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 | #_5

FABRIZIO CIRILLI

# Essere auditor o fare audit?

## Una vita tra norme, docenze e audit ISO

prefazioni di Corrado Giustozzi e Riccardo Bianconi

SAGGI

# Indice

Prefazione

# Auditor fantastici e dove trovarli

Entrate nella reception di un'azienda e, appesi in bella vista alla parete, noterete probabilmente uno o più "certificati". Cosa sono? In apparenza dei semplici pezzi di carta, anche piuttosto sobri, di cui però l'azienda va molto fiera perché le sono costati tempo, soldi e impegno. A che servono? Secondo l'opinione comune, ad attestare al mondo che quell'azienda "fa le cose per bene". Qualunque cosa ciò significhi.

Ed ecco il primo di molti equivoci che girano attorno al mondo delle certificazioni, dei certificati e dei certificatori. Innanzitutto, che vuol dire "fare le cose per bene?" E poi, chi ha deciso qual è il modo giusto di fare le cose? E infine chi ha stabilito, e come, che quell'azienda fa le sue cose davvero "per bene"? No, la storia è un po' più complessa di così: e per fortuna assai più seria di come superficialmente la conosce l'uomo della strada.

Prendiamo ad esempio la più antica e famosa tra le certificazioni aziendali, quella cosiddetta "della qualità" (e mai definizione fu più infelice e fuorviante di questa! Chiamiamola dunque ISO 9001, che è poi il suo nome ufficiale.). Al contrario di come generalmente si pensa, anche per colpa di una cattiva divulgazione iniziale, essa non attesta che chi la consegue faccia prodotti di elevata qualità, ossia migliori o superiori rispetto ad altri. Il termine "qualità" infatti non si riferisce al prodotto finale dell'azienda, quale che esso sia: ma al complesso dei *processi produttivi* che l'azienda adotta e applica per svolgere la sua attività. Il che fa una bella differenza.

Una certificazione dunque attesta "solo" che l'azienda rispetti le regole che si è data da sé stessa, in conformità alle norme e agli obblighi vigenti; e che le adotti sempre in modo costante e controllato, senza fluttuazioni casuali o variazioni impreviste che perturbino la sua attività con riflessi sul suo prodotto. In questo modo il frutto della sua attività, quale che esso sia, risulterà sempre uniforme e prevedibile, entro margini di tolleranza prestabiliti rispetto ai parametri operativi autodecisi. Ed è questa la "qualità" di cui si parla. In altre parole: se quell'azienda fa prodotti scadenti, ed è proprio quello che vuole fare, la certificazione "di qualità" garantisce che essi saranno sempre scadenti allo stesso modo!

Secondo punto: una certificazione si può ottenere solo se esiste una norma che la preveda. Non tutte le norme infatti nascono a fini certificativi: quella che detta le misure dei bulloni, ad esempio, non prevede certificazioni di sorta. Di solito le norme che nascono a fini certificativi riguardano *sistemi di gestione*, ossia quell'insieme insieme di procedure e regole che un'organizzazione adotta per migliorare i propri processi in aree specifiche come qualità, ambiente, sicurezza e salute sul lavoro, conformità legale, cybersecurity, e via dicendo. Le norme ci dicono come devono essere impostati e mantenuti questi sistemi di gestione affinché possano funzionare efficacemente per consentire all'organizzazione di perseguire i risultati attesi, e soprattutto per poter essere verificati da un soggetto esterno appositamente competente e autorizzato: l'organismo di certificazione. Questo ha il ruolo di verificare, in modo oggettivo e imparziale, l'effettiva corrispondenza tra ciò che l'azienda ha dichiarato di fare tramite il suo sistema di gestione, e ciò che fa realmente.

In altre parole, nel mondo della certificazione vige la stessa logica che sta dietro a una onesta partita di biliardo: tu dichiari cosa vuoi fare, e sei libero di darti gli obiettivi che vuoi purché rispettino le regole del gioco; ma poi devi effettivamente fare quello che hai dichiarato, altrimenti il colpo non è valido.

In questo curioso mondo, l'auditor è quel particolare professionista al quale l'organismo di certificazione affida il delicato inca-

rico di verificare che l'organizzazione che si sottopone alla certificazione faccia davvero quello che ha dichiarato di fare, secondo le regole del gioco. Ed è un mestiere davvero speciale, che richiede innanzitutto una *forma mentis* tutta sua. Tanto per cominciare, l'auditor non può e non deve giudicare nel merito di quello che vede, ossia non deve ragionare "da consulente". Non può ad esempio dire all'azienda che un certo processo o una certa soluzione tecnica adottata sono giusti o sbagliati: deve limitarsi a verificare se sono conformi a quanto l'azienda ha dichiarato di fare, secondo le regole ed entro i limiti stabiliti dalla norma.

Per fare bene il suo lavoro, un auditor deve possedere non solo uno spettro assai ampio di conoscenze tecniche, che vanno dalla "semplice" conoscenza delle norme a quella dei processi produttivi aziendali relativamente ai settori di riferimento; ma anche tante altre caratteristiche più attinenti alla famiglia delle soft skill. Ad esempio una mentalità fredda e analitica associata a una capacità di giudizio imparziale, ma anche la capacità di lavorare sotto stress con tempi assai compressi; un elevato livello di diplomazia per poter interagire con clienti stressati senza far esplodere conflitti, e la capacità di gestire al meglio gli inevitabili contrattempi e incidenti di percorso; la capacità di organizzare un lavoro di gruppo in ambienti e situazioni di elevata complessità, ma anche il fiuto dell'investigatore per accorgersi di eventuali situazioni sospette sapendo distinguere tra errore e dolo. E infine, tanta pazienza e una generosa dose di buon senso. Insomma, praticamente un essere mitologico!

E infatti il mestiere dell'auditor non è per tutti. Innanzitutto bisogna esserci davvero portati, e avere le caratteristiche personali giuste; e comunque, prima di andare sul campo da soli occorre aver fatto tanta esperienza in affiancamento di qualcuno davvero bravo, che insegni al neo-auditor tutto ciò che di non scritto c'è nel mestiere. In fondo, più che un mestiere è una missione: è duro e difficile, piuttosto sconosciuto e oscuro, e come se non bastasse espone chi lo fa a critiche e preconcetti ingiustificati; ma adempie a una importante funzione sociale, e dà anche tante soddisfazioni a chi lo esercita.

Ecco quindi che gettare un po' di luce sul poco noto ma affascinante mondo degli audit e degli auditor è innanzitutto un'operazione meritoria. Se poi chi lo fa è il decano degli auditor italiani, quello che in tanti anni passati sia in aula che sul campo ha insegnato il mestiere alla maggioranza delle nuove generazioni di professionisti, allora la cosa si fa non solo interessante ma anche gustosa e stimolante, per non dire divertente. Infatti Fabrizio, nella sua lunghissima carriera, ne ha viste veramente di tutti i colori: e ogni aneddoto della sua vita professionale si incastra perfettamente nelle lezioni che tiene nei corsi di formazione per gli auditor trasformandoli in un'esperienza memorabile, come ben sanno tutti coloro che hanno avuto la fortuna di averlo in aula come docente.

Conosco e stimo Fabrizio, come persona e come professionista, da oltre vent'anni: e lo ringrazio per aver voluto distillare la sua visione in un libro, raccontandola oltretutto con la verve e l'umorismo che lo contraddistinguono. Questa sua lunga "auto-intervista" non è solo un'opportunità per conoscere meglio il mondo ancora piuttosto oscuro degli auditor e degli audit, ma anche un'ottima occasione per rendere un po' di giustizia a una categoria professionale, gli auditor appunto, che vengono spesso visti solo come acidi ispettori il cui unico scopo nella vita è mettere in difficoltà le povere aziende.

Vedere le cose dall'altro lato del tavolo è sempre utile, e chi non è del settore leggendo il libro scoprirà tanti aspetti belli e addirittura appassionanti di una professione, e di un mondo, che al di là di tutto meritano in primo luogo rispetto: perché è anche grazie a loro se il moderno mondo dell'economia e della produzione si è sviluppato e continua a svilupparsi in modo sano e competitivo ma, soprattutto, equo e trasparente.

*Corrado Giustozzi*

Prefazione

# Amico e auditor

Conosco Fabrizio Cirilli ormai da quasi trent'anni. Ho sempre apprezzato il suo sorriso, che fa capolino, con una buona dose di humor, anche nei momenti di maggiore pressione. Apprezzo di lui la tenacia e l'apparente instancabilità, così come la versatilità. Non mi aspettavo di essere chiamato a scrivere le mie impressioni su un testo così ad ampio raggio. Un testo che attraversa, incrociandole, le esperienze di una vita professionale, con le più importanti direttrici della professione dell'auditor.

Fabrizio è questo: un professionista che ha visto nascere la professione dell'auditing e ne ha colto le caratteristiche più importanti.

La prima delle caratteristiche che trovo ripetuta e rimarcata più volte nel testo è la capacità di rispettare il lavoro altrui. La capacità di saper mantenere la propria dimensione di adeguata umiltà, e nello stesso tempo di assertività, nel processo integrato di analisi, confronto e valutazione del lavoro altrui, con il riferimento di una norma e non di assunzioni personali, che saprebbero di arroganza. Il rispetto dell'altro, il confronto per acquisire tutte le informazioni e l'altrui punto di visa, la capacità di rendicontare a fronte di un requisito e non di un preconcetto, anche nel saper dire cose scomode, ma importanti per il miglioramento. Questi sono gli ingredienti che Fabrizio evidenzia come linee guida per l'auditing. Altro aspetto che riflette l'atteggiamento mentale del nostro è il desiderio di migliorarsi e di aggiornarsi continuamente, passando attraverso ruoli diversi, tutti sinergici, come la docen-

za e la consulenza, non sottraendosi al proprio addestramento e formazione. Non si può essere buoni critici d'arte senza aver mai provato sulla propria pelle quanto sia difficile apprendere le diverse tecniche necessarie a creare dei manufatti artistici. Così come non si può essere bravi auditor senza aver avuto modo di stare dalla parte di chi costruisce, sulla base di requisiti normativi, talora anche difficili da interpretare, o di chi le norme le scrive. Tutte cose che Fabrizio ha fatto con efficacia e ottima utilità per i propri clienti.

L'altro aspetto che emerge dalla lettura del libro è quello della predisposizione a essere grato a tutti coloro che, in ruoli differenti, hanno contribuito alle "avventure" di vita che la professione dell'auditor porta a sperimentare. Fabrizio sa essere riconoscente a coloro che hanno collaborato alle diverse fasi di sviluppo delle attività svolte. Saper essere grati è un bell'atteggiamento dell'anima, che schiude le porte all'oggettività e allontana l'arroganza.

Fabrizio ha attraversato l'epopea dello sviluppo della professione, dagli anni '80 del secolo scorso, quando la professione nasceva, sino ad oggi, dove di auditor ce ne sono molti. Qui sta l'altro valore del testo: le raccomandazioni a chi vuole affrontare la professione e a chi l'ha scelta da qualche tempo. Cogliere dall'esperienza di chi ha vissuto le fasi iniziali e lo sviluppo, con il portato prima di tutto "etico" e anche "tecnico-professionale", significa avere a disposizione un bagaglio di indicazioni più che prezioso. Il testo è piano e lineare, ricco di aneddoti anche simpatici. Buona lettura, allora e un grazie a "Fab" per il proprio contributo alla professione. *Che la forza sia con te maestro!*

*Riccardo Bianconi*

# Introduzione

Viaggiare, apprendere costantemente, mettersi in discussione, ampliare le proprie vedute: benvenuti nel mondo dell'auditor ISO[1]. Una professione forse poco nota che offre opportunità uniche. È un percorso che ha profondamente modificato la mia vita, aprendo scenari impensabili.

Inizialmente ero titubante e mi chiedevo: "A chi può interessare un argomento del genere?". Poi ho superato questa ritrosia e ho deciso di raccogliere in questo libro le riflessioni, i dubbi e gli aneddoti nati dalla mia esperienza sul campo e nelle aule.

Questo libro nasce, quindi, dalla volontà di condividere un percorso professionale ricco di sfide e soddisfazioni: quello di auditor e docente nei sistemi di gestione ISO. Una professione che, pur non essendo sotto i riflettori, offre opportunità uniche di crescita personale e professionale. In queste pagine, ho raccolto le cose apprese e le risposte alle domande più frequenti che mi sono state poste in aula e sul campo, con la speranza di offrire una guida pratica e ispiratrice a chi desidera intraprendere questa strada. Più che un manuale teorico, questo è il racconto di un'esperienza vissuta, con l'obiettivo di chiarire dubbi, fornire spunti concreti e, perché no, accendere la passione per un lavoro che ha profondamente arricchito la mia vita, non solo professionale.

La prima domanda che mi sono posto è: come si fa? Non ho nessuna competenza in questo campo. Inventare è inutile. Essendo

1. International Organization for Standardization (www.iso.org).

coinvolto nel mondo della tecnologia e delle intelligenze artificiali ho pensato di unire l'utile al dilettevole pensando anche a come non rendere noiosa una lettura del genere. Da qui l'idea di una intervista sui vari temi che volevo affrontare. Chi avrebbe condotto una intervista simile? Non certo giornalisti o altri di questo livello. Allora proviamo con una delle IA, le domande generate sono in corsivo.

Infine, ho chiesto a due professionisti che stimo, personalmente e professionalmente, di scrivere una prefazione che potesse anche essere un contributo dai loro punti di vista.

Buon divertimento.

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

Ultimi volumi in collana

#2 Alessandro Alongi, Fabio Pompei, *Diritto della privacy e protezione dei dati personali. Il GDPR alla prova della data driven economy*

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

#4 Paolo Capodanno, *Il nuovo universo digitale. AI, etica e benessere*

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