure sono state introdotte dalla sua azienda per contenere i danni derivanti da una calamità naturale? (Possibili più risposte)

Base: Aziende che hanno subito un danno derivante da un evento naturale; Valori %
Q.29 La Sua impresa ha introdotto delle misure di prevenzione in risposta ai maggiori casi di calamità naturali? (Solo una risposta)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 26

La misura adottata più frequentemente è la polizza assicurativa, indicata dal 49% delle imprese che hanno adottato azioni preventive. Va detto che la copertura assicurativa non è un vero e proprio strumento di prevenzione ma per sua stessa definizione interviene quando il danno è già avvenuto. È un dato coerente con la centralità dello strumento assicurativo come strumento finanziario nella gestione dei rischi catastrofali. La formazione dei dipendenti ad agire in caso di calamità naturali raggiunge il 43%, segnalando che le imprese non interpretano la prevenzione solo come trasferimento finanziario del rischio, ma anche come capacità organizzativa di risposta. Seguono misure operative e infrastrutturali, tra cui piani di continuità, interventi sugli immobili, sistemi di protezione fisica e backup dei dati. Le risposte mostrano quindi che la prevenzione non si limita alla polizza, ma include anche strumenti organizzativi e operativi. La distribuzione delle risposte indica una scelta di prevenzione composita, nella quale convivono assicurazione, formazione, protezione fisica, protezione informativa e continuità operativa.

È utile leggere questi dati come il segnale di un progressivo cambiamento nell'approccio alla prevenzione. In passato, la calamità naturale poteva essere affrontata prevalentemente attraverso logiche di ripristino, intervenendo dopo il danno con il supporto di assicurazioni e consulenti. La fotografia 2026 suggerisce invece una progressiva anticipazione della risposta. Non tutte le aziende adottano ancora un approccio integrato, ma la varietà delle misure citate mostra un progressivo ampliamento della prevenzione, che non riguarda più solo il ripristino dopo il danno.

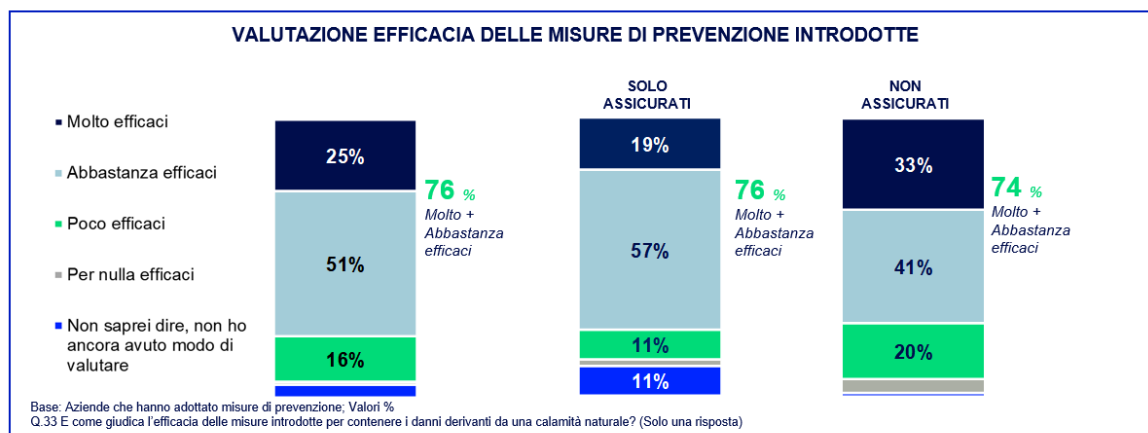
La presenza di backup regolari tra le misure di prevenzione è un dettaglio da non sottovalutare. Anche un evento fisico può generare un danno digitale, ad esempio rendendo indisponibili sistemi gestionali, archivi o dati aziendali. Il confine tra rischio fisico e rischio tecnologico è quindi sempre più sottile. Per una media impresa, proteggersi da un'alluvione o da una tromba d'aria significa anche predisporre copie dei dati, sistemi cloud, procedure di ripristino e piani di lavoro alternativi. La resilienza non è solo edilizia o assicurativa, ma anche informatica.

2.4 Efficacia percepita delle misure di prevenzione

La valutazione di efficacia conferma il valore percepito della prevenzione. Il 76% delle imprese che hanno adottato misure preventive le giudica molto o abbastanza efficaci; in particolare, una su quattro le considera molto efficaci. Il dato resta sostanzialmente stabile anche distinguendo tra aziende assicurate e non assicurate: 76% tra le prime e 74% tra le seconde. Tra le imprese non assicurate, tuttavia, è interessante osservare che la quota di chi valuta le misure molto efficaci sale al 33%.

Efficacia percepita delle misure di prevenzione delle calamità naturali

Chi adotta misure preventive le ritiene efficaci per il contenimento dei rischi: le misure preventive dirette sono percepite più efficaci delle coperture assicurative



Base: Totale campione; Valori %
Q.29 La Sua impresa ha introdotto delle misure di prevenzione in risposta ai maggiori casi di calamità naturali? (Solo una risposta)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 27

Internal And Trusted Partner Use Only Document owned by Prometeia

Ad ogni modo, la vicinanza sull'efficacia percepita da parte di imprese assicurate e imprese non assicurate suggerisce che questa non viene attribuita esclusivamente alla copertura assicurativa, ma all'insieme delle misure adottate. Le imprese sembrano riconoscere che l'assicurazione è necessaria per ridurre l'impatto economico del sinistro, ma non è sufficiente per evitare l'interruzione dell'attività o per contenere i danni operativi. Il risultato della quota di valutazioni "molto efficaci" più elevata tra le imprese non assicurate va interpretato con prudenza.

La gestione del rischio di calamità naturale sembra quindi basarsi su tre livelli: prevenzione, assicurazione e ripristino dell'attività. Le aziende che lavorano solo su uno di questi livelli possono rimanerne esposte. Ad esempio, chi si assicura ma non adotta piani di continuità può essere rimborsato, ma perdere comunque clienti e produzione; chi investe in misure dirette ma non trasferisce parte del rischio può trovarsi in difficoltà finanziaria in caso di evento severo. Il dato sulla percezione di efficacia, quindi, non deve essere letto come alternativa tra assicurazione e misure dirette, ma come conferma della necessità di un approccio integrato.

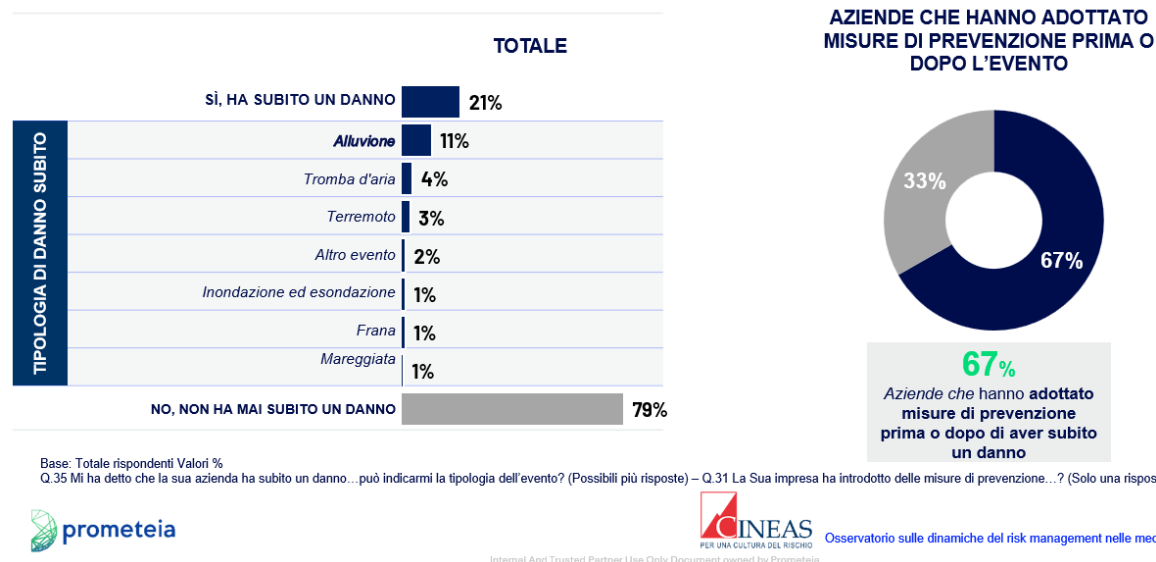
2.5 Eventi subiti, danni e gestione del danno

L'indagine mostra che il 21% delle imprese ha subito un danno derivante da un evento naturale. La maggioranza non ha quindi avuto un'esperienza diretta recente, ma la quota di aziende colpite è comunque significativa. Il fatto che una su cinque abbia subito un danno è sufficiente a rendere il rischio concreto nel tessuto delle medie imprese italiane. Secondo i risultati del questionario, tra gli eventi citati prevalgono le alluvioni, indicate dall'11% delle imprese totali, seguite da trombe d'aria, terremoti, inondazioni ed esondazioni, frane e mareggiate. La distribuzione conferma la centralità del rischio idro-meteorologico, ma richiama anche l'eterogeneità dei fenomeni a cui le imprese possono essere esposte.

Un dato rilevante è che, tra le aziende che hanno subito un danno, il 67% dichiara di aver già adottato misure di prevenzione prima dell'evento. Questo risultato suggerisce che la prevenzione non intervenga necessariamente solo dopo l'esperienza diretta del danno, ma possa essere presente anche in una fase precedente. Tuttavia, il fatto che una quota significativa di imprese fosse già intervenuta non implica automaticamente un livello di protezione sufficiente: l'evento dannoso si è comunque verificato. Il dato invita quindi a distinguere tra semplice adozione di misure preventive e loro effettiva adeguatezza rispetto ai rischi affrontati.

Eventi di calamità naturali subiti

Solo un'azienda su cinque ha subito un danno derivante da evento naturale e la maggior parte si sono assicurate prima di avere subito un danno



Quanto alla tipologia dei danni, prevalgono i danni alle strutture e alle attrezzature dell'azienda, registrati dal 41% delle imprese colpite da danni derivati da un evento naturale. Seguono l'interruzione dell'attività produttiva, al 28%, e il pericolo per i dipendenti, anch'esso intorno al 28%. Danni ai prodotti o alle merci, perdita di reddito per inattività prolungata e aumento dei costi assicurativi completano il quadro. La gerarchia delle risposte è significativa: il danno fisico agli asset è il primo livello di impatto, ma immediatamente dopo emergono continuità operativa e sicurezza delle persone. Il rischio naturale, quindi, non produce soltanto una perdita patrimoniale; produce un problema organizzativo e reputazionale.

La gestione del danno viene affidata in primo luogo a commercialisti o avvocati, citati dal 29%, seguiti da consulenti di gestione del rischio e intermediari assicurativi, entrambi intorno al 27%. Più distante è il ruolo del perito assicurativo, all'11%, mentre società di bonifica e ripristino e altre figure hanno un peso minore. Questa distribuzione suggerisce che, nella fase successiva all'evento, le imprese si rivolgono a figure di fiducia o a soggetti già presenti nel loro ecosistema professionale.

La lettura complessiva del capitolo mostra una crescente consapevolezza del rischio di calamità naturale, ma anche un processo di integrazione ancora incompleto. Monitoraggio ESG, misure preventive e coperture assicurative sono sempre più diffusi, ma non sempre sembrano ricondotti a una strategia unitaria. Il passaggio decisivo sarà collegare meglio prevenzione, trasferimento del rischio e ripristino operativo, trasformando singole iniziative in una reale capacità di resilienza aziendale.

I danni subiti riguardano prevalentemente le strutture/attrezzature dell'azienda

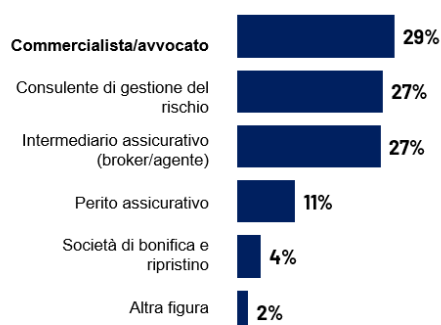
21%

Aziende che **hanno subito un danno**

TIPOLOGIA DEI DANNI SUBITI



GESTIONE DEL DANNO



Base: Aziende che hanno subito un danno derivante da un evento naturale; Valori %
 Q.36 Di quale tipologia è stato il danno subito dalla sua azienda in seguito alla calamità naturale? (Solo una risposta) - Q.37 Da chi è stato supportato nella gestione del danno subito in seguito alla calamità naturale e nella ripresa delle attività?

CAPITOLO 3. INTELLIGENZA ARTIFICIALE E RISCHIO TECNOLOGICO



3.1 Intelligenza artificiale, rischio tecnologico e rilevanza per le imprese

L'intelligenza artificiale non appare più come una tecnologia distante o limitata a pochi settori ad alta intensità digitale. Negli ultimi anni, strumenti generativi, sistemi predittivi e applicazioni di automazione sono entrati sempre più spesso nei processi aziendali. Questo ha reso più evidente il legame tra innovazione tecnologica, sicurezza dei dati, organizzazione del lavoro e continuità operative. Per le medie aziende italiane il tema non riguarda soltanto la possibilità di aumentare l'efficienza o ridurre i costi, ma anche la capacità di utilizzare la tecnologia in modo controllato, verificabile e coerente con i propri processi decisionali. In questa prospettiva, l'IA entra stabilmente nel perimetro del risk management aziendale.

Il contesto recente conferma questa centralità. Da un lato, l'evoluzione normativa europea e nazionale ha progressivamente spostato l'attenzione dall'adozione dell'IA alla sua regolamentazione e gestione, ponendo al centro temi come trasparenza, supervisione umana, protezione dei dati, sicurezza e responsabilità. Dall'altro, la crescita delle minacce informatiche e la maggiore dipendenza delle imprese da sistemi digitali, piattaforme esterne e infrastrutture tecnologiche mostrano come il rischio tecnologico possa produrre effetti concreti sull'operatività aziendale.

I recenti incidenti informatici e tecnologici hanno mostrato come il rischio digitale possa produrre effetti concreti sull'operatività delle imprese. L'interruzione globale legata a CrowdStrike nel 2024 ha evidenziato la dipendenza di imprese e servizi essenziali da software e infrastrutture esterne; l'attacco ransomware a Change Healthcare ha mostrato come un evento cyber possa compromettere processi amministrativi e rapporti con clienti e controparti; il caso della chatbot di Air Canada ha invece richiamato l'attenzione sulla responsabilità delle imprese rispetto a informazioni generate automaticamente ma non adeguatamente verificate. Questi esempi mostrano che un errore nell'uso dell'IA o un'interruzione dei sistemi digitali può avere conseguenze concrete sull'attività aziendale, dai processi interni alla relazione con clienti e fornitori. Per questo l'IA non può essere letta solo come leva di innovazione, ma anche come nuovo ambito di presidio del rischio. La sua integrazione richiede quindi competenze, regole interne e un controllo effettivo sull'utilizzo degli strumenti.

3.2 Adozione dell'IA e ambiti di utilizzo

L'edizione 2026 dell'Osservatorio dedica un'attenzione specifica all'intelligenza artificiale, considerandola una delle principali dimensioni attraverso cui leggere l'evoluzione dei rischi tecnologici per le imprese. Rispetto alle precedenti rilevazioni, il tema viene approfondito con uno speciale dedicato, costruito anche attraverso nuove domande rivolte alle aziende, con l'obiettivo di comprendere non solo il livello di utilizzo dell'IA, ma anche il grado di preparazione interna, le competenze disponibili, le iniziative di formazione e i principali rischi percepiti per la sicurezza aziendale.

La maggiore centralità dell'intelligenza artificiale nei processi aziendali è testimoniata dal progressivo aumento del suo utilizzo. Secondo i risultati dell'indagine, nel 2026 il 66% delle aziende dichiara di avere già utilizzato l'IA o sue applicazioni, con un incremento di 6 punti rispetto all'anno precedente. La quota di imprese che non ha ancora sperimentato applicazioni pratiche scende al 31%, mentre solo il 3% ritiene che l'IA non sia applicabile al proprio settore. Questi risultati indicano che la tecnologia è uscita dalla fase di curiosità generale e sta entrando progressivamente, pur con livelli di maturità differenti, nelle attività operative e organizzative delle medie imprese.

Aziende che hanno utilizzato l'IA e ambiti

Aumenta il numero delle aziende che ha sperimentato l'IA: il 66% delle aziende ha già utilizzato l'IA all'interno dei processi



Base: Totale rispondenti Valori %
Q.4 La sua azienda ha avuto modo di utilizzare l'IA (Intelligenza Artificiale) o le sue applicazioni? (Possibili più risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 31

Internal And Trusted Partner Use Only Document owned by Prometeia

Gli ambiti di utilizzo descrivono un'adozione ancora distribuita e non concentrata su una sola funzione. Il 28% cita la fase di produzione per automatizzare i processi; il 24% la progettazione; il 23% il tracciamento delle prestazioni del prodotto e i test di qualità; il 21% il customer care; il 20% la fase di produzione per limitare gli incidenti e garantire maggiore sicurezza dei dipendenti; il 12% l'inserimento dell'IA come elemento di novità nei prodotti o servizi offerti. La gerarchia delle risposte mostra che le imprese usano l'IA soprattutto come tecnologia di efficienza e controllo, per automatizzare, progettare meglio, verificare la qualità, gestire interazioni e ridurre alcuni rischi operativi. Ma il contesto è dinamico e in piena evoluzione, a breve potremmo assistere a qualche significativo cambiamento della classifica delle risposte.

Il dato sulla sicurezza dei dipendenti è particolarmente interessante. L'IA non viene percepita solo come strumento per accelerare processi o ridurre costi, ma anche come possibile leva di prevenzione. Alcune applicazioni possono infatti contribuire a ridurre incidenti e situazioni pericolose, collegando l'innovazione tecnologica alla prevenzione del rischio. Questa dimensione collega l'IA al tema più generale del risk management: l'innovazione tecnologica non è rilevante solo quando produce nuovi ricavi, ma anche quando migliora la capacità di prevenire danni e di conseguenza di contenerne i costi.

Allo stesso tempo, la quota di imprese che non ha ancora sperimentato l'IA va letta anche alla luce di un contesto nazionale in cui l'adozione di queste tecnologie nel sistema produttivo appare ancora meno avanzata rispetto ad altri paesi europei. Questo ritardo nell'adozione non dipende necessariamente da una semplice resistenza all'innovazione, ma riflette spesso la presenza di vincoli organizzativi, tecnici e strategici. Per molte imprese, soprattutto di dimensione medio piccola, la questione non è soltanto se adottare l'IA, ma come inserirla in modo coerente nei processi aziendali. Ne deriva un quadro in cui l'IA si diffonde con intensità crescente, ma la sua integrazione resta selettiva e dipende dalla capacità dell'impresa di collegare la tecnologia a obiettivi operativi, organizzativi e gestionali concreti.

3.3 Rischi e opportunità percepiti

Dal lato dei rischi, la sicurezza dei dati è la prima preoccupazione, citata dal 31%, superando la sostituzione del lavoro umano, al 29%, che era al primo posto nel ranking 2025. Seguono le questioni legali, al 26%, gli investimenti necessari per l'acquisto della strumentazione e la limitatezza delle strutture, entrambe al 22%. Il cambiamento rispetto all'anno precedente è rilevante: la paura della sostituzione del lavoro resta forte, ma viene affiancata e superata da rischi più specifici di governance, protezione informativa e compliance.

Questo spostamento indica che le imprese stanno leggendo i rischi dell'IA in modo più concreto. Nelle prime fasi di diffusione, l'IA è spesso letta attraverso timori generali, legati all'automazione, alla riduzione del lavoro umano e al cambiamento dei ruoli. Man mano che le imprese iniziano a sperimentarla emergono questioni più operative, sulla qualità dei dati, controllo degli output, responsabilità legali, investimenti e affidabilità delle infrastrutture.

Rischi e opportunità percepiti sulla IA

La «sicurezza dei dati» supera la «sostituzione del lavoro» umano tra i rischi dell'IA, mentre «l'efficientamento del lavoro» si conferma tra le opportunità



Base: Totale rispondenti; Valori %

Q.5 Secondo Lei, quali sono i fattori che potrebbero rappresentare un rischio all'introduzione dell'intelligenza artificiale nella sua impresa o nelle imprese del suo settore? (Massimo 5 risposte)

Q.6 E secondo Lei, in quali aree la sua azienda o le aziende del suo settore potranno trarre i maggiori vantaggi dall'evoluzione tecnologica e dall'introduzione dell'intelligenza artificiale? (Massimo 5 risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 32

Internal And Trusted Partner Use Only Document owned by Prometeia

Sul lato delle opportunità, l'organizzazione del lavoro più efficiente è al primo posto, con il 39%, seguita dalla possibilità di elaborare enormi quantità di dati molto velocemente, al 36%, e dai processi produttivi più efficienti, al 31%. Minori costi di produzione e possibilità di pianificare in anticipo si collocano entrambe al 25%. Anche qui emerge un profilo coerente: l'IA è vista soprattutto come leva di efficienza, capacità analitica e supporto alla pianificazione. Non prevale ancora l'idea di una tecnologia che crea nuovi modelli di business radicali; prevale invece la sua applicazione all'ottimizzazione di processi esistenti.

Questa lettura è coerente con la struttura delle medie imprese italiane. In questi contesti, l'IA può produrre valore anche senza rivoluzionare il modello di business: ridurre errori, migliorare la previsione della domanda, ottimizzare turni e magazzini, accelerare progettazione e controllo qualità, supportare customer care e manutenzione. Il contributo dell'IA può essere incrementale, ma non per questo marginale.

3.4 Sperimentazione e percezione di rischi e opportunità

In questa sezione viene approfondito il rapporto tra esperienza d'uso dell'IA e percezione dei suoi rischi e delle sue opportunità. Dal lato dei rischi, il dato più interessante non riguarda tanto la quantità complessiva di preoccupazione, perché la quota di imprese che cita almeno un rischio resta pari all'83% sia tra chi ha già utilizzato l'IA sia tra chi non l'ha ancora sperimentata. La differenza principale riguarda piuttosto il tipo di rischi indicati.

Tra le aziende che non hanno ancora utilizzato l'IA prevalgono rischi più generali e immediatamente riconoscibili. La sicurezza dei dati viene citata dal 37%, contro il 29% tra chi ha già sperimentato l'IA, mentre la sostituzione del lavoro umano raggiunge il 36% tra le non utilizzatrici e scende al 25% tra le utilizzatrici. Anche la limitatezza delle strutture tecnologiche e la scarsa affidabilità della tecnologia risultano leggermente più presenti tra le imprese che non hanno ancora avuto un'esperienza diretta. Al contrario, tra le aziende che hanno già utilizzato l'IA emergono con più forza rischi di tipo organizzativo e gestionale. Le questioni legali salgono al 28%, rispetto al 22% tra chi non ha utilizzato l'IA. Crescono anche la preoccupazione per la capacità di adattamento dei dipendenti, indicata dal 25% contro il 17%, e quella per il cambiamento della cultura del management, citata dal 23% contro il 17%. Ancora più evidente è il caso dei partner tecnologici inadeguati, che vengono segnalati dal 25% delle imprese utilizzatrici, contro il 12% delle non utilizzatrici.

Questi scostamenti suggeriscono che la sperimentazione dell'IA non elimina la percezione del rischio, ma la rende più concreta. Le imprese che non hanno ancora adottato queste soluzioni tendono a concentrarsi su timori più ampi, come la perdita di posti di lavoro o la violazione dei dati. Le imprese che le hanno già utilizzate, invece, sembrano misurarsi con problemi più vicini alla gestione quotidiana: regole, competenze, responsabilità, qualità dei fornitori e capacità interna di integrare l'IA nei processi aziendali.

In questo senso, l'esperienza diretta può essere letta come una forma di apprendimento organizzativo. Usare l'IA non significa percepirla come priva di rischi, ma consente di distinguere meglio quali rischi devono essere presidiati e con quali strumenti. La sperimentazione controllata diventa quindi un passaggio utile, a condizione

Rischi percepiti sulla IA da chi l'ha sperimentata e chi no

La sperimentazione dell'IA riduce la percezione del rischio

I RISCHI DELL'IA RANKING, AZIENDE 2026 (TOP 10)



Base: Totale rispondenti; Valori %

Q.5 Secondo Lei, quali sono i fattori che potrebbero rappresentare un rischio all'introduzione dell'intelligenza artificiale nella sua impresa o nelle imprese del suo settore? (Massimo 5 risposte)

che sia accompagnata da formazione, regole interne, valutazione degli impatti e una chiara attribuzione delle responsabilità.

Opportunità percepita sulla IA da chi l'ha sperimentata e chi no

Aumenta la consapevolezza dei vantaggi legati all'utilizzo dell'IA da chi l'ha sperimentata

I VANTAGGI DELL'IA RANKING, AZIENDE 2026 (TOP 10)



Base: Totale rispondenti; Valori %

Q.6 E secondo Lei, in quali aree la sua azienda o le aziende del suo settore potranno trarre i maggiori vantaggi dall'evoluzione tecnologica e dall'introduzione dell'intelligenza artificiale? (Massimo 5 risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 34

Internal And Trusted Partner Use Only Document owned by Prometeia

Guardando alle opportunità, l'esperienza d'uso dell'IA sembra rendere più concreti alcuni benefici. Le imprese che hanno già utilizzato l'intelligenza artificiale indicano più spesso vantaggi legati all'efficienza operativa: l'organizzazione del lavoro più efficiente sale al 40%, contro il 37% tra chi non l'ha utilizzata; i processi produttivi più efficienti arrivano al 33%, contro il 28%; la riduzione dei costi di produzione raggiunge il 27%, contro il 20%. Ancora più marcata è la differenza sul miglioramento della qualità dei prodotti e dei servizi, citato dal 26% delle imprese utilizzatrici rispetto al 13% delle non utilizzatrici. Lo stesso andamento si osserva su altri benefici più vicini alla gestione quotidiana dell'impresa.

Non tutti i benefici, però, risultano più elevati tra chi ha già utilizzato l'IA. La possibilità di elaborare grandi quantità di dati è indicata più spesso dalle imprese non utilizzatrici, 39% contro 35%, così come la creazione di nuovi modelli di business, 30% contro 21%. Il dato segnala una differenza interessante: chi non ha ancora usato l'IA tende a immaginarne soprattutto il potenziale generale; chi l'ha già provata guarda di più agli effetti pratici, come efficienza, qualità, riduzione dei costi e organizzazione del lavoro.

Nel complesso, il confronto suggerisce che l'IA appare più utile quando viene applicata a problemi reali. La sperimentazione non aumenta semplicemente l'ottimismo verso la tecnologia, ma rende più chiaro dove essa possa produrre valore per l'impresa.

3.5 Focus sulle aziende potenzialmente utilizzatrici di IA

Il focus dedicato all'Intelligenza Artificiale ha interessato 52 aziende su 380, individuate come potenzialmente utilizzatrici, in particolare realtà medio-grandi dove l'IA è stata sperimentata o valutata. Questo sotto-campione offre una fotografia utile delle imprese che stanno già usando l'IA o che la stanno valutando in modo operativo. Il questionario include 6 domande su utilizzo, competenze, rischi e gestione degli stessi attraverso la formazione. La rilevanza del focus consiste proprio nel mostrare cosa accade quando l'IA non è più soltanto un tema di scenario, ma entra nei processi, nelle competenze e nella formazione.

Focus sull'Intelligenza Artificiale

Il focus sull'Intelligenza Artificiale ha interessato solo una parte del campione e nello specifico grandi aziende dove teoricamente l'utilizzo dell'IA è già stato sperimentato o è stato valutato



TARGET

Medio Grandi aziende
250-499 addetti



DIMENSIONE CAMPIONARIA

52 interviste
equidistribuite per
dimensione (addetti),
territorio, settore e
riportate all'universo



LUNGHEZZA DEL QUESTIONARIO

6 domande su
Utilizzo, competenze,
rischi e gestione degli
stessi attraverso la
formazione



PERIODO DI RILEVAZIONE

Marzo 2026



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 35

Internal And Trusted Partner Use Only Document owned by Prometeia

Questo focus non va letto come una rappresentazione dell'intero universo delle imprese intervistate, ma come un approfondimento qualitativo sulle realtà più vicine all'adozione concreta o alla valutazione operativa della tecnologia.

Tra queste aziende, il 69% dichiara un utilizzo concreto dell'IA. In particolare, il 40% afferma che l'IA è già inserita in alcuni processi o attività aziendali, il 29% che ha già prodotto cambiamenti rilevanti nell'organizzazione o nel modo di lavorare, mentre il 5% segnala un utilizzo ancora limitato e sperimentale. Il 25% non utilizza ancora strumenti o applicazioni di IA. Sul piano della preparazione percepita, il 61% si considera molto o abbastanza preparato: 23% molto preparata e 38% abbastanza preparata. Resta però un 14% poco preparato, oltre al 25% che non utilizza IA.

La distanza tra utilizzo concreto e preparazione percepita merita attenzione. Lo scarto tra chi utilizza concretamente l'IA e chi si percepisce preparato suggerisce che alcune imprese stanno già usando strumenti di IA senza sentirsi pienamente attrezzate a farlo. È una condizione tipica delle tecnologie a rapida diffusione, e per il risk management, il punto non è solo favorire l'adozione, ma accompagnarla con regole, competenze e strumenti di controllo. L'IA può entrare in azienda attraverso sperimentazioni informali, strumenti disponibili online, iniziative di singole funzioni o fornitori esterni; senza regole e competenze, l'utilizzo può crescere più velocemente della capacità di controllo.

Il livello di utilizzo dell'Intelligenza Artificiale..

IA è già parte dei processi aziendali e ne determina i cambiamenti e le aziende si percepiscono preparate nel suo utilizzo



Base: Aziende potenzialmente utilizzatrici di IA (campione di 52 aziende su 380); Valori %
 Q.4B E come descriverebbe oggi il livello di utilizzo dell'Intelligenza Artificiale nella sua azienda?
 Q.4bis Quanto ritiene che la sua azienda sia oggi preparata all'utilizzo dell'Intelligenza Artificiale? (Solo una risposta)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 36

Internal And Trusted Partner Use Only Document owned by Prometeia

3.6 Competenze interne in azienda

Di pari passo con l'adozione dell'intelligenza artificiale cresce l'esigenza di presidiare le competenze interne, la formazione del personale e gli impatti sulla sicurezza aziendale. L'IA, infatti, non richiede soltanto strumenti tecnologici, ma anche capacità organizzative adeguate a utilizzarla in modo efficace, controllarne i rischi e integrarla correttamente nei processi aziendali. Solo 7 delle 52 aziende potenzialmente utilizzatrici campionate ritengono di disporre di competenze pienamente adeguate a utilizzare l'IA in modo efficace e gestirne i principali rischi. Il 31% dichiara competenze adeguate solo in parte, il 30% le considera ancora insufficienti e il

..E le competenze in azienda

Solo 1 su 7 ritiene di avere competenze adeguate e pertanto si stanno attrezzando con formazione interna al personale



Base: Aziende potenzialmente utilizzatrici di IA (campione di 52 aziende su 380); Valori %
 Q.4tris Ritiene che la sua azienda disponga oggi di competenze interne adeguate per utilizzare l'Intelligenza Artificiale in modo efficace e gestirne i principali rischi? (Solo una risposta)
 Q.4quater Rispetto all'introduzione dell'Intelligenza Artificiale, cosa sta facendo oggi la sua azienda per il personale? (Possibili più risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 37

Internal And Trusted Partner Use Only Document owned by Prometeia

25% non utilizza attualmente l'IA. In sintesi, anche tra le aziende più vicine all'adozione, sono ancora poche quelle che si sentono pienamente preparate.

Le iniziative di formazione mostrano una risposta in corso. Il 45% delle imprese campionate sta definendo regole interne per un uso corretto dell'IA; il 39% sta aggiornando le competenze digitali del personale; il 26% sta formando il personale sull'uso pratico degli strumenti; il 18% sui rischi legati all'utilizzo dell'IA; il 12% sta accompagnando responsabili e management nell'integrazione dell'IA nei processi aziendali. Solo il 4% dichiara che al momento non sono previste iniziative specifiche per il personale. Il dato più alto è quello relativo alle regole interne: ciò suggerisce che le imprese percepiscono l'urgenza di stabilire confini, policy e indicazioni operative prima ancora di completare la formazione tecnica.

La definizione di regole interne sull'utilizzo dell'IA è un passaggio importante, ma per essere davvero utile, deve tradursi in istruzioni operative chiare, comprensibili e applicabili nei diversi contesti aziendali. Per le imprese diventa quindi utile definire quali strumenti possono essere utilizzati, per quali attività e con quali limiti. Un punto particolarmente delicato riguarda i dati, perché non tutte le informazioni aziendali possono essere caricate su strumenti di IA senza una valutazione preventiva.

Allo stesso modo, è necessario chiarire come devono essere gestiti gli output prodotti dall'intelligenza artificiale. Le risposte generate dai sistemi non possono essere considerate automaticamente corrette, complete o utilizzabili senza controllo. È quindi utile chiarire come verificare gli output dell'IA e chi mantiene la responsabilità finale delle decisioni. Anche la scelta dei fornitori tecnologici rientra in questo presidio. In questa prospettiva, le regole interne non servono a frenare l'utilizzo dell'IA, ma a renderlo più sicuro e coerente con i processi aziendali.

3.7 Formazione e sicurezza aziendale

Il tema della governance interna trova un ulteriore riscontro nelle risposte legate ai rischi per la sicurezza aziendale. Secondo il questionario, il primo ambito di rischio è la protezione dei dati aziendali e delle informazioni riservate, citata dal 29%. Seguono la formazione del personale, al 23%, e la difesa da attacchi cyber, frodi digitali o accessi non autorizzati, al 20%. Supervisione delle decisioni automatizzate e controllo qualità/prevenzione errori sono entrambi al 15%; affidabilità di macchinari e sistemi automatizzati e continuità operativa si collocano intorno al 12% e all'11%, così come gestione dei fornitori tecnologici e dipendenza da piattaforme esterne. Il risultato conferma che il rischio IA non viene percepito soltanto come una questione etica, occupazionale o di trasformazione del lavoro. Nelle valutazioni delle imprese assume anche una dimensione più operativa, legata alla protezione dei dati, alla sicurezza dei sistemi e alla continuità dei processi aziendali.

Ambiti percepiti di maggior rischio per la sicurezza aziendale

La protezione dei dati, la mancata formazione del personale e la cybersecurity sono i principali rischi percepiti nell'utilizzo dell'IA

PERCEZIONE DEI RISCHI IA PER LA SICUREZZA AZIENDALE
(valori %)



Base: Aziende potenzialmente utilizzatrici di IA (campione di 52 aziende su 380); Valori % Q.6tris A suo avviso, in quali ambiti l'utilizzo dell'Intelligenza Artificiale può creare i maggiori rischi per la sicurezza aziendale nella sua impresa o nelle imprese del suo settore? (Max tre risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 38

Internal And Trusted Partner Use Only Document owned by Prometeia

Le competenze indicate dalle imprese delineano le principali aree su cui intervenire per rendere l'adozione dell'IA più sicura e controllata. Al primo posto c'è la formazione pratica dei dipendenti, indicata dal 37%; seguono le competenze di cybersecurity e protezione dei dati, al 29%; la capacità di mantenere supervisione umana e procedure di verifica, al 22%; la conoscenza delle regole, al 21%; la capacità del management di integrare l'IA nei processi in modo controllato, al 18%; la capacità di valutare l'affidabilità dei risultati, al 17%. La gerarchia è chiara: l'adozione dell'IA richiede un insieme di competenze tecniche, organizzative e regolative: non basta introdurre la tecnologia, bisogna anche saperla governare.

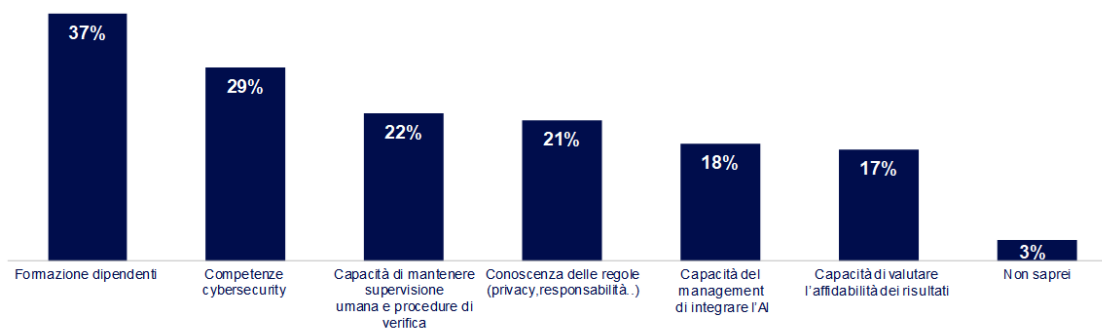
Nel complesso, i risultati mostrano che l'intelligenza artificiale è ormai entrata nell'agenda delle medie imprese, ma non ancora in modo pienamente maturo e uniforme. Le aziende ne riconoscono il potenziale, soprattutto in termini di efficienza organizzativa, capacità di elaborare grandi quantità di dati, miglioramento dei processi produttivi e supporto alla pianificazione. Allo stesso tempo, però, l'IA viene associata a rischi che toccano aspetti centrali dell'attività aziendale, come la protezione dei dati, la sicurezza informatica, le responsabilità legali, la continuità operativa, le qualità degli output e l'impatto sul lavoro.

Per questo motivo, la diffusione dell'IA non può essere letta soltanto attraverso il numero di imprese che la utilizzano. Il punto decisivo riguarda il modo in cui viene adottata. Per le medie imprese, usare l'intelligenza artificiale in modo efficace significa inserirla nei processi con obiettivi chiari, regole interne, competenze adeguate e controllo sulle decisioni, sui dati e sulle responsabilità. In questa prospettiva, l'IA diventa non solo uno strumento di innovazione, ma anche un nuovo ambito del risk management.

Competenze ritenute importanti per la riduzione dei rischi legati all'IA

Formazione dipendenti, competenze di cybersecurity e capacità di mantenere la supervisione sono gli ambiti che consentiranno di ridurre i rischi legati all'utilizzo dell'IA

COMPETENZE PER LA RIDUZIONE DEI RISCHI DELL'IA
(valori %)



Base: Aziende potenzialmente utilizzatori di IA (campione di 52 aziende su 380); Valori %
Q.6bis A suo avviso, quali competenze saranno più importanti per ridurre i rischi legati all'adozione dell'AI nelle PMI? (Massimo tre risposte)

CAPITOLO 4. SISTEMI DI GESTIONE DEL RISCHIO



4.1 Dalla consapevolezza alla gestione strutturata del rischio

Dopo l'approfondimento sui rischi specifici, l'indagine si concentra sul modo in cui le medie imprese organizzano internamente la gestione del rischio. In un contesto caratterizzato da minacce sempre più interconnesse, come quelle climatiche, tecnologiche, cyber e geopolitiche, la sola consapevolezza dei rischi rappresenta un primo passaggio. Diventa però importante osservare se le aziende dispongano anche di strumenti, responsabilità e processi adeguati a presidiarli.

Le evidenze dell'Osservatorio indicano un livello di strutturazione ormai significativo. Più del 60% delle imprese dichiara di adottare un modello di mappatura dei rischi a livello di Consiglio di Amministrazione, mentre il 75% ha realizzato un metodo di gestione dei rischi. Sono due indicatori che segnalano il passaggio verso un approccio più formalizzato, in cui i rischi vengono identificati, classificati e collegati a responsabilità organizzative più definite.

Accanto agli strumenti, resta centrale il tema delle responsabilità. La supervisione è affidata soprattutto al Risk Manager o al titolare dell'impresa, a conferma di una funzione che si sta progressivamente professionalizzando, pur mantenendo spesso un presidio diretto del vertice aziendale. L'efficacia del sistema dipende però dalla capacità di integrare la gestione del rischio con le diverse funzioni aziendali, evitando che resti confinata a un singolo ufficio o a un adempimento formale.

Il quadro è completato dal ricorso alle coperture assicurative. Le aziende si proteggono in media con circa 6-7 prodotti assicurativi tra quelli indagati, con valori più elevati in alcuni settori, come farmaceutica e metallurgia. Accanto alle coperture più tradizionali, una parte crescente del budget viene destinata a rischi oggi percepiti come più centrali, tra questi le calamità naturali e il cyber risk.

L'analisi dei dati consente quindi di osservare il livello di maturità raggiunto dalle imprese italiane. Da un lato, emerge una crescente attenzione verso approcci più strutturati; dall'altro, resta importante verificare quanto questi strumenti siano effettivamente integrati nella governance aziendale e nelle scelte operative. La qualità

del sistema di gestione del rischio dipende infatti non solo dalla presenza formale di procedure, ma dalla loro capacità di orientare decisioni, investimenti e comportamenti organizzativi.

4.2 Importanza percepita e comitati presenti in azienda

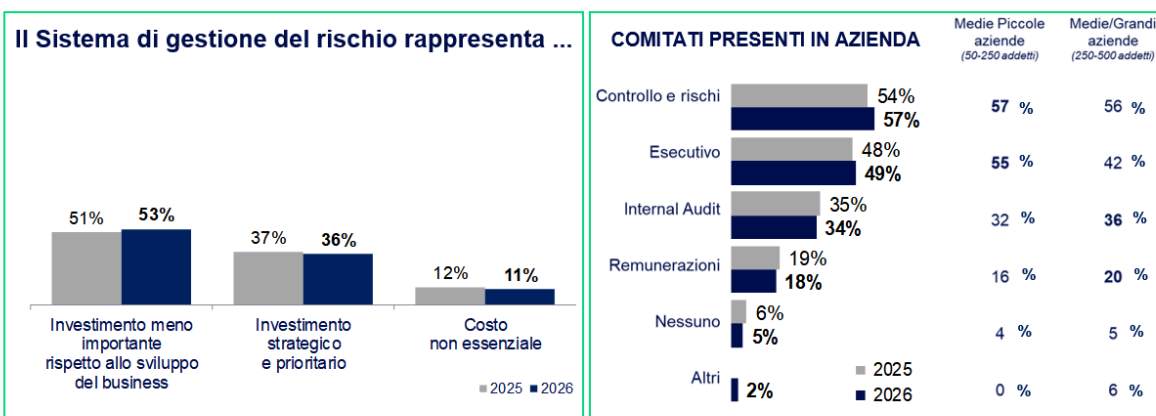
La sezione sui sistemi di gestione del rischio mostra un quadro in evoluzione, ma non privo di ambivalenze. Alla domanda su come venga considerata la realizzazione di un sistema di gestione del rischio, il 53% delle imprese lo definisce un investimento meno importante rispetto a quelli legati allo sviluppo del business; il 36% lo considera un investimento strategico e prioritario; l'11% un costo non essenziale. Rispetto al 2025, il peso dell'investimento strategico resta sostanzialmente stabile. La gestione del rischio viene quindi riconosciuta dalle imprese, ma fatica ancora a imporsi come leva primaria di competitività.

Occorre però considerare che quando le imprese indicano che la gestione del rischio è meno importante rispetto allo sviluppo dell'attività, il dato non va letto necessariamente come disinteresse verso il tema. Non significa necessariamente che il rischio venga ignorato, ma più semplicemente, tendono a privilegiare investimenti con ritorni più immediati. Il punto è che crescita e protezione del business restano collegate: un investimento può risultare fragile se non considera anche i rischi che possono comprometterne la continuità.

Sul versante della governance, i comitati più presenti sono Controllo e Rischi, al 57%, e Comitato Esecutivo, al 49%. Seguono Internal Audit, al 34%, e Remunerazioni, al 18%. Solo il 5% dichiara di non avere comitati rilevanti. La presenza dei comitati è più articolata nelle aziende medio-grandi: ad esempio, l'Internal Audit raggiunge il 36% nella fascia 250-500 addetti, contro il 32% nelle aziende 50-250; il Comitato Remunerazioni è al 20% contro il 16%; la voce "altri" è più presente nelle realtà maggiori. La differenza dimensionale conferma che la strutturazione del risk management cresce con la complessità organizzativa.

Importanza percepita di sistemi di gestione del rischio

La gestione del rischio continua ad essere subordinata allo sviluppo del business



Base: Totale rispondenti; Valori %
 Q.19 All'interno della sua azienda come viene considerata la realizzazione di un sistema di "gestione del rischio"? (Solo una risposta)
 Q.16 Quale di questi Comitati è presente nella Sua azienda? (Possibili più risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |41

Il dato sui comitati è importante perché aiuta a capire quanto la gestione del rischio sia collegata alle decisioni aziendali. La presenza di un Comitato Controllo e Rischi segnala che esiste un presidio dedicato alla supervisione del tema; il coinvolgimento del Comitato Esecutivo, invece, indica un possibile legame più diretto con le scelte operative e strategiche dell'impresa. Tuttavia, la presenza di un comitato non basta da sola a garantire una gestione efficace. Perché il sistema funzioni davvero, la presenza deve essere accompagnata da attività concrete.

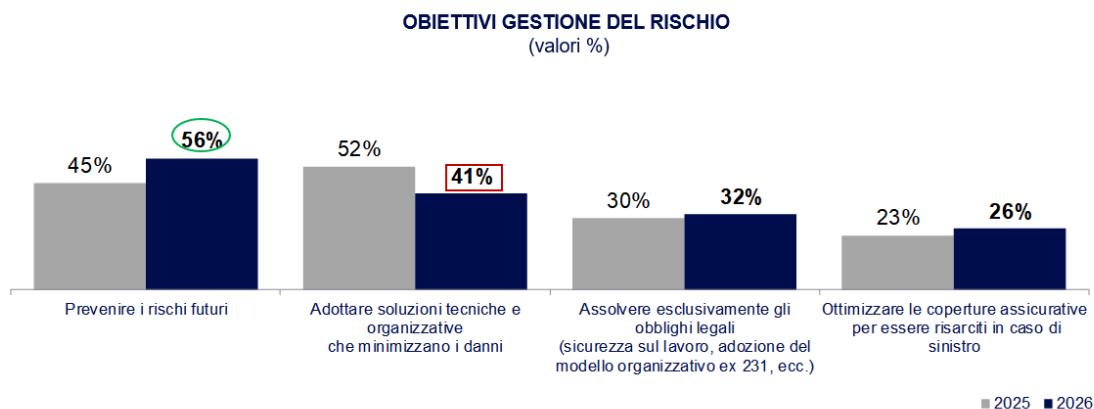
4.3 Bisogni a cui risponde la gestione del rischio

Dopo aver osservato come le imprese strutturano la governance del rischio, è utile capire quale funzione attribuiscono concretamente al risk management. Dai dati emerge che la gestione del rischio viene associata sempre di più alla prevenzione di rischi futuri. Il 56% delle imprese afferma che risponde al bisogno di prevenire i rischi futuri, in aumento rispetto al 45% del 2025. Il 41% la collega all'adozione di soluzioni tecniche e organizzative che minimizzano i danni, in calo rispetto al 52% dell'anno precedente. Il 32% la associa all'assolvimento degli obblighi legali, mentre il 26% all'ottimizzazione delle coperture assicurative. Il risultato mostra un passaggio interessante: cresce l'idea di prevenzione e anticipazione, mentre perde peso la dimensione più strettamente tecnica di contenimento del danno. L'aumento della prevenzione dei rischi futuri è coerente con il contesto descritto nei capitoli precedenti. Calamità naturali, cyber risk e IA sono rischi che non possono essere gestiti solo dopo l'evento, ma richiedono monitoraggio, preparazione e capacità di intervento. Il calo delle soluzioni tecniche non indica necessariamente una minore attenzione al tema; può segnalare, piuttosto, che le imprese stanno descrivendo la gestione del rischio in termini più ampi.

La quota del 32% sugli obblighi legali mostra che la compliance resta importante. Sicurezza sul lavoro, privacy, modelli organizzativi, normative ambientali e requisiti di settore sono driver concreti di risk management. Il punto è evitare che la gestione del rischio venga ridotta ad adempimento. Il rispetto delle norme resta necessario, ma da solo non basta a preparare l'impresa di fronte a eventi imprevisti. Un'azienda può essere formalmente conforme e tuttavia non pronta a gestire un'interruzione cyber, un'alluvione, un blocco di forniture o una crisi reputazionale. Il valore strategico del risk management emerge quando l'obbligo normativo diventa base minima su cui costruire capacità di anticipazione.

Bisogni cui rispondono i sistemi di gestione del rischio

La gestione del rischio non è valutata solo un obbligo normativo ma anche una pratica necessaria di prevenzione



Base: Totale rispondenti. Valori %
Q.18 Secondo lei a quali bisogni risponde la "gestione del rischio"? (Massimo due risposte)



Valori superiori di almeno 5 punti rispetto al totale
Valori inferiori di almeno 5 punti rispetto al totale

Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 42

4.4 Modelli di mappatura dei rischi

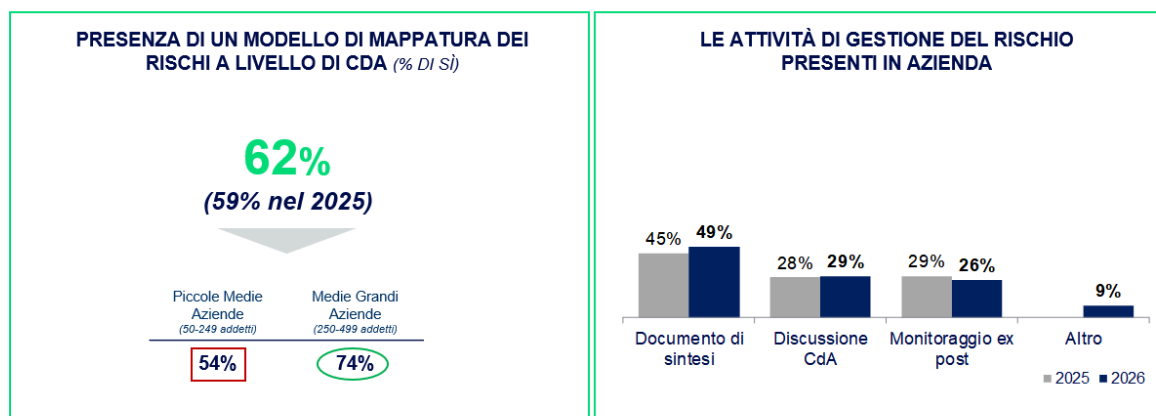
Un indicatore del livello di organizzazione della gestione del rischio è la presenza di strumenti formalizzati per identificare e monitorare i principali rischi aziendali. In particolare, la mappatura dei rischi a livello di Consiglio d'Amministrazione indica l'esistenza di un sistema che porta i rischi più rilevanti all'attenzione del CdA, rendendoli parte delle valutazioni strategiche e non solo della gestione operativa. Il 62% delle imprese dichiara la presenza di un modello di mappatura dei rischi a livello di Consiglio d'Amministrazione, in crescita rispetto al 59% del 2025. Il dato conferma una progressiva istituzionalizzazione della gestione del rischio. La differenza dimensionale è però netta: il modello è presente nel 54% delle aziende con 50-250 addetti e nel 74% delle aziende più grandi con 250-500 addetti. La distanza di 20 punti percentuali mostra che la maturità del risk

management resta legata alla dimensione aziendale, alla disponibilità di competenze interne e alla maggiore complessità organizzativa delle imprese più grandi.

La crescita della mappatura a livello di CdA è particolarmente significativa perché sposta il rischio dal piano operativo al piano di governance. Quando il rischio entra nel CdA, diventa parte della valutazione strategica dell'impresa. Questo passaggio è essenziale per rischi come IA e cyber, che possono essere sottovalutati se confinati alle funzioni tecniche. La mappatura a livello di CdA non deve però trasformarsi in una fotografia statica. In un contesto di rapido cambiamento, la mappa dei rischi risulta più utile quando viene aggiornata, discussa e collegata a scenari.

Aziende che hanno modelli di mappatura dei rischi e relative attività

Cresce l'adozione di un modello di mappatura dei rischi a livello di CdA



Base: Totale rispondenti; Valori %

Q.17 Nella sua azienda esiste un modello di mappatura dei rischi a livello del CdA? (Solo una risposta)

Q.20 Quali delle seguenti attività relative alla gestione del rischio sono presenti nella Sua azienda? (Massimo due risposte)

○ Valori superiori di almeno 5 punti rispetto al totale

□ Valori inferiori di almeno 5 punti rispetto al totale



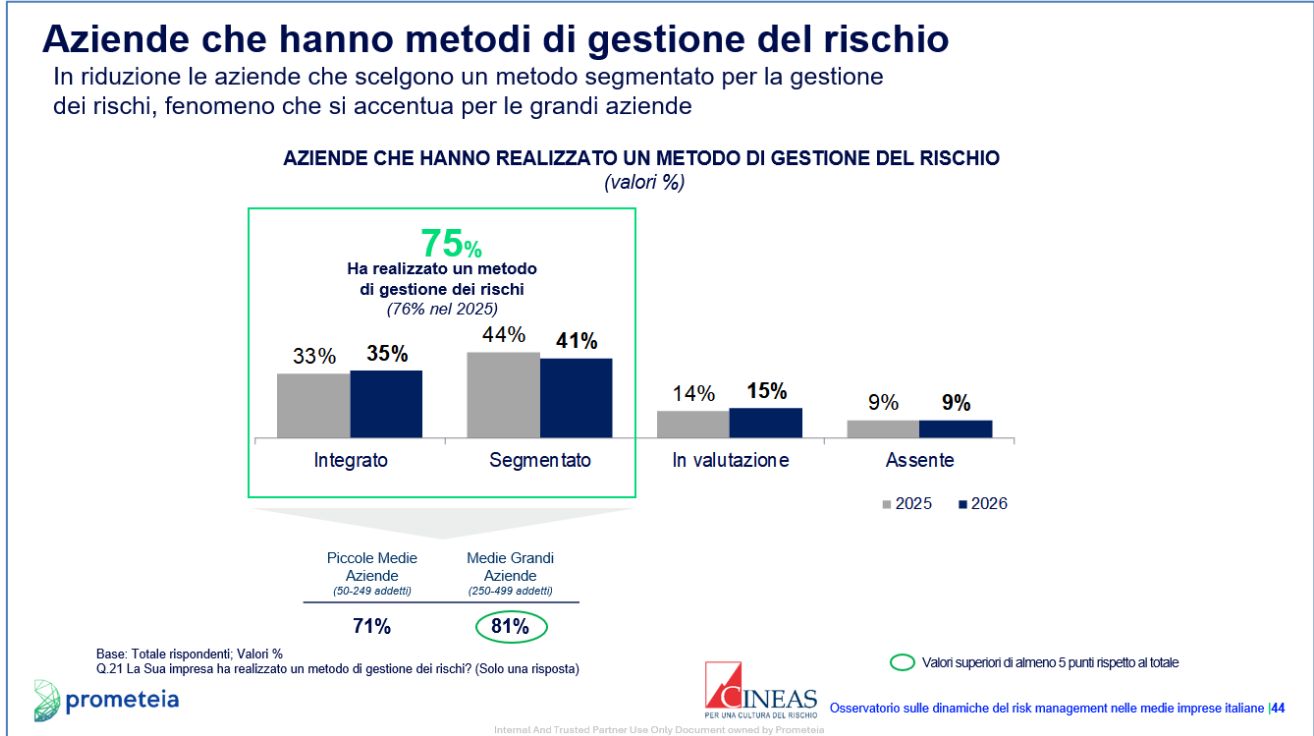
Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 43

Internal And Trusted Partner Use Only Document owned by Prometeia

Tra le attività di gestione del rischio presenti in azienda, secondo i risultati dell'indagine il documento di sintesi raggiunge il 49%, la discussione in CdA il 29% e il monitoraggio ex post il 26%. Il documento di sintesi è l'attività più diffusa, e rappresenta un passaggio importante perché permette di rendere visibile il rischio, aggregando informazioni che spesso sono distribuite tra funzioni diverse. Tuttavia, la vera efficacia dipende dalla qualità del processo successivo. Il documento deve essere discusso, aggiornato periodicamente e collegato a decisioni concrete. La sola produzione del documento non garantisce che la gestione del rischio sia effettivamente integrata nei processi aziendali.

4.5 Metodi di gestione: integrato, segmentato, in valutazione

Riguardo la metodologia di gestione del rischio, il 75% delle imprese dichiara nel questionario di avere realizzato un metodo di gestione del rischio, dato sostanzialmente stabile rispetto al 76% del 2025. La composizione



interna mostra il 35% con sistema integrato, il 41% con gestione segmentata, il 15% attualmente in valutazione e il 9% senza metodo. La gestione segmentata resta quindi più diffusa del sistema integrato, pur con una lieve riduzione rispetto al 2025. Le aziende medio-grandi presentano un livello di adozione più elevato: 81% contro il 71% delle aziende con 50-250 addetti.

La presenza di modelli segmentati può essere letta come il riflesso di una gestione ancora organizzata per ambiti specifici. Per molte medie imprese è un approccio funzionale, perché rende chiare competenze e responsabilità. Tuttavia, l'interconnessione tra i rischi rende sempre più utile rafforzare il coordinamento tra le diverse aree aziendali, soprattutto quando uno stesso evento può avere effetti su più funzioni.

4.6 Supervisione del sistema di gestione dei rischi

Per quanto riguarda la supervisione del sistema di gestione dei rischi, tra le aziende che hanno realizzato un metodo di gestione del rischio, il Risk Manager si conferma il principale responsabile della supervisione, con il 42%, in crescita rispetto al 38% del 2025. Seguono il titolare dell'impresa, al 22%, il direttore finanziario o amministrativo, al 19%, il responsabile Internal Audit, al 10%, l'Insurance Manager, al 6%, e altre figure, all'1%.

Il rafforzamento del Risk Manager è uno dei segnali più chiari di professionalizzazione della funzione. La supervisione del rischio tende progressivamente a essere affidata a una figura dedicata, anziché restare dispersa tra proprietà, amministrazione o consulenti esterni.

Il calo del direttore finanziario o amministrativo, dal 29% al 19%, è altrettanto significativo, poiché indica una distinzione più chiara tra gestione economico-finanziaria e governo complessivo del rischio. Il CFO resta un interlocutore importante, ma rischi come cyber, IA, clima e supply chain richiedono competenze più trasversali.

A chi spetta la supervisione del sistema di gestione dei rischi

Il Risk Manager si conferma il principale responsabile nella supervisione del rischio



Base: hanno realizzato un metodo di gestione dei rischi Valori %
Q.22 A chi spetta la responsabilità della supervisione del sistema di gestione dei rischi nella Sua azienda? (Solo una risposta)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |45

Internal And Trusted Partner Use Only Document owned by Prometeia

La presenza ancora rilevante del titolare dell'impresa, al 22%, ricorda però che molte medie imprese conservano modelli decisionali concentrati. Questo può essere un vantaggio in termini di rapidità, ma anche un limite se la gestione del rischio dipende troppo dalla sensibilità individuale. La sfida consiste nel trasformare l'attenzione del vertice in processi stabili e responsabilità chiare. Il Risk Manager, quando presente, può svolgere proprio questa funzione di raccordo tra governance e operatività.

4.7 Fattori di efficacia e prospettive di investimento

Gli aspetti ritenuti importanti per rendere efficace la gestione del rischio confermano la necessità di integrare dati, persone e processi. La disponibilità di dati sull'azienda e sul mercato di riferimento è considerata molto o abbastanza importante dal 90% delle imprese, in crescita rispetto al 75% del 2025; la disponibilità di personale specializzato dedicato alla funzione di risk management dall'85%; l'integrazione della funzione di risk management nelle altre attività aziendali dall'80%. Quest'ultimo dato è particolarmente rilevante: le imprese riconoscono che il risk management non può essere una funzione separata, ma deve interagire con produzione, acquisti, commerciale, IT, amministrazione, HR e direzione.

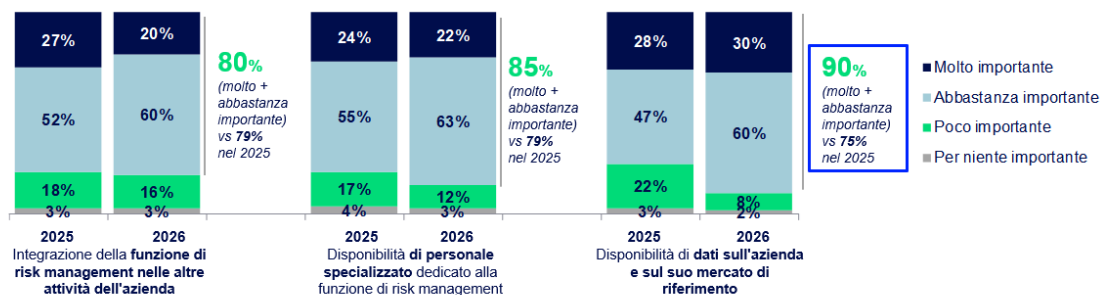
L'elevata importanza attribuita all'integrazione segnala una lettura più ampia del ruolo del risk management. I rischi, infatti, non riguardano soltanto una funzione dedicata, ma attraversano processi produttivi, fornitori, sistemi informatici, scelte commerciali e organizzative. In questa prospettiva, il collegamento con le altre attività aziendali è importante perché permette di raccogliere informazioni da più aree dell'impresa e di capire meglio dove si concentrano i principali rischi. Il tema non è quindi solo la presenza di una funzione dedicata, ma il suo collegamento con i processi in cui i rischi si formano e vengono gestiti.

Sul piano prospettico, l'orientamento prevalente sembra essere quello di confermare gli attuali livelli di investimento nella gestione del rischio. La maggioranza delle imprese, infatti, dichiara che gli investimenti legati alla gestione del rischio rimarranno stabili nei prossimi tre anni. Tuttavia, emergono differenze significative tra imprese di diversa dimensione. Nelle aziende con 250-500 addetti il 33% prevede un aumento, mentre nelle aziende con 50-249 addetti la quota scende al 20%. Per settore, l'intenzione di aumentare è più alta nell'industria, al 33%, nei servizi alle imprese, al 25%, e nel commercio, al 21%; Nel complesso, il dato suggerisce che la gestione del rischio viene considerata un ambito di investimento da mantenere, più che da ridurre.

Ambiti di efficacia della gestione del rischio

Elevata l'importanza riconosciuta alla presenza di personale dedicato e la disponibilità di dati sull'azienda e sul suo mercato di riferimento

ASPETTI CHE RENDONO EFFICACE LA GESTIONE DEL RISCHIO (valori %)



Base: Totale campione; Valori %
Q.25 In generale, affinché il sistema di gestione dei rischi sia efficace per l'azienda, quanto è importante ciascuno dei seguenti aspetti? (Una risposta per ogni item)

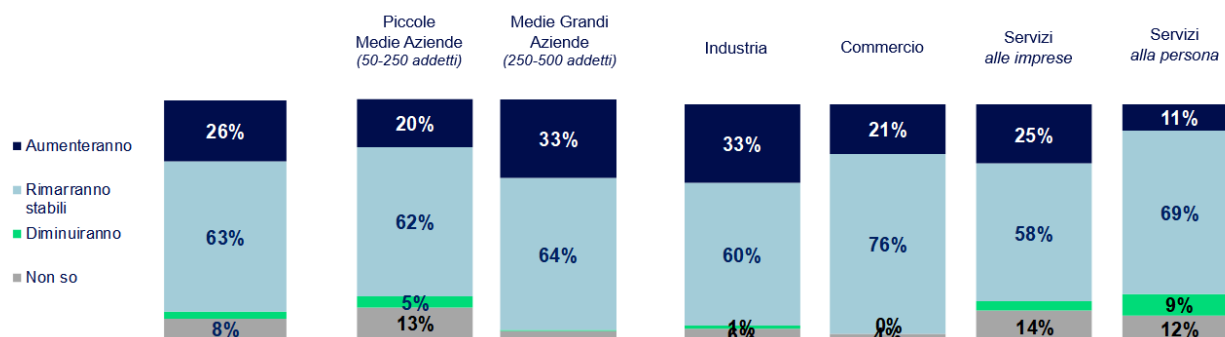


Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 46

Prospettiva di investimento per la gestione del rischio nel triennio

Generale stabilità prospettica degli investimenti legati alla copertura dei rischi: le aziende medio grandi e l'industria mostrano una maggiore intenzione ad investire di più

PROSPETTIVA INVESTIMENTI PER LA GESTIONE DEL RISCHIO (valori %)



Base: Totale rispondenti Valori %
Q.45 Infine, nella sua prospettiva, ritiene che gli investimenti legati alla gestione del rischio della sua azienda nei prossimi 3 anni... (Solo una risposta)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 47

In una fase di incertezza economica, questa stabilità non va letta come disinteresse. Indica piuttosto una gestione prudente delle risorse. Per questo, diventa importante che le imprese usino la mappatura dei rischi per scegliere con maggiore precisione dove intervenire.

4.8 Coperture assicurative

Il quadro dei sistemi di gestione del rischio si completa con l'osservazione delle coperture assicurative, che rappresentano uno degli strumenti più diffusi di protezione rispetto ai principali profili di rischio aziendale. Le aziende detengono in media circa 6-7 coperture assicurative tra quelle analizzate, con differenze settoriali significative. I valori più elevati si osservano nel farmaceutico, con una media di 8,5 coperture, e nel metallurgico, con 8,1. Sopra la media si collocano anche il commercio, con 7,3 coperture, la metalmeccanica, con 7,1, e l'agroalimentare, con 7,0. Più vicini alla media risultano invece l'energetico, con 6,9, il manifatturiero, con 6,6, e alcuni comparti dei servizi, intorno a 6,4 coperture medie.

Guardando alle singole coperture, emerge una forte concentrazione sui rischi più tradizionali e tangibili. La copertura più diffusa riguarda l'incendio, indicata dal 96% delle imprese. Seguono gli infortuni sul lavoro, all'87%, e le catastrofi naturali, all'86%, confermando la centralità dei rischi fisici, operativi e direttamente collegati alla continuità aziendale. Su livelli ancora elevati si collocano anche i rischi legati alla salute sul posto di lavoro, al 77%, e la difettosità del prodotto, al 65%. Più distanziate risultano invece le coperture relative ai rischi regolamentari, al 55%, al cyber risk, al 42%, e ai rischi di natura finanziaria, al 41%. Ancora meno diffuse sono le coperture legate a ricadute negative sull'ambiente delle attività d'impresa e alla perdita di competenze professionali chiave, entrambe al 36%, mentre imitazione e contraffazione dei prodotti si attestano al 34%. I rischi geopolitici o commerciali risultano i meno coperti, con il 23%.

Il peso del budget assicurativo risulta maggiormente concentrato sulle coperture tradizionali. La quota più elevata riguarda gli infortuni sul lavoro, a cui è destinato in media il 24,3% del budget assicurativo, seguiti dall'incendio, con il 21,4%, e dalle catastrofi naturali, con il 18,4%. Si tratta di rischi concreti, facilmente identificabili e direttamente collegati alla continuità aziendale, alla protezione delle persone e alla salvaguardia degli asset produttivi. Su livelli più contenuti si collocano il cyber risk, con il 13%, la perdita di competenze professionali, con il 12,3%, la difettosità del prodotto, con il 12,2%, e i rischi legati alla salute sul lavoro, con l'11,6%. Ancora più basso è il peso del budget destinato ai rischi di natura finanziaria, al 9,1%, all'imitazione o contraffazione dei prodotti, all'8,8%, ai rischi regolamentari, all'8,4%, e alle ricadute negative sull'ambiente, all'8,0%. I rischi geopolitici e commerciali risultano invece quelli con il peso più contenuto, pari al 5,6%.

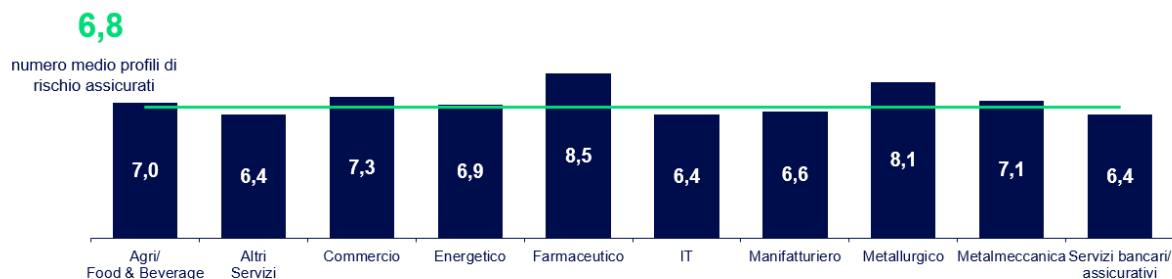
L'analisi di rilevanza e willingness to pay mostra che non sempre i rischi percepiti come più importanti assorbono una quota equivalente di budget assicurativo, ma dipende anche dal costo della copertura che riflette i calcoli attuariali delle compagnie. Gli infortuni sul lavoro e le catastrofi naturali rappresentano i casi più coerenti, perché sono tra i rischi più rilevanti e raccolgono anche la quota più alta di budget. Per altri rischi, invece, la distanza è più evidente. I rischi regolamentari e il cyber risk hanno una rilevanza elevata ma pesano poco per il budget. Il rischio geopolitico e commerciale mostra una dinamica simile: pur risultando più presente nelle preoccupazioni delle imprese, resta tra le coperture con il peso di budget più contenuto.

Nel complesso, i dati confermano che l'assicurazione resta uno strumento centrale nella gestione del rischio, ma continua a concentrarsi soprattutto sui rischi più tradizionali e misurabili. Incendio, infortuni sul lavoro e catastrofi naturali risultano infatti molto presenti sia per diffusione delle coperture sia per peso sul budget assicurativo. Per i rischi più complessi, come cyber, regolamentari, geopolitici e commerciali, emerge invece una distanza maggiore tra rilevanza percepita e investimento assicurativo. Questi ambiti sono considerati importanti, ma trovano ancora meno spazio nell'insieme delle coperture attivate dalle imprese. Per questo, le coperture assicurative andrebbero lette insieme alla mappatura dei rischi, così da individuare anche le esposizioni non pienamente coperte.

Coperture medie assicurative per settore

Le aziende detengono in media circa 6/7 coperture assicurative: i settori Farmaceutico e Metallurgico hanno una maggior propensione alla copertura del rischio

NUMERO MEDIO DI COPERTURE ASSICURATIVE PER SETTORE



Base: Totale rispondenti
Q.26 Ora le elencherò alcuni rischi, saprebbe indicarmi nella sua azienda se esistono delle coperture assicurative e se no?

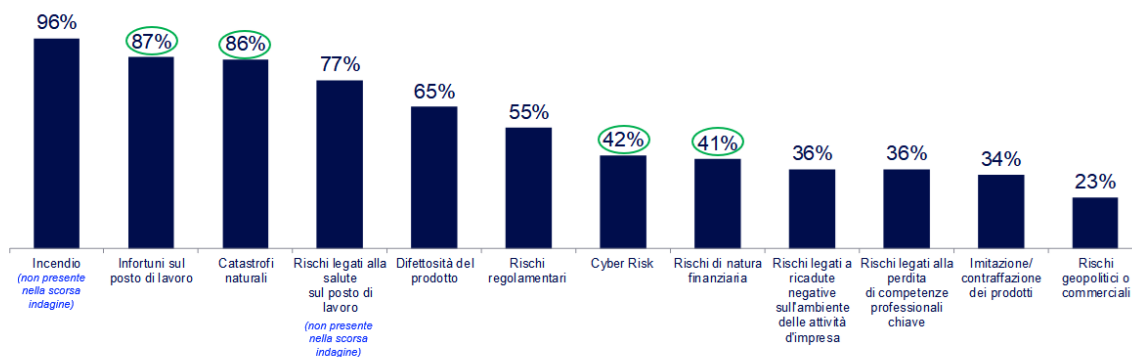


Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |48

Internal And Trusted Partner Use Only Document owned by Prometeia

Diffusione delle coperture assicurative

LE COPERTURE ASSICURATIVE PER PRODOTTO (valore %)



Base: Totale rispondenti Valori %
Q.26 Ora le elencherò alcuni rischi, saprebbe indicarmi nella sua azienda se esistono delle coperture assicurative e se no?

○ Valori superiori di almeno 5 punti rispetto al 2025



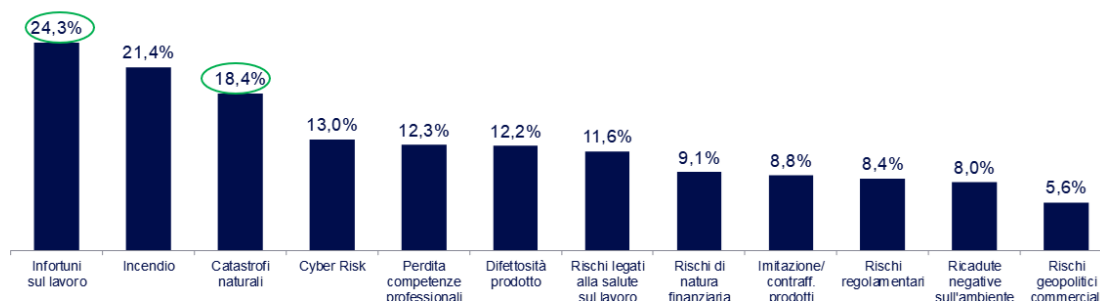
Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |49

Internal And Trusted Partner Use Only Document owned by Prometeia

Peso del budget per le coperture assicurative per prodotto

Aumento nella spesa per gli infortuni sul lavoro e le catastrofi naturali: negli altri ambiti la quota di copertura è minore ma bisogna considerare il differente campione di riferimento

PESO DEL BUDGET DEDICATO ALLE COPERTURE ASSICURATIVE PER PRODOTTO
(valore %)



Base: assicurati per i profili di rischio considerati; Valore medio Q.28 (Solo se hanno sottoscritto una relativa polizza assicurativa) Fatto 100 il costo assicurativo complessivo sostenuto dalla Sua azienda, indichi il valore percentuale delle polizze che coprono ciascuno dei rischi indicati. (Possibili più risposte)

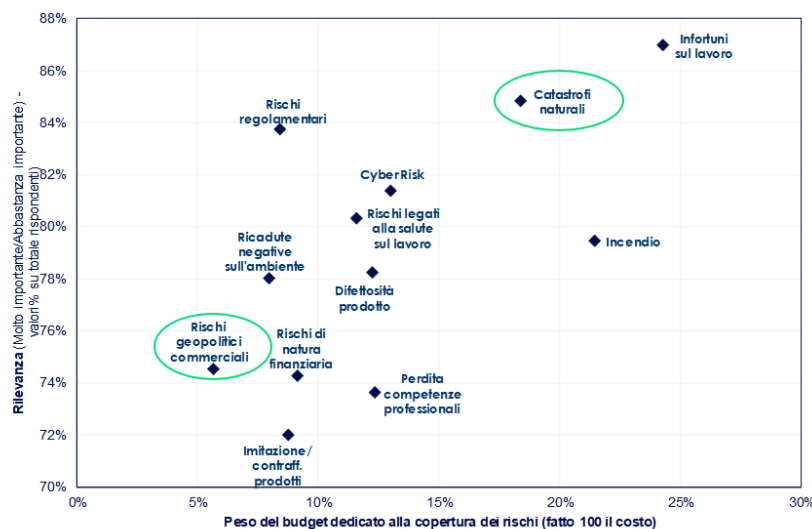
Valori superiori di almeno 5 punti rispetto al totale



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |50

Internal And Trusted Partner Use Only Document owned by Prometeia

Rilevanza e Willingness to pay per le coperture assicurative



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane |51

Internal And Trusted Partner Use Only Document owned by Prometeia

Aumento rilevanza rispetto al 2025

4.9 Sinistri subiti dalle aziende

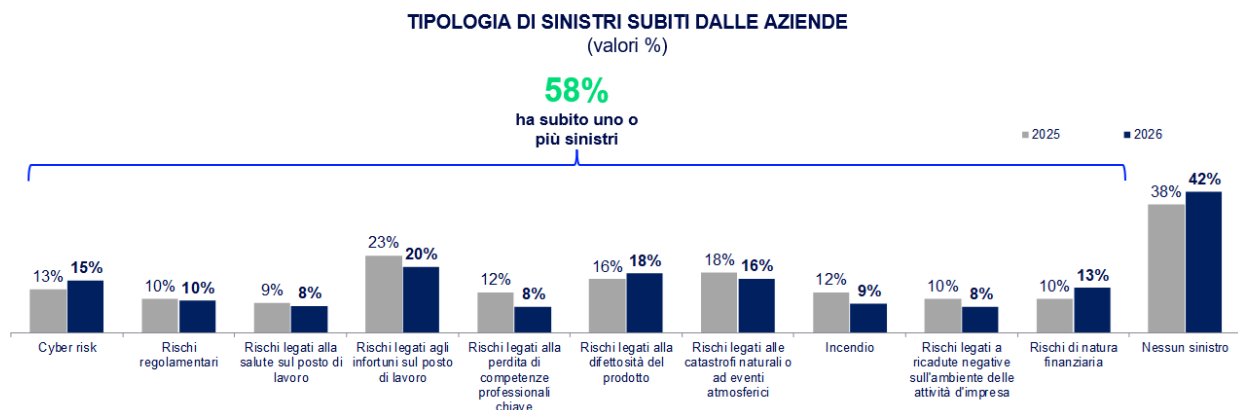
L'osservazione dei sinistri subiti negli ultimi 24 mesi aggiunge un elemento importante al quadro delle coperture assicurative appena presentato. Il 58% delle imprese dichiara di aver subito almeno un sinistro, dato che conferma che l'esposizione al rischio riguarda una quota ampia del campione e che gli eventi avversi non rappresentano casi isolati.

Tra le tipologie più frequenti si confermano gli infortuni sul posto di lavoro, indicati dal 20% delle imprese. Seguono i rischi legati alla difettosità del prodotto, al 18%, le catastrofi naturali o eventi atmosferici, al 16%, e il cyber risk, al 15%. Questi valori mostrano una distribuzione articolata dei sinistri: non emerge una sola area critica, ma diversi eventi capaci di incidere sull'operatività aziendale. Più contenuti, ma comunque presenti, risultano i rischi di natura finanziaria, al 13%, i rischi regolamentari, al 10%, e l'incendio, al 9%. Il confronto tra frequenza dei sinistri e diffusione delle coperture è particolarmente interessante nel caso dell'incendio: pur essendo la copertura più diffusa, la quota di imprese che dichiara di aver subito un sinistro di questo tipo è relativamente bassa. Questo conferma che la copertura assicurativa non risponde solo alla frequenza dell'evento, ma anche alla gravità potenziale del danno.

Nel complesso, il dato mostra che i sinistri non riguardano solo eventi eccezionali, ma toccano aree diverse della gestione aziendale: persone, prodotti, eventi naturali, sicurezza digitale e profili finanziari.

Sinistri subiti dalle aziende

Il 58% delle aziende dichiara di aver subito un sinistro negli ultimi 2 anni: gli infortuni sul lavoro si confermano leggermente più frequenti delle altre tipologie di rischio



Base: Totale rispondenti; Valori %
Q.27 Negli ultimi 24 mesi la Sua azienda ha subito un sinistro legato a uno dei seguenti rischi? (Possibili più risposte)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 52

Internal And Trusted Partner Use Only Document owned by Prometeia

CAPITOLO 5. FORMAZIONE AZIENDALE



5.1 La formazione aziendale

Dopo aver osservato sistemi di mappatura, modelli organizzativi, responsabilità interne e coperture assicurative, l'attenzione si sposta sulle competenze delle persone. Molti rischi non dipendono solo dall'esistenza di procedure o strumenti formali, ma anche dalla capacità delle persone di riconoscerli, segnalarli e gestirli correttamente nelle attività quotidiane.

In questa prospettiva, la formazione può essere letta come uno strumento operativo di risk management. Serve ad aggiornare le competenze e a rendere più coerenti i comportamenti delle persone rispetto alle procedure aziendali. In un contesto segnato da nuove tecnologie, cybersecurity, sostenibilità e IA, il presidio del rischio non può dipendere solo da una funzione dedicata. I dati sulla formazione suggeriscono l'importanza di diffondere conoscenze di base anche nelle diverse aree dell'impresa, affinché procedure, controlli e misure di prevenzione siano applicati in modo coerente.

Il tema della formazione assume particolare rilievo anche alla luce di alcune novità recenti. Da un lato, l'evoluzione normativa in materia di intelligenza artificiale richiama le imprese alla necessità di rafforzare le competenze interne sull'uso corretto e consapevole degli strumenti di IA. Dall'altro, il nuovo quadro sulla formazione in materia di salute e sicurezza sul lavoro conferma l'importanza di percorsi formativi aggiornati, capaci di accompagnare le aziende nella gestione dei rischi operativi.

Seguendo i risultati dell'indagine, il dato sulla diffusione della formazione interna è significativo: tre aziende su quattro dichiarano di offrire percorsi formativi in materia di rischi. Si tratta di un dato rilevante, perché mostra come la formazione non venga considerata soltanto un'attività di aggiornamento professionale, ma anche un presidio utile a rafforzare la prevenzione e la gestione delle criticità aziendali. Tra i principali temi formativi troviamo la regolamentazione e la cybersecurity, due ambiti che riflettono bene l'evoluzione dei rischi per le imprese. Da un lato, cresce l'esigenza di adeguarsi a normative sempre più articolate; dall'altro, la digitalizzazione dei processi rende più importante la capacità di proteggere dati, sistemi e continuità operativa.

In prospettiva, il 75% delle aziende dichiara di voler mantenere o aumentare le attività formative per affrontare le future sfide del mercato. Questo orientamento conferma il ruolo della formazione come leva di preparazione

organizzativa: un sistema di gestione del rischio è più efficace quando le procedure sono accompagnate da competenze diffuse e da comportamenti coerenti nelle diverse aree dell'impresa.

5.2 La formazione in materia di rischio

Come introdotto brevemente nella sezione precedente, il questionario mostra che il 72% delle aziende dichiara di avere in programma attività di formazione in materia di rischio. La diffusione risulta più elevata tra le aziende di dimensione maggiore: il 77% delle imprese con 250-500 addetti dichiara di avere in programma attività di formazione in materia di rischio, contro il 68% delle aziende con 50-250 addetti. Questo scarto segnala una maggiore strutturazione dei percorsi formativi nelle realtà più grandi.

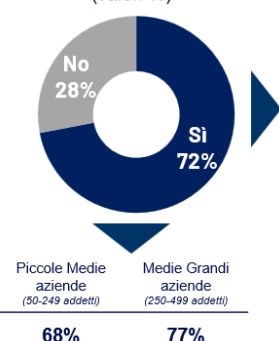
La maggior parte delle imprese che formano il personale coinvolge sia dipendenti sia dirigenti: il 63% indica entrambe le figure, il 30% solo i dipendenti e il 7% solo i dirigenti. Questo elemento è positivo, perché molti rischi richiedono comportamenti corretti a tutti i livelli dell'organizzazione. Inoltre, il 69% delle imprese dichiara di finanziare internamente le attività, mentre il 29% ricorre a fondi esterni e solo il 2% segnala percorsi senza costi.

Il dato indica che, per molte imprese, la formazione in materia di rischio rappresenta un investimento aziendale diretto, più che un'attività residuale o occasionale. Questi dati indicano che molte imprese considerano la formazione non solo come un adempimento o un'attività occasionale, ma come un investimento organizzativo utile a rafforzare la capacità di prevenire e gestire i rischi. Allo stesso tempo, la quota di aziende che non prevede percorsi formativi segnala che esiste ancora uno spazio di crescita, soprattutto per rendere la gestione del rischio più diffusa e meno dipendente da singole funzioni o responsabilità.

La formazione in azienda per la gestione del rischio

Il 72% delle aziende ha in programma attività di formazione interna, nella maggior parte dei casi coinvolge tutti i dipendenti

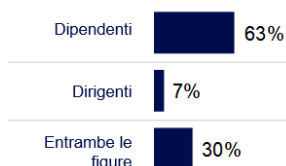
ATTIVITÀ DI FORMAZIONE IN MATERIA DI RISCHIO
(valori %)



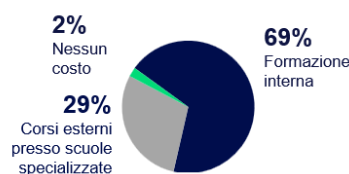
Base: Totale rispondenti; Valori %

Q.10 Attualmente, la sua azienda ha in programma attività di formazione in materia di rischio per il personale interno? Solo una risposta)

FIGURE IN AZIENDA INTERESSATE DALLA FORMAZIONE
(valori %)



FINANZIAMENTO DEI PROGRAMMI DI FORMAZIONE
(valori %)



Base: Aziende che hanno in programma attività di formazione; Valori %

Q.11 Quali sono le figure professionali coinvolte nei programmi di formazione in materia di rischio presenti in azienda? (Solo una risposta)

Q.13 I programmi di formazione aziendale in materia di rischio sono finanziati... (Solo una risposta)

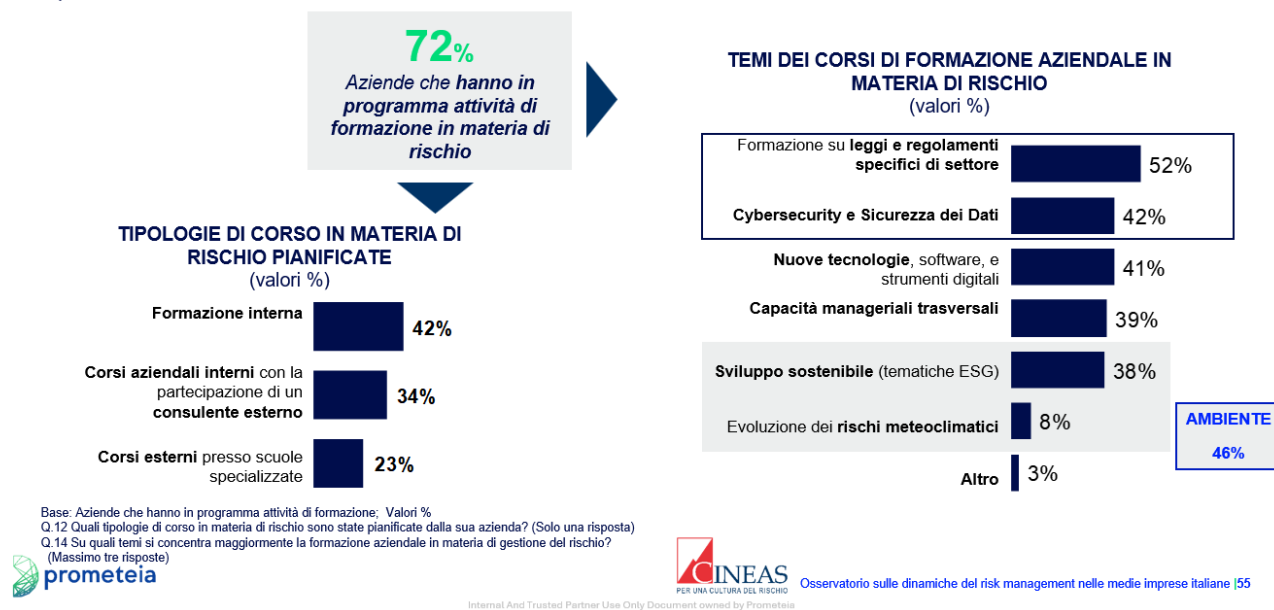
5.3 Tipologie di corso e temi prioritari

Tra il 72% di aziende partecipanti al questionario che hanno in programma attività di formazione in materia di rischio, il 42% prevede formazione interna, il 34% corsi aziendali interni con la partecipazione di un consulente esterno e il 23% corsi esterni presso scuole specializzate. La prevalenza della formazione interna è coerente con la necessità di adattare i contenuti ai processi specifici dell'azienda. Tuttavia, la presenza di consulenti

esterni e scuole specializzate resta rilevante, soprattutto quando i temi richiedono competenze verticali o aggiornamento normativo.

Quali tipologie di formazione e su quali temi

Si prevede una formazione interna o la partecipazione di consulenti esterni per affrontare le normative di settore o la protezione dei dati



Le tematiche trattate dai corsi di formazione confermano il cambiamento dell'agenda del risk management discusso nei capitoli precedenti. Al primo posto si collocano formazione su leggi e regolamenti di settore, con il 52%. Seguono, al 42% cybersecurity e sicurezza dei dati, nuove tecnologie al 41%, capacità manageriali trasversali al 39%, sviluppo sostenibile (ESG), al 38%. L'evoluzione dei rischi meteo climatici restano più distanti all'8%.

La quota più contenuta di formazione sulle capacità manageriali trasversali segnala comunque un possibile spazio di crescita. Nei rischi che coinvolgono più aree aziendali, competenze come coordinamento e comunicazione possono aiutare a rendere più efficace la risposta dell'organizzazione.

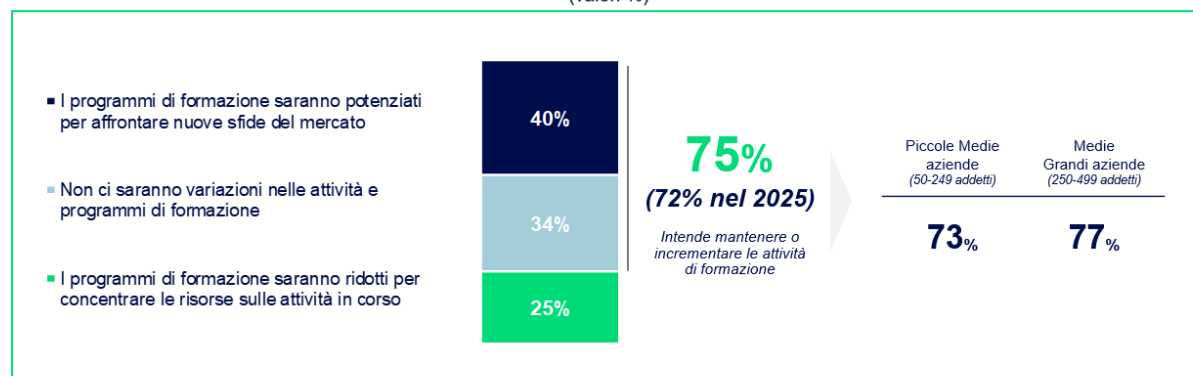
5.4 Prospettive per il prossimo anno

Guardando al prossimo anno, il 75% delle imprese intende mantenere o incrementare le attività di formazione, in aumento rispetto al 72% del 2025. Il dato segnala una sostanziale continuità dell'investimento formativo, con un 40% di aziende che prevede di potenziare i programmi formativi per affrontare nuove sfide del mercato, nonostante il contesto economico incerto. È un segnale importante perché la formazione è spesso una delle

Prospettive in tema di formazione per il prossimo anno

La maggior parte delle aziende pianifica nel prossimo anno di aumentare o mantenere i programmi di formazione interna

PROSPETTIVE IN TEMA DI FORMAZIONE (valori %)



Base: Totale rispondenti; Valori %
Q.15 E pensando al prossimo anno, considerando l'attuale situazione all'interno della sua azienda, lei ritiene che (Solo una risposta)



Osservatorio sulle dinamiche del risk management nelle medie imprese italiane | 56

prime voci a essere ridimensionata quando le risorse sono sotto pressione. In questo caso, invece, la maggioranza delle imprese sembra riconoscere il ruolo per affrontare rischi nuovi o in evoluzione.

La prospettiva appare quindi nel complesso positiva, ma non uniforme. Le aziende di dimensione maggiore mostrano un orientamento leggermente più favorevole alla continuità o all'aumento della formazione: il dato raggiunge il 77% tra le imprese con 250-499 addetti, contro il 73% tra quelle con 50-249 addetti. La differenza non è ampia, ma conferma una maggiore stabilità dell'investimento formativo nelle realtà più strutturate.

Questo orientamento va letto insieme alla varietà dei contenuti formativi richiesti alle imprese. Nei prossimi anni sarà probabilmente necessario aggiornare con continuità le competenze interne, soprattutto sulle aree più esposte a cambiamenti normativi e tecnologici. La formazione tende quindi a diventare un'attività ricorrente, non un intervento isolato.

Nei capitoli precedenti è emerso che strumenti, procedure e coperture funzionano meglio quando sono compresi dalle persone che operano nei processi aziendali. La formazione contribuisce proprio a questo passaggio: aiuta a riconoscere il rischio, sapere quando segnalarlo e applicare le procedure corrette. In questo modo, il sistema di risk management diventa più concreto e meno formale.

Per questo motivo, la formazione può rendere più efficace l'intero sistema di risk management. Se le persone conoscono i principali rischi, sanno riconoscere i segnali di allarme e comprendono il proprio ruolo, gli strumenti aziendali diventano più concreti e meno formali. Al contrario, anche un buon modello di mappatura rischia di restare distante dall'operatività quotidiana se non è accompagnato da competenze diffuse e da indicazioni comprensibili per chi lavora nei processi aziendali.



CINEAS - CONSORZIO UNIVERSITARIO PER L'INGEGNERIA NELLE ASSICURAZIONI
VIA PACINI, 11 - 20131 MILANO • TEL 02 36635000 — INFO@CINEAS.IT