Ruoli, responsabilità e adempimenti utili e inutili

Negli ultimi mesi, anche con l'approssimarsi della "scadenza GDPR" si è molto parlato di "nomine" e "designazioni". Il 25 maggio è stato il "privacy spam day" per l'enorme numero di informative e nomine inviate spesso senza ragione da tante aziende, anche di primaria importanza (che avrebbero dovuto essere più attente, oltre che evitare di ridursi all'ultimo momento e fare le cose in modo spesso sciatto).

Allora approfittiamo per ripassare i ruoli emersi negli ultimi anni in virtù di norme e standard e il loro reale impatto sulle organizzazioni. Ci si limita qui ad alcuni ruoli collegati alla sicurezza informatica.

Responsabile qualità

Il Responsabile qualità era inizialmente la persona addetta ai controlli dei semilavorati e del prodotto finito nelle aziende manifatturiere.

Con la diffusione della ISO 9001 (soprattutto dal 1999), il suo ruolo ha assunto caratteristiche diverse, orientato a mantenere i "documenti della qualità", solitamente numerosi, prolissi e complessi, più utili a far contenti gli auditor che assicurare l'effettiva qualità del prodotto finito o dei servizi erogati.

Il Responsabile qualità, anche quando molto competente, ha quindi perso la sua caratteristica tecnica e si è ritrovato con il ruolo di mantenere documenti e di intrattenere gli auditor perdendo autorevolezza e potere per migliorare i processi. Spesso questo ruolo è assunto direttamente dalla Direzione, ma raramente con l'attenzione nei confronti della qualità.

Poche organizzazioni hanno saputo valorizzare la visione complessiva dei processi e delle attività e la capacità di coordinarne i progetti di miglioramento.

Gli standard della serie ISO 9000 richiedevano fosse nominato un “Rappresentante della Direzione per la qualità” (non un “Responsabile qualità”). Spesso però il vero rappresentante non era un membro della Direzione. Nell’ultima versione della norma, questa figura è scomparsa, forse auspicando una maggiore responsabilizzazione della Direzione.

Responsabile della sicurezza (delle informazioni)

La qualità di un prodotto è solitamente facilmente identificabile dai suoi stessi produttori. Molto più difficile quando si tratta di un servizio erogato, viste le sue molte caratteristiche intangibili (provate a dire ad un impiegato che non ha svolto correttamente il suo lavoro!). Ancora più arduo è stabilire il proprio livello di sicurezza.

Proprio per l’intangibilità della materia, la sicurezza delle informazioni richiede la presenza di persone altamente specializzate e dedicate all’argomento, che devono trovare soluzioni per bilanciare le esigenze di flessibilità con quelle di sicurezza.

Molti criteri adottati per dimostrare l’approccio di un’organizzazione alla sicurezza (standard ISO/IEC 27xxx, linee guida NIST CFS, normativa eIDAS, eccetera) sono controllati dagli auditor attraverso molti documenti spesso inutili nella pratica e di cui deve occuparsi il “Responsabile della sicurezza”.

Similmente a quanto è successo per la qualità, un ruolo importante e in alcuni contesti molto utile sta perdendo di autorevolezza.

Questo non succede solo a causa di consulenti ed “esperti” con la capacità di proporre modi per complicare un’organizzazione, ma anche perché molti dirigenti sono più motivati a raggiungere obiettivi (e bonus) a breve termine che assicurare la sostenibilità dell’organizzazione. Questo è stato ben dimostrato dai recenti casi di cronaca come quello relativo a Equifax.

Responsabile esterno del trattamento

Con la normativa privacy, dal 1996 molti fornitori sono stati “nominati” o “designati” responsabili esterni del trattamento. Il GDPR non richiede alcuna nomina (anche perché stonerebbe con il ruolo di “processor”, malamente tradotto con “responsabile”), ma un contratto con specifiche caratteristiche.

In molti non hanno colto l’importante cambiamento normativo e il 25 maggio (il privacy spam day) hanno inondato i propri clienti e fornitori con nomine assolutamente generiche, in molti casi inadeguate al contesto (per esempio, a singoli consulenti è stato chiesto di avere un DPO). In più alcuni hanno accompagnato le nomine a questionari inutili.

Ancora una volta si sta imponendo un modello basato su tanti documenti prolissi, complicati, con prescrizioni inattuabili e difficili da mantenere. Purtroppo la massa di carta (digitale) prodotta ha tolto energie per capire veramente a chi sono trasferiti i dati e quali misure chiedergli.

Responsabile interno del trattamento

Negli ultimi mesi è stato detto e ripetuto che il “responsabile interno” non è oggetto del GDPR. Ovviamente ogni organizzazione può, e deve, specificare al proprio interno le responsabilità come meglio ritiene necessario (un po’ ridicoli quelli che auspicano che questo logico adempimento venga ribadito dalla normativa).

In passato e in alcune organizzazioni, la nomina di pochi "responsabili interni" ha permesso agli altri di ritenersi esentati dal prestare attenzione alla privacy.

Il GDPR avrebbe dovuto rimettere al centro il principio per cui ciascuno, dall'ultimo impiegato all'Amministratore delegato, è responsabile, per la propria parte, del trattamento dei dati personali.

Purtroppo, ancora una volta, in molti hanno imboccato la strada della burocrazia inutile e hanno rinnovato le "nomine interne" (scritte spesso anche male).

Auditor interno

Molti standard e regolamenti richiedono che vengano condotti audit interni e che gli auditor siano indipendenti dalle attività oggetto di audit.

L'auditor, se specializzato in una certa materia, è una figura molto importante perché garantisce il presidio di certe competenze, oltre che il controllo di certi adempimenti.

Purtroppo alcuni hanno spinto gli auditor interni a chiudersi in una torre d'avorio, permettendo loro di scendere qualche volta per condurre gli audit, scrivere rapporti e elencare tante raccomandazioni.

Questo ha fatto perdere autorevolezza anche a questo ruolo, dopo aver unito la burocrazia (rapporti prolissi e troppe raccomandazioni) con la torre d'avorio (raccomandazioni non aderenti al contesto, senza alcun aiuto per trattarle, commenti astratti e tardivi alle procedure da applicare).

Da diversi anni alcuni auditor partecipano direttamente alla redazione delle procedure e ai riesami di progetto (indicando sin dall'inizio alcune misure da prevedere e alcuni rischi da considerare) e alle discussioni per rispondere alle loro stesse raccomandazioni.

Questo non è contrario all’indipendenza degli auditor (devono infatti verificare come sono attuate le procedure dall’organizzazione, non evitare di progettarle) e assicura una maggiore significatività ai loro contributi.

Responsabile della protezione dei dati (DPO)

Ed infine poche parole sulla figura che negli ultimi 3 o 4 anni è stata al centro dell’attenzione: il DPO.

Il ruolo richiede elevate competenze e sarebbe importante fornire suggerimenti e indicazioni, organizzare e condurre, non necessariamente in prima persona, gli audit interni e mantenere i rapporto con le entità esterne quando si parla di privacy.

Purtroppo si sta cercando di rovinarlo burocratizzandolo e spingendolo verso la torre d’avorio (alcuni DPO si sono rifiutati di partecipare alle discussioni per impostare le procedure e le misure di sicurezza), esattamente come è successo agli auditor interni.

Le premesse non sono incoraggianti, ma è necessario lavorare perché questi ruoli riconquistino reale utilità e autorevolezza.

A cura di: **Cesare Gallotti**

L’articolo Ruoli, responsabilità e adempimenti utili e inutili proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/ruoli-responsabilita-e-adempimenti-utili-e-inutili/