

Resilienza aziendale nell'era digitale, rinnovarsi o morire

La resilienza non è solo la risposta alle crisi, ma una capacità strategica fondamentale. Aiuta a prosperare in un'economia globale dinamica e volatile e cogliere opportunità. Le tecnologie digitali, come l'Intelligenza Artificiale, svolgono un ruolo abilitante

di Bernardo Nicoletti

Il panorama economico globale del XXI secolo è caratterizzato da una volatilità e un'interrazionalità senza precedenti. Eventi dirompenti come la pandemia di COVID-19, le tensioni geopolitiche, le guerre commerciali, gli attacchi informatici e gli shock climatici hanno evidenziato la profonda vulnerabilità di modelli operativi e di catene di approvvigionamento ottimizzati per l'efficienza, ma fragili di fronte all'imprevisto. La gestione tradizionale del rischio, concentrata sulla prevenzione di minacce note e probabili, si rivela insufficiente in un contesto di eventi imprevedibili e di vasta portata.

È in questo scenario che il paradigma della resilienza emerge non solo come una difesa necessaria. È una vera e propria capacità strategica che consente alle organizzazioni non solo di sopravvivere, ma anche di adattarsi e cogliere nuove opportunità nel caos. La resilienza va oltre la semplice continuità operativa. Come evidenziato nella letteratura manageriale, essa rappresenta un processo dinamico di adattamento positivo prima, durante e dopo l'avversità. Comprende le diverse abilità di anticipare, ridurre l'impatto, far fronte e riprendersi dagli effetti degli eventi negativi. In un'epoca di accelerata trasformazione digitale, il ruolo dell'Information and Communication Technology e dell'Intelligenza Artificiale diventa un abilitatore critico per costruire questa agilità sistemica.

Gestione della Resilienza

La resilienza, in ambito aziendale, è definita come il processo di adattamento positivo prima, durante e dopo l'avversità. Non è una reazione puntuale, ma una capacità continua che integra l'anticipazione, la riduzione dell'impatto, la gestione e il recupero dagli effetti di eventi dirompenti. Si distingue dalla semplice risposta a un evento negativo, poiché incorpora una propensione all'apprendimento e

al rinnovamento. Il posizionamento teorico della resilienza è multidisciplinare e attinge a diversi campi di studio. La resilienza ingegneristica si concentra sulla resistenza di un sistema e sulla velocità di recupero allo stato originale dopo uno shock. La resilienza ecologica enfatizza la capacità di un sistema di assorbire i disturbi e riorganizzarsi, mantenendo le stesse funzioni essenziali. La resilienza organizzativa è considerata una capacità dinamica che consente all'organizzazione di adattarsi e rinnovarsi in risposta a un ambiente in costante cambiamento. La resilienza della Supply Chain sintetizza i concetti precedenti in un contesto di rete, definita come l'abilità di anticipare, prepararsi, assorbire, rispondere e riprendersi dalle interruzioni.

È cruciale distinguere la resilienza da concetti spesso confusi. La robustezza è la capacità di resistere a una variabilità attesa. L'agilità è la velocità di adattamento. La flessibilità è l'ampiezza delle opzioni disponibili. L'affidabilità è la capacità di mantenere una performance costante in condizioni normali. L'antifragilità è la capacità di migliorare e trarre vantaggio dagli shock. In sintesi, mentre la gestione del rischio tradizionale chiede "cosa potrebbe andare storto e come possiamo fermarlo?", la gestione della resilienza chiede "come sopravviveremo e prospereremo quando qualcosa andrà storto?" la prima è preventiva e basata su probabilità note; la seconda è adattiva e preparata all'ignoto.

Modelli di resilienza

Diversi modelli concettuali aiutano a strutturare l'approccio alla resilienza. Il modello del framework delle 4R offre una visione sistemica. La robustezza è la capacità di resistere allo stress senza un fallimento catastrofico del sistema, ad esempio attraverso infrastrutture rinforzate o riserve finanziarie. La ridondanza è la presenza di



La Virtual Data Room è una richiesta crescente

La crescente pressione normativa ha profondamente trasformato il modo in cui aziende e istituzioni sono chiamate a proteggere i dati. Lo sottolinea **Marco Iannucci, Amministratore Delegato di Boole Server**, azienda italiana specializzata in soluzioni di sicurezza informatica. Fanno eccezione, nella maggior parte dei casi, le PMI, dove la sensibilità sul tema resta ancora bassa. Va però riconosciuto che qualcosa è cambiato: eventi gravi hanno rappresentato un campanello d'allarme, contribuendo a una maggiore consapevolezza. A favorire la diffusione della cultura digitale è anche il ricambio generazionale, che in alcuni casi porta in azienda manager più aggiornati. Tuttavia, gli spazi di miglioramento restano ampi.

In questo contesto, la digitalizzazione rappresenta una leva fondamentale per migliorare la qualità del lavoro e, in definitiva, creare valore. "L'obiettivo di ogni impresa resta quello di generare reddito e renderlo sostenibile nel tempo. Ma in un mondo dove il dato è diventato una risorsa strategica, la protezione dei documenti interni è parte integrante di questo obiettivo", riflette Iannucci. Non si tratta solo di mettere al sicuro i contenuti, ma di permettere collaborazione e condivisione in modo sicuro, all'interno e all'esterno dell'organizzazione.

Questa trasformazione apre nuove opportunità, ma comporta anche una grande responsabilità. Così come in passato i ladri potevano introdursi fisicamente in azienda per sottrarre beni materiali, oggi possono farlo digitalmente, mirando a dati e informazioni sensibili. Ecco perché la sicurezza informatica non può più essere considerata un elemento accessorio. Proteggere l'accesso alla Rete rappresenta la prima linea di difesa. Ma la sicurezza non si ferma qui: è fondamentale adottare sistemi di cifratura che accompagnino i file lungo tutto il loro ciclo di vita. In questo modo, anche in caso di attacco, i contenuti resterebbero illeggibili. A queste misure si aggiungono soluzioni come la posta elettronica criptata e strumenti per il trasferimento sicuro di file di grandi dimensioni. Un esempio avanzato è quello delle Virtual Data Room (VDR): spazi digitali temporanei, accessibili solo a soggetti autorizzati – come l'ufficio legale, il reparto HR o consulenti esterni – per la condivisione di documenti riservati. "Un tempo tutto questo avveniva in stanze fisiche, presso la sede aziendale, tra documenti fotocopiati e consultazioni su appuntamento. Oggi avviene in cloud, ma la logica non è cambiata".

Ma la vera sfida è all'orizzonte. Il quantum computing, una volta applicato su larga scala, metterà in discussione le attuali certezze. Gli algoritmi che oggi consideriamo sicuri potrebbero diventare vulnerabili, mentre la potenza di calcolo in arrivo avrà la capacità di superare molte delle difese attuali. "Le aziende che oggi sottovalutano il tema della protezione digitale devono attivarsi. La protezione non è più un'opzione, ma una parte strutturale dell'identità dell'impresa".

elementi sostituibili e di riserva, come data center di backup o fornitori diversificati. La prontezza di spirito è la capacità di gestire una crisi in modo efficace, mobilitando risorse e prendendo decisioni, attraverso una leadership agile e protocolli di comunicazione chiari. La rapidità è la capacità di contenere le perdite e recuperare le funzioni critiche, grazie a piani di recupero collaudati e a processi decisionali accelerati. Robustezza e ridondanza sono investimenti proattivi fatti prima di una crisi. Prontezza e rapidità sono capacità adattive che si manifestano durante e dopo la crisi. Un'organizzazione veramente resiliente bilancia tutte e quattro le componenti.

Un altro modello concettualizza la resilienza come una capacità organizzativa stratificata che integra le dimensioni individuali, di gruppo e organizzative. Il Livello Individuale si riferisce

all'ottimismo, alla fiducia e all'adattabilità dei dipendenti. Il Livello di Gruppo è la capacità del team di collaborare sotto pressione e di apprendere dai fallimenti senza ricadere nella cultura della colpa. Il Livello Organizzativo è l'integrazione strategica di tutti i livelli per creare una capacità di sistema. Questo modello può essere ulteriormente scomposto in tre componenti chiave: la Resilienza Cognitiva, che è come pensiamo e la capacità di notare e formulare risposte a minacce complesse; la Resilienza Comportamentale, che è come agiamo e la capacità di azione collaborativa e di improvvisazione; la Resilienza Contestuale, che è il nostro ambiente, la cultura e la fiducia che abilitano azioni resilienti.

Modelli specifici per la supply chain identificano dimensioni chiave quali flessibilità, velocità, collaborazione, visibilità e ridondanza. Altri distinguono

tra strategie di buffering, ossia la creazione di scorte e capacità di tampone, e strategie di agilità, ossia la flessibilità e la rapidità di risposta. La resilienza della supply chain richiede un approccio olistico che copra l'approvvigionamento, la produzione e la distribuzione, enfatizzando la visibilità end-to-end e la collaborazione con i partner.

Meccanismi causali

I modelli di resilienza sono alimentati da meccanismi causali dinamici che spiegano come le organizzazioni generano risultati resilienti. Questi meccanismi formano un ciclo continuo. L'anticipazione è il meccanismo di guardare avanti per identificare potenziali minacce e opportunità, che comprende la scansione ambientale, le previsioni e il rilevamento di segnali deboli. L'assorbimento è la capacità di assorbire l'impatto di un evento

dirompente senza collassare, utilizzando meccanismi di "ammortizzazione" come buffer, ridondanze e modularità.

L'adattamento è la capacità di rispondere in tempo reale a condizioni impreviste, modificando processi e strutture attraverso l'improvvisazione, i cicli decisionali rapidi e i team autorizzati. L'apprendimento è il meccanismo per capitalizzare le esperienze per migliorare le capacità future, attraverso la revisione post-evento e l'apprendimento a doppio ciclo. Il rinnovamento è il meccanismo più avanzato, che implica un riposizionamento strategico per emergere dalla crisi più forte di prima, attraverso l'evoluzione del modello di business e la trasformazione digitale. Questi meccanismi non sono sequenziali ma spesso si sovrappongono e si rafforzano a vicenda, creando un sistema organizzativo vitale e adattivo.

La Nis2 sprona a un cambiamento culturale

La direttiva Nis2 rappresenta un punto di svolta: impone nuovi obblighi, alza il livello minimo di sicurezza e allarga lo spettro dei settori coinvolti, estendendosi all'intera filiera. Tuttavia, è spesso affrontata dalle aziende con un approccio riduttivo, quasi fosse sufficiente installare un antivirus per ritenersi conformi. In realtà, ciò che la direttiva richiede è una trasformazione profonda, che deve investire l'intera organizzazione. Lo sottolinea **Denis Ceriolo, IT Manager di Dgroove**, azienda specializzata in tecnologie e formazione IT.

In molte realtà italiane, secondo l'osservatorio di Dgroove, questa consapevolezza tarda ad affermarsi. Nel settore manifatturiero, per esempio, la sensibilità varia da caso a caso: le strutture tecniche spesso sono pronte e consapevoli, ma il management tende a minimizzare il rischio, soprattutto in assenza di esperienze dirette. Per superare questa visione miope, strumenti come il Return on security investment (Rosi) e il Single loss expectancy (Sle) diventano fondamentali, spiega Ceriolo. Permettono infatti di quantificare chiaramente sia il costo delle misure di protezione sia il fermo dell'attività causato da un attacco. "Confrontare questi due valori è spesso l'unico linguaggio che riesce a coinvolgere concretamente uffici acquisti e le direzioni non tecniche."

Questa comprensione può sbloccare così anche l'investimento tecnologico, in un contesto dove l'evoluzione è rapidissima. Dall'antivirus tradizionale si è, infatti, passati in pochi anni a sistemi sempre più sofisticati, con presidi attivi 24 ore su 24 e il supporto dell'AI. "L'AI è ormai un elemento chiave nella raccolta e interpretazione degli eventi, ma serve attenzione. È utilizzata in modo sempre più raffinato anche da chi attacca". Ed è proprio qui che si impone un cambio di paradigma: se gli attacchi evolvono, non si può più pensare che la tecnologia da sola basti. Serve una strategia chiara e una governance definita. "Password condivise, utenti non nominali, assenza di controlli e monitoraggi sono ancora troppo frequenti; eppure, si tratta di errori banali, risolvibili con un impegno minimo".

Guardando al futuro, diventa essenziale rafforzare la formazione a tutti i livelli, creare team dedicati e introdurre simulazioni periodiche. Così come si provano evacuazioni antincendio – è la metafora usata da Ceriolo – anche in azienda bisogna sapere esattamente come comportarsi nei minuti cruciali dopo un attacco. "Alcune aziende hanno già avviato percorsi di sensibilizzazione continua, come brevi comunicazioni interne, consigli settimanali e avvisi nei luoghi comuni. Altre investono in veri e propri programmi formativi, con l'obiettivo di costruire una cultura solida e quotidiana della sicurezza. Questa è la strada da percorrere". In questo modo la cybersecurity non è più vista come un costo, ma come parte integrante dell'organizzazione.





Resilienza digitale: come governare il cambiamento (e non subirlo)

di Filippo Ollari, Senior Team Leader & ERP Project Manager di Sinfo One

Leggendo l'articolo di Nicoletti, il pensiero va oltre il singolo ambito applicativo e tocca un tema che, nelle imprese, è sempre più decisivo: la capacità dei sistemi – tecnologici e organizzativi – di reggere la complessità senza rallentare l'azienda. L'AI è spesso raccontata come una scorciatoia. In realtà è un abilitatore potente solo se inserito in architetture solide, integrate e governabili. Altrimenti accelera il rumore invece del valore. *Primum non nocere*: prima di correre, serve stabilità.

Velocità e flessibilità, richiamate nell'articolo, non sono sinonimi di improvvisazione. Per un'impresa, essere veloce significa poter decidere rapidamente perché i dati sono affidabili, i processi sono chiari e i sistemi rispondono. Essere flessibile non vuol dire cambiare direzione ogni mese, ma adattarsi senza rompersi quando cambiano mercati, volumi, canali o modelli di business.

È qui che i sistemi IT diventano un fattore strategico. Non come sommatoria di strumenti, ma come infrastruttura capace di sostenere crescita, trasformazione e innovazione continua. Oggi l'AI può rafforzare questa capacità: aiutare a leggere segnali complessi, supportare decisioni, aumentare la velocità di risposta. Ma funziona solo se poggia su basi robuste e su una governance chiara.

È una dinamica che in Sinfo One osserviamo da oltre 40 anni. Abbiamo accompagnato aziende che negli ultimi due decenni sono letteralmente esplose, con fatturati che sono in 15 anni ventuplicate (neologismo coniato per questo articolo) arrivando a fatturare oltre mezzo miliardo. Aziende che hanno aperto mercati internazionali, creato filiali, affrontato percorsi di crescita sia organica sia per acquisizioni.

Lo hanno fatto restando sulla stessa piattaforma applicativa, che li ha supportati nel tempo perché studiata e verticale per un determinato mercato. Questo ha consentito loro di crescere velocemente, restare flessibili e, soprattutto, non perdere il controllo. Per me, questa è la vera resilienza: non resistere al cambiamento, ma renderlo attraversabile. È ciò che permette di integrare nuove tecnologie, compresa l'AI, senza sacrificare affidabilità, sicurezza e coerenza interna. *Non multa sed multum*: non più tecnologia, ma tecnologia migliore. La sfida per gli imprenditori oggi non è inseguire l'ultima innovazione, ma costruire un'impresa capace di essere veloce, flessibile e solida allo stesso tempo. Perché solo così si governa il cambiamento, invece di subirlo.

Tecnologie abilitanti

Le tecnologie digitali sono il moltiplicatore di forza per la resilienza aziendale, abilitando visibilità, intelligenza e agilità su scale prima impensabili. L'Intelligenza Artificiale (AI) e il Machine Learning sono il cuore della resilienza predittiva e adattiva. Le applicazioni spaziano dall'analisi predittiva per prevedere le interruzioni della supply chain, alla manutenzione predittiva, al rilevamento delle frodi e all'automazione dei processi. I chatbot basati sull'AI forniscono supporto costante. La blockchain fornisce trasparenza, tracciabilità immutabile e fiducia nelle transazioni. Le sue applicazioni includono la tracciabilità dei prodotti e gli smart contract per automatizzare i pagamenti.

L'Internet of Things fornisce dati in tempo reale sullo stato e sulla posizione di asset fisici, consentendo il monitoraggio in tempo reale dei prodotti in transito e la gestione di infrastrutture intelligenti. Il Cloud Computing fornisce

un'infrastruttura scalabile, flessibile e resiliente di per sé, cruciale per il disaster recovery e per il supporto alla forza lavoro remota. Le tecnologie di cybersecurity proteggono l'infrastruttura digitale e i dati, asset critici per la resilienza. Applicazioni come il rilevamento delle minacce guidato dall'AI e i framework Zero Trust sono essenziali per proteggere dai cyber-rischi. L'integrazione sinergica di queste tecnologie crea un "sistema nervoso digitale" per l'organizzazione.

Maturità digitale e IDC Benchmark

La maturità della resilienza è strettamente correlata alla maturità digitale dell'organizzazione. IDC fornisce un quadro per valutare il livello di avanzamento delle organizzazioni tramite il suo "MaturityScape Benchmark: Digital Supply Chain Resiliency". Il benchmark identifica cinque stadi di maturità: Ad Hoc, in cui i processi sono non definiti e reattivi; Opportunistico, con primi tentativi di standardizzazione; Ripetibile, con processi

definiti e documentati; Gestito, con processi integrati e misurati, con un approccio proattivo; e Ottimizzato, in cui la resilienza è una capacità strategica alimentata dall'automazione e dall'AI. I dati mostrano che la maggior parte delle organizzazioni è nelle fasi iniziali, con una percentuale significativa negli stadi ad hoc e opportunistici. Solo una minoranza si trova negli stadi più maturi. IDC classifica, inoltre, le organizzazioni in Sopravvissuti, che applicano sforzi minimi per la resilienza, e Prosperi, che digitalizzano e ottimizzano la supply chain per la resilienza, utilizzandola per ottenere un vantaggio competitivo. L'analisi per dimensioni mostra dove le organizzazioni sono più indietro: ad esempio, molte lottano nella dimensione Persone, faticando a trasformare la cultura. Questo evidenzia che la tecnologia da sola non basta: sono il fattore umano e la strategia a fare la differenza.

Dibattiti critici e implicazioni strategiche

L'adozione di un approccio resiliente non è priva di tensioni e dibattiti critici che i leader devono affrontare. Il trade-off classico è tra efficienza e resilienza. I costi di buffer e di ridondanza sembrano antitetici all'ottimizzazione lean. L'implicazione strategica è che un certo grado di "inefficienza" calcolata è il prezzo da pagare per la sopravvivenza. Un altro dibattito riguarda la Standardizzazione vs. l'Improvvisazione, bilanciando il rispetto dei protocolli con l'empowerment dei team per deviare quando necessario.

Il Paradosso della Digitalizzazione sottolinea come la tecnologia fortifichi la resilienza, ma crei anche nuove vulnerabilità, il che richiede investimenti concomitanti in digitalizzazione e cybersecurity. Le questioni di responsabilità ed

Resilienza nella permacrisi: leggere il cambiamento, decidere, adattarsi

di Vincenzo Natile, Managing Partner di EIM Italia

La permacrisi definisce l'attuale assetto dell'economia globale come una condizione di instabilità continua, economica, geopolitica, tecnologica e sociale. Non si tratta più di una sequenza di shock temporanei, occasionali e distanti nel tempo, ma di una nuova normalità che impone alle organizzazioni di operare in contesti complessi, incerti e in rapido mutamento.

Tre competenze emergono come centrali. La prima è la capacità di leggere costantemente il cambiamento, intercettando segnali deboli, trend emergenti e discontinuità. Ciò richiede organizzazioni data-driven, capaci di integrare informazioni provenienti dal mercato, dai processi interni e dagli ecosistemi esterni, superando logiche di analisi episodica a favore di un ascolto continuo.

La seconda competenza è decidere con coraggio e rapidità. In condizioni di permacrisi, la qualità della decisione non deriva dalla completezza dell'informazione, ma dalla capacità di agire tempestivamente, accettando margini di incertezza e correggendo il percorso in itinere. Questo implica il superamento di modelli decisionali gerarchici e l'adozione di strutture di governance più snelle, fondate su fiducia, delega, responsabilizzazione diffusa e allineamento sugli obiettivi.

La terza competenza riguarda la capacità di adattarsi con flessibilità e intelligenza, riconfigurando modelli operativi, processi e ruoli in funzione dei cambiamenti del contesto. L'adattabilità non è solo strutturale, ma soprattutto cognitiva: nasce dall'apertura mentale, dalla contaminazione esterna (sia di sistema e networking sia di governance aziendale), dall'apprendimento continuo e dalla disponibilità a sperimentare. In questo senso, la complessità diventa una risorsa strategica, poiché stimola innovazione, collaborazione e nuove soluzioni.

La leadership manageriale e imprenditoriale giocano un ruolo abilitante decisivo. La permacrisi accelera il passaggio da un management tradizionale, orientato al controllo, a una leadership autentica e partecipativa, capace di ascolto, ispirazione e valorizzazione delle competenze. Le organizzazioni più resilienti sono quelle che favoriscono il confronto, integrano competenze eterogenee e utilizzano la tecnologia come supporto alle decisioni, senza sostituire il giudizio umano.

In conclusione, la resilienza nella permacrisi deriva dalla capacità di sviluppare competenze adattive sostenute da leadership evolute e assetti organizzativi flessibili. Leggere il cambiamento, decidere rapidamente e adattarsi con intelligenza consente alle imprese non solo di sopravvivere, ma di trasformare la complessità in un vantaggio competitivo sostenibile nel lungo periodo.



etica mettono in guardia dal rischio di trasferire l'onere della resilienza sui dipendenti o sui fornitori più deboli, il che implica la necessità di una resilienza equa e collaborativa. Infine, esistono tensioni con la sostenibilità, in cui alcune scelte di resilienza possono confliggere con gli obiettivi Environment, Social e Governance (ESG), mettendo i leader di fronte all'obbligo di integrare la sostenibilità nell'identità della resilienza. L'implicazione strategica generale è che la resilienza non è una funzione a sé stante, ma deve essere integrata orizzontalmente in tutte le decisioni aziendali, dalla strategia alla finanza, dalle operations alle risorse umane. Richiede un cambio di mentalità da "prevenire e proteggere" a "preparare e prosperare".

Agenti AI a supporto della gestione della resilienza

L'AI rappresenta oggi il più potente abilitatore di resilienza aziendale, trasformando la capacità di risposta alle crisi da reattiva a proattiva e predittiva. In particolare, gli agenti AI – sistemi autonomi in grado di percepire, decidere e agire – stanno rivoluzionando questo ambito. Questi agenti operano come un "sistema nervoso digitale" continuo, monitorando in tempo reale flussi di dati interni ed esterni, dalle performance operative ai trend di mercato, dalle condizioni logistiche alle minacce informatiche. Il loro valore risiede nella capacità di rilevare anomalie e segnali deboli di disruption prima che si materializzino in crisi. Un agente AI può, ad esempio, identificare un potenziale collo di bottiglia in una supply chain globale, simularne l'impatto e attivare automaticamente piani di mitigazione, come il riordino presso un

fornitore alternativo o il cambio di rotta di una spedizione, senza necessità di un intervento umano.

Allo stesso modo, in caso di un attacco informatico, un agente di cybersecurity può non solo rilevare l'intrusione, ma anche isolare automaticamente i segmenti di rete compromessi, contenendo la minaccia in pochi millisecondi. Oltre all'automazione della risposta, gli agenti AI potenziano l'adattamento e l'apprendimento. Analizzando gli esiti delle strategie passate, questi sistemi raffinano continuamente i loro modelli predittivi e le loro risposte, creando un circolo virtuoso di miglioramento continuo. In sostanza, gli agenti AI non sono solo strumenti di allerta, ma veri e propri partner operativi che elevano la resilienza da mera capacità di sopravvivenza a leva strategica per un vantaggio competitivo sostenibile in un mondo imprevedibile.

Utilizzi eccellenti in aziende

La società aerospaziale, della difesa e della sicurezza Leonardo rappresenta un caso eccellente di resilienza guidata dalla tecnologia. Leonardo utilizza l'AI per la manutenzione predittiva dei suoi velivoli e dei sistemi complessi. Analizzando i dati dei sensori in tempo reale, i loro sistemi AI possono identificare anomalie e potenziali guasti prima che si verifichino, riducendo i tempi di fermo non pianificati e garantendo l'operatività. Il colosso multinazionale dell'energia Enel ha abbracciato la digitalizzazione per costruire una rete energetica più resiliente e sostenibile. Enel utilizza l'AI per ottimizzare le prestazioni dei suoi parchi eolici e solari.

Analizzando dati meteorologici e di produzione, l'AI aiuta a prevedere la produzione di energia e a gestire la domanda, rendendo la rete più stabile e adattabile. La maggior energetica ENI applica l'AI nell'esplorazione di idrocarburi. Utilizzando algoritmi di machine learning per analizzare dataset sismici di grandi dimensioni, ENI può identificare con maggiore precisione i potenziali giacimenti di petrolio e gas, riducendo il rischio associato alle perforazioni e rendendo il proprio business upstream più resiliente alle volatilità dei prezzi.

Conclusioni

Le raccomandazioni strategiche per i leader sono chiare. È necessario adottare una visione olistica della resilienza, che integri i modelli 4R e multilivello. La resilienza deve essere misurata e gestita attraverso un dashboard equilibrato di KPI. Gli investimenti in tecnologie abilitanti, in particolare AI e cybersecurity, devono essere prioritari, ma sempre accompagnati da un focus parallelo sulle



Rinnovarsi per resistere, il ruolo dei servizi nell'industria

di Fabio Di Martino, CEO DI Mechinno

Oggi viviamo in un'epoca di cambiamenti rapidi e continui: mercati interconnessi, innovazioni tecnologiche veloci, vincoli normativi in evoluzione, ma anche situazioni imprevedibili legate a tensioni geopolitiche e variabili macroeconomiche; tutti fattori che possono modificare la strategia di un'azienda dall'oggi al domani. In questo contesto, la resilienza non è più una qualità accessoria, ma un elemento essenziale per continuare a sviluppare progetti, innovare e prendere decisioni consapevoli. Non si tratta solo di essere in grado di reagire agli shock, ma anche della capacità di adeguarsi, essere flessibili e mantenere coerenza e visione in un ambiente complesso e incerto.

Per le imprese manifatturiere, questa combinazione di resilienza, adattabilità e visione si traduce in decisioni concrete: come sviluppare nuovi prodotti, in che modo ottimizzare tempi e costi, come scegliere dove investire e dove invece fermarsi. E per le società di servizi che le affiancano, il ruolo va ben oltre l'esecuzione tecnica: significa mettere a disposizione competenze ed esperienza specialistica, in modo che diventino strumenti reali e adattabili a supporto delle scelte strategiche, aiutando le aziende a valutare alternative, misurare rischi e trasformare l'incertezza in opportunità concrete.

Per chi opera nei servizi di ingegneria e sviluppo prodotto, la capacità di tenere il passo con il cambiamento rappresenta una sfida quotidiana: aggiornare costantemente competenze e approcci, adeguare i processi a nuove esigenze e garantire standard elevati di qualità e affidabilità. Questo richiede la capacità di trasformare il know-how in soluzioni operative, integrandole nei percorsi di innovazione dei clienti senza perdere la visione d'insieme. È in tale prospettiva che la resilienza delle aziende di servizi si intreccia con quella delle imprese che accompagnano, dando vita a un valore condiviso e duraturo.

In questo contesto, le tecnologie digitali amplificano ulteriormente queste possibilità: strumenti di simulazione avanzata, modellazione, analisi dei dati e applicazioni di intelligenza artificiale non sostituiscono l'esperienza, ma la rendono più efficace, condivisibile, accessibile e adattabile. Consentono di esplorare scenari alternativi, testare ipotesi complesse e trasformare competenze specialistiche in decisioni concrete e ponderate, supportando un'organizzazione in evoluzione continua.

La resilienza, dunque, non è un traguardo da raggiungere una volta per tutte, ma un percorso continuo di apprendimento, aggiornamento, adattamento e collaborazione. Per le aziende manifatturiere e per chi le affianca nello sviluppo prodotto, rinnovarsi significa creare le condizioni per prendere decisioni migliori, trasformando l'incertezza in scelte ponderate. È in questo equilibrio tra solidità tecnica, apertura al cambiamento e visione strategica che resilienza e capacità di adeguamento diventano un vero vantaggio competitivo.



persone e sulla cultura organizzativa. Le organizzazioni devono evolversi da uno stadio reattivo o responsivo a uno predittivo e presciente, ponendosi l'obiettivo di diventare "Prosperare" e non solo "Sopravvissute". Questo richiede di affrontare consapevolmente i dibattiti critici, trovando un equilibrio dinamico tra efficienza e resilienza, tra standardizzazione e improvvisazione.

La visione futura della resilienza è quella di un ecosistema interconnesso e intelligente. La supply chain del futuro sarà un sistema nervoso digitale capace non solo di resistere agli shock, ma anche di anticiparli e adattarsi quasi in modo organico. L'AI generativa e agentica promette di automatizzare ulteriormente la risposta alle crisi, mentre

l'edge computing porterà l'elaborazione dei dati sempre più vicino al punto di bisogno. In questo contesto, la resilienza non sarà più soltanto una funzione di difesa, ma una fonte primaria di vantaggio competitivo. Come suggerisce un noto aforisma di McKinsey, la resilienza non è solo questione di rimbalzare, ma di rimbalzare in avanti. In un mondo di continui cambiamenti, la capacità di un'organizzazione di apprendere, adattarsi e trasformarsi diventa la sua unica vera sostenibilità.

Bibliografia online

Per accedere alla bibliografia online dell'articolo è sufficiente scansionare il QR Code presente nel sommario.