10.3280/for2026-002oa23607

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'allocazione 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

10.3280/for2026-002oa23607

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-processitecnologie", 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 2[1] 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 Tecnologie[2].

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).

10.3280/for2026-002oa23607

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 fattori 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 autority 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.

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.bancaditalia.it/media/approfondimenti/2024/regolamento-dora/index.html?dotcache=refresh.