

FOR

Le ITS Academy e la formazione tecnica superiore

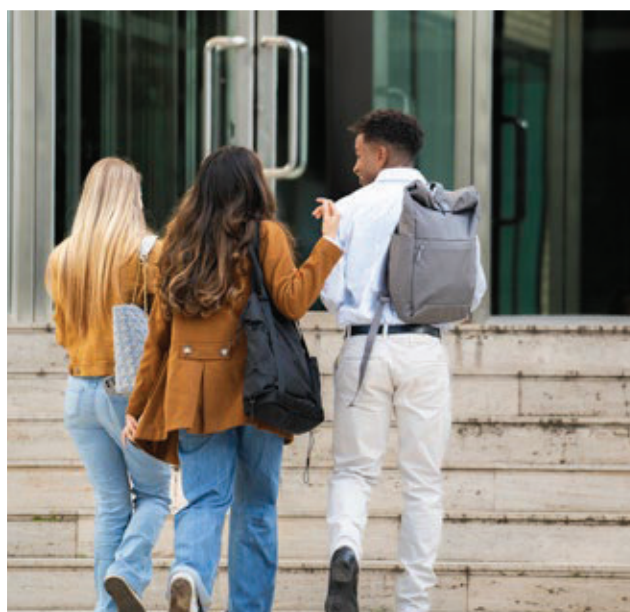
Patrizia Cinti

Negli ultimi anni il tema della formazione tecnica superiore è tornato al centro del dibattito sulle politiche educative e industriali italiane. In particolare, le ITS Academy rappresentano oggi uno dei principali tentativi di rafforzare il collegamento tra sistema formativo e sistema produttivo. Questo contributo propone una riflessione sul ruolo delle ITS Academy alla luce del pensiero e delle attività di Federico Butera, che ha dedicato gran parte della propria ricerca alla relazione tra organizzazione del lavoro, innovazione tecnologica e formazione delle competenze professionali. L'ipotesi di fondo è che le ITS Academy possano essere interpretate non semplicemente come un segmento della formazione terziaria, ma come una componente strategica per lo sviluppo dei sistemi produttivi e per la valorizzazione del Made in Italy¹. Ripercorrere le attività realizzate da Federico Butera e i suoi collaboratori della Fondazione IRSO nel mondo dell'istruzione è una impresa non semplice, anche per chi vi ha lavorato fin dagli inizi. Butera ha sempre avuto uno sguardo attento, critico e lungimirante

per quella che considerava l'istituzione e organizzazione strategica per realizzare l'innovazione del sistema paese, al pari dello sviluppo delle imprese e del superamento dei modelli burocratici tradizionali nella pubblica amministrazione. Molti sono i libri, i saggi, i documenti di ricerca dedicati al sistema dell'istruzione. In essi si trovano idee che hanno accompagnato l'innovazione degli istituti scolastici, lo sviluppo delle professioni dei *knowledge worker* che vi lavorano, i sistemi per la condivisione delle conoscenze e delle esperienze, l'accompagnamento alla realizzazione di reti scolastiche, e poi la nascita e lo sviluppo degli ITS Academy. È proprio nel variegato mondo delle ITS Academy che ho potuto realizzare con Federico Butera l'ultimo lavoro insieme, ed è di questo che tratto in questo breve saggio.

Perché le ITS Academy

Chi osserva da vicino il funzionamento delle imprese italiane, in particolare quelle manifatturiere di media dimensione, si imbatte spesso in una contraddizione piuttosto evidente: da una



parte le aziende segnalano una crescente difficoltà nel reperire tecnici qualificati; dall'altra il sistema educativo forma laureati e diplomati che faticano a trovare una collocazione coerente con il proprio percorso di studi. Questo squilibrio non è un fenomeno recente, ma negli ultimi anni è diventato più visibile. La digitalizzazione dei processi produttivi, lo sviluppo dell'intelligenza artificiale e la crescente integrazione tra produzione e gestione dei dati hanno trasformato molte professioni tecniche. In fabbrica, nella logistica, nel settore agroalimentare o nella moda ma

anche nelle pubbliche amministrazioni che adottano sistemi professionali basati sulle competenze, il lavoro richiede sempre più spesso competenze che combinano conoscenze tecniche, capacità di interpretazione dei dati e abilità di collaborazione all'interno di gruppi di lavoro interdisciplinare complessi. E flessibilità e disponibilità al cambiamento e alla formazione continua. Il sistema formativo italiano, tradizionalmente diviso tra istruzione tecnica secondaria e università, ha faticato a rispondere in modo rapido a questi cambiamenti. In questo scenario le ITS Academy

1 Ministero dell'Istruzione e del Merito, *Sistema ITS Academy: monitoraggio nazionale e sviluppo*, ultimi rapporti disponibili.

ESPERIENZE e VISSUTI



sono state pensate come una possibile risposta istituzionale a tale problema. Con la riforma del 2022 esse sono state riconosciute come istituzioni di formazione terziaria professionalizzante e sono state dotate di strumenti organizzativi più strutturati².

Le ITS Academy rappresentano oggi uno degli esperimenti più interessanti nel panorama della formazione italiana. Pur con differenze tra territori e settori produttivi, esse stanno contribuendo a costruire un sistema di formazione tecnica superiore più vicino alle esigenze delle imprese. I lavori di Federico Butera hanno offerto teorie, metodologie e strumenti utili per progettare queste istituzioni formative come sistemi sociotecnici. Le sue ricerche hanno mostrato come pro-

cessi di lavoro, innovazione tecnologica, organizzazione del lavoro e sviluppo delle competenze siano dimensioni strettamente interconnesse. Per comprendere meglio il significato di questa evoluzione può essere utile richiamare il contributo teorico e di ricerca di Federico Butera, fino al progetto triennale del MIM denominato FORTES³.

Il contributo di Butera

Federico Butera è noto soprattutto per i suoi studi sulla sociologia delle organizzazioni e sulla trasformazione del lavoro nelle economie avanzate. Fin dagli anni Settanta le sue ricerche e la sua attività, avviata nella Olivetti di Adriano Olivetti, hanno cercato di comprendere in che modo le imprese cambiano

quando si trovano di fronte a innovazioni tecnologiche significative⁴.

Con il suo approccio sociotecnico ha creato il forte legame tra ricerca teorica e osservazione empirica, la ricerca intervento. Molte delle sue analisi nascono infatti da studi condotti direttamente all'interno delle imprese e delle pubbliche amministrazioni. Questo gli ha permesso di osservare, proprio come architetto sociotecnico, come le trasformazioni tecnologiche non producano effetti automatici sulle modalità di lavoro, ma richiedano sempre processi di adattamento organizzativo e professionale. Secondo Butera, l'innovazione non consiste soltanto nell'introduzione di nuove macchine o software, neanche ora con la AI. L'innova-

zione, infatti, implica anche la creazione di nuove competenze professionali e di nuove forme di cooperazione tra lavoratori, già individuate e perseguite con i gruppi autoregolati dell'Olivetti. Per questo motivo la formazione assume un ruolo centrale: senza un adeguato sviluppo delle competenze, le tecnologie rischiano di rimanere sottoutilizzate o di generare inefficienze organizzative. Un altro punto chiave della sua riflessione riguarda il superamento della tradizionale separazione tra sapere teorico e sapere pratico.

Le economie basate sulla conoscenza richiedono figure professionali capaci di integrare competenze diverse: progettazione, gestione dei processi, utilizzo delle tecnologie e capacità di lavoro collaborativo⁵.

Diventa evidente l'importanza di istituzioni formative capaci di operare creando sinergia tra sistema educativo e sistema produttivo.

Le ITS Academy come modello

Le ITS Academy rappresentano un tentativo concreto di costruire questo tipo di istituzioni che creano sinergia, un volano per l'innovazione e lo sviluppo dei territori e dei settori produttivi. La loro caratteri-

2 Legge 15 luglio 2022, n. 99, *Istituzione del Sistema terziario di istruzione tecnologica superiore (ITS Academy)*.

3 Ministero dell'Istruzione e del Merito, Progetto FORTES (Formazione Tecnica Superiore), documentazione ufficiale di progetto.

4 F. Butera, *Il cambiamento organizzativo: analisi e progettazione*, Laterza, 2009.

5 F. Butera, *Lavoro e organizzazione nella società della conoscenza*, Marsilio, 2020.

stica principale è il modello organizzativo basato su fondazioni che riuniscono diversi attori: scuole, università, imprese, enti locali e centri di ricerca.

Questo assetto non è semplicemente una soluzione giuridica e amministrativa. L'obiettivo è creare un contesto in cui i percorsi formativi possano essere progettati tenendo conto dei fabbisogni reali delle filiere produttive presenti sul territorio, che partecipano in modo attivo alla formazione degli studenti e delle studentesse.

Le imprese partecipano fin dalla progettazione dei corsi e della didattica.

Una parte consistente dei docenti proviene dal mondo produttivo e porta in aula esperienze concrete di lavoro. Inoltre, una quota significativa del percorso formativo si svolge attraverso stage e tirocini in azienda. Dal punto di vista pedagogico questo modello presenta alcuni elementi interessanti.

L'apprendimento non avviene soltanto attraverso lezioni teoriche, ma anche attraverso attività laboratoriali ed esperienze dirette in contesti produttivi.

In questo modo gli studenti e le studentesse hanno l'opportunità di confrontarsi con problemi reali e

di sviluppare competenze operative. Proprio questa integrazione tra formazione e lavoro rappresenta uno degli aspetti più coerenti con la prospettiva teorica di Butera, secondo cui l'innovazione organizzativa richiede sempre processi di apprendimento situati nei contesti di lavoro⁶. Scrive Butera: "Come è noto, gli Istituti Tecnici Superiori (ITS) assicurano l'85% di occupabilità dopo un anno e creano competenze essenziali per l'innovazione delle imprese e delle organizzazioni. Gli ITS in Italia oggi contano circa 18.000 allievi contro i corrispondenti 900.000 della Germania.

Il Piano Next Generation EU prevede un investimento fino a un miliardo e mezzo di euro con due requisiti a) generare un aumento esponenziale degli allievi, arrivando a un incremento di 18.000 l'anno, outcome che sarà monitorato dagli organi comunitari; b) avviare una riforma del sistema ITS, svolta in rapporto sia ai sistemi di formazione e istruzione tecnica secondaria e sia alla formazione terziaria universitaria"⁷. Proprio per le ITS Academy Butera ha lavorato come direttore scientifico nel Progetto FORTES, realizzato con altre società di consulenza e voluto dal Ministe-

ro dell'Istruzione. In questo progetto la Fondazione IRSO e i suoi collaboratori hanno condiviso e utilizzato le teorie, metodologie e la propria strumentazione originale: la *check list* per le organizzazioni 4C, i processi del *Change Management Strutturale*, la descrizione del sistema socio-tecnico, l'analisi e diagnosi dei processi, la descrizione dei ruoli agiti e delle competenze professionali, la comunicazione estesa, la rete governata.

In particolare, il *Change Management Strutturale* consiste in tre classi di attività interrelate fra loro in una spirale ricorsiva sia di eventi di cambiamento strutturale sia di processi di apprendimento che si rafforzano a vicenda.

In una parola, cambiare insieme competenze e struttura, con la partecipazione di soggetti coinvolti, attraverso: a) un piano di cambiamento del sistema, come in questo caso il sistema ITS Academy, in particolare per le dimensioni organizzative e di *governance*; b) lo sviluppo di progetti sperimentali; c) il supporto al miglioramento continuo, attraverso la ricerca intervento e la formazione tecnica, digitale e relazionale⁸.

In questa prospettiva la formazione tecnica superiore

non è più considerata un ambito marginale del sistema educativo.

Al contrario, essa costituisce una delle infrastrutture fondamentali per la competitività dei sistemi produttivi e per la qualità del lavoro.

Bibliografia

F. Butera, *Il cambiamento organizzativo: analisi e progettazione*, Laterza, 2009.

F. Butera, *Organizzazione e società della conoscenza*, Marsilio, 2011.

F. Butera, *Lavoro e organizzazione nella società della conoscenza*, Marsilio, 2020.

F. Butera, *Organizzazione e società. Innovazione, partecipazione e sviluppo*, FrancoAngeli, 2021.

F. Butera, G. De Michelis, *L'Italia che compete*, FrancoAngeli, 2011.

F. Butera, G. De Michelis, *Intelligenza artificiale e lavoro, una rivoluzione governabile*, Marsilio, 2024.

Fondazione IRSO, documentazione sul progetto FORTES.

Ministero dell'Istruzione e del Merito, Legge n. 99/2022 – ITS Academy, 2022.

Patrizia Cinti

Sociologa dell'organizzazione PhD, Eduviva, Università Cattolica del Sacro Cuore di Roma.

Copyright © FrancoAngeli

This work is released under Creative Commons Attribution - Non-Commercial – No Derivatives License. For terms and conditions of usage please see: <http://creativecommons.org>

6 C. Argyris, D. Schön, *Organizational Learning*, Addison-Wesley, 1978 (per il concetto di apprendimento nei contesti organizzativi).

7 F. Butera, *Istituti tecnici superiori, la nuova legge e la sua realizzazione. L'analisi del prof. Butera*, in Formiche.net, 2021.
F. Butera, documenti e interventi su ITS Academy e occupabilità, Fondazione IRSO materiali progettuali.

8 F. Butera, *Organizzazione e società. Innovazione, partecipazione e sviluppo*, FrancoAngeli, 2021.

ESPERIENZE e VISSUTI

Persone, tecnologie e organizzazione del lavoro nella gestione del rischio

Marco Di Luzio

Il Sistema Socio-Tecnico, nelle scienze dell'organizzazione e in sociologia, è un modo di vedere le organizzazioni come insiemi integrati di “parte sociale” (persone, gruppi, cultura, processi organizzativi) e “parte tecnica” (tecnologie, strutture formali) che devono essere progettate insieme per funzionare in modo efficiente. Questo approccio nasce negli anni '50 con gli studi del Tavistock Institute (Trist ed Emery), dove emerge che cambiare solo la tecnologia senza ripensare ruoli, gruppi di lavoro e relazioni genera inefficienze organizzative rispetto agli obiettivi prefissati.

Nella scienza dell'organizzazione il Sistema Socio-Tecnico è quindi un principio di progettazione: non esiste una “migliore” struttura valida per tutte le imprese, ma occorre trovare ogni volta il giusto accoppiamento tra variabili sociali (competenze, motivazioni, cultura, leadership) e variabili tecniche (macchine, procedure, layout) in rapporto all'ambiente esterno. In sociologia del lavoro e delle organizzazioni, lo stesso concetto viene usato per analizzare come le tecnologie influenzano

relazioni di potere, identità professionali e forme di cooperazione o conflitto, e come le scelte sociali possono orientare l'uso delle tecnologie verso esiti più collaborativi ed efficaci.

Inquadrare il rischio cyber

Il concetto di Sistema Socio-Tecnico, storicamente adottato nelle scienze dell'organizzazione aziendale, emerge oggi con rinnovata rilevanza nel contesto della gestione del rischio cyber. Tale ambito, inizialmente caratterizzato da un approccio prevalentemente tecnologico, evidenzia sempre più la necessità di una prospettiva integrata che consideri congiuntamente dimensioni organizzative, umane e tecnologiche.

La cybersecurity nasce negli anni '80-'90 come estensione della sicurezza informatica e di rete, in un contesto in cui le minacce erano prevalentemente tecniche, gli ambienti più chiusi e controllabili e gli incidenti considerati eventi eccezionali. In questo contesto, la mitigazione del rischio cyber è stata inizialmente concepita come *un problema tecnico da risolvere con contromisure tecniche*.

Per molti anni ha dominato un modello implicito basato sul paradigma: “più tecnologia uguale più sicurezza.

L'idea sottostante era che l'implementazione di un numero sufficiente di tecnologie di sicurezza fosse in grado di prevenire o eliminare il rischio cyber. Questo ha portato ad una forte focalizzazione su tool e infrastrutture, prestando una limitata attenzione a processi organizzativi e comportamenti umani, e circoscrivendo la tematica ad una responsabilità esclusiva dell'IT.

Il tempo ha dimostrato come questo approccio esclusivamente *technology driven*, non fosse il modo più efficace per contrastare le minacce sempre nuove, sempre più insidiose, con impatti sempre più estesi a cui le organizzazioni sono esposte. Infatti, nonostante l'allocation di budget su progetti IT sempre più rilevanti, per l'implementazione di tecnologie volte a contrastare il rischio cyber, continuavano e continuano a verificarsi con sempre maggiore frequenza incidenti cyber relativi a:

- incidenti causati da errori di configurazione, non da mancanza di tecnologie;

- attacchi di phishing e social engineering, che bypassano le difese tecniche;
- mancanza di processi di incident response strutturati;
- scarsa consapevolezza degli utenti;
- assenza di governance e accountability.

Incidenti gravi di cybersecurity si sono verificati e continuano a verificarsi con una numerosità sempre crescente, proprio per queste cause, nonostante la presenza di tecnologie avanzate.

Questo evidenzia che la tecnologia in sé, non rappresenta una risposta efficace alle sempre maggiori minacce a cui le organizzazioni e le aziende sono esposte.

Definire il perimetro cyber

Alla luce di questi risultati non soddisfacenti l'approccio alla gestione del rischio cyber si estende ad altre dimensioni dell'organizzazione aziendale, ponendo al centro delle strategie di cybersecurity aspetti quali: i processi organizzativi, la definizione di ruoli e strutture organizzative ben identificate, le persone, con le

Tabella comparativa: ISO 22301 ↔ NIS2 ↔ DORA ↔ NIST CSF su dimensioni Sistema Socio-Tecnico.

DIMENSIONE SOCIO-TECNICA	NIS2 Totale Controlli 116	NIST CSF Totale Controlli 106	ISO 22301 Totale Controlli ~40-45 (stima)	DORA Totale Controlli ~40-50 (stima)
Persone	- Ruoli e responsabilità chiaramente definiti - Formazione e awareness obbligatorie - Coinvolgimento del management nella gestione dei rischi	- Awareness e formazione del personale - Ruoli e responsabilità per gestione rischi e incidenti - Coinvolgimento del management nella strategia di cybersecurity	- Leadership e governance (Clausola 5) - Competenze, formazione, awareness (Cl. 7) - Cultura della continuità - Ruoli e responsabilità per il miglioramento e la risposta agli incidenti	- Governance e supervisione del board e management - Competenze e formazione continua - Cultura della resilienza digitale - Ruoli e responsabilità per incident response e gestione fornitori critici
n. controlli / (%)	~20-30 (~17-26%)	~25-30 (~24-28%)	~8-10 (~20-25%)	~12-17 (~30-35%)
Processi	- Risk management e governance (Art. 7-15) - Incident response e reporting (Art. 18-21) - Supervisione fornitori, audit e controllo interni	- Funzioni Identify, Protect, Detect, Respond, Recover - Policy, processi e procedure di gestione del rischio - Incident response, valutazione e miglioramento continuo	- Contesto organizzativo, pianificazione BCMS (Cl. 4-6) - Piani di continuità, BIA, Risk Assessment (Cl. 8) - Monitoraggio, audit, miglioramento (Cl. 9-10)	- Risk management ICT - Gestione incidenti ICT ed escalation - Supervisione fornitori ICT critici - Pianificazione resilienza digitale e test di stress
n. controlli / (%)	~50-60 (~43-52%)	~50-60 (~47-57%)	~25-30 (~60-65%)	~20-27 (~45-55%)
Tecnologie	- Controlli tecnici obbligatori (firewall, IDS, logging) - Sistemi di monitoraggio e rilevamento incidenti	- Implementazione di controlli tecnici (IDS, SIEM, endpoint protection) - Soluzioni ICT per protezione, rilevamento e risposta agli incidenti	- Supporto dei sistemi ICT per piani di continuità - Backup, disaster recovery, strumenti di monitoraggio (Cl. 7-8)	- Sistemi resilienti e sicuri - Monitoraggio e logging ICT - Backup e disaster recovery - Strumenti per resilienza operativa digitale
n. controlli / (%)	~25-35 (~22-30%)	~20-25 (~19-24%)	~25-35 (~22-30%)	~6-10 (~15-20%)

loro competenze e cultura organizzativa. Queste indicazioni sono perfettamente sovrapponibili alle dimensioni organizzative identificate proprio dal Sistema Socio-Tecnico.

Nel linguaggio della sicurezza informatica il “perimetro cyber” è l’insieme dei confini, degli asset e dei punti di accesso che delimitano ciò che deve essere protetto dai rischi digitali (reti, sistemi, dati, servizi e infrastrutture critiche di un’organizzazione o di un Paese). Include sia componenti tecniche sia aspetti organizzativi e fisici. Le persone sono a pieno

titolo una componente del perimetro cyber, anche se in modo diverso rispetto agli asset tecnici. Ogni utente può diventare un punto di ingresso per attacchi.

Per questo, quando si definisce il perimetro cyber, si includono anche identità digitali, ruoli, comportamenti e livello di consapevolezza del personale, non solo reti, server e applicazioni.

Questo implica che le misure di sicurezza devono quindi coprire formazione, policy d’uso accettabile, gestione degli accessi e delle autorizzazioni, separazione dei compiti, procedure disciplinari.

Nella prospettiva “persone-processi-tecnologie”, il perimetro cyber maturo considera le persone come risorsa di difesa (sensibilizzazione, segnalazione di incidenti) oltre che come possibile vulnerabilità. Questo orientamento nuovo nella gestione del rischio cyber è attestato dalle recenti normative e standard di certificazione che integrano queste dimensioni nelle prescrizioni definite dalle Regulation Authority. Se prendiamo in considerazione la recente normativa NIS 2¹ a cui organizzazioni e aziende classificate come “Essenziali” o “Importanti”

ed analizziamo i 116 punti di controllo previsti dalla norma vediamo come in realtà i requisiti a cui le organizzazioni devono rispondere ricalcano le tre dimensioni del Sistema Socio-Tecnico: Tecnologia, Persone Processi. In particolare, se vediamo le percentuali dei controlli per tipologia sul totale dei controlli previsti dalla norma, si evidenzia una particolare attenzione alla dimensione Processi e una rilevanza analoga alle dimensioni Persone e Tecnologie².

1 Decreto legislativo 4 settembre 2024, n. 138, <https://www.acn.gov.it/portale/nis/la-normativa>.

2 Si veda Tabella comparativa di sintesi riportata a fine documento. In questa tabella sono classificati i controlli/requisiti previsti dalla regolamentazione in oggetto rispetto alle dimensioni del Sistema Socio-Tecnico. Parliamo di stime perché in alcuni casi i controlli/requisiti fanno riferimento a uno o più dimensioni. Queste stime sono indicative e servono a confrontare l’approccio del Sistema Socio-Tecnico tra i diversi quadri normativi/framework: NIS2 ha un totale ufficiale di circa 116 controlli/requisiti (livello soggetto essenziale). NIST CSF 2.0 conta circa 106 sottocategorie nel suo core (fonte NIST). ISO 22301 non ha “controlli numerati” come standard tecnico di sicurezza, ma possiamo stimare una mappatura equivalente di 40-45 requisiti/aree di controllo basata sulle clausole. DORA non fornisce un elenco numerico esplicito di controlli: la stima di 40-50 requisiti è derivata dalla struttura normativa (articoli e categorie).

ESPERIENZE e VISSUTI**FOR****Framework e normative**

Anche standard internazionali come il NIST Cybersecurity Framework³ (NIST CSF) che è ad oggi uno dei modelli più utilizzati a livello internazionale per strutturare, valutare e migliorare la postura di sicurezza cyber delle organizzazioni pubbliche e private, prevede che la tecnologia sia sempre inserita in un contesto organizzativo e di governance.

In questo caso le percentuali dei requisiti definiti dallo standard danno una rilevanza percentuale maggiore alle dimensioni Persone e Processi rispetto alla dimensione Tecnologie. Allo stesso modo lo standard ISO 22301 (Business Continuity Management System – BCMS)⁴ definisce dei requisiti fortemente orientati ai processi e alla governance, e si fonda su un equilibrio socio-tecnico tra processi, persone e tecnologie, con una enfasi maggiore rispetto alle altre norme sui requisiti relativi alla dimensione Processi.

Per completezza, anche se dedicata in modo specifico al settore finanziario, citiamo la normativa DORA – Digital Operational Resilience Act⁵. Questa normativa definisce i requisiti a cui devono

rispondere le istituzioni finanziarie affinché possano resistere, rilevare, rispondere e riprendersi da eventi ICT (cyberattacchi, guasti sistemi, interruzioni servizi digitali). DORA, come NIS2 e ISO 22301, segue un approccio socio-tecnico integrato, con i processi come nucleo centrale, le persone responsabili della governance e delle decisioni, e le tecnologie come strumenti abilitanti della resilienza digitale.

Tutti i framework e normative convergono più o meno consapevolmente sui principi organizzativi definiti a suo tempo dal modello del Sistema Socio-Tecnico: le tecnologie servono, ma la resilienza si costruisce con processi chiari e persone preparate. L'analisi comparativa dei requisiti/controlli delle norme ISO 22301, NIS2, DORA e NIST CSF conferma l'attualità e la centralità del Sistema Socio-Tecnico nell'organizzazione aziendale, anche in contesti di forte innovazione tecnologica e digitale.

Pur in presenza di strumenti avanzati, sistemi automatizzati e soluzioni ICT sofisticate, la resilienza, la sicurezza e la continuità operativa non possono essere garantite esclusivamente dalla tecnologia. Le componenti persone e processi emergono come fat-

tori strategici: la leadership, i ruoli chiari, le competenze specifiche, la formazione continua, la cultura della sicurezza e della resilienza rappresentano leve fondamentali per la gestione dei rischi e per l'efficacia delle soluzioni tecnologiche.

Allo stesso modo, i processi strutturati di governance, pianificazione, gestione degli incidenti e dei fornitori, insieme a procedure chiare e continuamente aggiornate, assicurano che le tecnologie possano essere utilizzate in modo efficace e sicuro.

In un futuro caratterizzato da trasformazioni digitali rapide, cyber threat sempre più sofisticate e interconnessione globale, il Sistema Socio-Tecnico diventa non solo un modello teorico di riferimento, ma una strategia imprescindibile.

La sua capacità di integrare persone, processi e tecnologie sarà determinante per costruire organizzazioni resilienti, capaci di adattarsi, innovare e garantire continuità anche in scenari complessi e in continua evoluzione.

Possiamo dire che quelli che erano principi inediti identificati da Trist ed Emery ormai 75 anni fa con la definizione del Sistema Socio-Tecnico, risultano essere oggi non

solo confermati, ma anche introiettati nella cultura organizzativa ormai largamente diffusa.

Abbiamo visto come Fonti normative differenti, con provenienze, obiettivi e regulation authority distinte, seguono gli indirizzi provenienti proprio dall'eredità ormai diffusa e condivisa che questi autori con i loro studi ci hanno messo a disposizione.

Marco Di Luzio
CIO | CISO Tinexta Cyber.

Copyright © FrancoAngeli
This work is released under Creative Commons Attribution - Non-Commercial – No Derivatives License.
For terms and conditions of usage please see:
<http://creativecommons.org>

- 3 NIST Cybersecurity Framework (NIST CSF) è un framework di riferimento volontario per la gestione del rischio di cybersecurity, sviluppato dal National Institute of Standards and Technology (NIST) degli Stati Uniti. <https://www.nist.gov/cyberframework>.
- 4 L'obiettivo della ISO 22301 è garantire la continuità operativa dell'organizzazione, riducendo al minimo l'impatto di eventi disruptivi e assicurando che i servizi e i processi critici possano continuare o essere ripristinati entro tempi accettabili. <https://www.iso.org/standard/75106.html>.
- 5 Regolamento UE 2022/2554 ha l'obiettivo di rafforzare la resilienza operativa digitale delle istituzioni finanziarie nell'Unione Europea. In altre parole, punta a garantire che banche, assicurazioni, gestori di fondi e altri enti finanziari possano continuare a operare anche in presenza di eventi informatici o tecnologici disruptivi, riducendo rischi per il sistema finanziario e per i clienti. <https://www.bancaitalia.it/media/approfondimenti/2024/regolamento-dora/index.html?dotcache=refresh>.