

Deloitte.
Private



Trasformazione digitale e *Cybersecurity*: le nuove sfide per le PMI nell'era della Direttiva NIS2

Osservatorio Deloitte Private
sulle prospettive delle PMI in Italia

MAKING AN
IMPACT THAT
MATTERS
since 1845

Indice

Uno sguardo introduttivo sul contesto attuale	3
La fiducia delle imprese e l'attenzione verso l'evoluzione del mondo esterno	6
Il digitale come pietra angolare per la creazione di valore	8
Il giusto approccio alla sicurezza informatica tramite la governance aziendale	13
Riflessioni conclusive	20
Contatti	21

Uno sguardo introduttivo sul contesto attuale

In un contesto internazionale determinato dalle tensioni geopolitiche e che si prospetta ancora incerto, per l'economia italiana si prevede una crescita dell'0,5% nel 2024 e dell'0,8% nel 2025 ([Istat, Prospettive per l'economia italiana 2024-2025](#)).

Nell'evoluzione dello scenario competitivo industriale e dei servizi, dipendente dallo **sviluppo dell'economia nazionale**, le imprese dovranno continuare ad investire e mettere in atto le proprie strategie di crescita che, tra le altre, sono guidate dal crescente fenomeno della digitalizzazione ([Istat, Imprese e ICT - Anno 2024](#)).

Elemento decisivo per stimolare gli investimenti da parte delle aziende italiane è infatti la spinta tecnologica e digitale che, a differenti livelli, e grazie a forme di agevolazione come il PNRR (Industry 4.0 e Industry 5.0), coinvolge tutti i settori industriali e stakeholder sia pubblici che privati. Perseguire la direzione di investimenti digitali e nell'Artificial Intelligence per migliorare la competitività economica, aumentare la produttività, attrarre e trattenere giovani talenti, promuovendo una crescita sostenibile nel lungo periodo, non solo dell'industria ma dei territori, sono obiettivi comuni fondamentali che richiedono un approccio normativo condiviso e infrastrutture robuste e resilienti del Paese e delle imprese. Tale processo di trasformazione digitale sta spingendo le imprese ad affrontare sfide sempre più complesse anche in materia di sicurezza informatica. Da questo punto di vista, a livello europeo, è stata implementata una nuova direttiva (Direttiva NIS2), approvata nel 2022, che affronta le crescenti minacce informatiche e rafforza la resilienza delle infrastrutture digitali nell'Unione Europea, il cui scopo principale è quello di migliorare

la sicurezza delle reti e dei sistemi informativi delle aziende che operano in settori ritenuti essenziali, aumentando il dialogo con le autorità pubbliche competenti.

Sebbene si rivolga in particolare a realtà di grandi e medie dimensioni che operano in settori strategici, l'attuazione della direttiva europea può comportare implicazioni essenziali per la crescita di breve e lungo periodo anche delle aziende che hanno dimensioni ridotte. Quest'ultime dovranno, in ogni caso, essere in grado di adattarsi al nuovo contesto e ai cambiamenti introdotti da tale normativa, ridisegnando il modo in cui dialogare e rapportarsi con le altre aziende, in particolare quelle clienti, all'interno della catena del valore. Gli investimenti in sicurezza digitale delle PMI sono, quindi, destinati verosimilmente ad aumentare nei prossimi mesi, proprio in funzione di tale spinta regolamentare.

In effetti, la Direttiva NIS2 è da considerarsi uno strumento strategico alla crescita e agli investimenti digitali delle imprese e, come rilevato dalla presente indagine, ritenuto elemento di stimolo e con possibili effetti positivi per il contesto nazionale e aziendale.

Il presente approfondimento - basato sulle evidenze di una ricerca di Deloitte Private presso 200 leader di PMI italiane - si focalizza sul processo di **transizione digitale delle aziende** alla luce di questo nuovo contesto, in cui diventa cruciale governare la tematica della sicurezza informatica per competere sul mercato.



Approfondimento sulle imprese intervistate

Nel mese di gennaio 2025 si è conclusa una ricerca con cui l'Osservatorio Deloitte Private ha esplorato il punto di vista di 200 leader di aziende italiane di piccole e medie dimensioni. L'indagine ha trattato l'importanza del **processo di trasformazione digitale** e l'attenzione dei *key decision maker* aziendali nei confronti di temi strategici quali la **Cybersecurity** e l'**Intelligenza Artificiale**, analizzando le **sfide** che dovranno affrontare in futuro, in funzione dell'**evoluzione normativa** e del **contesto di mercato** in cui operano.

Dal punto di vista demografico, il panel delle aziende italiane coinvolte presenta le seguenti caratteristiche:

- Un fatturato annuale compreso tra i 2 e i 50 milioni di euro
- Oltre il 90% delle imprese intervistate è sul mercato da oltre 10 anni
- Oltre il 40% delle imprese risulta di proprietà familiare

Inoltre, il panel di intervistati rappresenta, nel complesso, i vari settori: quelli maggiormente presenti sono la manifattura industriale, i prodotti di largo consumo, i servizi professionali, le attività operanti nell'abbigliamento/tessile e nell'ambito della salute.

Nota: Alcune percentuali nei grafici riprodotti in questo report potrebbero non contribuire ad un totale di 100% a causa degli arrotondamenti, oppure per la presenza di domande per cui i partecipanti all'indagine avevano la possibilità di scegliere tra risposte multiple.

Deloitte Private è la business solution strategica, attiva in 40 paesi del mondo, dedicata alle aziende del Mid Market, alle famiglie ed ai loro consulenti (private bankers, wealth manager, Family office). In quanto Trusted Business Advisor, offre servizi multidisciplinari: dallo sviluppo dell'innovazione, alla gestione della continuità generazionale, dal risk management, alla governance fino all'ottimizzazione dei processi e l'internazionalizzazione. Deloitte Private sviluppa ricerche e analisi sui bisogni dei Clienti, disponibili per finalità informative e formative. Al tempo stesso, in Italia sviluppa e facilita le attività di networking organizzando il Premio Best Managed Companies (programma volto a premiare l'eccellenza imprenditoriale, giunto nel 2024 alla sua settima edizione, assegnando oltre 400 riconoscimenti ad aziende che, attraverso una community internazionale, interagiscono tra i premiati degli altri 27 paesi in cui il premio è attivo).*

**Sono incluse le Piccole e Medie Imprese ("PMI") e tutte quelle che ne posseggono i requisiti qualitativi (struttura proprietaria e governance, mercati di riferimento, modelli organizzativi, ecc.).*

Sito Internet: www.deloitte.com/it/private

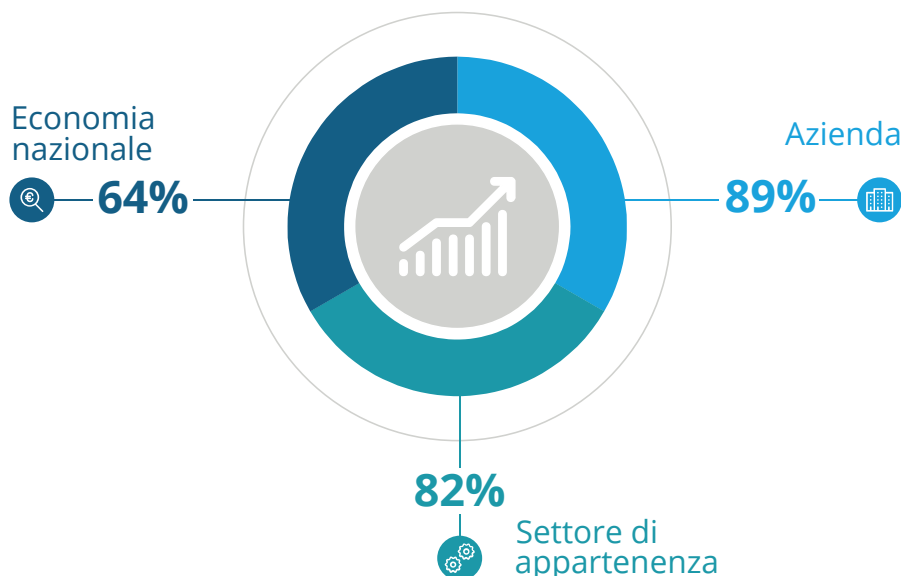
La fiducia delle imprese e l'attenzione verso l'evoluzione del mondo esterno

Le imprese intervistate mostrano un certo grado di incertezza circa il futuro dello scenario competitivo e di mercato in cui operano. Infatti, la percezione principale che emerge dal panel è che nei prossimi 12 mesi opereranno in un **contesto generale incerto** (63%); tuttavia, la quasi totalità del campione si attende una qualche crescita del proprio business (89%). Prospettive più attenuate, seppur positive, si rilevano rispetto all'incremento del proprio settore di appartenenza (82%) e del sistema Paese (64%). Come rilevato anche nel precedente studio ([Deloitte Private, Trasformazione digitale: un'opportunità per la crescita e l'adeguamento dell'assetto organizzativo aziendale](#)), la fiducia delle imprese sul proprio business si conferma maggiore rispetto a quella relativa al contesto economico generale, incrementando peraltro il suo valore rispetto alla precedente ricerca (+14%).

In questo panorama, per le aziende intervistate è necessario prestare attenzione alle **minacce congiunturali esterne alla propria organizzazione**. Prioritario per salvaguardare la strategia di crescita aziendale da qui ai prossimi 12 mesi resta il tema dell'inflazione (54%). Altro rischio percepito come elevato per la strategia di business è quello relativo alla stabilità dei mercati finanziari, citato da oltre un'azienda su quattro; mentre quello della crisi energetica resta un fenomeno più marginale da monitorare.

La complessità dello scenario attuale e le relative sfide pongono le imprese nella condizione di dover **operare in modo proattivo, implementando alcune azioni specifiche**. Nel breve termine, per il campione intervistato, risulta importante concentrarsi principalmente sull'innovazione dei processi.

Figura 1 | Le prospettive di crescita nei prossimi 12 mesi



Ulteriori azioni, a cui le aziende dichiarano di voler fare ricorso, sono investire sulle risorse umane e trasformare la struttura organizzativa, sviluppando nuove aree di business, effettuando nuove assunzioni e implementando nuove tecnologie.

Elemento trasversale e comune a tali azioni è il focus sulla tecnologia e l'innovazione: in questo senso, l'adeguamento del

proprio assetto organizzativo rispetto alla complessità dello scenario attuale è percepito come uno degli aspetti principali su cui concentrarsi già nell'immediato e testimonia quanto la capacità di **evolversi rapidamente e adattarsi alle nuove condizioni** sia un aspetto fondamentale per le imprese di medie e piccole dimensioni.

Figura 2 | Le principali azioni per affrontare la complessità dello scenario nei prossimi 12 mesi



Assumere un atteggiamento proattivo di fronte al cambiamento significa essere nella condizione di poter cogliere le opportunità di crescita che si presentano ogni qual volta si verifichi un evento *disruptive*. Nello scenario attuale, infatti, diventa cruciale la capacità di generare solidità organizzativa, pur in condizioni complesse; essere una PMI, per la maggior parte del panel degli intervistati, garantisce una marcia in più nell'affrontare momenti complessi come quello attuale (70%), ma soprattutto nell'implementare una strategia e soluzioni tecnologiche e innovative (79%).



Il digitale come pietra angolare per la creazione di valore

La trasformazione digitale è vista dalle aziende come l'**investimento più importante** per incrementarne il valore sia oggi che in futuro (84%). Si tratta di un percorso sfidante che comporta un notevole impegno già nell'immediato: la diffusione delle tecnologie, infatti, richiede già oggi un

profondo ripensamento dei modelli di business esistenti secondo oltre sette leader su dieci. Ad essere convinti di ciò sono soprattutto i vertici delle medie imprese (85% contro il 68% delle piccole imprese).

Figura 3 | La tecnologia come catalizzatore di cambiamento del modello di business



La quota di aziende secondo cui la diffusione delle tecnologie richiede già oggi un ripensamento del modello di business



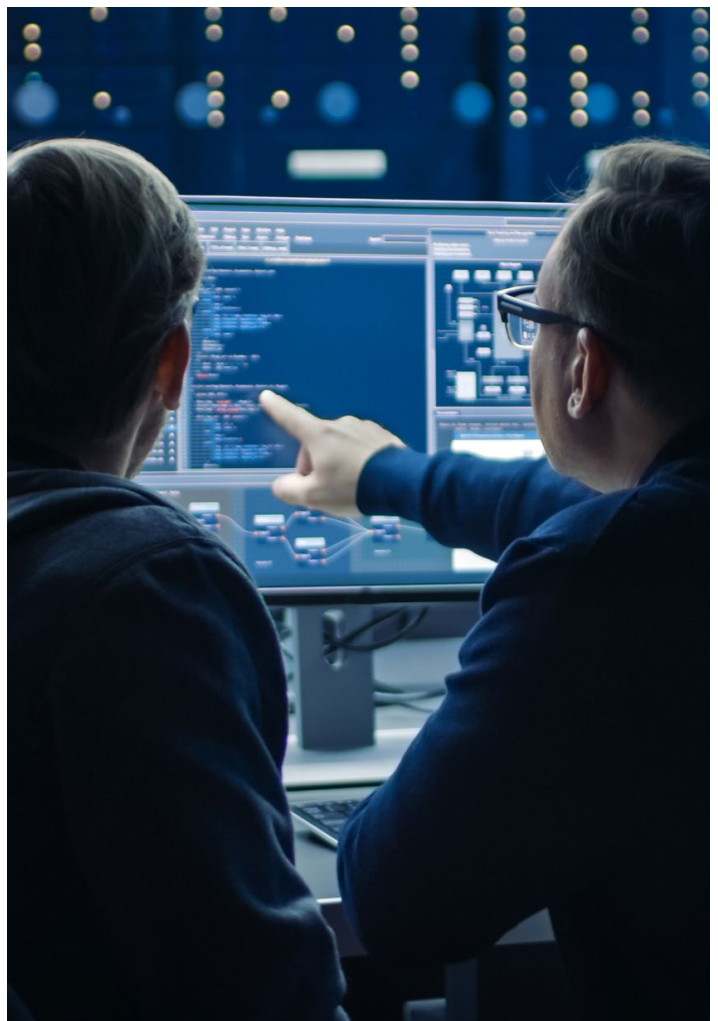
77% Totale campione



85% Medium company



68% Small company



Cogliere la sfida digitale è cruciale per incrementare il livello tecnologico e innovativo attuale delle imprese che per meno di un'azienda intervistata su tre è considerato attualmente alto. Assicurare alla propria impresa degli standard digitali più elevati le consente di migliorare la propria competitività. Si pensi ad esempio all'incremento rilevato da Istat sulle PMI che ricorrono alle vendite *online*, dove emerge anche che tale quota cresce con la dimensione aziendale.

(Istat, Imprese e ICT - Anno 2024)

Le imprese di dimensioni più ridotte, aumentando il proprio livello di adozione di tecnologie, possono colmare il gap con le realtà più strutturate; anche dalla presente ricerca emerge che la dimensione aziendale è un elemento che delinea un livello differente di adozione digitale e tecnologica, ed infatti le piccole imprese si dichiarano *follower* sull'aspetto digitale rispetto alle medie aziende. Per le imprese, operanti in un contesto di competitività "estesa" dove sta emergendo una forte attenzione alla sicurezza sui temi digitali e la percezione sul tasso di innovazione del proprio settore è vista come "alta" da circa un'azienda su tre, è necessario **valorizzare il loro potenziale e posizionamento anche all'interno della propria catena di fornitura**. Infatti, circa il 60% delle aziende intervistate si sta orientando verso soluzioni digitali per individuare fornitori alternativi e migliorare la forza e l'agilità della propria catena di fornitura. Contestualmente all'evoluzione del contesto, in termini di rischi informatici e in riferimento all'ecosistema di business, le aziende del panel prevedono che fornitori e clienti diretti chiederanno un'attenzione maggiore rispetto alla sicurezza informatica (65%) e pertanto dovranno investire in digitalizzazione, e quindi anche *cybersecurity*, per adeguarsi al nuovo scenario regolamentare (67%).

L'importanza data dalle imprese alla **digitalizzazione** è testimoniata dal fatto che è un elemento **presente nelle strategie aziendali**. Nelle organizzazioni c'è attenzione alla trasformazione dei modelli aziendali e all'integrazione di considerazioni su questi temi in tutte le *operation*.

Se il *desiderata* delle aziende è quello di trasformare i propri modelli aziendali per affrontare il cambiamento e integrare la digitalizzazione all'interno delle funzioni aziendali, ad oggi il focus principale delle aziende del panel risulta quello di attuare cambiamenti incrementali di processo o operativi per migliorarla, soprattutto nelle medie imprese.

Inoltre, anche per le organizzazioni dove ancora la digitalizzazione non ha un impatto sul modello aziendale principale, vi è comunque un riconoscimento diffuso della sua importanza.

In tale contesto, tra le **priorità strategiche** che le imprese devono perseguire, in riferimento all'innovazione tecnologica, risultano il miglioramento dei servizi innovativi e l'adozione di nuove soluzioni tecnologiche, ma anche il potenziamento delle misure di sicurezza informatica.

A fronte di una generalizzata ed elevata consapevolezza dell'esigenza di rivedere il proprio modello di business per facilitare la diffusione delle tecnologie, la media di coloro che dichiarano di essere attualmente impegnati a ripensare la propria strategia di innovazione per garantire la **piena transizione digitale nei prossimi 5 anni** si attesta al 65%. Questo *sentiment* risulta in linea con gli obiettivi del decennio digitale europeo sulla transizione digitale, che prevede un progresso da parte di tutte le imprese anche di piccole dimensioni, affinché cresca l'utilizzo della tecnologia per prendere decisioni aziendali migliori, interagire con i propri clienti e migliorare parti delle loro *operation*.

Ma quali sono le principali sfide che, secondo il panel di aziende intervistate, la tecnologia può aiutare a risolvere? Facendo leva sulle loro peculiarità e sul **ruolo di "gamechanger" della trasformazione digitale**, le PMI possono stimolare la propria crescita conseguendo benefici su più fronti, primo fra tutti sull'aumentare la propria produttività e competitività. Ulteriori aspetti percepiti come positivi sono la riduzione dei costi operativi e lo sviluppo di nuove competenze.

Figura 4 | Le sfide che la tecnologia può aiutare a risolvere alle imprese





Inoltre, cogliendo le nuove opportunità che la trasformazione digitale sta creando, le aziende Private possono **generare valore** sia per l'impresa medesima che **per l'intero ecosistema in cui operano**. Per oltre quattro intervistati su dieci, infatti, la trasformazione digitale resta un elemento che può portare benefici significativi "oltre le mura" dell'azienda e impattare positivamente anche l'individuo e la società, motivo per cui la *digital transformation* deve essere incentivata. Per compiere questo *journey* a livello Paese è necessario il coinvolgimento di tutti gli stakeholder: di questo ne è convinto l'81% del panel di aziende intervistate.

Le imprese possono dotarsi di **competenze digitali** per supportare i successivi progetti di trasformazione, facendo diventare la digitalizzazione parte del DNA aziendale. A questo proposito, oltre sette leader su dieci affermano che l'esplorazione e l'applicazione di soluzioni innovative per generare valore sia già insita nella cultura della propria azienda.

L'**elemento culturale** è cruciale per far sì che un'azienda possa abbracciare la trasformazione digitale: i dati dell'Osservatorio Deloitte Private indicano che la maggior parte delle imprese intervistate (79%) dichiara di avere un livello di preparazione e una cultura imprenditoriale necessari per affrontare la transizione digitale nel medio termine. Considerando la prospettiva dimensionale, le medie imprese risultano maggiormente dotate su questi aspetti rispetto alle piccole imprese; livelli di maturità diversi dal punto di vista culturale e della preparazione imprenditoriale si riscontrano tra le aziende presenti da più tempo sul mercato e quelle più "giovani", con quest'ultime che mostrano un gap da colmare da questo punto di vista.

Per quanto concerne gli **investimenti**, le aziende intervistate si stanno focalizzando su tecnologie di tipo infrastrutturale, le quali permettono accesso ai servizi Web e la gestione digitale di una o più funzioni aziendali. Le realtà aziendali del panel che, in questo senso, risultano più avanzate sono quelle che geograficamente operano in più mercati, rispetto a quelle che si rivolgono solo al mercato domestico.

Tutte le aziende dovranno però compiere un percorso di investimenti e di assunzione di maggiore maturità, per far sì che le realtà ad oggi meno pronte dal punto di vista digitale possano avviare concretamente questo percorso; inoltre, le imprese digitalmente più mature e strutturate dovranno focalizzarsi su investimenti verso quelle tecnologie più avanzate, atte ad aumentare la produttività tramite processi di automazione e simulazione e, con soluzioni più trasversali, in grado di ridurre il rischio di perdita di dati determinata da azioni interne o esterne.

Nel complesso, 2 aziende su 5 dichiarano che nel prossimo anno gli investimenti digitali della propria azienda aumenteranno, mentre la restante parte di imprese prevede di investire in modo stabile. Le realtà più votate ad incrementare i propri investimenti risultano le aziende più giovani e quelle che dichiarano di avere una conoscenza dell'evoluzione del nuovo contesto normativo e dell'introduzione della Direttiva NIS2.

L'importanza dell'Intelligenza Artificiale

Il contributo alla crescita delle imprese in questo panorama può essere offerto dall'**adozione di nuove tecnologie come quelle AI-based**. Di questo sono consapevoli sette imprese intervistate su dieci, soprattutto quelle realtà che hanno una visione più ottimistica dello scenario economico generale e del proprio contesto aziendale. Tuttavia, il primo passo, per le PMI, è comprendere in che modo l'Artificial Intelligence possa essere implementata concretamente nella propria realtà e quali benefici possa dare. In primo luogo, tramite l'AI, anche le PMI potrebbero automatizzare quei processi ripetitivi, migliorando l'efficienza operativa e riducendo i costi. Inoltre, il ricorso a tecnologie e strumenti avanzati di analisi dei dati permetterebbe loro di prendere decisioni più informate e strategiche, così come potrebbe migliorare l'esperienza del cliente, oppure facilitare la gestione delle risorse umane, ottimizzando l'assunzione e la formazione del personale. Il livello di implementazione di specifiche tecnologie e soluzioni governate dall'AI dipende dal grado di maturità digitale delle imprese, le quali, investendo su questa direttrice, possono migliorare la propria competitività e puntare verso il successo a lungo termine.

A prescindere dall'aspetto dimensionale e grado di maturità digitale, il panel di aziende intervistate riconosce **3 principali benefici nel ricorrere alle tecnologie basate sull'AI**: avere maggiore efficienza e produttività, ridurre i costi aziendali e ottimizzare le risorse, nonché controllare meglio ed essere più efficaci nel gestire i rischi esterni ed interni all'azienda.

Figura 5 | I 3 benefici dell'Artificial Intelligence percepiti dalle aziende



Pianificare investimenti, così come trovare nuovi modi per semplificare e automatizzare le operazioni aziendali grazie alle nuove tecnologie e innovazioni, va quindi di pari passo con l'**attenzione al tema della sicurezza**. Per implementare con successo l'Artificial Intelligence e garantirne un utilizzo sicuro e consapevole, la maggior parte delle aziende (76%) dichiara che è necessario monitorare i rischi associati (ad esempio *cybersecurity*, frodi, implicazioni etiche) e le normative di riferimento, come la recente Direttiva NIS2.

Secondo quanto suggerito recentemente da alcuni executive intervistati da Deloitte a livello globale, le aziende stanno facendo leva sull'Artificial Intelligence nelle proprie strategie e azioni di *cybersecurity* (Deloitte, [Future of Cyber](#)). Da qui emerge che alcuni dei principali modi in cui le organizzazioni si concentrano sull'uso dell'Artificial Intelligence per migliorare le proprie capacità di sicurezza informatica includono il monitoraggio dell'infrastruttura digitale, simulazioni avanzate e sicurezza automatizzata. In altre parole, mentre il futuro dell'Artificial Intelligence si sta evolvendo, lo stesso vale per il futuro della sicurezza informatica; il trend a livello globale mostra che, in media, il 39% delle aziende utilizza in larga misura le capacità dell'Artificial Intelligence nei propri programmi di sicurezza informatica.

In questo contesto, tutte le risorse aziendali legate alle informazioni sono dei potenziali bersagli per i *cybercriminali* e questo pone il tema di disporre di sistemi di rilevamento e prevenzione efficaci. Dalla presente ricerca dell'Osservatorio Deloitte Private emerge che un'azienda su quattro utilizza soluzioni di Artificial Intelligence in ambito *cybersecurity*, di cui però, la maggior parte, ne fa ancora un uso marginale. Per queste realtà, le principali funzionalità di tali soluzioni *AI-based* riguardano: l'identificazione di nuove minacce (57%), la ricerca e l'analisi di correlazione tra eventi (31%) e la rilevazione di anomalie (12%). Alla quota di aziende che fa ricorso a tali soluzioni, si aggiunge quella che ad oggi non le adotta ma ne prevede l'adozione nei prossimi 12 mesi (17%), a fronte di quella che dichiara di non avere alcuna intenzione di adottarle (57%). Quest'ultima percentuale, che rappresenta oltre la metà del panel, mostra che il percorso per l'adozione dell'Artificial Intelligence richiede ancora un impegno significativo da parte delle PMI. È fondamentale migliorare la loro consapevolezza non solo su quelli che sono i vantaggi generali, ma anche sull'adozione di soluzioni specifiche e settoriali, che consentano una implementazione immediata e su misura rispetto alle esigenze aziendali.

Il giusto approccio alla sicurezza informatica tramite la governance aziendale

Con la crescente diffusione delle soluzioni tecnologiche, l'approccio per identificare e affrontare i rischi sta diventando sempre più sofisticato per le aziende. La maggior parte delle imprese del panel (74%) indica che l'aumento del rischio informatico legato alla **gestione di nuovi dati** sia una delle più grandi sfide legate all'implementazione di tecnologie basate sull'Artificial Intelligence nella propria azienda.

Per tenere il passo con l'innovazione tecnologica, accelerata dall'Artificial Intelligence, e difendere il proprio patrimonio informativo da attacchi e minacce provenienti da vari fronti, per le imprese è necessario disporre di una **strategia a livello organizzativo**.

Il comportamento e le intenzioni del panel di investire in sicurezza mostrano come l'attenzione delle aziende sia più che un *desiderata* da perseguire in futuro, quanto piuttosto un elemento cruciale per poter investire e attuare le proprie strategie e azioni in ambito digitale e tecnologico: per il 77% il tema della sicurezza informatica è prioritario nell'ambito della strategia complessiva della propria azienda.

Sebbene il 79% delle aziende ritiene di poter affrontare un attacco informatico, il fenomeno degli incidenti informatici (o *data breach*), che possono determinare danni gravi all'operatività o all'immagine aziendale, sta generando consapevolezza rispetto alla necessità di **investire in sicurezza informatica e avere un piano strategico**.

Piano che è cruciale per definire le priorità e indirizzare gli investimenti a tutela del proprio patrimonio informativo. Infatti, al netto di chi ancora non sa o non vuole esprimersi, per circa due aziende su cinque gli investimenti in sicurezza informatica nel prossimo anno dovrebbero crescere.

La propensione delle aziende intervistate ad aumentare i propri investimenti in *cybersecurity* e a riconoscergli importanza si traduce concretamente nel possedere una **pianificazione in ambito di cybersecurity**. Infatti, dalla presente indagine emerge che il 74% ne ha sviluppato una: il 28% indica di avere un approccio consolidato, mentre il 46% dichiara che il proprio approccio potrebbe essere migliorato.

Figura 6 | Lo sviluppo di una pianificazione in ambito di cybersecurity



Per fronteggiare il contesto e migliorare il proprio atteggiamento alla sicurezza informatica, le PMI possono mettere in pratica **diverse azioni in materia di cybersecurity**. Anche sul tema *cybersecurity*, essere una PMI è considerato dal panel come un fattore positivo nell'ambito della **gestione dei temi legati alla sicurezza informatica**, facendo riferimento alla propria *resilience culture* e propensione generale dell'impresa al rischio.

L'azione in ambito *cyber* ritenuta principale dalle aziende è relativa al tema della formazione dei talenti al proprio interno. Investire sulle persone e su nuovi potenziali talenti con le giuste skill è fondamentale sia per mantenere la continuità aziendale che per crescere; il focus sulle persone è elemento imprescindibile per la gestione dei rischi tanto quanto quello sui processi e le tecnologie.

Un secondo elemento, in ordine di priorità, è quello relativo al controllo del proprio ecosistema di business dal punto di vista dei rischi. Garantire la sicurezza all'interno della propria catena di fornitura è considerato un aspetto da cui non si può prescindere per operare e conferire valore al proprio

business. Considerare lo stato dell'arte e le **aspettative dei molteplici stakeholder** – anche esterni, come investitori e partner strategici – è un aspetto che può spingere l'impresa a **“modernizzare” il proprio approccio alla gestione del rischio**. Ciò si traduce nella diffusione di un cambiamento culturale, in grado di stimolare una integrazione e coordinamento all'interno dell'azienda. In tal modo, si potrà rendere la gestione del rischio utile non solo per individuare possibili minacce alla strategia, ma anche per identificare nuove opportunità e creare una resilienza organizzativa.

Ulteriore tassello, che presuppone i precedenti punti, è relativo al dotarsi di un modello di governo che tenga conto dei fenomeni esterni ed interni all'azienda e indirizzi quelle che sono le azioni aziendali, sostenendole sulla base di una strategia del rischio. Questa urgenza di dotarsi di una governance basata su una strategia e su infrastrutture robuste e resilienti, per le imprese potrebbe realizzarsi proprio a seguito dell'attuale evoluzione del quadro normativo italiano ed europeo (Direttiva NIS2 e DORA), e comportare anche un incremento degli investimenti aziendali in sicurezza informatica.

Figura 7 | Le top 3 azioni ritenute prioritarie in materia di *cybersecurity*

78 %

Realizzazione di un programma di formazione e sensibilizzazione rivolto a tutti i dipendenti dell'organizzazione



77 %

Monitoraggio della condizione di sicurezza di partner e fornitori per garantire la sicurezza della propria impresa



73 %

Sviluppo di una governance in grado di orientare e gestire in modo operativo le decisioni aziendali tramite una strategia di *cybersecurity*



Come anticipato, oggi, per cercare di incrementare il livello di sicurezza, ridurre il rischio di attacchi informatici a danno di imprese, ma anche istituzioni e cittadini, e creare una strategia *cyber* univoca, l'Unione Europea ha emanato la Direttiva NIS2, che è entrata in vigore in Italia lo scorso ottobre 2024 tramite il recepimento del D.lgs. 138/2024.

In questo nuovo scenario, le organizzazioni italiane e gli enti della pubblica amministrazione, che sulla base D.lgs. 138/2024 rientrano nella definizione di soggetti essenziali e importanti, sono tenuti a stabilire processi interni più strutturati e dettagliati, con canali di comunicazione ben definiti tra i vari livelli di governance interni all'azienda e con le autorità competenti. Ai soggetti cui si applica tale Direttiva viene richiesto di valutare la criticità di tutti gli asset aziendali, al fine di implementare misure di gestione del rischio *cyber* secondo un approccio *Risk-based*.

Con la Direttiva NIS2, che modernizza il quadro regolatorio esistente e amplia l'ambito di applicazione a nuovi settori rispetto alla precedente normativa NIS1, si cerca di rafforzare i requisiti di sicurezza, migliorare gli obblighi di segnalazione degli incidenti, fare leva su requisiti di applicazione più rigorosi, nonché potenziare la sicurezza della *supply chain*. Quest'ultimo aspetto esemplifica come tale Direttiva NIS2 abbia un impatto molto pervasivo e incisivo, in quanto vincola le aziende sottoposte alla suddetta normativa a **valutare, monitorare e gestire i rischi della propria catena di fornitura**. Ciò si traduce nell'assumere un'attitudine elevata alla sicurezza anche da parte di quelle aziende che non sono soggette alla norma, come ad esempio le piccole imprese che operano all'interno di filiere e collaborano con grandi o medie realtà vincolate alla Direttiva NIS2.



NIS2: l'evoluzione del quadro normativo e le principali sfide per le imprese italiane

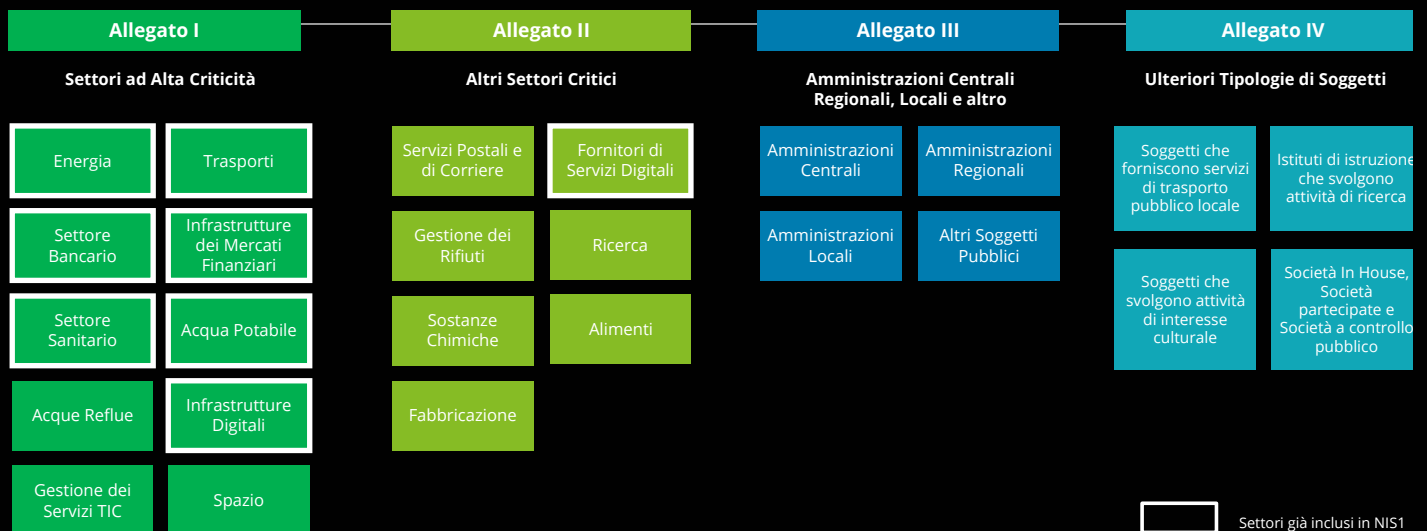
La nascita della Direttiva Europea NIS2

La **Direttiva (UE) n. 2555/2022 (NIS2)** è un'evoluzione normativa che risponde all'esigenza di **aggiornare e rafforzare** il sistema già previsto dalla NIS1, **superandone limiti e carenze** e adattando obblighi e indicazioni alle esigenze attuali, rendendola a prova di futuro

NIS1	2016 → 2025	NIS2
<ul style="list-style-type: none"> Classificava due tipologie di soggetti: Operatori di servizi essenziali (OSE) e Fornitori di servizi digitali (FD) Ciascuno Stato Membro era responsabile nel determinare quali Soggetti considerare in perimetro Il perimetro era limitato ai soli sistemi e reti critiche del Soggetto 	AMPLIAMENTO E ARMONIZZAZIONE DELL'AMBITO NORMATIVO	<ul style="list-style-type: none"> Introduce due diverse categorie di soggetti: Soggetti essenziali e Soggetti importanti Fornisce criteri uniformi per permettere ai Soggetti di identificarsi autonomamente in perimetro Il perimetro è composto dalla totalità dei sistemi e reti del Soggetto
<ul style="list-style-type: none"> Ciascuno Stato Membro era responsabile nel determinare i requisiti di sicurezza da indirizzare verso i Soggetti, comportando notevoli disallineamenti e divergenze nel recepimento 	RAFFORZAMENTO DELLE MISURE DI SICUREZZA E APPROCCIO RISK - BASED	<ul style="list-style-type: none"> Riduce il margine di interpretazione e migliora l'armonizzazione delle misure, identificando 10 ambiti di misure di sicurezza che ogni Stato membro è tenuto a declinare in requisiti puntuali tramite un approccio multi-rischio
<ul style="list-style-type: none"> È risultata limitata in termini di applicazione (<i>enforcement</i>) Non definiva chiaramente eventuali sanzioni o ammende amministrative 	ENFORCEMENT E REGIMI SANZIONATORI E DI SUPERVISIONE	<ul style="list-style-type: none"> Regime sanzionatorio comune con sanzioni fino a 10 milioni di euro o fino al 2% del fatturato annuo mondiale (per enti essenziali) Responsabilità del management in caso di infrazioni Regime di supervisione proattivo e reattivo

Settori e Imprese Interessate

Il Decreto Legislativo 4 settembre 2024 n. 138 identifica agli Allegati I, II, III e IV i soggetti a cui si applicano i requisiti normativi della Direttiva NIS2 e del decreto stesso



La Direttiva NIS2 si applica a tutte le grandi e medie imprese che contano **almeno un numero di dipendenti ≥ 50** o un **fatturato annuo o totale di bilancio annuo > 10 mln €**, secondo i criteri definiti dall'Allegato alla Raccomandazione 2003/361/EC

La normativa NIS2 potrebbe **applicarsi anche ai soggetti dei settori sopracitati, indipendentemente dalle loro dimensioni**, individuati dall'Autorità nazionale competente NIS, su proposta delle Autorità di settore

Ambiti Di Prescrizione e Obblighi

Risk Ownership	Elencazione Attività	Misure di Gestione Rischio Cyber	Sicurezza della Supply Chain	Segnalazione degli Incidenti	Enforcement
<p>Gli organi di gestione devono avere un ruolo attivo nella gestione dei rischi, in particolare nella definizione della strategia di gestione del rischio Cyber utile ad evolvere e migliorare la sicurezza e resilienza Cyber dei soggetti</p>	<p>I soggetti identificati comunicano e aggiornano, sull'apposita piattaforma digitale, l'elenco delle proprie attività e servizi comprensivo della relativa categoria di rilevanza, secondo le indicazioni dell'ACN</p>	<p>La Direttiva identifica un elenco di misure tecniche, operative e organizzative di gestione del rischio Cyber che tutti i soggetti essenziali e importanti sono tenuti ad attuare</p>	<p>I soggetti identificati devono garantire la Cybersecurity lungo la Supply Chain. A tal fine, devono valutare il livello di maturità Cyber dei propri fornitori, considerando i presidi e le procedure definite dagli stessi per la gestione dei rischi di Cybersecurity</p>	<p>I soggetti identificati devono inviare un preallarme entro 24 ore dal momento in cui vengono a conoscenza di un incidente significativo ed entro 72 ore inviare una notifica dell'incidente che aggiorni le informazioni già comunicate in fase di preallarme</p>	<p>Per i soggetti essenziali prevede un regime di vigilanza completo e sanzioni fino a 10 mln € o pari al 2% del fatturato annuo globale; per i soggetti importanti prevede un regime di vigilanza leggero e sanzioni fino a 7 mln € o pari all'1,4% del fatturato annuo globale</p>
<p><i>Gli organi di gestione dei soggetti che rientrano nella Direttiva devono approvare le misure di gestione dei rischi di Cybersecurity e supervisionarne l'attuazione</i></p>	<p><i>I soggetti devono redigere un elenco completo delle attività che svolgono e dei servizi che offrono, con tutti gli elementi necessari alla loro categorizzazione, con le modalità definite dall'ACN ed entro il termine prestabilito</i></p>	<p><i>Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi Cyber</i></p>	<p><i>I soggetti dovrebbero valutare e tenere conto della qualità complessiva dei prodotti e delle pratiche di Cybersecurity dei propri fornitori e prestatori di servizi, comprese le loro procedure di sviluppo sicuro</i></p>	<p><i>Gli Stati membri dovrebbero garantire che l'obbligo di presentare una notifica dell'incidente non sottragga le risorse del soggetto notificante dalle attività relative alla gestione degli incidenti, in quanto considerate prioritarie</i></p>	<p><i>Gli Stati membri provvedono affinché le autorità competenti dispongano di risorse adeguate per svolgere, in modo efficace ed efficiente, i compiti loro assegnati</i></p>

Pur rivolgendosi direttamente solo a quelle realtà definite specificamente come “essenziali” o “importanti” (per la criticità dei loro sistemi informativi e dei servizi da loro erogati per il funzionamento del sistema Paese), la nuova Direttiva NIS2 disegna un nuovo scenario e nuove sfide per tutte le imprese. Infatti, secondo la maggior parte del panel di PMI intervistate (74%) il nuovo contesto normativo determinato dall'introduzione della Direttiva NIS2 richiede un ripensamento del modello di business esistente. A prescindere dal loro coinvolgimento diretto, tali cambiamenti non preoccupano le aziende che al momento vedono l'introduzione di tale misura come positiva, non solo per la propria impresa ma per l'intero ecosistema di business.

In particolare, gli ambiti aziendali che sarebbero impattati positivamente sono molteplici, si va dall'organizzazione del lavoro e dei nuovi processi, alla formazione e attrazione della forza lavoro, al migliorare standard di qualità dei prodotti/servizi offerti, alle decisioni e strategie di investimento, passando per la reputazione e comunicazione esterna.

Sebbene la Direttiva NIS2, quindi, non dovrà essere obbligatoriamente seguita da tutte le aziende, c'è un impatto

“indiretto” che le imprese, a prescindere dalla loro dimensione o dal settore in cui operano, dovrebbero tenere in considerazione. Da questa prospettiva, infatti, **la Direttiva NIS2 potrebbe fare da catalizzatore per tutte le aziende e imprimere un effettivo miglioramento e potenziamento della sicurezza digitale dei loro sistemi informativi aziendali**, grazie ad esempio al coinvolgimento del vertice dell'azienda nella gestione delle strategie e delle misure relative alla sicurezza digitale.

Secondo questo nuovo quadro, per le aziende, il tema della sicurezza digitale non è solo destinato a coinvolgere figure aziendali specifiche come il Responsabile della Sicurezza Informatica (CISO) o il Responsabile Informatico (CIO), quanto anche i profili che dirigono e governano l'azienda. Figure responsabili della sicurezza informatica sono attualmente presenti nel 74% delle aziende intervistate, mentre nel 26% dei casi si tratta di realtà che al momento ne sono sprovviste. Di queste, una su tre si sta attivando per individuare una figura interna o esterna all'impresa, mentre per le altre 2 aziende su tre al momento tale tematica non risulta prioritaria.

Figura 8 | La presenza di un responsabile aziendale sui temi di sicurezza informatica



Le fondamentali attività di **“governance” del sistema informatico e della sua sicurezza** - come approvare le misure per la gestione del rischio, supervisionare l’implementazione di tali misure e partecipare a formazioni specifiche, estendendo quest’opportunità anche ai collaboratori, al fine di valutare l’efficacia e l’adeguatezza delle misure di sicurezza adottate - rientrano quindi nel **perimetro di chi dirige e governa l’azienda**. Infatti, la Direttiva NIS2 prevede che gli **organi di gestione** delle realtà che rientrano nell’ambito di applicazione della stessa, ricoprano un ruolo attivo nel definire e supervisionare la strategia di gestione del rischio *cyber* dell’organizzazione, e siano responsabili per la propria formazione e per quella di tutti i dipendenti su rischi e minacce *cyber*.

La sicurezza digitale non è quindi solo un problema “tecnico”, ma un aspetto fondamentale per il business e per le attività dell’azienda nel suo complesso. Senza un’idonea sicurezza digitale non viene garantita la continuità operativa, e questo è un tema di business che il vertice aziendale deve porsi e governare. Nelle aziende impattate direttamente dalla normativa, si prevede la presenza di organi di amministrazione e direttivi che dovranno assicurare un livello di controllo e responsabilità a tutti i livelli: le aziende dovranno strutturarsi internamente in modo adeguato al fine di essere *compliant* con la Direttiva NIS2.

Nell’analisi dei rischi, l’organizzazione deve considerare non solo quelli legati al sistema informativo, ma verificare, in un’ottica “multirischio”, quelli derivanti dalla gestione degli incidenti, dalla continuità operativa, dall’approvvigionamento e manutenzione, nonché quelli relativi alla catena di fornitura, al fattore umano e alle misure di sicurezza fisica. Andando oltre il mero concetto di *cybersecurity*, la Direttiva NIS2 pone maggiore enfasi sulla *cyber resilience*, in cui gli aspetti di adattabilità e resilienza sono pertanto cruciali per garantire la continuità operativa del sistema informativo e il funzionamento dell’organizzazione.

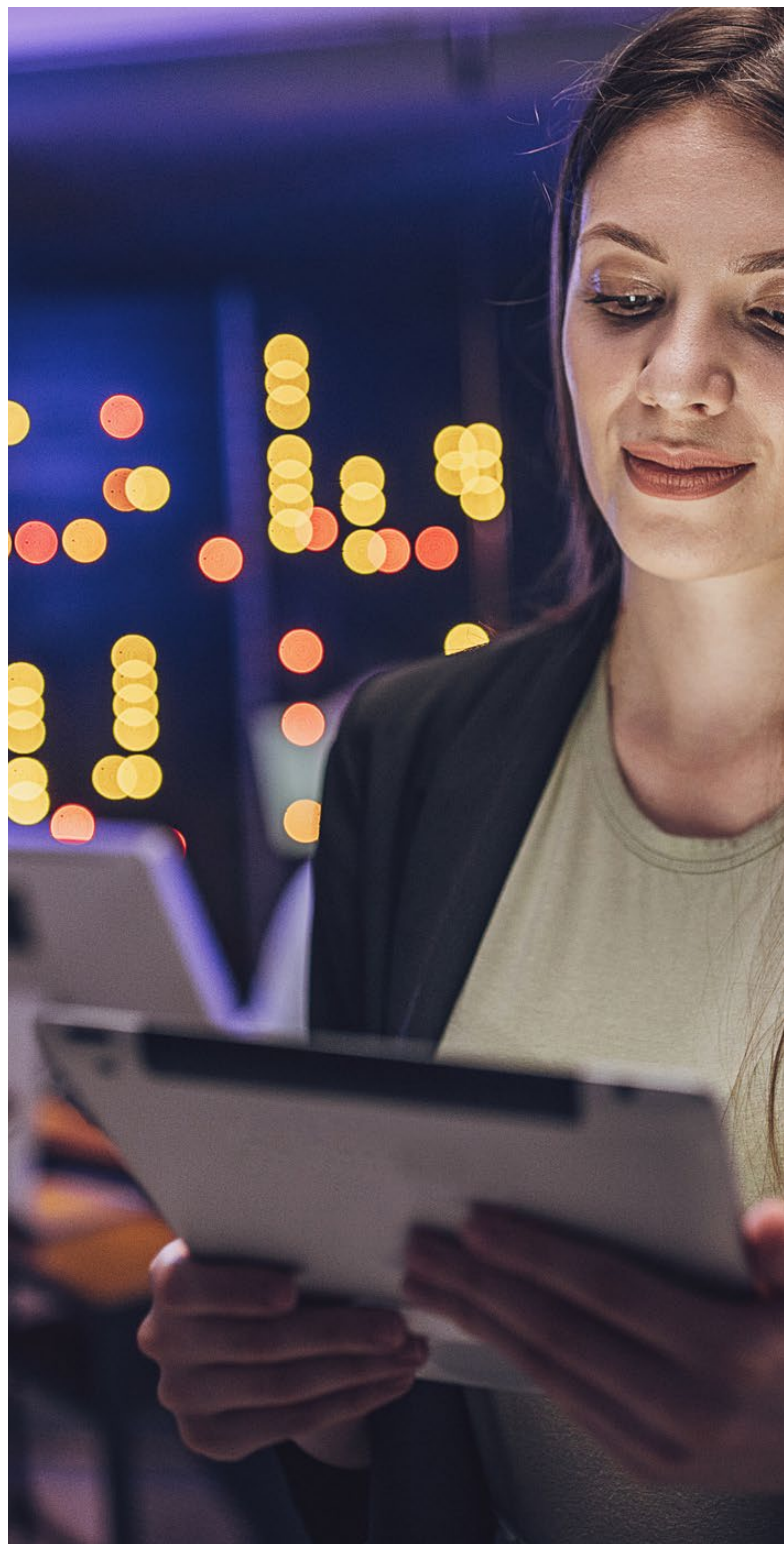
Il fattore umano rimane uno dei rischi più complessi da gestire e le organizzazioni possono avviare a questo punto, orientandosi verso **percorsi formativi** del proprio personale, tenendo in considerazione anche fornitori e clienti.

Questi aspetti rilevanti insiti nella Direttiva NIS2 ricalcano le azioni che le aziende del panel riconoscono come prioritarie nell’ambito della *cybersecurity*, ovvero governance, formazione e monitoraggio dell’ecosistema.

In definitiva, la Direttiva NIS2 rappresenta un’opportunità per tutto il tessuto aziendale e produttivo italiano di mantenere e rafforzare la propria posizione nel mercato. E questo vale tanto per le realtà che ad oggi hanno un qualsiasi grado di conoscenza della norma che per quelle PMI che mostrano un gap in tale senso (dalla ricerca, il livello di conoscenza di tale

norma è maggiore tra chi ha una pianificazione in ambito di *cybersecurity* (62%) rispetto a chi ne è sprovvisto (50%).

Adeguarsi proattivamente alle sue misure significa non solo proteggersi dalle minacce *cyber*, ma anche posizionarsi come partner affidabili e innovativi nel panorama nazionale ed europeo.



Riflessioni conclusive

Le PMI intervistate nell'ambito di questa ricerca dell'Osservatorio Deloitte Private mostrano una certa incertezza riguardo al futuro del contesto in cui operano. Infatti, la percezione principale che emerge dal panel è che nei prossimi 12 mesi si troveranno a operare in un ambiente generale incerto.

Affrontare la sfida digitale è cruciale per elevare il loro attuale livello tecnologico e innovativo. Garantire standard digitali elevati alla propria azienda permette di migliorare la competitività e questo può consentire in particolare alle imprese di dimensioni più ridotte di aumentare il proprio livello di adozione delle tecnologie e colmare il divario con le realtà più strutturate.

La trasformazione digitale è vista dal panel come l'investimento più importante per aumentare il valore aziendale, sia nel presente che nel futuro, e richiede già oggi una profonda revisione dei modelli di business esistenti; inoltre, le PMI possono stimolare la propria crescita ottenendo benefici su più fronti, generando valore sia per se stesse che per l'intero ecosistema in cui operano. In questo percorso, l'elemento culturale è cruciale: i dati indicano che la maggior parte delle imprese intervistate dichiara di avere un livello di preparazione e una cultura imprenditoriale necessari per affrontare la transizione digitale nel medio termine.

Un maggiore grado di maturità può stimolare investimenti nel digitale, così da consentire anche alle realtà non ancora orientate a una strategia di digitalizzazione di avviare concretamente questo percorso.

L'adozione di nuove tecnologie come quelle basate sull'Intelligenza Artificiale (AI) può contribuire alla crescita aziendale: in primo luogo, è fondamentale comprendere in che modo applicarle e quali sono i rischi ad esse connessi.

Oggi, l'innovazione tecnologica e l'uso dell'AI comportano una maggiore attenzione sul tema dei rischi e delle strategie

di difesa del proprio patrimonio informativo da attacchi e minacce provenienti da vari fronti. Per affrontarli le PMI possono mettere in pratica diverse azioni in materia di *cybersecurity*, in accordo con il nuovo contesto normativo determinato dall'introduzione della Direttiva NIS2 in Europa e recepita in Italia lo scorso ottobre. Questa ha l'obiettivo di incrementare il livello di sicurezza, ridurre il rischio di attacchi informatici a danno di tutti gli stakeholder e creare una strategia *cyber* univoca. Tramite la Direttiva NIS2, le imprese italiane che rientrano nel perimetro della normativa devono adottare un approccio più strutturato e proattivo nel governare il tema della sicurezza informatica.

La Direttiva NIS2 aggiorna il quadro giuridico e amplia l'ambito di applicazione a nuovi settori rispetto alla precedente normativa NIS, imponendo una gestione dei rischi sulla base di requisiti di sicurezza più rigidi, tenendo conto anche della sicurezza della *supply chain* per le imprese. Quest'ultimo aspetto dimostra l'impatto pervasivo e incisivo della direttiva, poiché impone alle aziende soggette alla normativa di valutare, monitorare e gestire i rischi della propria catena di fornitura. Ciò comporta che le aziende non soggette alla norma, come le piccole imprese che operano all'interno di filiere e collaborano con realtà più grandi o medie vincolate alla Direttiva NIS2, dovranno strutturarsi in modo adeguato al fine di adottare una attitudine di sicurezza elevata.

Andando oltre il mero concetto di *cybersecurity*, la Direttiva NIS2 pone enfasi sul concetto di *cyber resilience*, cruciale per assicurare la continuità operativa del sistema informativo e il funzionamento dell'organizzazione. Indipendentemente dal diretto coinvolgimento e dalla loro dimensione, tutte le aziende dovranno essere in grado di strutturare una governance tale da consentire loro un certo grado di conformità al nuovo quadro normativo e cogliere l'opportunità di rafforzare la propria posizione digitale, operando con consapevolezza e con un'adeguata preparazione.

Contatti



Ernesto Lanzillo

Senior Partner

Deloitte Private Leader per l'area
Central Mediterranean
(Italia, Grecia e Malta)

elanzillo@deloitte.it

Research & Editorial

Mario Filice

Senior specialist

DCM Growth – Eminence & Market Insights

mfilice@deloitte.it



Deloitte.

La presente pubblicazione contiene informazioni di carattere generale, Deloitte Touche Tohmatsu Limited, le sue member firm e le entità a esse correlate (il "Network Deloitte") non intendono fornire attraverso questa pubblicazione consulenza o servizi professionali. Prima di prendere decisioni o adottare iniziative che possano incidere sui risultati aziendali, si consiglia di rivolgersi a un consulente per un parere professionale qualificato. Nessuna delle entità del network Deloitte è da ritenersi responsabile per eventuali perdite subite da chiunque utilizzi o faccia affidamento su questa pubblicazione.

Il nome Deloitte si riferisce a una o più delle seguenti entità: Deloitte Touche Tohmatsu Limited, una società inglese a responsabilità limitata ("DTTL"), le member firm aderenti al suo network e le entità a esse correlate. DTTL e ciascuna delle sue member firm sono entità giuridicamente separate e indipendenti tra loro. DTTL (denominata anche "Deloitte Global") non fornisce servizi ai clienti. Si invita a leggere l'informativa completa relativa alla descrizione della struttura legale di Deloitte Touche Tohmatsu Limited e delle sue member firm all'indirizzo www.deloitte.com/about.