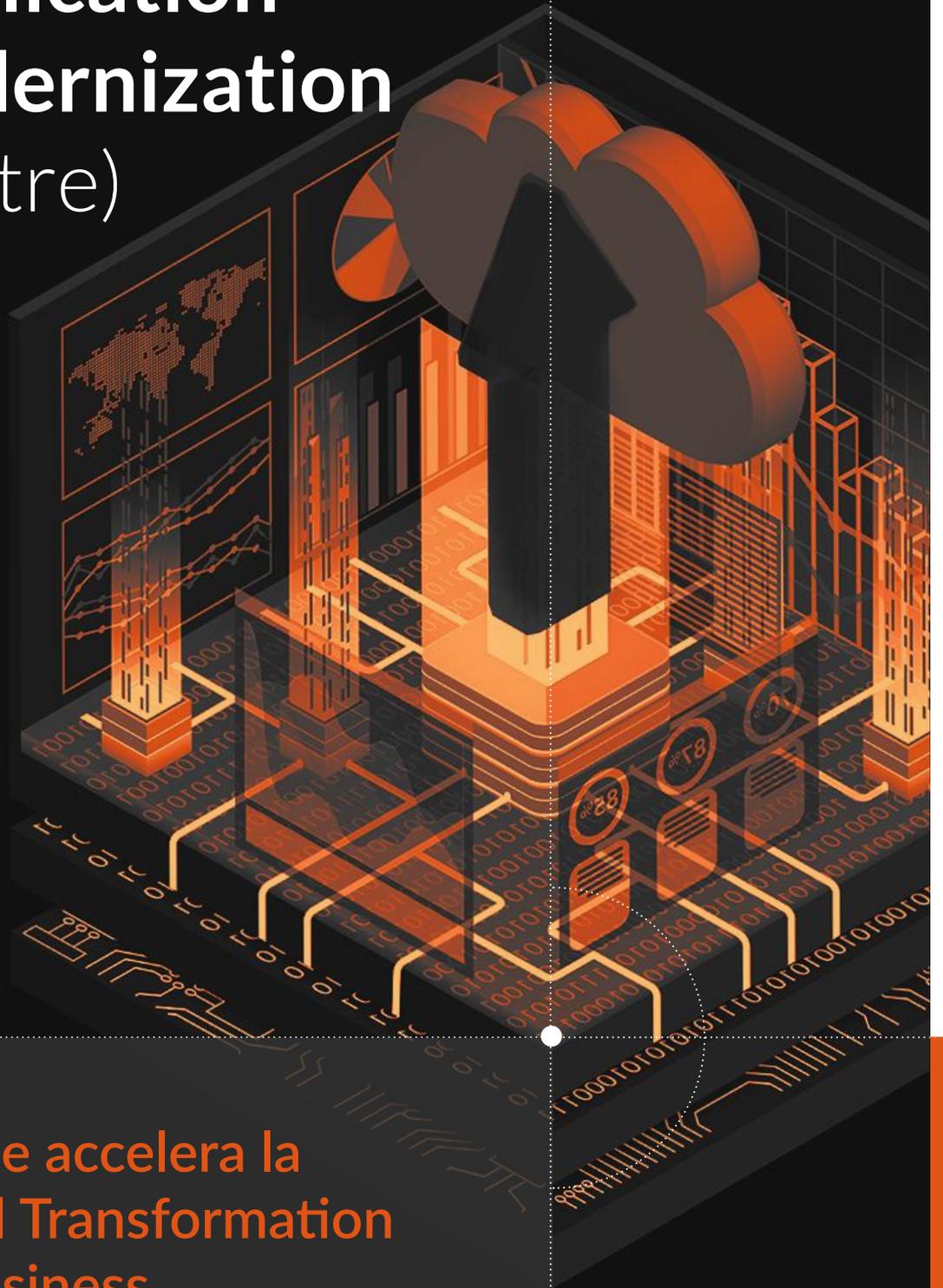


Application modernization (e oltre)



L'IT che accelera la
Digital Transformation
del Business

LE SFIDE PRIORITARIE (E LE OPPORTUNITÀ) PER LA TRASFORMAZIONE DIGITALE DELLE ORGANIZZAZIONI

Il ritmo accelerato dell'evoluzione tecnologica impone oggi alle aziende un **ripensamento delle proprie strutture IT**, sempre più chiamate a guidare e supportare la trasformazione digitale del business. Un contesto di trasformazione reso ancor più urgente e critico a fronte di “nuove” sfide legate a “cornici” di crisi e cambiamenti di natura economica, energetica, ambientale e geopolitica.

Nei processi di Digital Transformation delle aziende, quello della **modernizzazione delle applicazioni costituisce una fase nodale, finalizzata a rendere applicazioni e servizi digitali sempre più attuali e “pronti” alle esigenze di mercati dinamici, volatili, incerti e complessi.**

La digitalizzazione però è un percorso complesso e strutturato fatto di

tecnologie abilitanti e servizi digitali evoluti che possono esprimersi al massimo delle loro potenzialità solo grazie a una progettualità accurata, proattiva e responsabile e da un'azione di monitoraggio continua da diversi punti di vista.

Ecco perché **la modernizzazione delle applicazioni va inserita in una strategia di ampio respiro**, che guarda all'ottimizzazione di tutti i modelli operativi aziendali dal **business process reengineering**, alla **sicurezza** e alla **sostenibilità** (economica e finanziaria) del Cloud, senza trascurare l'importantissimo pilastro delle **competenze**.

Alla radice di ogni percorso verso la modernizzazione vi è, per le aziende, la volontà di **trasformare l'intera attività di business e di restare competitive sul mercato** sfruttando, in quest'ottica, le enormi poten-

zialità del Cloud e dell'approccio applicativo ai microservizi, sia per lo sviluppo di nuove applicazioni, cloud native di nome e di fatto, sia per la migrazione in Cloud delle applicazioni legacy (ancora molto presenti in svariate realtà).

Per molte organizzazioni, che spesso hanno sostenuto rilevanti investimenti in ambito IT sia in termini di sistemi informativi che di know-how interno – un elemento di differenziazione competitiva – **la risposta alle sfide della digitalizzazione non può essere sinonimo di implementazione di soluzioni completamente nuove e aggiunta continua di strati tecnologici.** Oggi l'attenzione alla sostenibilità, non solo ambientale ma anche economica e di business, impone alle aziende scelte differenti più orientate a **soluzioni al passo con i tempi per rinnovare e modernizzare il panorama applicativo esistente ed i processi di business, anche in termini di sicurezza e servizi Digital Trusted.**

Ma affinché la trasformazione digitale sia organica ed efficiente è necessario agire su dei pilastri fondamentali, **fattori strategici in grado di abilitare una serie di servizi e processi** che vanno a nutrire tutto l'ecosistema produttivo ed economico.

Nel corso di un confronto aperto, in occasione dell'evento **“DoITNow”** – organizzato da Aruba per l'inaugurazione di due nuovi data center all'interno del Global Cloud Data Center di Ponte San Pietro a Bergamo – manager aziendali e professionisti dell'IT hanno avuto modo di confrontarsi per capire a che punto si trovano nel percorso di modernizzazione delle loro applicazioni aziendali per migrare verso quelle cloud native, più agili e improntate sul paradigma DevSecOps. Un tema chiave e vitale per il presente e il futuro delle imprese cui sono direttamente e strettamente collegati gli altri temi che sono stati oggetto di analisi e dibattito tra manager e professionisti in diversi tavoli di lavoro, dalla cybersecurity alla reingegnerizzazione dei processi in ottica Trust, dal focus sulla sostenibilità (economica ed ambientale) del Cloud a quello sulla people strategy legato all'importanza e alla valorizzazione delle competenze.

Lo scopo dei tavoli di lavoro è stato indagare le sfide richiamate dalla trasformazione digitale attraverso il confronto attivo di visioni, obiettivi, execution e risultati attesi o monitorati.

SOM MA RIO

1 APPLICATION
MODERNIZATION,
LA STRADA È
TRACCIATA MA CI
SONO ANCORA NODI
DA SCIogliere
p. 5

2 DIGITAL TRANSFORMATION E
BUSINESS PROCESS REENGINEERING:
DAL CAMBIAMENTO DI MINDSET E
DI APPROCCIO AL RUOLO CHIAVE
DELLA FIDUCIA VERSO UNA NUOVA
VISION
p. 13

3 LA SOSTENIBILITÀ (ANCHE)
ECONOMICA DEL CLOUD: DAL
PARADIGMA FINOPS AL GREEN IT
p. 21

4 STAY CLOUD STAY
SECURE: L'ADOZIONE
DEL CLOUD COME
ELEMENTO CHIAVE
DELLA SECURITY
STRATEGY
p. 30

5 HR DIGITAL
TRANSFORMATION:
ANCHE LA PEOPLE
STRATEGY AL CENTRO
DELLE SFIDE DEI CIO
p. 37

Le sfide prioritarie
della trasformazione
digitale nelle
organizzazioni

1 Application Modernization – Cloud Native e DevOps

2 Reingegnerizzazione dei processi in ottica Trust

3 Sostenibilità (anche) economica del Cloud: dal FinOps al GreenIT

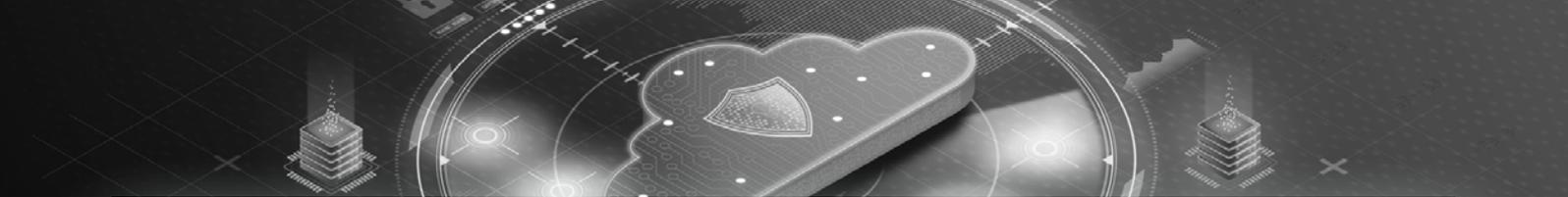
4 Cybersecurity: Stay Cloud Stay Secure

5 People Strategy



1

**APPLICATION
MODERNIZATION,
LA STRADA È TRACCIATA
MA CI SONO ANCORA
NODI DA SCIogliere**



Il ritmo di evoluzione tecnologica imposto alle imprese dalla digital transformation richiede alle organizzazioni IT cambiamenti nell'architettura applicativa, necessari per supportare le nuove esigenze di business. In quest'ottica, gli **strumenti di modern application development** permettono sia di modernizzare i sistemi legacy esistenti, sia di creare una **nuova generazione di applicazioni**, più **agili nei rilasci** e **rapide da sviluppare** e **distribuire** agli utenti.

Ma qual è la strategia giusta? Quali i servizi corretti da usare? Quali gli strumenti e le tecnologie più idonee ad indirizzare la modernizzazione degli applicativi?



La pandemia ha cambiato alla radice il nostro modo di approcciare e chiedere servizi digitali. Latenza, velocità, sicurezza, immediatezza, i professionisti e i manager oggi pretendono sempre più di avere tra le mani il servizio, l'applicazione che serve, quando serve e come serve con pochissima tolleranza per ritardi, complessità e interruzioni.

Uno scenario diffuso, tra PMI e organizzazioni di livello enterprise, che sta mettendo l'acceleratore alla spinta del **parco applicativo in direzione Cloud**: questione di agilità, immediatezza, sicurezza. Agile, DevSecOps, cloud native... il punto è scrivere e distribuire applicazioni più velocemente e in maniera più agile per permettere a tutti di **prendere decisioni migliori in meno tempo** ma, al netto di una strada tracciata, ci sono ancora ostacoli, dubbi e problemi tecnologico-culturali da affrontare senza, al mo-

mento, certezza di una via di uscita precisa.

Mancano infatti **figure specializzate** in grado di guidare questa evoluzione, manca un'**adeguata sensibilità** verso la trasformazione dei processi in ottica digital, ad esempio, non è più possibile lavorare in ottica waterfall (a cascata) ma serve svoltare in ottica DevSecOps, combinazione di "Development" (sviluppo), "Operations" (operazioni) e Security (sicurezza), ovvero muoversi verso l'**interdipendenza tra sviluppo software, IT operations e sicurezza**, puntando ad aiutare un'organizzazione a sviluppare in modo più rapido, efficiente e sicuro prodotti e servizi software. **La sicurezza è un aspetto critico**, infatti ci sono timori diffusi rispetto alla capacità o meno di rendere sicura un'applicazione cloud native. Infine diventa cruciale **l'attenzione ai costi**. Accedere alla massima scala-

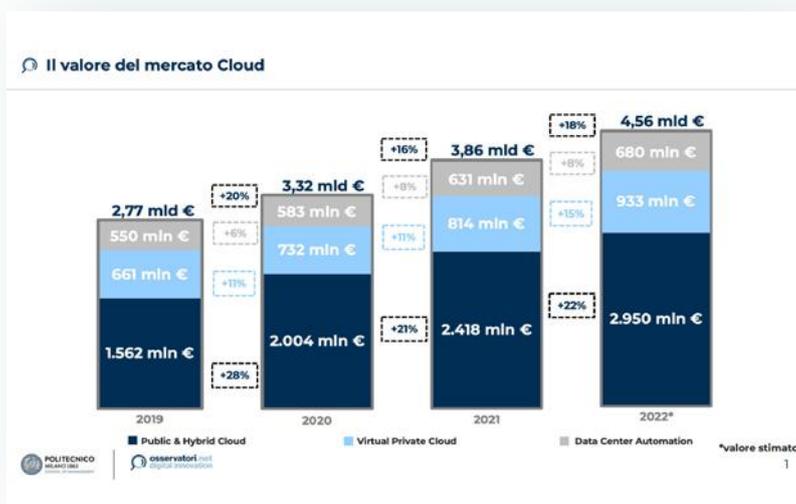
bilità e flessibilità possibile con un parco applicativo moderno (basato su tecnologie cloud native) significa anche sostenere potenzialmente costi molto alti: più gli utenti richiedono di entrare nell'applicazione e più l'applicazione deve **scalare** per poter sostenere la domanda senza impatti sulla disponibilità e le performance.

Insomma il Cloud è chiaramente percepito come una **necessità per trasformare il business**, ma richiede anche un **cambiamento di processi** e di **mindset**, richiede un percorso di adozione graduale per cui l'azienda, prima di compiere questo salto, deve valutare la propria maturità rispetto a passaggi come: **migrazione al Cloud dell'infrastruttura, containerizzazione** - sviluppo applicazioni, **ripensamento dei processi in ottica Cloud**, cambiamenti su cui non tutti si sentono ancora pronti anche solo a livello embrionale.

Ma cosa vuol dire parlare di Cloud in Italia e soprattutto cosa vuol dire parlare di applicazioni in Cloud? La risposta è fatta di molte luci e di alcune inevitabili ombre che spaventano le imprese intorno al tavolo, soprattutto in tema di costi energetici.

Lo chiarisce bene l'**Osservatorio Cloud Transformation della School of Management del Politecnico di Milano** che, attraverso i suoi ricercatori, ha dato il proprio contributo durante il dibattito.

Nonostante l'inflazione e l'incertezza del contesto economico, il mer-



cato del Cloud in Italia si conferma in consolidamento e **supera i 4,5 miliardi di euro**, con una **crescita del +18%**, tuttavia composta da un +15% di crescita organica in continuità con gli scorsi anni e da un +3% dovuto all'impatto delle aspettative di rialzo dei prezzi dei servizi Cloud.

Il 2022 ha portato grande incertezza in tutti i mercati a livello internazionale: la delicata **situazione geopolitica**, la **conseguente crisi energetica**, le difficoltà in più catene di **fornitura** e il forte aumento dell'**inflazione** minacciano il potere d'acquisto delle organizzazioni. In un simile panorama anche il mercato Cloud, basato su infrastrutture energivore, non è esente da impatti. Se il trend positivo di spesa e di consapevolezza osservato nel corso degli ultimi anni ha finora subito limitate conseguenze dal contesto attuale, è ora necessario avviarsi verso una **nuova fase di collaborazione nell'intero ecosistema** con la partecipazione dei diversi attori del mercato Cloud in ottica di **sostenibilità economica e ambientale**.

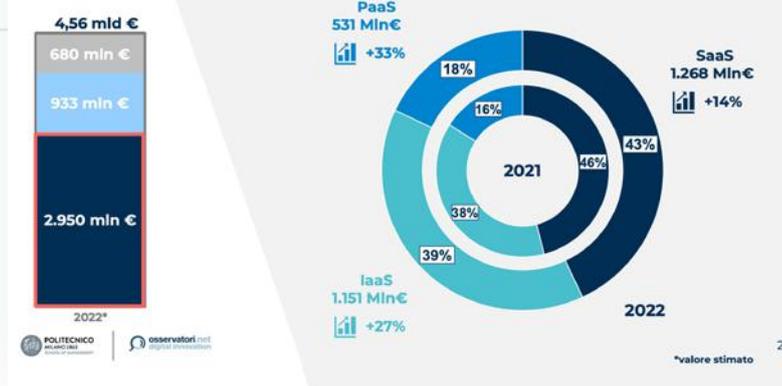


La spesa in Cloud In Italia

Il **Public & Hybrid Cloud**, ovvero l'insieme dei servizi forniti da provider esterni e l'interconnessione tra Cloud pubblici e privati, evidenzia la dinamica di crescita più significativa, per una spesa di **2,95 miliardi di euro, in crescita del +22% sul 2021**.

In particolare, all'interno del **Public & Hybrid Cloud**, i **servizi PaaS** (Platform as a Service) registrano la dinamica principale raggiungendo il valore di **531 milioni di euro (+33% sul 2021)** e si confermano la base per lo sviluppo e la modernizzazione delle applicazioni. In termini di crescita c'è poi lo **IaaS**, che registra un **+27% per un totale di 1,15 miliardi di euro**, con un'interessante dinamica degli strumenti per la gestione dei container e, infine, il **SaaS**, in crescita del **+14%, per un totale di 1,27 miliardi di euro**.

Il mercato Public & Hybrid Cloud



Tra le altre componenti della spesa complessiva Cloud, il **Virtual & Hosted Private Cloud**, cioè i servizi infrastrutturali residenti presso fornitori esterni, raggiunge i **933 milioni di euro (+15%)** mentre la **Data Center Automation**, ossia la modernizzazione delle infrastrutture on-premise, cresce del **+8% per un totale di 680 Milioni di Euro**.



L'adozione del Cloud tra grandi imprese e PMI e la spinta verso la modernizzazione delle applicazioni

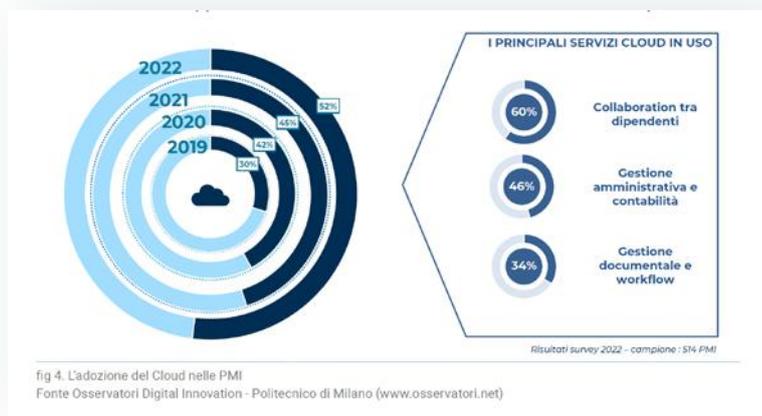
Nelle **grandi imprese** l'adozione del Cloud è ormai una certezza e rappresenta la **modalità di erogazione del 44% del parco applicativo**, in sostanziale bilanciamento con gli ambienti on-premise. Ma veniamo al tema chiave, la **modernizzazione del parco applicativo in ottica Cloud**: superata la prima importante fase di adozione del Cloud, basata prevalentemente sugli approcci più semplici, veloci e meno rischiosi, si è oggi accumulata una consapevolezza e una base di esperienza utile per affrontare le sfide più complesse che inevitabilmente richiedono anche interventi di modernizzazione delle applicazioni core.



La ricerca 2022 dell'Osservatorio Cloud Transformation ha rilevato un rafforzamento della tendenza in atto nel concentrare le attività progettuali in importanti percorsi di durata pluriennale capaci di abilitare una più profonda trasformazione digitale.

Anche il comparto delle PMI, dopo anni di scetticismo, ha recentemente realizzato un passo avanti.

Nel 2022, infatti, il **52% delle PMI adotta almeno un servizio Cloud** (+7 punti percentuali rispetto al 2021) e complessivamente **la spesa Cloud delle PMI crescerà quest'anno del +24%**, attestandosi a un valore di 351 milioni di euro.



Solo una questione di “maturità”

Fatto un quadro di massima del mercato e delle tendenze in atto, è bene focalizzarsi, in particolare, sui due aspetti delicati al centro di questa evoluzione.

Il primo riguarda i dubbi legati all'opportunità di **portare l'intero parco applicativo in direzione Cloud**. Diversi imprenditori e CIO, al di là di servizi che ormai nascono in Cloud in forma SaaS come il CRM, la Posta Elettronica, ecc., soprattutto per alcune categorie di applicativi “storici” e legati alle attività core dell'azienda, fanno fatica a trovare maggior vantaggio nell'aver più controllo e visibilità rispetto alle versioni on-premise.

Il secondo è legato alla **complessità crescente** nel gestire e orchestrare un parco applicativo che inevitabilmente si complica tra software legacy, software nativamente in Cloud e software che, insieme ai processi di cui si occupano, devono cambiare i loro DNA per muoversi rapidamente verso uno sviluppo agile e nativamente Cloud.

Tuttavia, riconducendo il dibattito all'interno di un quadro di mercato più ampio, il percorso di migrazione degli applicativi in Cloud è una **“salita in discesa”**. Se il livello di maturità delle aziende che intendono appoggiare il percorso di modernizzazione ha un ruolo decisivo, come del resto la conseguente capacità di superare la complessità tecnologica/organizzativa e il gap di competenze che ne derivano, **sul medio-lungo periodo le organizzazioni “più coraggiose” riescono ad ottenere vantaggi strutturali che in fin dei conti superano di gran lunga l'effort iniziale**.



La crisi delle competenze e la “bolla” in arrivo

Complessità che ci porta a virare verso quello che viene ritenuto come il più grande e grave problema a monte di una evoluzione così importante, articolata e inevitabile. Le **competenze** ma, soprattutto, **la capacità di trovare, attirare e “trattenere” i migliori talenti** a livello di sviluppo software. Una carenza cronica che sta generando una pericolosa bolla speculativa che, nei prossimi anni, porterà ad avere sul mercato del lavoro una quantità enorme di professionisti dello sviluppo software inquadriati con stipendi completamente fuori standard.

In sostanza, a oggi, la penuria di sviluppatori con competenze cloud native e di professionisti capaci di approcciare il ciclo di vita delle applicazioni tramite metodologia De-



vSecOps sta portando le risorse disponibili sul mercato a chiedere, in piena logica di domanda/offerta, trattamenti economici sempre più problematici da garantire. Se i ricercatori del Politecnico invitano a sviluppare **politiche di retention meno legate al fattore economico** e più alla centralità di queste figure e al loro coinvolgimento/motivazione in ottica progettuale, dall'altra CIO e imprenditori lamentano una situazione di sostanziale scacco di fronte alla quale fanno fatica a divincolarsi. Carenza di talenti, costi enormi per reclutare figure anche “mediocri” e una competizione feroce stanno mettendo davvero in difficoltà le organizzazioni





Una delle vie di uscita può e deve essere legata ad una maggiore collaborazione con università ed enti di ricerca ma, soprattutto, scuole di specializzazione e istituti tecnici. Una collaborazione che, però, proprio per la necessità di un confronto sempre più serrato e aperto con le generazioni “native digitali” deve, ancora una volta, portare le imprese a **rivedere profondamente le proprie politiche di lavoro**, organizzazione e gestione di tempi e impegni in un’ottica smart, aperta e flessibile.

Un cerchio che si chiude insomma: la necessità, per coloro i quali non hanno già affrontato un percorso di modernizzazione end-to-end, sia a livello di HR sia di strategia digitale, di evolvere e trasformare processi e modalità di lavoro prima ancora di muoversi verso scelte tecnologiche decisive ma solo secondarie rispetto a simili trasformazioni.



2

**DIGITAL TRANSFORMATION
E BUSINESS PROCESS
REENGINEERING:
DAL CAMBIAMENTO DI
MINDSET E DI APPROCCIO AL
RUOLO CHIAVE DELLA FIDUCIA
VERSO UNA NUOVA VISION**



La modernizzazione delle applicazioni va inserita in una strategia di ampio respiro, che guarda all'ottimizzazione di tutti i modelli operativi aziendali e dei processi di business, compresi quelli legati al **business process reengineering**, vero e proprio pilastro delle strategie e dei percorsi di trasformazione digitale delle imprese.

Perché quando si parla di processi di business, la loro trasformazione in ottica "digital" è molto di più di una trasformazione, è una vera e propria rivoluzione copernicana che implica, all'interno delle organizzazioni, un cambio di prospettiva e di mindset che deve necessariamente guardare (anche) alla valorizzazione e al rafforzamento della Fiducia tra tutte le parti coinvolgendo tecnologia, persone e cultura... senza perdere di vista sicurezza, compliance e privacy.

Il contesto di “Fiducia”

In un mondo sempre più digitalizzato ed interconnesso, la Fiducia è divenuta elemento di differenziazione significativo. Il paradosso è che la digitalizzazione può essere vista sia come la causa sia come la soluzione al bisogno di Fiducia che coinvolge i nostri sistemi sociali ed economici.

Perché il tema sta acquisendo sempre più importanza? I motivi di fondo sono raggruppabili in tre principali dimensioni:



Organizzazione interna

Senza Fiducia non sarebbero possibili i nuovi modelli gestionali emergenti (agile, empowerment, decentralizzazione delle decisioni, organizzazione liquida, ecc.) che sono sempre più importanti negli attuali contesti di business in continuo e forte cambiamento. Inoltre, l'avvento del lavoro da remoto ha reso per definizione necessari nuovi modelli di relazione e di controllo basati sulla Fiducia.



Relazioni tra l'azienda e l'esterno

La Fiducia è una capacità sempre più critica nel rapporto con gli stakeholder esterni (clienti, comunità locali, regolatori, finanziatori, ecc.); le relazioni con questi soggetti sono sempre più strette e interdipendenti tra loro; si pensi ai temi di sostenibilità e agli indicatori ESG e al loro impatto su tutte le imprese.



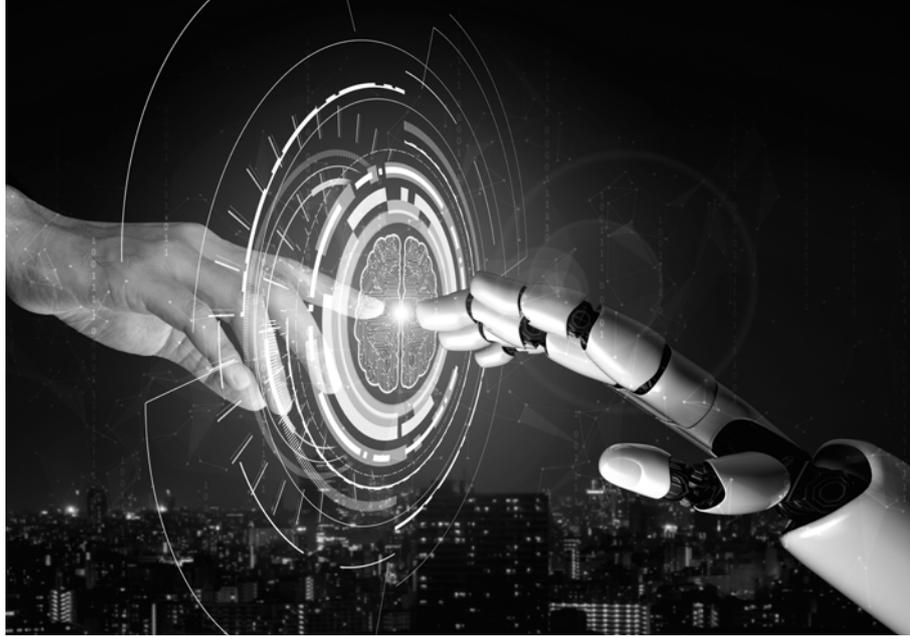
Abilità comportamentale

Le aziende si sono storicamente focalizzate su competenze e abilità tecniche e gestionali, queste ultime ispirate a logiche top-down e di “command and control”. I nuovi leader delle aziende moderne hanno invece la necessità di sviluppare uno stile di gestione basato sulla Fiducia che deve però trovare il corretto supporto da parte delle soluzioni e dei servizi digitali.

Guardando lo scenario dalla prospettiva IT e dei cosiddetti Digital Trust Services - servizi e soluzioni informatiche che consentono, tra gli altri, servizi di autenticazione, certificazione identità, firma elettronica, ecc. - esistono due macrocategorie di rischio digitale che hanno un impatto sul livello di Fiducia.

La prima è quella del **rischio IT in senso stretto**, che fa riferimento alla sicurezza dei processi di back-end dei sistemi informativi e alla loro integrazione tramite processi condivisi tra diverse funzioni aziendali. La seconda categoria di rischio è quella riguardante la **reputazione delle attività digitali**, in primis, i processi front-end, e la reputazione dell'organizzazione nel suo complesso.

E come si affrontano e mitigano questi rischi in percorsi di modernizzazione applicativa?



Una prima risposta va cercata nella definizione di Digital Transformation, non così facile da identificare. Quel che è certo è che Digital Transformation **non significa passare dalla carta ai file**. Prima ancora di un cambio di passo tecnologico si tratta di affrontare un **cambiamento culturale e organizzativo**. Anche se, va detto, utilizzare strumenti di supporto e sistemi ausiliari standardizzati e automatizzati rappresenta un elemento di forte armonizzazione tra le aziende, i loro fornitori, i loro partner e i loro clienti.

Provando a ragionare su differenti possibili **definizioni di Digital Transformation**, ciò su cui quasi tutti gli esperti concordano è che il focus deve andare sul **valore culturale della trasformazione digitale**, che spesso implica una vera e propria **metamorfose organizzativa** ed una rivisitazione dei processi e cambi di paradigmi.

Dal punto di vista tecnologico e di servizio verso gli utenti (siano essi utenti interni, collaboratori, partner, clienti, fornitori...), significa **guardare al processo nel suo insieme**, puntando a “mascherare la complessità tecnologica” offrendo una **esperienza utente accattivante, unica, interessante** ma al contempo **affidabile e sicura**. In quest’ottica, **la modernizzazione applicativa diventa al tempo stesso driver di accelerazione e elemento operativo** di possibili percorsi di trasformazione digitale.



“

Le possibili definizioni di Digital Transformation

La trasformazione digitale è una vera e propria metamorfosi culturale, organizzativa ed economica. È un cambiamento dirompente che agisce sulle logiche convenzionali e consolidate imponendo nuovi paradigmi.

La trasformazione digitale comporta l'integrazione delle tecnologie e soluzioni digitali in ogni area di business, contribuendo a rendere più efficiente la forza lavoro, ottimizzare i processi e rendere più efficaci i modelli di business.

La trasformazione digitale è il processo di utilizzo delle tecnologie digitali per creare nuovi processi aziendali, o modificare quelli esistenti, per soddisfare i requisiti aziendali e di mercato.

La digital transformation è un insieme di cambiamenti tecnologici, culturali, organizzativi, sociali, manageriali, associati con le applicazioni di tecnologia digitale, in tutti gli aspetti della società umana.

La trasformazione digitale è il processo che sostituisce completamente le modalità manuali, tradizionali e legacy di fare business con le alternative digitali più recenti.

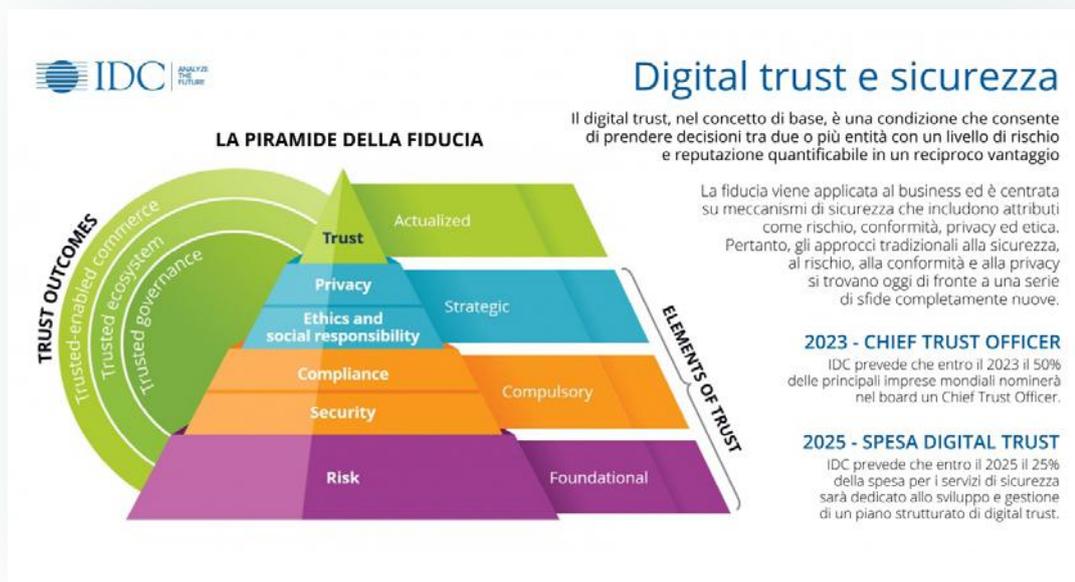
”

Rispetto a tre anni fa la società è cambiata. Adesso prendiamo atto che viviamo in una società di informazione ed esperienza e iniziamo, come singoli utenti, ad avere maggiore consapevolezza sugli aspetti di protezione e trattamento dei dati. Non solo, facciamo molta attenzione al posizionamento dei brand, ai loro valori e questo **nuovo “patto di Fiducia”** (molto delicato e spesso instabile) richiede alla base tecnologie abilitanti che non tradiscano tale premessa. In altre parole, servizi cosiddetti “trust” (QTS - Qualified Trust Services) sui quali modellare un nuovo rapporto di Fiducia tra l'azienda ed i suoi interlocutori, dal mercato più ampio al singolo utente/cliente.

In alcuni contesti aziendali inizia ad emergere chiaramente la necessità di avere una vista chiara e completa di tutti i processi, una sorta di **“mappatura” dell'as-is** sia per poter **innescare percorsi di modernizzazione applicativa** sia per poter **avviare una trasformazione digitale in modo strutturato** e non “a compartimenti stagni”. Ed è proprio in quella fase di mappatura che sarebbe meglio **interfacciarsi con un QTSP - Qualified Trust Services Provider**. È infatti nelle fasi di assessment che un QTSP può dare un significativo contributo, in ottica di “metamorfosi digitale”, mettendo a disposizione delle aziende la propria **esperienza** per individuare i **flussi operativi**, i processi, le procedure e gli strumenti maggiormente utili per modellare i processi aziendali sfruttando a pieno i Trust Services, **inserendoli “nativamente”** nella ridefinizione dei processi stessi.

Dalla reingegnerizzazione dei processi alla Trust Chain

La Fiducia non si può basare solo su singoli prodotti/servizi ma presuppone una visione ed una logica più ampie che pone la stessa al centro di un framework lungo il quale si snodano “tasselli” quali le **relazioni collaborative** tra più attori (interni o esterni all’azienda, in un nuovo concetto di Trust Chain), **l’interoperabilità** e **l’utilizzo sicuro di piattaforme tecnologiche, l’allineamento dei processi interni...**



Fonte grafico:
IDC Perspective:
Future of Trust:
Defining Trust
#US46185920 –
Aprile 2020

La crescente rilevanza del tema ha spinto alcuni ricercatori a prevedere l’emergere di figure quali il **Chief Trust Officer**, con una presenza anche a livello di Board aziendali. A questo si aggiungono le stime di crescita degli investimenti: entro il 2025, una ricerca IDC sostiene che il 25% della spesa per i servizi di sicurezza sarà dedicato allo sviluppo e gestione di piani strutturati di Digital Trust. In quella dicitura, “piani strutturati di Digital Trust”, si annida una questione importante legata ai processi ed alla loro digitalizzazione, con una visione del concetto stesso di Trust incentrato sulla **trasparenza**, come testimoniato da al-

cuni professionisti durante il dibattito. Sebbene la traduzione letterale di Trust sia Fiducia, è il concetto di trasparenza che ne definisce il valore di business ribaltando persino le relazioni tra provider ed aziende clienti, molto spesso caratterizzate da logiche di lock-in.

Questo “nuovo” rapporto con il QTSP, incentrato appunto sulla trasparenza, potrebbe rappresentare il grande **elemento di “rottura” con il passato, svincolando i processi dal prodotto**, cioè dalla tecnologia, e spostando finalmente l’attenzione sulle soluzioni attuabili - in una logica Trust Chain - con più flessibilità, apertura e, appunto, trasparenza.

Venti di cambiamento



I Digital Trust Services sono un abilitatore chiave del processo di digitalizzazione, offrendo strumenti per l'agire digitale, servizi e soluzioni per operare in scenari sempre più virtualizzati, garantendo requisiti base come la **sicurezza e la compliance alle normative, l'integrità del dato o del documento**, la necessità di **riconoscere l'identità delle persone**, l'esigenza dell'**opponibilità a terzi**, di assicurare il **valore legale di un documento**.

Tuttavia, molto spesso vengono visti come “servizi da scaffale” da acquistare al bisogno, senza tenere invece conto del loro “peso” sul processo. Molto spesso i servizi Trust, dalle soluzioni di firma elettronica a quelle di gestione documentale e workflow, passando per la conservazione digitale, la fatturazione elettronica, l'identità digitale, la PEC, ecc., vengono richiesti dai dipartimenti Legal o da quelli Finance e Amministrazione, e quasi sempre come risposta ad una compliance normativa. Oggi, questi servizi non sono ancora entrati nel core di un IT, o meglio di un IT-Business, promotore di una cosiddetta Trust Chain estesa.



TRUST



In diversi progetti di dematerializzazione/digitalizzazione, a titolo di esempio, molto spesso ciò che emerge prioritario da parte di più aziende è **l'importanza critica dei processi di identificazione degli utenti** (pensiamo per esempio la rigidità con la quale è necessario identificare gli utenti nei processi di stesura di rapporti di sicurezza e controllo, oppure nei processi complessi che integrano differenti livelli di autorizzazione e controllo).

Durante la fase di reingegnerizzazione di questi processi, in chiave digitale, un QTSP potrebbe impattare positivamente identificando e suggerendo modalità di riconoscimento degli utenti in modo più smart, più agevole sia per gli utenti sia per il processo, oppure valutando alternative più “stringenti”, ove necessario sfruttando anche dispositivi fisici o fornendo agli utenti strumenti di identificazione quali i kit di firma o lo SPID.

Segue →

Ma il vento sta cambiando... Se **fino a un paio d'anni fa il tema della Fiducia**, da un punto di vista tecnologico, era relegato alle **transazioni elettroniche** (dai pagamenti alla gestione delle identità, degli accessi, dei profili utente, ecc.), con un focus prevalente sull'interoperabilità dei servizi di identificazione e autenticazione, firme, sigilli, marche temporali, documenti elettronici - e più in generale di tutti i servizi digitali in cui è essenziale la Fiducia nella controparte - negli ultimi anni il **ruolo**

stesso dei Qualified Trust Service Provider, ossia il fornitore di servizi fiduciari ai quali è stato riconosciuto uno status di ente qualificato da un organo di governo e vigilanza e che ha ricevuto l'autorizzazione per l'erogazione dei propri servizi Trust, sta evolvendo verso un ruolo più esteso, di **partner della trasformazione digitale aziendale**, soprattutto in ottica di **reingegnerizzazione dei processi** e in percorsi strategici di modernizzazione applicativa.

Le aziende, ad oggi, non hanno ancora "sfruttato" il Qualified Trust Service Provider in quest'ottica; tuttavia, iniziano a riconoscere il valore ed il possibile impatto avviando un percorso di valutazione del loro **supporto in una fase iniziale di ridisegno dei processi**, inserendo il Digital Trust nativamente nei nuovi processi. La strada è lunga, ma il percorso è tracciato.





3

LA SOSTENIBILITÀ (ANCHE) ECONOMICA DEL CLOUD: DAL PARADIGMA FINOPS AL GREEN IT

Non si può parlare di Digital Transformation, in generale, e di modernizzazione applicativa, più nello specifico, senza tenere conto dell'accelerazione garantita dal paradigma del **Cloud** e del suo potenziale in ottica **Green IT e sostenibilità**.

Tutte le aziende stanno correndo la propria maratona verso il Cloud, una corsa inevitabile in cui le sfide non mancano soprattutto se si alza lo sguardo verso l'attuale scenario macro-economico, geo-politico ed energetico-ambientale. Stiamo vivendo una fase di passaggio in cui molti postulati validi fino a ieri si stanno ridefinendo e parole-chiave come **cambiamento, flessibilità e resilienza** stanno diventando dei veri e propri mantra.



Negli ultimi anni, complice la pandemia, si sta assistendo alla maturazione dei percorsi di adozione del Cloud da parte delle organizzazioni (complici anche i percorsi e i processi di modernizzazione applicativa), alla crescente consapevolezza organizzativa sulla sua rilevanza strategica e all'aumento della complessità dei sistemi informativi a cui sta conseguendo la necessità di strutturare un nuovo modello di governance e di gestione operativa.



In questo contesto, una delle sfide maggiormente sentite è relativa alla **gestione finanziaria** e all'**ottimizzazione dei costi** generati dalla nuvola, su cui le aziende stanno ancora muovendo i primi passi. La previsione dell'aumento delle tariffe dei servizi Cloud fa della **sostenibilità**

economica una necessità ancor più sentita i cui impatti potranno essere mitigati attraverso la ricerca di nuovi spazi di efficientamento, accrescendo le **capacità di previsione e ottimizzazione** della spesa per poter garantire la sostenibilità economica del proprio ambiente IT.

In che modo, dunque, le grandi organizzazioni che utilizzano la nuvola stanno rispondendo a questa nuova sfida gestionale e strategica? Quali cambiamenti comporta l'introduzione del Cloud nei modelli di gestione dei costi? Quali sono i principali modelli di gestione dei costi adottati dalle imprese? Infine, non può esserci transizione blu senza transizione verde, anche per le organizzazioni, il che stimola molte domande e preoccupazioni: quanto è green il Cloud?

FinOps: “chi era costui?”

Quello del FinOps è uno scenario complesso, sempre più al centro dell'interesse di aziende di varie dimensioni, anche in Italia. La possibilità di ottimizzazione dei costi del Cloud procede, di pari passo, con l'evoluzione della tecnologia in uso.



Survey end-user Campione: 120 grandi organizzazioni

Avere capacità di **FinOps** e del cosiddetto **Cloud Financial Management** significa trarre il massimo valore dalle piattaforme che l'azienda ha deciso di adottare. Secondo i dati dell'**Osservatorio Cloud Transformation del Politecnico di Milano**, il contributo del Cloud alla sostenibilità economica della trasformazione digitale delle imprese e della pubblica amministrazione dipende molto dalla capacità dell'ecosistema di fare un **salto culturale** e di **competenze**, così da consentire alle organizzazioni di gestire in modo efficace e trasparente i costi della nuvola.

Necessaria in questa logica anche l'evoluzione delle **piattaforme di cost management** che l'Osservatorio ha classificato, attraverso un confronto fra offerta ed esigenze

della domanda. Dall'analisi, emerge che il 58% delle grandi imprese attribuisce i costi del Cloud in modo centralizzato all'IT, così da perdere quella necessaria caratteristica di flessibilità e dinamismo, anche nella governance, importante per distribuire meglio le forze, dove necessario, quando necessario.

Meno della metà (48%) delle grandi imprese ha avviato almeno un'azione organizzativa connessa all'adozione del Cloud, orientandosi, in primo luogo, verso **tool applicativi per il monitoraggio** e il **controllo dei costi**. Risultano molto limitate, stando alle rilevazioni dell'Osservatorio, le azioni per aumentare la cultura e le competenze, in termini di FinOps, attraverso la formazione o l'inserimento di nuove figure professionali.

Non sottovalutare il “peso” delle competenze

Quando si parla di “competenze”, non tanto dal punto di vista del sapere **“come”** approcciare il **paradigma del FinOps**, spesso conosciuto con altri termini, ma soprattutto del **“chi” delegare a occuparsene**, le aziende, in generale, attuano in modo differente e a più livelli flussi di gestione dei costi della nuvola o direttamente ricorrendo alle figure dei CIO o mediante il reparto IT.

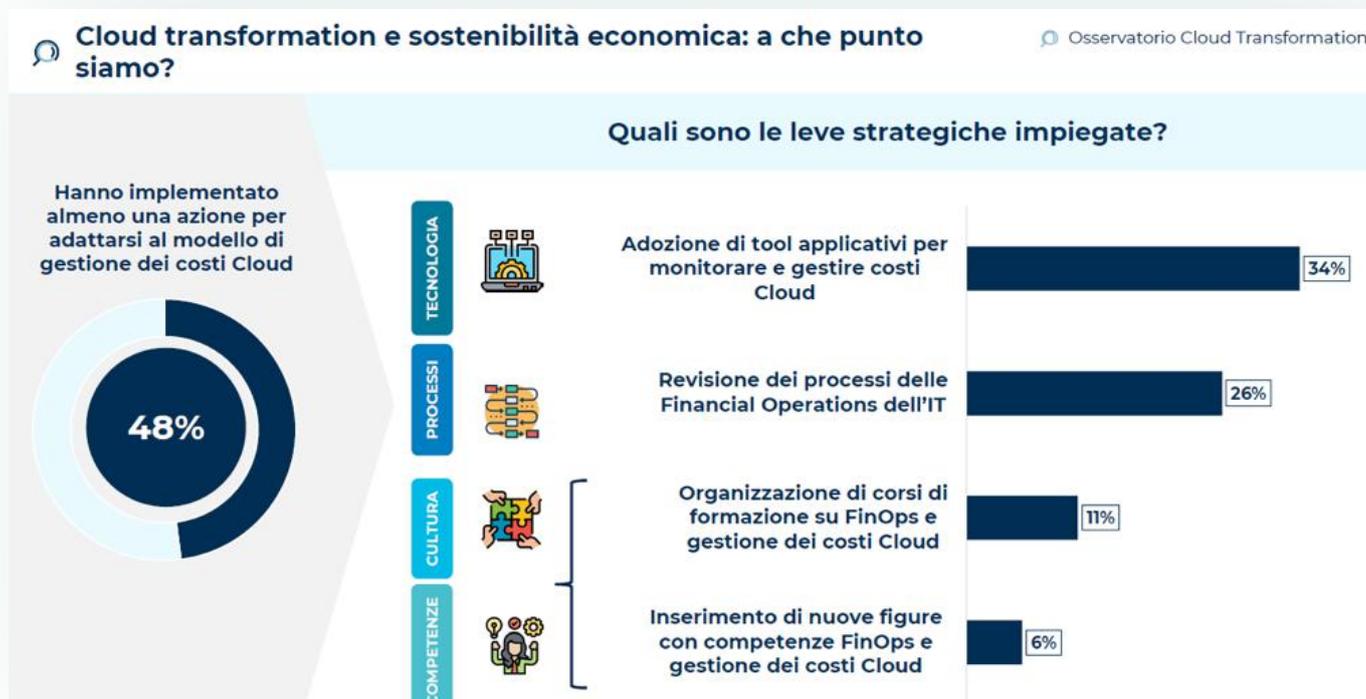
Survey end-user Campione: 120 grandi organizzazioni

Uno scenario che, evidentemente, soffre di un **overload di lavoro su compiti specifici** tale da **non poter**

trarre il massimo da una strategia FinOps dedicata, oggi sempre più possibile attraverso l'**utilizzo di tool automatizzati**.

Va detto che in alcune realtà aziendali italiane esiste una **forma embrionale di organizzazione trasversale** alle funzioni aziendali per governare le spese legate al Cloud, secondo una logica di partecipazione collaborativa, basata sul concetto di riconducibilità dei sistemi che sono in Cloud a centri di costo chiari.

Questa organizzazione vede **l'IT come promotore delle dinamiche FinOps** e rappresenta un primo passo nel fisiologico percorso di maturità necessario quando si attuano nuovi modelli organizzativi.



Segue →



In contesti simili, le aziende possono:



far leva su risorse interne, oppure **cercare di velocizzare il percorso di maturità con cui vengono adottate queste pratiche**, delegando all'esterno alcuni task di ordine tecnico per le attività legate ad analisi e reportistica, in modo da concentrarsi sulla governance di quelli che sono gli ambienti in Cloud;



delegare la gestione tecnica di una parte dei sistemi, in modo da rifocalizzare delle figure tecniche sull'analisi dei costi per capire quali sono gli spazi di ottimizzazione al fine di migliorare la spesa, in modo da potersi dedicare alla governance.

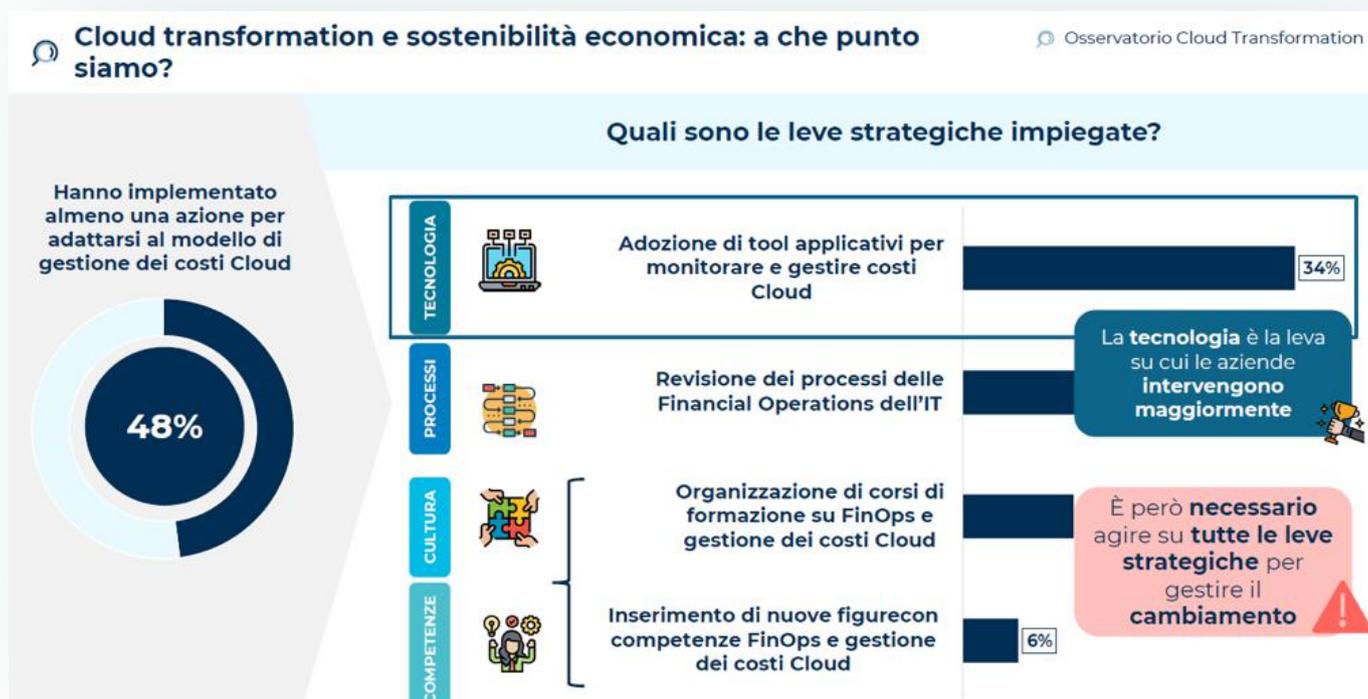
Il Cloud apre le porte alla collaborazione: team interdisciplinare per la governance della nuvola

Un altro aspetto legato al FinOps – anche guardando alle strategie ed ai percorsi di modernizzazione applicativa delle aziende – spesso è **la poca chiarezza nei contratti Cloud** che rende difficile capire **cosa si sta pagando**, con **quali limiti e opportunità** di adattamento della tecnologia.

Una maggiore trasparenza sarebbe l'elemento più atteso per un ecosistema che, proprio partendo dal Cloud, potrebbe non solo incenti-

vare l'uso della tecnologia ma anche accelerare scelte di modernizzazione applicativa aprendo ad innovazioni ulteriori, permeate di **intelligenza artificiale, machine learning e modelli di apprendimento contestuali**. Spesso, la scarsa conoscenza tecnica dei contratti porta le aziende a restare dove sono, adoperando quello che hanno in casa e spesso "subendo" passivamente le scelte dell'IT quanto ad aggiornamento di piattaforme e servizi. Urge dunque avere un **ruolo cross tra le diviso-**

Survey end-user Campione: 120 grandi organizzazioni



Segue →

ni, non necessariamente da formare solo sui temi del FinOps, ma che sappia destreggiarsi tra gli aspetti più tecnici del Cloud, dall'adozione vera e propria alla sua **governance**, riportando periodicamente i costi e i benefici degli investimenti eseguiti. Le organizzazioni più lungimiranti in tal senso hanno allestito al loro interno dei veri e propri **centri di competenza** per analizzare le spese connesse al Cloud. Chi non lo ha ancora fatto ci sta pensando, conscio della necessità di dedicare tempo e risorse a quello che, ancora oggi, viene considerato un "costo nel costo", ossia dedicare persone ad un aspetto che, seppur centrale nella più ampia logica del business, non viene sempre inteso come a valore.

Il tema è "per ogni euro speso per il Cloud quanti euro riesco a fatturare nel mio business?"

Tutto questo ci porta a costruire un modello dei costi di dettaglio che influenza il posizionamento di mercato e conduce a migliorare l'efficienza. D'altro canto, si afferma anche il concetto che è importante selezionare piattaforme in modo da disporre dei seguenti vantaggi:



Costi certi e flat rate

consuntivazione che non risulta variabile nel corso del tempo perché il modello di pricing dipende dall'utilizzo.

Pensiamo alle casistiche in cui la banda viene consuntivata in ragione dell'utilizzo, oppure lo storage in ragione delle operazioni fatte verso lo stesso.



Logiche per evitare i lock-in

Deve esservi apertura in un futuro che ormai è ibrido e multcloud, con una distribuzione dei workload in funzione delle necessità applicative. La selezione della piattaforma Cloud deve dunque tenere in considerazione anche gli strumenti che sono disponibili per interoperare tra i "diversi" Cloud e non subire lock-in tecnologici e di processo.





Dalla sostenibilità economica a quella ambientale: il GreenOps

In questi contesti di cambiamento emerge chiaramente la **centralità della “governance” del dato**. Sposare una strategia Cloud e di FinOps, ad un certo punto, sottende il dover concedere un pezzo dei propri dati a terzi. Un rischio, per qualcuno, un beneficio per altri, che delegando questo aspetto della produzione a un partner di fiducia, si libera da un’attività che può benissimo essere svolta all’esterno, anche in termini di compliance e rispetto delle eventuali informazioni sensibili gestite. Peraltro, **l’ottimizzazione del Cloud**, unito alla logica del FinOps, consente di raggiungere quel grado di **sostenibilità ambientale**, legato alla nuvola, che sempre più spesso entra nei report e bilanci annuali. Anzi, non di rado accade che vengano svolti degli audit, anche dall’esterno, nei quali prospect e potenziali partner, chiedano di valutare **l’impatto ambientale dato dalle tecnologie in uso**. Se ottimizzare il carico di lavoro del Cloud ha il fine di portare un **risparmio economico**, va di per sé, che uno scopo possibile è anche quello del **risparmio in termini energetici**. Da qui, il termine “GreenOps”.

Dobbiamo considerare che gli investitori, gli azionisti, le realtà di governo, da un lato spingono le aziende a produrre adeguata reportistica per tutti gli aspetti legati alla sostenibilità, il cosiddetto **impatto ESG (Environmental, Social and Governance)**, dall’altro i governi stringono le maglie, chiedono che siano prodotti dei report riguardo gli impatti ambientali. Questo supera i proclami di greenwashing e pone di più l’accento su delle **azioni concrete e documentabili**.



Il modello organizzativo che viene implementato per il FinOps diviene quindi molto utile anche per il Green IT. Immaginando di dover decidere dove posizionare il sito di DR solo da un punto di vista sistemistico, probabilmente la scelta sarà guidata da latenza, RPO, RTO. Nel merito del FinOps, invece, entrano in gioco anche i costi.



Con uno sguardo ancora più ampio, si potranno poi considerare gli impatti in termini di sostenibilità ambientale delle scelte, ottenendo **un trade off che sia tecnico-economico e, allo stesso tempo, sostenibile.**

In sintesi, **il tema del FinOps è ormai centrale nell'operatività quotidiana** delle aziende.

Lo è, chiaramente, in proporzione alla tipologia di business, alla grandezza dell'organizzazione e del mercato in cui si è inseriti. Ma chi ha deciso di "salire sul treno del cloud" anni fa, quando si parlava solo di "spostare dati su un data center", si ritrova oggi ad avere un grado di maturità più elevato anche in termini di volontà nel capire **come migliorare gli investimenti**, senza lasciare indietro la tecnologia.

Di contro, chi non ha mai sentito parlare di FinOps, anche al di là del termine ma anche come modalità di approcciare in maniera sistemica il costo del Cloud, sa che questo rappresenta un terreno su cui bisognerà confrontarsi molto presto, per affrontare al meglio le sfide del domani.



4

**STAY CLOUD STAY SECURE:
L'ADOZIONE DEL CLOUD
COME ELEMENTO CHIAVE
DELLA SECURITY STRATEGY**



Se il Cloud rappresenta un enorme volano per la modernizzazione applicativa ed i percorsi di Digital Transformation delle aziende, come approfondito nel precedente capitolo, la sua “messa in sicurezza” non può rappresentare in alcun modo l’anello debole delle strategie aziendali. Se ciò valeva in passato, ancor di più la **cybersecurity** assume un ruolo cruciale e di rilevanza critica nell’attuale contesto storico nel quale l’approccio al rischio non può non tenere conto delle tensioni geopolitiche, così come dell’onda lunga della trasformazione digitale che, a livello globale, ha investito le aziende di ogni dimensione e settore di appartenenza.

Tale contesto impone una riflessione attorno al modo in cui le organizzazioni percepiscono e gestiscono, al proprio interno, il cyber risk, anche sulla base delle scelte IT presenti e future.

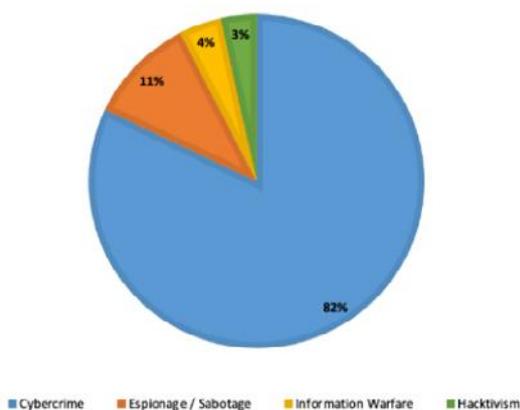
Il quadro delle minacce

Secondo i dati emersi dal Rapporto CLUSIT 2023, negli ultimi 5 anni la situazione è peggiorata nettamente, seguendo un trend pressoché costante. Confrontando i numeri del 2018 con quelli del 2022 la crescita del numero di attacchi rilevati è stata del 60% (da 1.554 a 2.489). Nello stesso periodo la media mensile di attacchi gravi a livello globale è passata da 130 a 207. Oltre alla maggiore frequenza, anche la valutazione



della Severity media (indice di gravità) di questi attacchi è drasticamente peggiorata, il che rappresenta un significativo moltiplicatore dei danni. Dal 2022 si può inoltre dire che “l’Italia è nel mirino”, ricevendo ormai il 7,6% degli attacchi globali (contro un 3,4% del 2021).

TIPOLOGIA E DISTRIBUZIONE ATTACCANTI 2022



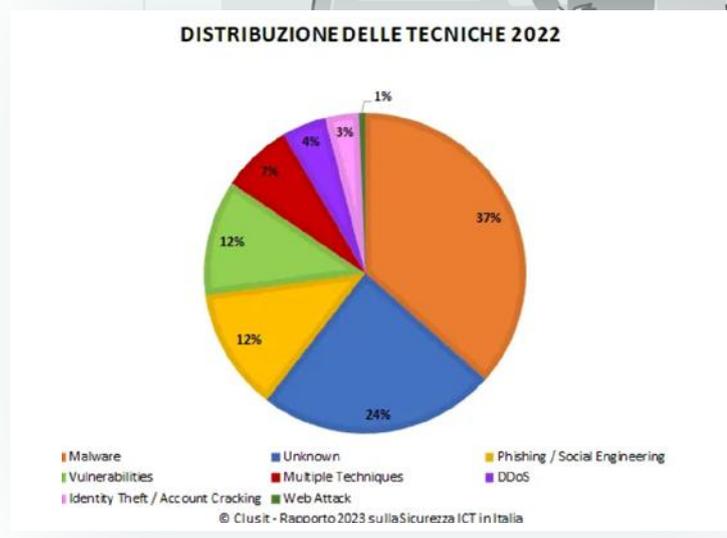
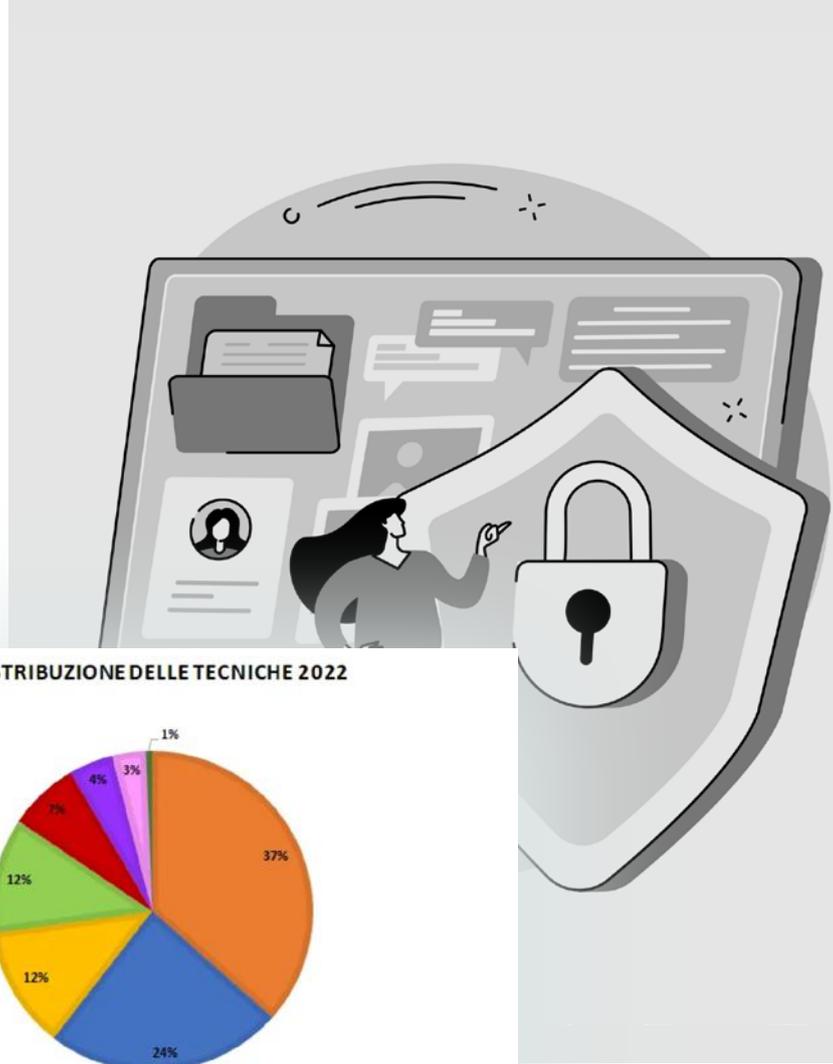
Analizzando lo storico degli attaccanti dal 2018 al 2022 - si legge nel Report CLUSIT 2023 - si nota che si mantiene la prevalenza degli attaccanti del tipo “cybercrime”, con un andamento regolarmente in crescita come numero di attacchi. L’aumento, sia pure con numeri più bassi, si registra anche per le altre tipologie

di attaccanti. I dati del 2022 mostrano con immediatezza l’enorme preponderanza degli attaccanti Cybercrime: è comunque un settore che attira grande attenzione da parte del crimine, probabilmente per i significativi risvolti economici legati alla sempre maggiore diffusione degli attacchi ransomware.

Segue →



C'è però un'altra faccia della medaglia da osservare. Il 64% degli incidenti hanno come causa azioni "maldestre", degli utenti o del personale ICT. Malware, Vulnerabilità (ad esclusione della componente di attacchi basati sui c.d. "0-day"), Phishing e Account Cracking dicono che ancora non sappiamo gestire correttamente i nostri account, non teniamo aggiornati i nostri dispositivi (o i nostri server/servizi) e clicchiamo incautamente "cose" sbagliate nelle email. Problemi che conosciamo dal millennio scorso e sui quali, forse, oggi dovremmo avere una maturità, una postura, diversa da quella che abbiamo.



A questo quadro drammatico, si aggiunga il fatto che, secondo lo studio dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano, nel 2022 l'Italia ha speso nel 2022 per prodotti e servizi di sicurezza informatica un miliardo e ottocentocinquanta milioni di euro. Si tratta dell'0,1% del PIL dato in crescita del 18% rispetto al 2021 ma si tratta pur sempre, in valore assoluto, della metà di Germania, Francia, Canada e Giappone e di un terzo di Stati Uniti e Regno Unito.

L'approccio preventivo

Fortunatamente, inizia ad emergere tra le aziende italiane una maggior **propensione all'approccio di tipo preventivo** e, talora, a investimenti di un certo spessore dal punto di vista delle tecnologie impiegate.

Nello specifico, le realtà multinazionali e le organizzazioni più strutturate sono quelle che spesso risultano più focalizzate sulla propria postura cyber, adottando, ad esempio:



Modelli di difesa in profondità prevedendo tecnologie diverse per ogni livello;



Soluzioni di monitoraggio e correlazione degli eventi di sicurezza (Security Information and Event Management - SIEM) per la rilevazione di potenziali violazioni e minacce, nei casi più sofisticati coadiuvate anche da tecniche di intelligenza artificiale per l'analisi comportamentale dei sistemi informatici;



Programmi di educazione continua del personale interno e organizzando sessioni di "allenamento" attraverso simulazioni (come accade nell'ambito della prevenzione incendio), per evidenziare eventuali debolezze tecniche e/o organizzative e mettere alla prova le proprie prestazioni di fronte ai rischi cyber.

Interessante - tra le aziende che Aruba ha riunito attorno ad un tavolo di dibattito nel 2022 - il caso di una multinazionale che, come strumento di tutela economica dalle minacce e dagli attacchi informatici, ha attivato una **polizza cyber risk**. Scelta - questa - al momento poco diffusa tra le aziende italiane e spesso dibattuta per gli aspetti relativi al premio assicurativo.

In linea con i dati illustrati nel rapporto, anche per la **Pubblica Amministrazione** il budget per la cybersecurity, in molti casi, non consente investimenti di rilievo determinando i rischi conseguenti come dimostrato dai recenti casi di cronaca. Spesso, **solo dopo attacchi cyber severi**, che hanno fermato per diverso tempo le attività, si è passati da soluzioni di sicurezza cosiddette "artigianali" a **soluzioni avanzate**, iniziando a lavorare sulla prevenzione con investimenti economicamente importanti.

La cyber security awareness

Nelle pratiche di messa in sicurezza della propria azienda, l'**elemento "umano"** è spesso quello sul quale c'è maggiormente da lavorare rispetto all'**elemento tecnologico** e, forse, quello più complesso da gestire perché difficile da monitorare.

Più in particolare, molte aziende rimarcano l'**importanza della consapevolezza**, da parte di dipendenti, collaboratori interni ed esterni nonché del top management, circa i rischi cyber e le buone pratiche di sicurezza atte a prevenirli, utilizzando in modo corretto e sicuro computer, posta elettronica, reti, server e dispositivi mobili aziendali.

Abitudini e comportamenti errati, contrari alle policy di sicurezza aziendale, oltre alla mancanza di competenze nell'utilizzo dei sistemi informativi rappresentano altrettanti rischi per la cybersecurity.



Poche le aziende che, ad oggi, hanno intrapreso la strada del **training interno continuo**, delle **campagne anti-phishing** e dei **corsi rapidi e ripetuti nel tempo**. La maggioranza, invece, risente della **mancanza di una precisa metodologia** e di un intervento sistematico, tesi a creare una "cultura" della cybersecurity tra tutti coloro che, a diversi livelli e quotidianamente, lavorano all'interno delle aziende.

La sovranità digitale

Sollecitato dai recenti eventi geopolitici, un altro tema di grandissima rilevanza riguarda il concetto di **sovranità digitale** - introdotto qualche anno fa dall'**Unione Europea** e sul quale la Commissione sta ancora lavorando per giungere a una sua completa regolamentazione - per il quale è centrale, da parte delle organizzazioni, il controllo sui dati sotto il profilo della loro localizzazione sul territorio.

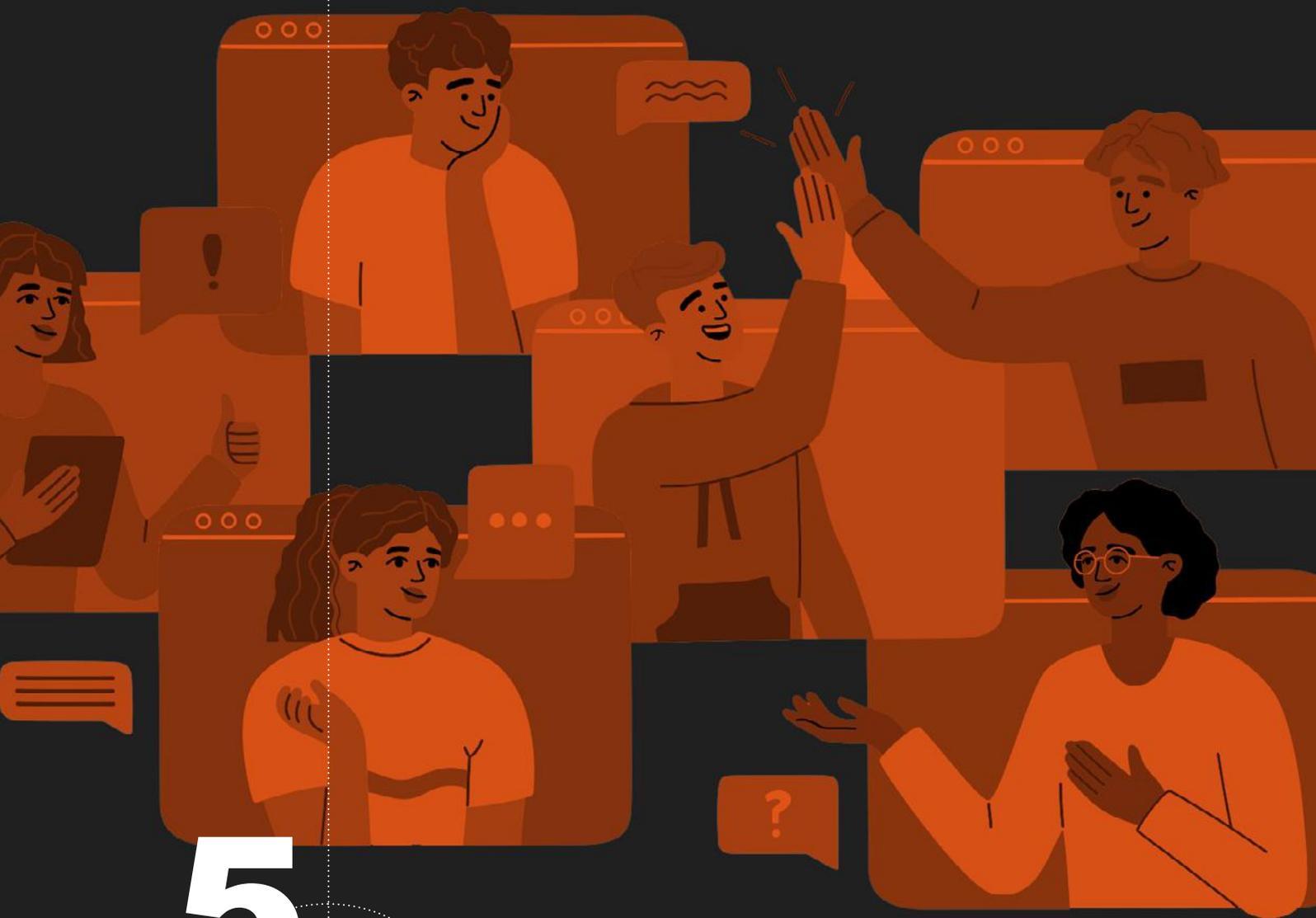
La prima riflessione da fare è che la sovranità digitale getta nuova luce sul concetto di **resilienza**, specie in un momento, come quello attuale, dominato da continue tensioni internazionali che hanno messo in crisi alcuni comparti del tessuto economico e che, in futuro, potrebbero minacciarne altri.



Un altro aspetto rilevante riguarda la **“residenza” dei dati** rispetto al loro utilizzo, alla loro protezione e al fatto di potervi accedere per continuare a generare, attraverso di essi, valore per la propria organizzazione. Il riferimento è alle sedi delle multinazionali italiane in paesi extra-UE come, ad esempio, la Cina: la sovranità digitale, in questo caso specifico, imporrebbe una localizzazione dei dati in ciascun paese ove è presente l'azienda comportando maggiori rischi legati alla mancata minimizzazione dei dati, nonché complessità per necessità di rispondere a obblighi normativi potenzialmente differenti.

Oggi, non è possibile ragionare in termini di prevenzione e cybersecurity non tenendo conto anche di questi aspetti e del ruolo cruciale che giocheranno le normative e gli interventi governativi italiani ed Europei in ottica di sovranità digitale.





5

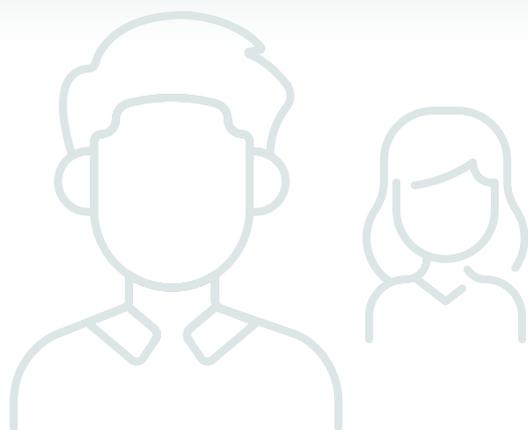
**HR DIGITAL
TRANSFORMATION:
ANCHE LA PEOPLE
STRATEGY AL CENTRO
DELLE SFIDE DEI CIO**



Come accennato nei capitoli precedenti, modernizzazione applicativa e Digital Transformation sono ormai percorsi avviati che coinvolgono diversi ambiti della vita delle aziende. Gli ultimi due anni ci hanno mostrato come il **digitale** non sia più solo uno strumento, ma un vero e proprio **asset per la crescita**. Non solo, la trasformazione in atto **ha cambiato i rapporti tra le persone** all'interno delle aziende, **ha ridefinito il modo di lavorare** e di interagire con un conseguente ritorno alla **centralità del fattore umano**.

Le sfide che si pongono davanti riguardano soprattutto come il management affronterà questo cambiamento, lo sviluppo di una nuova leadership, come creare nuove modalità di coinvolgimento dei dipendenti all'interno delle organizzazioni e, soprattutto, come acquisire e trattenere i propri talenti visto che il dato acquisito è che un lavoratore su quattro pianifica di lasciare la propria organizzazione entro i prossimi sei mesi.

E allora, come fare?



Talent Acquisition e Talent Retention: le sfide principali nell'attuale scenario in continuo mutamento

Se in questa nuova fase le persone sono sempre meno "Risorse" e sempre più "Talent" prima di individuare una strategia atta a risolvere queste principali criticità è fondamentale iniziare ad **analizzare in modo puntuale il proprio contesto di riferimento** chiedendosi perché il Talento cerca altrove nuove opportunità.

Ricorrendo a exit interview strutturate è possibile comprendere cosa porta i colleghi a guardarsi attorno e le reali criticità interne. Dopodiché con il commitment sia dei CEO che del proprio management è opportuno iniziare a lavorare per mettere a terra delle strategie di consolidamento del talento stesso.

Una prima risposta può arrivare dalla **formazione interna** affinché faccia affiorare quelle skill, sia hard che soft, che spesso e volentieri non sono valorizzate a dovere. In aggiunta, considerata la **nuova centralità dei CIO** in azienda e la sua **pervasività anche in altri ambiti**, sarebbe ottimale attivare percorsi dedicati a queste figure per sviluppare quelle competenze che vanno oltre il proprio ruolo. A tal proposito è fondamentale un'attenta mappatura dei bisogni, un continuo **re-skilling** con percorsi professionalizzanti e un processo formativo agile e digitale,

anche perché oggi le **academy** non trasferiscono conoscenza, ma insegnano alle proprie persone "come" apprendere, agevolando anche l'auto apprendimento.

Assecondare una crescita nei giusti tempi, favorendo anche l'individuazione di figure di backup che agevolino un ciclo ottimale di sviluppo, risulta essere strategico per le aziende e porta ad un win-win sia per il management che per le risorse stesse.

Da qui, per le aziende è venuta a delinearsi, in modo preponderante, la consapevolezza della necessità di un **cambio di approccio**, in prima istanza attraverso le prime linee manageriali: il **manager è fondamentale** per definire strategie, obiettivi da raggiungere e nell'individuare i "talenti" che possono contribuire a tali scopi e per far questo deve mostrare **ampiezza di vedute, capacità di inclusione e di coinvolgimento**.

In secondo luogo, non meno importante, l'organizzazione deve essere in grado di attrarre i "talenti" a partire da ciò che essa stessa rappresenta, aprendosi e raccontandosi di più.





Il ruolo della comunicazione interna

Ecco che quindi la **comunicazione** assume un ruolo fondamentale: la **storia**, i **traguardi** raggiunti, i **valori** e i **“tatuaggi”** impressi nel tempo possono, se raccontati in maniera coinvolgente, diventare forti elementi di attrazione. Infatti, un sistema valoriale condiviso internamente e ben comunicato e raccontato in modo adeguato all'esterno può portare ad una cassa di risonanza utile a ingaggiare e incuriosire le risorse esterne e interessarle al contesto di riferimento. L'obiettivo è arrivare ad una **fidelizzazione delle risorse** trasmettendo il più possibile l'importanza del far parte di una **famiglia professionale**, i cui valori possono essere sposati e abbracciati a tutto tondo.

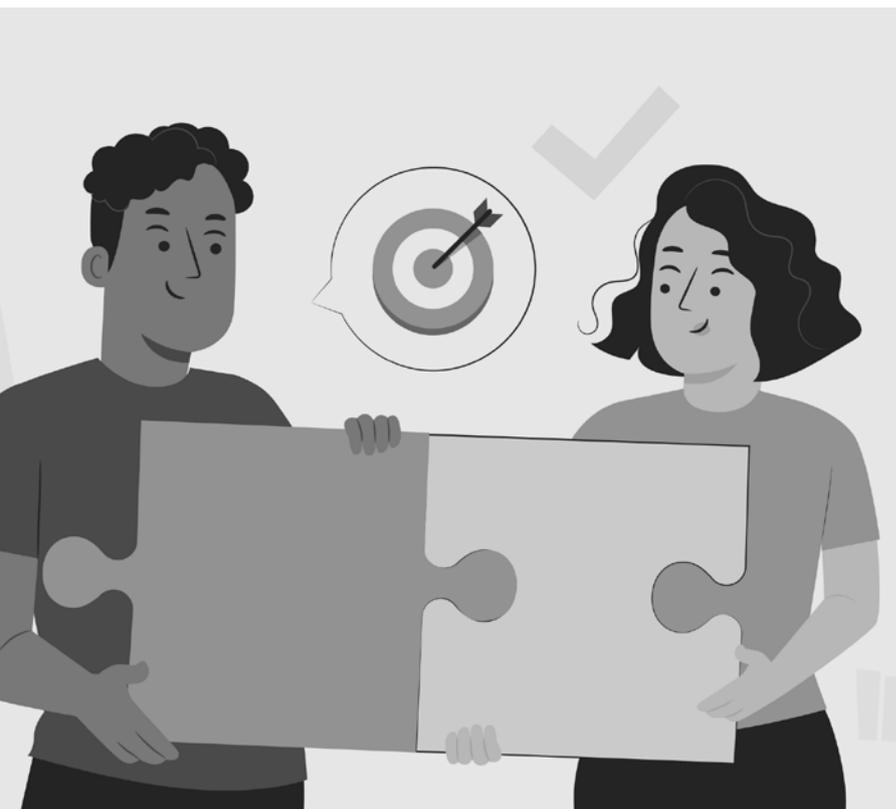
Ma la capacità comunicativa è fondamentale anche rivolta all'interno che passa sia dalla **condivisione** di strategie, obiettivi, successi e non, ma anche dalla propensione al **coinvolgimento** e all'**ascolto**, altra parola-chiave ricorrente emersa più volte durante il confronto.

Ogni azienda ha una sua storia da raccontare e da condividere solo che spesso si trova in difficoltà nel farlo. Maggiore condivisione e coinvolgimento delle persone al racconto può essere un modo per sentirsi parte dell'organizzazione per promuoverne i valori. Questo potrebbe attirare nuove risorse e nuovi talenti.

E nel racconto della storia, è opportuno far emergere anche i citati **“tatuaggi”** che non sono altro che quelle fasi che hanno segnato la storia dell'organizzazione, in modo tale che possano essere fonte di ispirazione per nuovi talenti.

Alla ricerca del nuovo leader

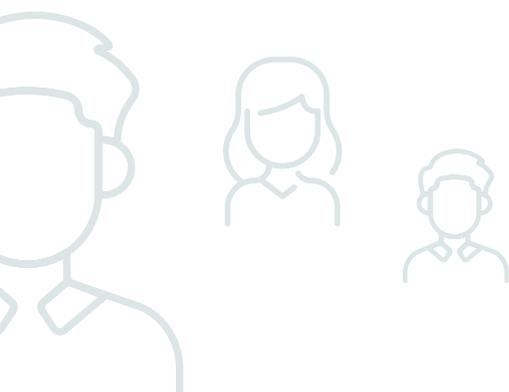
Ma, in tutto questo, chi tiene le fila di questa nuova rotta? Chi è il nuovo **leader**? Quali caratteristiche deve avere?



Il nuovo leader non è più il “condottiero”, bensì il “talento” in grado di interpretare e condividere il cambiamento muovendosi all’interno di un grande schema fatto di **collaborazione, ascolto e fiducia**. Ne è un esempio il progetto “Academy Aruba” che lavora su uno stile di **leadership ispirazionale**, che coinvolge le persone, le responsabilizza e ne favorisce l’indipendenza.

A fronte di tanti sforzi, tanti investimenti in formazione, ricerca e selezione di talenti dall’esterno, per le aziende varrebbe davvero la pena impegnarsi nel **guardarsi meglio all’interno** perché sempre più spesso il “Talento” che si sta cercando è già nell’organizzazione ma non si è in grado di riconoscerlo.

Allora, come fare? Sarebbe meglio “ascoltarsi” meglio, comunicare di più e dare fiducia.





aruba.it
ENTERPRISE

Aruba S.p.A.
Via San Clemente, 53
24036 Ponte San Pietro (BG)
enterprise.aruba.it

aruba.it
IT3 - DATA CENTER C

Aruba Enterprise è la divisione del Gruppo Aruba che da oltre dieci anni si dedica allo sviluppo e gestione di progetti IT complessi per le grandi aziende e la Pubblica Amministrazione in ambito data center, cloud e servizi fiduciari qualificati.

Un team di esperti in grado di studiare ed offrire soluzioni all'avanguardia, consulenza mirata, assistenza dedicata e servizi di gestione dell'infrastruttura tecnologica personalizzati. La visione enterprise di Aruba si basa sul dialogo con il cliente, sulla comprensione delle sue esigenze e sulla combinazione delle migliori tecnologie a supporto disponibili sul mercato.

Cloud e Data Center: supportiamo le aziende che guardano oltre i confini dell'infrastruttura data center tradizionale con soluzioni cloud altamente personalizzate. Disponiamo di un network di data center proprietari certificati secondi i più elevati standard di qualità e sicurezza del settore, dotati di infrastrutture "green by design" ad altissime prestazioni ed efficienza. Una scelta strategica per ospitare progetti come colocation, cloud o soluzioni ibride. **Trust Services:** offriamo ad aziende e P.A. soluzioni software come firma digitale, posta elettronica certificata e conservazione a norma. Aiutiamo le organizzazioni a snellire e ottimizzare i processi interni, sviluppando modelli di business efficaci ed efficienti. Favoriamo la dematerializzazione documentale per una crescita digitale sostenibile.

**LA TUA ORGANIZZAZIONE STA ANDANDO NELLA
DIREZIONE DELL'APPLICATION MODERNIZATION?**

Scopri cosa può fare per te Aruba Enterprise