AGENDA DIGITALE, *una* LEVA PER *la* SICUREZZA

Il progetto che mira ad accrescere il livello di informatizzazione del nostro Paese ha messo in evidenza le criticità delle imprese italiane su questo tema. Il passaggio richiede l'adozione di strumenti adeguati, ma soprattutto l'aumento della consapevolezza da parte del top management

di **FEDERICA MARIA RITA LIVELLI,** *business continuity & risk management consultant*

L'Agenda digitale italiana (Adi) prevede l'attuazione di numerosi progetti atti a colmare il gap che divide l'Italia dagli altri Paesi europei in termini di norme e azioni mirate all'innovazione digitale del Paese, attraverso la trasformazione digitale della Pubblica amministrazione, la copertura della banda larga per tutti i cittadini, l'innovazione delle aziende (i.e. piano Industria 4.0 / Impresa 4.0, e a breve 5.0 con avvento del 5G) e il supporto alle start up innovative così da attuare un cambiamento positivo, aumentando l'efficienza e la trasparenza del sistema Paese.

La trasformazione digitale implica consapevolezza e comprensione sia dei vantaggi sia dei rischi dello spazio cyber al fine di fungere da *volano* di diversi modelli di business, di innovazione sociale, di formazione permanente e di miglioramento della filiera a favore della competitività.

Uno scenario non maturo

È estremamente importante per la realizzazione dei programmi dell'Adi che le aziende tutte siano in grado di *tenere il passo* rispetto a chi ha investito ampiamente negli ultimi anni nell'industria 4.0 e si accinge ad affrontare le sfide dell'industria 5.0 con l'avvento della rete 5G.
In particolare, se le piccole e medie imprese italiane, che costituiscono la *dorsale* del Paese, non intraprendono prontamente il processo di digitalizzazione, rischiano di rimanere ai margini del mercato e di non poter continuare a far parte della filiera e, conseguentemente, di non riuscire ad affrontare le sfide di questo mondo sempre più digitalizzato e globalizzato.

Secondo l'ultimo rapporto di **EY**, *Digital manifacturing maturity index 2019*, solo il 14% delle aziende manifatturiere italiane ha raggiunto un livello avanzato di sviluppo digitale e di interconnessione; il 49% ha concepito di attuare una trasformazione digitale completa, mentre il 37% è ancora alle prese con una fase sperimentale. Si eviden-

zia che solo il 5% delle aziende ha attuato un sistema strutturato e automatizzato completo di dati integrati di fornitori e clienti. Dunque è evidente che, a livello Paese, sono ancora poche le imprese 4.0. Non dobbiamo dimenticare che i mutati contesti socio-economici, geopolitici e climatici rendono ancor più urgente questa trasformazione, che implica, oltre alla disponibilità di risorse economiche, anche una diffusione della cultura digitale e un'adeguata formazione.

Management e personale pronti al cambiamento

La digitalizzazione comporta l'utilizzo di tecnologie (i.e *IoT, artificial intelligence, machine learning, blockchain, supply & logistic software*, etc.) a tutti i livelli e in tutti i settori che si avvalgono di reti e *cloud* per lo scambio di informazioni e dati.
Indipendentemente dal settore di operatività, le aziende dovranno poter contare, per la diffusione e incorporazione della cultura digitale, sul coinvolgimento e il supporto del top management.
La diffusione di policy adeguate, unitamente a un'opportuna gestione della continuità operativa e a una valutazione dei rischi, contribuiranno a garantire la resilienza dei sistemi, la protezione dei dati e la sicurezza cyber. Fondamentale sarà anche la pianificazione di training continuo e *ad hoc* del personale oltre all'*accountability* nell'accezione di "responsabilità di operare in modo sicuro".
Esistono sul mercato software che effettuano simulazioni di *cyber attack*, atte a identificare le aree deboli che necessitano di una migliore protezione, o che debbano essere riorganizzate in un'ottica di maggiore sicurezza. Software che permettono di svolgere attività di training del personale misurandone il grado di capacità di identificare attività di *phishing* (i.e. *malware, pharming, malware-based, tabnapping*, ecc.), aumentandone la conoscenza e consapevolezza della sicurezza informatica.


© manjik - iStock

Le norme educano alla sicurezza

Come precauzione sarà altresì necessario digitalizzare i file più critici e tutto ciò che è importante avere a disposizione in caso di *cyber attack*, malfunzionamenti, incidenti e danni fisici, attuando *back-up* periodici non solo su *cloud* ma anche su dischi esterni, e custodire le copie in un luogo separato.
Altrettanto importante sarà la digitalizzazione dei documenti cartacei, ricordando che, anche se le copie fisiche risultano necessarie per i processi formali, vi sono casi in cui la copia digitale può risultare utile sia per un ripristino veloce sia per un'emergenza. Attraverso la scannerizzazione si potranno acquisire i documenti e archiviarli sia sul cloud sia su dischi esterni, oltre ad avvalersi della funzionalità di ricerca dei file in Pdf e indicizzazione automatica.
Tutte le normative e regolamentazioni, unitamente alle *best practice*, mirano di fatto all'autoanalisi, alla autovalutazione e implementazione di misure di gestione e controllo più sicure per le aziende, indipendentemente dal settore di appartenenza, dato che è sempre più provato che chi implementa piani di continuità operativa e di gestione del rischio è maggiormente resiliente e in grado di agire prontamente, di contrastare crisi, incidenti e attacchi cyber.
Dunque, una sicurezza che sottende la trasformazione digitale, e che mira alla gestione dei rischi e a garantire la continuità operativa, ma si rivela anche come un'opportunità per attuare una prevenzione, eliminare o mitigare danni e interruzioni, non più quindi solo una difesa del perimetro aziendale, bensì una strategia di sicurezza più dinamica e agile, che tuteli l'intera catena del valore di un'azienda.