Cyber | Security | Defence spazia tra le tecnologie e i contesti coinvolti nel complesso mondo della sicurezza informatica, più comunemente la cybersecurity, analizzandone in maniera trasversale i diversi ambiti di applicazione, interazione e sviluppo, e trattando tutti gli elementi correlati: tecnici, tecnologici, organizzativi, economici, politici, giuridici, sociali e umani.

I testi proposti hanno sia un taglio didattico e tecnico-pratico che saggistico e divulgativo, e sono destinati a molteplici interlocutori: istituti e università, enti e aziende di settore, appassionati e cultori della materia | #_06

FABRIZIO CIRILLI

# Implementazione dei sistemi di gestione dalle basi alla certificazione

## Progettazione e sviluppo di ISO/IEC 27001 e ISO/IEC 42001 passo dopo passo

prefazione di Emanuele Riva e Domenico Squillace

contributi di Alessio Aresta, Gabriele Beghini, Marco Ciampi, Flavio Marangi e Massimiliano Perrone

UNIVERSITÀ

# Indice

Contributi esterni

# Prefazione

Le certificazioni di sistema sono spesso raccontate come strumenti tecnici, talvolta complicati, utili a dimostrare conformità a requisiti definiti da norme internazionali. Questa lettura, pur non errata, è profondamente incompleta. Le certificazioni sono, prima di tutto, un *linguaggio comune*: un'infrastruttura invisibile che consente alle organizzazioni di comprendersi, fidarsi reciprocamente e cooperare oltre i confini geografici, culturali e normativi.

Nel corso della mia esperienza nel sistema dell'accreditamento, maturata a livello nazionale, europeo e internazionale, ho potuto osservare come le certificazioni rappresentino uno dei più efficaci strumenti di *riduzione del rischio* non solo all'interno delle organizzazioni, ma anche e soprattutto nelle relazioni economiche e sociali. Riducono l'asimmetria informativa tra clienti e fornitori, tra imprese e istituzioni, tra mercati diversi. Rendono trasparenti i processi, misurabili le prestazioni, verificabili le promesse. Ma soprattutto, creano fiducia.

Questa fiducia non è un concetto astratto. È il presupposto indispensabile per il commercio internazionale, per la cooperazione industriale, per l'innovazione responsabile. Dove esiste un sistema condiviso di regole, valutato da terze parti competenti e indipendenti, le barriere si abbassano, gli scambi si semplificano e le opportunità si moltiplicano. In questo senso, le certificazioni non sono soltanto uno strumento di competitività: sono un *fattore di pace*.

Ridurre le barriere tecniche al commercio significa favorire il dialogo tra sistemi economici differenti. Occorre considerare sempre che il ruolo dell'accreditamento e della valutazione della conformità come infrastruttura globale di fiducia trova il suo fondamento giuridico e politico negli *Accordi sugli Osta-*

*coli Tecnici al Commercio (Technical Barriers to Trade – TBT)* dell'Organizzazione Mondiale del Commercio (WTO).

Il TBT Agreement nasce con un obiettivo chiaro: *evitare che regolamenti tecnici, norme e procedure di valutazione della conformità diventino strumenti di protezionismo mascherato*, pur salvaguardando il diritto degli Stati di tutelare salute, sicurezza, ambiente e interessi pubblici legittimi.

In questo contesto, l'accreditamento e la certificazione (insieme alla normazione e alla taratura) assumono un ruolo centrale. Gli Accordi TBT riconoscono che la fiducia reciproca negli esiti della valutazione della conformità è una condizione essenziale per facilitare gli scambi internazionali. Perché tale fiducia sia possibile, è necessario che gli organismi di certificazione, ispezione e prova operino secondo criteri comuni di *competenza, imparzialità e indipendenza*, verificati da un soggetto autorevole e riconosciuto: l'ente di accreditamento.

L'accreditamento nasce dunque come *risposta strutturata e multilaterale* all'esigenza, sancita dal WTO, di rendere equivalenti e accettabili a livello internazionale i risultati della valutazione della conformità. Attraverso gli accordi di mutuo riconoscimento tra enti di accreditamento, i certificati e i rapporti di prova possono circolare tra i Paesi senza necessità di duplicazioni, riducendo costi, tempi e conflitti commerciali.

In questo senso, l'accreditamento non è un mero strumento tecnico, ma una *architettura di fiducia istituzionale* che traduce in pratica i principi del multilateralismo commerciale. Dove l'accreditamento è solido e riconosciuto, il commercio è più fluido, le controversie diminuiscono e le relazioni economiche si fondano su regole condivise anziché su rapporti di forza.

È per questo che l'accreditamento può essere considerato, a pieno titolo, uno *strumento di pace*: perché riduce le barriere tecniche al commercio, previene conflitti economici tra Stati, rafforza la cooperazione internazionale e consente a sistemi regolatori diversi di dialogare su basi oggettive e verificabili.

Adottare un sistema di gestione, e confrontarsi con una norma, significa rafforzare il *multilateralismo*, oggi messo a dura prova da tensioni geopolitiche, frammentazione normativa e crisi di fiducia tra Stati e mercati. Le norme internazionali e i sistemi di certificazione basati su di esse rappresentano uno degli ultimi veri terreni di cooperazione globale, costruiti sul consenso, sulla partecipazione e sulla responsabilità condivisa.

Questo libro si colloca esattamente in questa prospettiva. Non si limita a spiegare *che cosa* richiedono le norme sui sistemi di gestione, ma accompagna il lettore nella comprensione del *perché* e del *come* applicarle in modo efficace, coerente e sostenibile. Mostra come un sistema di gestione ben progettato non sia un insieme di documenti, ma un sistema vivo, fatto di persone, decisioni, cultura organizzativa e miglioramento continuo.

In un contesto in cui nuove sfide – dalla sicurezza delle informazioni all'intelligenza artificiale, dalla sostenibilità alla responsabilità sociale – richiedono strumenti di governance sempre più maturi, i sistemi di gestione e le relative certificazioni assumono un ruolo strategico. Non come fine, ma come mezzo: per migliorare le organizzazioni, tutelare l'interesse generale e contribuire a un'economia globale più affidabile, trasparente e cooperativa.

È con questo spirito che invito il lettore ad affrontare le pagine che seguono: non come un manuale di adempimenti, ma come una guida alla costruzione di sistemi che parlano un linguaggio universale. Un linguaggio che, quando è condiviso, non solo migliora le organizzazioni, ma avvicina le persone e gli Stati.

*Emanuele Riva*
direttore Dipartimento Certificazione & Ispezione di Accredia
vicedirettore generale di Accredia
vice chair di Global Accreditation Cooperation Incorporated
IAF Chair
presidente Commissione UNI "Valutazione della Conformità"

La trasformazione digitale è divenuta la cornice entro cui si ridefiniscono strategie, processi e responsabilità delle organizzazioni: la normazione tecnica è il pilastro della governance che traduce la complessità tecnologica in regole condivise, che rende confrontabili le prestazioni, che supporta le decisioni informate e che abilita un miglioramento continuo e misurabile.

Su questa infrastruttura si fonda l'efficacia dei sistemi di gestione che integrando qualità, sicurezza delle informazioni, intelligenza artificiale, sostenibilità e conformità, trasformano i requisiti in pratiche operative e responsabilità chiare.

La sfida, al giorno d'oggi, non è più "se" adottare standard, ma come renderli "vivi", come incorporare i principi di risk management, trasparenza e accountability nei processi quotidiani, come assicurare che politiche e controlli siano coerenti con il contesto, come essere certi che gli indicatori di prestazione guidino davvero le scelte.

I sistemi di gestione sono particolarmente rilevanti nelle aree che oggi definiscono la competitività digitale: sicurezza delle informazioni e governance dell'intelligenza artificiale. Un approccio basato sul rischio alla protezione degli asset informativi, insieme a pratiche "robuste" di gestione dei dati e dei modelli, costituisce la base di un ecosistema affidabile. La tracciabilità delle decisioni, la validazione dei modelli, l'allineamento tra processi e tecnologie sono elementi imprescindibili per coniugare innovazione e responsabilità.

Inoltre, la integrazione tra sistemi (qualità, sicurezza, ambiente, AI) consente di evitare ridondanze e incoerenze, di valorizzare le sinergie e rendere più efficiente il governo dell'organizzazione: siamo in presenza di un'unica architettura che orchestra obiettivi, processi, rischi e misure, sostenuta da audit interni progettati per apprendere e non per "superare" adempimenti.

Il volume *Implementazione dei sistemi di gestione dalle basi alla certificazione* offre al lettore un percorso pragmatico: dal "cosa" richiedono le norme tecniche al "come" realizzarlo. Il valore sta nell'accompagnare l'organizzazione dalla lettura dei requisiti alla loro traduzione operativa, con attenzione alla struttura armonizzata, ai documenti di supporto, alla gestione dei rischi e agli aspetti di valutazione e certificazione. È un contributo che aiuta a evitare l'errore più comune: ridurre la norma tecnica a una checklist, rinunciando alla sua funzione di guida per la progettazione di sistemi efficaci e sostenibili.

La cultura della applicazione reale della normazione e della certificazione fa la differenza: portare i principi nei processi, nei ruoli, nelle metriche, nel riesame della direzione; far evolvere il sistema con i cambiamenti del contesto; misurare l'efficacia non solo nella conformità, ma nell'impatto sui risultati.

Come presidente di UNINFO, l'ente federato UNI responsabile della normazione tecnica dell'ICT, considero essenziale promuovere una cultura che riconosca il valore strategico sia delle norme tecniche che dei sistemi di gestione che su di esse si fondano. La competitività delle imprese, la fiducia dei mercati e l'efficacia delle politiche pubbliche dipendono sempre più dalla capacità di adottare modelli organizzativi basati su standard condivisi e riconosciuti a livello internazionale. In questo senso il libro offre un contributo rilevante, perché guida il lettore nell'interpretazione e nell'applicazione degli standard mostrando come un sistema di gestione, quando è progettato e implementato in modo completo e consapevole, è un vero strumento di governo dell'organizzazione. Un governo che, attraverso la normazione tecnica e la certificazione, rende possibile coniugare innovazione, affidabilità e responsabilità in un'economia sempre più interconnessa.

*Domenico Squillace*
presidente UNINFO

# Nota dell'autore

## L'arte di costruire sistemi (senza perdere l'anima)

Questo non è un libro scritto dall'intelligenza artificiale. È un libro scritto per l'intelligenza umana, quella che serve a gestire le organizzazioni quando le procedure sembrano non bastare più.

Mi hanno chiesto di mettere nero su bianco quanto ho imparato prima che sia "troppo tardi", una sorta di eredità per chi oggi si trova ad affrontare la sfida di implementare un sistema di gestione (o SG) per la sicurezza delle informazioni (SGSI) o per l'intelligenza artificiale (SGIA). In queste pagine non troverete solo i "devi" e i "dovresti" delle norme ISO, ma troverete il metodo per leggerle, interpretarle e, soprattutto, applicarle senza soffocare l'azienda nella documentazione inutile.

Dalle basi del PDCA alle riflessioni a "Coccia Di Morto", questo testo vuole essere un ponte tra chi ha scritto le norme e chi, ogni mattina, deve renderle vive in ufficio o in fabbrica. Perché un sistema di gestione è, prima di tutto, un sistema di persone.

Scegliendo questo libro, non stai solo investendo nella tua formazione professionale. Stai sostenendo attivamente la ricerca scientifica contro le malattie genetiche e degenerative. Un piccolo passo per un sistema di gestione, un grande passo per la vita.

# Introduzione

## Perché questo libro

Nelle aziende di tutto il mondo arriva prima o poi il momento in cui il top management richiede una certificazione ISO. Da quel momento iniziano ricerche di consulenti, testi e modelli per costruire il sistema di gestione in previsione della certificazione.

In questo libro voglio provare a dare un indirizzo a tutti coloro i quali si trovano in questa condizione: dover avviare un sistema di gestione per poi certificarlo.

Non lo farò però in modo generico, partiremo proprio dalle norme, capendo passo dopo passo la trasformazione del "cosa" richiede la norma nel "come" poterlo realizzare.

Lo faremo per due delle norme che mi sono più affini (non me ne vogliano gli specialisti di altri settori). Provo quindi a riportare le esperienze maturate in oltre 30 anni di audit, consulenza e formazione sugli standard ISO.

Ovviamente non potrà mai essere un testo esaustivo, viste le infinite sfaccettature che un sistema di gestione può assumere in un'azienda, però provo a mettere almeno le basi per le parti fondamentali, i concetti base e altri elementi utili per iniziare in modo più consapevole e scegliere le soluzioni più idonee.

Il testo è diviso in 4 sezioni principali:

- fondamenti, terminologia e concetti di base;
- lo sviluppo di un sistema di gestione per la sicurezza delle informazioni;
- lo sviluppo di un sistema di gestione per l'intelligenza artificiale;
- le certificazioni.

Potrebbe quindi essere letto come una sorta di manuale per chi avesse già conoscenze e competenze in una o più delle sezioni[1].

Infine, ho chiesto ad alcuni colleghi e amici di riportare le loro esperienze su temi di cui si parla nel libro, così da dare un contributo indipendente al testo. Sono professionisti che stimo, ognuno di loro ha un percorso diverso ma li accomunano due cose: la passione per il loro lavoro e la condivisione di parte delle mie esperienze. Stili diversi, culture diverse, origini diverse. Il loro contributo è esattamente come lo hanno scritto, proprio per lasciare "la loro voce" così come è nella vita reale.

Una nota importante: alcuni standard potrebbero essere stati aggiornati nel periodo in cui il testo verrà pubblicato, il lettore è perciò esortato a verificarne lo stato di aggiornamento sul sito www.iso.org per valutare eventuali differenze.

Buona lettura.

1. Il testo riporta brani originali tratti dagli standard, in alcuni casi il testo è stato tradotto dall'autore per agevolarne la lettura ma in quel caso i riferimenti permettono comunque di risalire al testo originale dello standard.

# Fondamenti, terminologia e concetti di base

Partiamo dalle definizioni di base del mondo normativo e proviamo a rispondere ad alcune domande di carattere generale che spesso rappresentano l'inizio di un sistema di gestione.

## Cosa è uno standard

Il modo migliore per spiegarlo è attingere alle fonti ufficiali, partiamo quindi dalla definizione contenuta nel sito UNINFO[1]: semplicemente un documento che dice "come fare bene le cose", garantendo sicurezza, rispetto per l'ambiente e prestazioni certe.

Secondo il Regolamento UE 1025 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, per "norma" si intende:

> una specifica tecnica, adottata da un organismo di normazione riconosciuto, per applicazione ripetuta o continua, alla quale non è obbligatorio conformarsi, e che appartenga a una delle seguenti categorie:
>
> 1. *norma internazionale*: una norma adottata da un organismo di normazione internazionale;
> 2. *norma europea*: una norma adottata da un'organizzazione europea di normazione;
> 3. *norma armonizzata*: una norma europea adottata sulla base di una richiesta della

1. Cos'è una norma? – Uninfo – Ente federato all'UNI – (UNINFO Ente Federato all'UNI – Tecnologie informatiche e loro applicazioni).

Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione;
4. *norma nazionale*: una norma adottata da un organismo di normazione nazionale.

Le norme, quindi, sono documenti che definiscono le caratteristiche (dimensionali, prestazionali, ambientali, di qualità, di sicurezza, di organizzazione ecc.) di un prodotto, processo o servizio, secondo lo stato dell'arte e sono il risultato del lavoro di decine di migliaia di esperti in Italia e nel mondo. Le caratteristiche peculiari delle norme tecniche sono:

- *consensualità*: deve essere approvata con il consenso di coloro che hanno partecipato ai lavori;
- *democraticità*: tutte le parti economico/sociali interessate possono partecipare ai lavori e, soprattutto, chiunque è messo in grado di formulare osservazioni nell'iter che precede l'approvazione finale;
- *trasparenza*: UNI segnala le tappe fondamentali dell'iter di approvazione di un progetto di norma, tenendo il progetto stesso a disposizione degli interessati;
- *volontarietà*: le norme sono un riferimento che le parti interessate si impongono spontaneamente.

Meglio di così non è possibile definire una norma e il suo significato.

## Come nasce una norma

Anche qui ci avvarremo di quanto spiegato chiaramente nel sito UNINFO: semplificando numerosi passaggi, l'iter che porta alla nascita di una norma si articola in diverse fasi:

- la messa allo studio;
- la stesura del documento;
- l'inchiesta pubblica;
- l'approvazione da parte della commissione centrale tecnica;
- la pubblicazione.

# Imparare a guardare diversamente[1]

## Il mio ingresso nel mondo degli audit

Ricordo ancora con grande lucidità la mattina del mio primo "vero" audit. Avevo ripassato normative, procedure, check-list, qualunque informazione documentata. Sulla carta ero pronto. Ma quando mi sono trovato davanti alla porta scorrevole dell'azienda che stavo per "auditare", con il taccuino in mano e il badge, ho capito che nessun corso ti prepara davvero alla parte più importante: le persone, le emozioni, le dinamiche invisibili.

Avviare una carriera nell'audit significa convivere con una strana miscela di emozioni: entusiasmo per il ruolo di "custode" di processi e standard, curiosità verso mondi organizzativi sempre nuovi, ma anche la paura sottile di non essere all'altezza. Arrivo con alle spalle circa vent'anni di vita d'azienda, tredici dei quali vissuti in una grande multinazionale; eppure, varcare quella soglia è come oltrepassare un confine tra ciò che un'organizzazione ha deciso di mostrare e ciò che ha scelto di custodire gelosamente. All'inizio ti senti un po' in mezzo al guado: da una parte le norme, fredde e precise; dall'altra le persone, calde, complesse e, soprattutto all'inizio, diffidenti.

Lungo il corridoio – e ce n'è sempre uno da attraversare, prima di arrivare alla "camera dei segreti" dell'audit – mi chiedevo: "Sarò troppo rigido? Sarò troppo morbido? Saprò farmi rispettare senza diventare un giudice? Riuscirò a vedere davvero cosa c'è dietro i documenti?". Questi dubbi non sono un difetto: sono il primo segnale che stai prendendo sul serio il tuo ruolo.

Al primo giro di tavolo si scoprono le prime carte: chi sei, cosa porti con te e chi hai di fronte. È importante inquadrare chi guida la squadra, l'"alfa" del gruppo: il suo stato d'animo, la temperatura delle sue parole e l'ampiezza del

1. Alessio Aresta, SW features manager – CNH SpA.

suo gesticolare sono la chiave per capire che tipo di audit stai per affrontare. Ho scoperto presto che non è solo un esercizio tecnico: è un viaggio doppio, dentro le organizzazioni e dentro sé stessi. Ogni audit costringe a osservare senza dare nulla per scontato, a fare domande senza giudicare, ad ascoltare non solo quello che viene detto, ma anche ciò che viene omesso, minimizzato, sdrammatizzato. Cogliere il codice non verbale di chi è di fronte aiuta a distinguere le aree dove tutto scorre liscio da quelle dove si è cercato di porre rimedio: spesso è lì che abitano le vere criticità.

Con il susseguirsi degli audit mi sono convinto che un'azienda non è mai solo processi, flussi e KPI: è fatta di paure, orgogli, abitudini, compromessi, scorciatoie creative e, spesso, di tantissima buona volontà che non sempre trova la strada giusta. Nel frattempo, impari a leggere gli altri, ad allentare la tensione con brevi rituali, a riannodare la fiducia con una battuta al momento giusto, a riportare a fuoco una discussione lasciando che il racconto arrivi fino in fondo. E mentre tutto questo accade, impari anche a leggere te stesso: scopri quanta tensione sai reggere in una riunione difficile, quanto riesci a rimanere lucido quando qualcuno si sente messo "sotto accusa", quanto sai mantenere integrità anche quando sarebbe molto più semplice chiudere un occhio.

Qui sta forse l'elemento più affascinante di questo mestiere, o comunque quello che oggi mi incuriosisce di più: il peso (e la bellezza) della responsabilità. Non che la responsabilità mi sorprenda: quotidianamente ne affronto molte nel mio lavoro, ma questa è diversa. La responsabilità di tutti i giorni riguarda le mie scelte e i miei orientamenti verso il mio gruppo di ricerca e sviluppo: è comunque il riflesso del mio fare e della mia visione. Sedersi in un audit ti espone a una responsabilità diversa: non più ancorata solo al tuo operato, ma basata su prove ed evidenze che, se non arrivano da sole, vanno ricercate. È un giudizio per conto terzi: rappresenti il "buon nome" di un organismo di certificazione e, al tempo stesso, la speranza dell'azienda che hai davanti di poter partecipare a un bando o a un concorso inseguito a lungo.

Ricordo bene i momenti in cui apro per la prima volta il foglio delle annotazioni (rituale che si rinnova a ogni nuovo audit): quel report non è un pezzo di carta, ha conseguenze concrete. Può innescare cambiamenti, investimenti, discussioni. Può essere usato come leva o come scudo. Persino una parola, il modo in cui formuli un'osservazione, il tono con cui la condividi fanno la differenza tra una difesa a oltranza ("ce l'hanno con noi") e una riflessione sincera

("ok, forse qui possiamo davvero migliorare"). Sentire questo "peso" non è comodo, ma è prezioso: mi ricorda che non sono lì per "trovare errori", ma per aiutare un sistema a conoscersi meglio e a diventare più robusto. A migliorare nel tempo. A rotolare sul famoso piano inclinato del miglioramento continuo, magari in ostinata direzione contraria.

Una costante, quasi divertente, è la diffidenza iniziale. Entrando in reparto o in ufficio si sentono gli sguardi e le domande non dette: "Cosa vuole trovare?", "Dove vuole andare a parare?".

Ci vuole tempo e ci vogliono buoni maestri per capire che una parte essenziale del mestiere è gestire le relazioni, non solo verificare i requisiti. In questo ho avuto la fortuna di iniziare con Fabrizio e Antonio, tanti anni di audit di qualità e cybersicurezza alle spalle. È una gestione particolare: non si è amici, ma nemmeno nemici. Si diventa una figura scomoda ma necessaria. Quello che si prova quando pian piano questa diffidenza si allenta è difficile da descrivere. Quando qualcuno ti dice, magari sottovoce, ad audit concluso: "Sai che alla fine è stato utile? Ci avete fatto notare cose che non vedevamo più da tempo", allora tutto assume un senso, non solo un ruolo.

Uno dei passaggi emotivamente più forti è capire quanto ascoltare sia molto più importante che parlare. Agli inizi immaginavo che la mia credibilità passasse dal mostrare quanto conoscessi la materia e la norma. Poi, con il tempo, ho scoperto che la vera autorevolezza nasce dal saper fare le domande giuste e poi... tacere e ascoltare: dove il racconto fila troppo liscio, dove emergono contraddizioni, dove spuntano frasi come "abbiamo sempre fatto così", dove c'è imbarazzo o, al contrario, un entusiasmo troppo difensivo. È in quei momenti che uno sguardo d'intesa con la tua squadra basta a segnare il confine sottile tra "controllare" e comprendere.

Alla fine di una lunga giornata le luci si spengono, il badge torna in portineria, la porta scorrevole si chiude e un veloce saluto con i tuoi compagni di avventura sancisce il fischio finale. Non appena la portiera dell'auto si richiude, sulla strada verso l'hotel o verso casa, la testa si riempie di domande: Ho esagerato? Sono stato troppo morbido? Ho capito davvero il contesto? Se da un lato questa solitudine può essere pesante, dall'altro è lo spazio in cui si amplia la propria coscienza professionale. Nei silenzi dopo un audit complesso si decide – e si rinnova – l'equilibrio difficile tra rigore e comprensione. Il rischio è doppio: essere così rigidi da diventare ciechi al contesto, oppure così

comprensivi da annacquare le evidenze. Ciò che si impara, con il tempo e con qualche cicatrice, è che si può essere fermi ma non aggressivi, chiari ma non umilianti, esigenti ma rispettosi. E quando ti riesce, lo senti addosso: esci stanco, ma con la sensazione di aver "tenuto la posizione" senza calpestare nessuno.

Una cosa importante da chiarire è che nessun audit assomiglia davvero a un altro, ma la prima mattina ha sempre lo stesso respiro. C'è l'apertura: l'incontro con il management, gli obiettivi, il perimetro, i vincoli del tempo. Una sorta di rituale che sancisce un tacito patto di buona fede.

Poi si entra nel vivo: revisione documentale e campionamenti, interviste, walk-through nei processi, traccia delle decisioni. Le ore in mezzo scorrono tra verbali, schermate proiettate a parete, diagrammi, una policy che deve "parlare" con una procedura, una procedura che deve "parlare" con le "evidenze" riportate nei nostri log. È un continuo salire e scendere di quota: dall'alto della governance al dettaglio di una registrazione; dal "chi decide cosa" al come è stato deciso, quando, con quale dato.

La giornata si chiude quasi sempre con una mini-sintesi provvisoria: ciò che è emerso, ciò che va chiarito, ciò che sembra un sintomo e non una causa. Non è mai un verdetto: è una fotografia mossa, un po' sfocata, da mettere a fuoco insieme negli appuntamenti seguenti.

Ricordo un audit in cui tutto sembrava perfetto. Carta ineccepibile, metriche ordinate, grafici puliti. Eppure, durante un'intervista, un ingegnere ha esitato un attimo su una domanda semplice: "Chi può fermare il rilascio se un rischio supera la soglia?". La risposta è arrivata, ma dopo un piccolo lunghissimo attimo di silenzio. È stato il segnale. Siamo tornati su quello snodo. Abbiamo ricostruito un caso reale, e lì è emerso che, tra la policy e la pratica, si era aperta una fessura e questa, come spesso accade, non era cattiva fede, era la frizione tipica tra velocità del business e la prudenza del controllo.

Riflettevo proprio dopo questo episodio, occupandomi essenzialmente di audit su SG per l'intelligenza artificiale, come in questo ambito l'equilibrio tra carta e realtà sia ancora più delicato.

Dietro un algoritmo c'è sempre una catena di scelte: il dato raccolto, il dato escluso, la metrica privilegiata, la soglia tagliata, l'ipotesi scartata. Il prodotto AI rende visibili i risultati, ma rende invisibili molte decisioni intermedie. Il nostro compito è proprio quello di far riemergere quelle decisioni e a chiedere: chi ha deciso cosa, come, quando, con quale consapevolezza del rischio?

In questo contesto, il lessico cambia, ma la sostanza resta: governance, ruolo dell'alta direzione, registro dei rischi, gestione del ciclo di vita, gestione dei cambiamenti, analisi degli incidenti, competenze, accountability.

E si aggiungono parole più specifiche: bias, robustezza, tracciabilità, human-in-the-loop.

Mi accorgo che ciò che fa la differenza non è avere la policy giusta, ma saperla "abitare": usarla nei momenti scomodi, quando costringe a rallentare un rilascio, a scartare un dataset brillante ma opaco, a rifare un'analisi d'impatto perché la realtà è cambiata. L'audit non blocca l'innovazione: le mette un corrimano. Ricorda che certe scorciatoie, oggi convenienti, domani presentano il conto. E lo presentano, spesso, alle persone più fragili o meno visibili nei processi.

Se dovessi elencare gli strumenti che uso di più, molti non si trovano in nessun manuale:

- la domanda semplice fatta al momento giusto ("Chi può fermare il rilascio?");
- la ripetizione gentile ("Mi aiuta a capire di nuovo questo passaggio?") che smussa le difese;
- la pausa: il silenzio che lascia spazio a una risposta vera;
- la sintesi imparziale: restituire ciò che ho capito usando parole dell'interlocutore, per vedere se davvero ho capito;
- la curiosità disciplinata: non la curiosità che invade, ma quella che apre porte chiuse con rispetto.

Attraverso questi semplici strumenti, l'audit ti allena a vedere: a distinguere tra causa e sintomo, tra eccezione e regola, tra coincidenza e pattern. Ti insegna a non avere fretta di concludere e a non avere paura di concludere quando serve. Ti restituisce anche umiltà: nessuno vede tutto, da solo.

Per questo gli audit migliori sono sempre lavoro di squadra: tra auditor, e tra auditor e auditati.

Se potessi dire tre cose a chi inizia oggi: partirei dallo scegliere le proprie domande, saranno la vostra identità professionale. Vi aiuteranno a riconoscere e dubitare. Poi, fate pratica con l'arte della buona perdita di tempo. Il tempo apparentemente "inutile" di un racconto lungo, di un esempio ripreso, di una

verifica di comprensione, spesso fa affiorare gli elementi più utili. Infine, scrivete per essere capiti da chi non era in sala; un report deve aiutare altri, domani, a prendere decisioni migliori (questa l'ho rubata a uno dei miei maestri).

Infine, un breve appunto personale. Ogni volta che entro in una nuova realtà sento un piccolo nodo allo stomaco, lo riconosco: non è paura, è rispetto. Rispetto per le persone che incontrerò, per il lavoro che fanno, per le decisioni che il mio giudizio potrà influenzare. Ed è proprio da quel rispetto che nasce, ogni volta, la responsabilità di continuare a fare le domande giuste e di avere il coraggio di ascoltare davvero le risposte. La sfida, almeno in ambito AI, è rendere visibili le scelte invisibili che vivono tra i dati e gli algoritmi. È qui che sento di voler stare: nel punto scomodo in cui si incontrano innovazione, rischio e coscienza. Per ricordare – a me per primo – che l'efficienza senza consapevolezza è solo velocità, e che la conformità senza etica è solo ordine apparente.

Un passo alla volta, un'evidenza alla volta, una conversazione alla volta.

Cyber | Security | Defence_Tecnologie e contesti della sicurezza informatica è una collana diretta da Paolo Capodanno e Massimo Montanile.

Ultimi volumi in collana

#3 Claudio Santo Malavenda, Massimo Montanile, Stefano Voci, *La sicurezza del software. Guida alla progettazione e allo sviluppo*

#4 Paolo Capodanno, *Etica del mondo digitale* (in corso di pubblicazione)

#5 Fabrizio Cirilli, *Essere auditor o fare audit? Una vita tra norme, docenze e audit ISO*

#6 Fabrizio Cirilli, *Implementazione dei sistemi di gestione dalle basi alla certificazione. Progettazione e sviluppo di ISO/IEC 27001 e ISO/IEC 42001 passo dopo passo*