LEXELLENT	Data: 7 novembre 2022
Testata: Cybersecurity360	

CYBERSECURITY360

CONFORMITÀ NORMATIVA

Modelli di gestione e protocolli integrati: approccio integrato tra privacy, sicurezza sul lavoro e 231

Quali sono i costi diretti, indiretti e invisibili per lavoratori, società e comunità della mancata compliance alle norme su privacy, sicurezza e 231/01? Analizziamo i presupposti e le modalità per costruire un modello organizzativo di compliance per ridurre i rischi e agevolare le strategie di business, il tutto con costi sostenibili e senza ingenti investimenti in tecnologia, risorse, strumenti e macchinari

3 ore fa

D

Ugo Ettore Di Stefano

Senior Partner LEXELLENT – Presidente UGI-Unione Giuristi d'Impresa

La percezione della **reale portata degli impatti sul business** di un cattivo (o nullo) sistema di compliance è difficile e quasi sempre parziale.

Infatti, la valutazione delle conseguenze dannose dell'evento/rischio è spesso limitata ai cosiddetti **rischi diretti** e, più precisamente, solo ad alcuni di essi: tipicamente è noto il rischio di multe e sanzioni o di spese giudiziarie, ma più raramente vengono calcolati i costi derivanti dalla **riduzione dei ricavi**, il **deterioramento delle relazioni con i clienti**, la **riduzione di quote di mercato**, le **carenze di liquidità**.

A questi vanno aggiunti anche i cosiddetti **costi indiretti**: per esempio, per le società quotate, la **riduzione del prezzo delle azioni e il valore della società**, una **riduzione del rating della società**, gli **effetti sulle risorse umane** e il **peggioramento dell'immagine (danno reputazionale)**, la **perdita di relazioni o accordi strategici**, l'**incremento di costi**, l'**esclusione da bandi di gara** e via dicendo.

A tali rischi vanno aggiunti i **mancati vantaggi** dell'adozione di un corretto modello di gestione della compliance. Essi sono innumerevoli quali: i **vantaggi sulle riduzioni di premi assicurativi** INAIL o la funzione esimente sulla responsabilità, l'**aumento del coinvolgimento del personale**, la **miglior conoscenza dell'azienda e degli obiettivi strategici** da raggiungere, l'**efficienza dei processi**, la **possibilità di partecipare a bandi di gara pubblici**, la **tutela del patrimonio aziendale e delle informazioni**, del know how e dei segreti commerciali nonché molti altri.

Indice degli argomenti

Sicurezza sul lavoro: un buon esempio da seguire
Un modello da riproporre in ambito privacy e 231
Le PMI e i problemi della compliance "selettiva"
Serve un approccio integrato alla compliance
La figura del Manager Compliance
Best practice per la creazione di un sistema di compliance
Requisiti e contenuti di un sistema di compliance
L'importanza dei sistemi di certificazione
Conclusioni

Sicurezza sul lavoro: un buon esempio da seguire

Un esempio per tutti di quanto detto è rinvenibile nell'ambito della **sicurezza sul lavoro**. L'European Agency for Safety and Health at Work ha calcolato che il peso dei costi diretti rappresenta meno del 10% del totale dei costi conseguenti ad un infortunio sul lavoro.

L'azienda subisce i costi (diretti, indiretti e intangibili) derivanti dall'assenza retribuita per malattia, i costi di risarcimenti e assicurazione, le spese mediche a carico del datore di lavoro, i costi legali, amministrativi e di giustizia, i costi di produttività ridotta per salute compromessa, la perdita di produzione per inattività temporanea, i costi di reclutamento, i danni di immagine, gli effetti negativi sui colleghi, i danni collaterali a macchinari e materiali e via dicendo.

Il lavoratore soffre i costi delle spese sanitarie non coperte da assicurazione, la perdita di reddito durante l'assenza, i costi di caregiver, la riduzione di capacità lavorativa, la potenziale perdita di redditi futuri, il pensionamento anticipato, il dolore e la sofferenza morale e psicologica, i cambiamenti di stile di vita, la disabilità, la ridotta capacità di accesso al mercato del lavoro e via dicendo.

Peraltro, il costo globale non comprende solo i costi sostenuti dall'azienda o dal lavoratore, ma vi sono anche costi sociali quali ad esempio, sempre in ambito sicurezza sul lavoro: costi del Servizio Sanitario nazionale, sussidi aggiuntivi per rimborsi medici e sostituzione salariale, costi di giustizia, oneri connessi a pensionamenti anticipati, disabilità.

Un modello da riproporre in ambito privacy e 231

Ovviamente il ragionamento fatto per gli infortuni sul lavoro e la compliance in materia di sicurezza è replicabile anche negli altri ambiti della compliance aziendale: privacy e 231.

Anche in questi casi i costi complessivi da considerare vanno ben oltre le pur pesantissime sanzioni previste dal Reg. UE 679/2016 (GDPR) in caso di illecito trattamento dei dati personali o quelle di cui al sistema sanzionatorio del decreto 231 del 2001.

Preso atto della rilevanza di rischi di una mancata compliance e dei vantaggi di un sistema ben gestito, occorre conoscere come concretamente progettare ed introdurre un modello di compliance e come farlo secondo una modalità efficiente.

Il primo problema è che le numerose disposizioni normative che impattano la cosiddetta compliance societaria sono generalmente presidiate (in particolare nelle medie-grandi imprese) dalle numerose funzioni aziendali preposte, eventualmente supportate da consulenti specializzati nei rispettivi ambiti (privacy, sicurezza sul lavoro, responsabilità amministrativa degli enti ecc.).

Questo approccio è però possibile solo con un'organizzazione interna articolata, che non è invece replicabile (sostenibile) nelle piccole imprese.

Inoltre, tale modello articolato comporta il rischio che ciascuna funzione possa agire in maniera non coordinata con inefficienze, duplicazioni, contraddizioni nella definizione dei presidi aziendali e dei processi volti a gestire le differenti tematiche. Per ovviare a ciò, nelle società più strutturate esiste talvolta una funzione di compliance dedicata, ma ciò solitamente non è considerato economicamente vantaggioso nelle PMI.

Le PMI e i problemi della compliance “selettiva”

La conseguenza è che l'imprenditore nelle PMI, quasi sempre, opta per una **compliance “selettiva”** destinando risorse solo alle tematiche che ritiene, in base alla propria esperienza e percezione (non certo legale), prioritarie per il proprio business.

Quando però questa scelta viene effettuata da un imprenditore/manager senza competenze normative e senza che sia stato condotto un preventivo assessment sulle specifiche criticità, il risultato è che anche le risorse impiegate a tal fine risultano non idonee a garantire una corretta compliance aziendale e una efficiente gestione dei rischi e quindi, di fatto, si riducono a puri costi perdendo invece la possibilità di risultare utili investimenti.

Occorre dunque superare il problema dato dal fatto che gli ambiti da presidiare sono differenti e sono altresì molteplici gli argomenti (tra cui qualità del prodotto o del servizio, prestazioni ambientali, salute e sicurezza sul lavoro e molti altri) per i quali esistono specifici standard e possibili sistemi di gestione aziendale.

Serve un approccio integrato alla compliance

Negli ultimi tempi, pertanto, si è iniziato a sperimentare in alcune aziende un **approccio integrato** che, oltre alla non duplicazione di attività e documentazione aziendale, permette l'ottimizzazione dei flussi di comunicazione interni e della reportistica anche verso tutti gli organi societari di governance, amministrazione e controllo della società.

Il processo richiede una fase preliminare di risk assessment che faccia prendere esatta cognizione dell'attuale contesto aziendale, dei processi, delle policies e dell'organizzazione.

Occorrerà dunque identificare i rischi, valutarli, gestirli e monitorarli concentrandosi su quelli a probabilità e rilevanza maggiore (rischi primari).

Si tratta, dunque, di un processo trasversale non finalizzato all'individuazione di potenziali rischi di settore (es. reati ex 231/01) bensì una mappatura completa dei processi funzionale ad una valutazione, appunto, integrata.

La figura del Manager Compliance

L'individuazione di una figura di Manager Compliance, anche in outsourcing laddove i costi non consentissero all'azienda il mantenimento di una struttura interna, è il primo step per le piccole e medie imprese.

La risorsa dovrà possedere una solida conoscenza delle conseguenze legali e della struttura delle fattispecie alle quali le differenti normative del sistema compliance si riferiscono, oltre a padroneggiare la metodologia con la quale approcciare la normativa in relazione non solo alla propria esperienza professionale, ma anche e soprattutto al contesto della società.

Best practice per la creazione di un sistema di compliance

Il processo di creazione del sistema di compliance dovrà quindi essere volto a perseguire uno snellimento del sistema di procedure mediante, per esempio, la cancellazione delle policies non attuali e l'accorpamento di quelle possibili, un'automazione dei processi di report e dei flussi informativi e una definizione e coordinamento del sistema di audit.

Ovviamente laddove sia presente un ODV, un Collegio Sindacale, altre funzioni di Audit il loro preventivo coinvolgimento risulta indispensabile.

Se certamente il costo dell'implementazione di un modello di gestione integrato nelle PMI è proporzionalmente più impattante rispetto ad una grande azienda, è però altrettanto vero che la sua realizzazione risulta meno complessa in quanto i rischi da valutare sono generalmente in numero più limitato, così come la quantità dei processi da verificare o costruire è ridotta.

Inoltre, proprio per la contenuta dimensione, il sistema probabilmente sarà capace di mostrare una maggiore reattività all'adozione dei processi, mentre occorrerà prestare attenzione a presidiare una sufficiente standardizzazione e regolarità dei report informativi.

Il modello di gestione dovrà essere formalmente adottato e sostanzialmente condiviso dal vertice aziendale ma, nelle realtà medio piccole, coinvolgerà pochi soggetti apicali coordinati dal Manager Compliance.

Requisiti e contenuti di un sistema di compliance

Il modello, rispettando i requisiti di cui al D.lgs. n. 231 del 2001, sarà costituito dalla parte generale e dai protocolli costituenti la parte speciale. I protocolli costituiscono l'asse portante del sistema integrato.

Possono infatti contenere e coordinare le procedure e le policy aziendali per tutti i sistemi di compliance relativi ai vari ambiti: richiamare i protocolli sicurezza, le privacy policy, le procedure di whistleblowing, le procedure relative alle denunce per stress da lavoro correlato, le policy anticorruzione e antiriciclaggio, il codice etico, la procedura antitrust, le procedure di sicurezza informatica, i protocolli sui flussi di comunicazione, informazione e trasparenza, policy di cooperative compliance e la tax compliance d'impresa, i protocolli di gestione ambientale e rifiuti e via dicendo.

In merito ai contenuti occorrerà un coordinamento che consenta la sintesi dei vari protocolli evitando, proprio perché richiamati in un unico modello di gestione integrata, inutili duplicazioni ed eventuali contraddizioni. L'elaborazione congiunta delle regole aziendali consentirà anche di trovare il giusto equilibrio in quelle ipotesi in cui occorre giungere ad un compromesso e ad un bilanciamento di interessi talvolta contrapposti (si pensi, ad esempio, alle politiche di data retention sulla conservazione dei dati e ai limiti nel rispetto della privacy compliance o al tema della riservatezza in ambito whistleblowing, e alla necessità opposta di conoscere e conservare informazioni rilevanti per conseguire gli scopi).

Evidentemente occorrerà procedere per gradi, redigendo i protocolli più rilevanti (a seguito del ricordato assessment) e successivamente definendone di nuovi.

Si tratta di un lavoro continuativo che, oltre all'arricchimento dei rischi presidiati, comporterà l'analisi di quelli già individuati e gestiti per verificarne l'attualità, oltre che (se necessario) la revisione dei protocolli che li disciplinano.

L’importanza dei sistemi di certificazione

Un prezioso aiuto per la definizione dei contenuti e soprattutto in merito alla struttura del modello è dato innanzitutto dai sistemi di certificazione ISO/UNI e dagli standard internazionali, nonché dalle nuove linee guida di Confindustria (giugno 2021).

La predisposizione di idonea documentazione, manuali interni, procedure, istruzioni operative, registri è guidata per esempio dalle norme contenute nelle ISO 9001 (reati societari e PA, diritto d’autore, etc.) , ISO 37001 (anticorruzione, societari,), ISO 45000 (sicurezza sul lavoro), ISO 27001 (sicurezza e IT), ISO 14001 (ambientale); in particolare il processo di gestione del rischio, valido per qualunque settore di attività, è delineato nello standard internazionale UNI ISO 31000:2018 e nel sistema di gestione certificato ISO 9001-2015 con l’approccio cosiddetto “risk based thinking”.

Conclusioni

Certamente un processo aziendale che miri ad ottenere certificazioni e accreditamenti in tutti gli ambiti ricordati risulta sproporzionato e spesso proibitivo per le PMI, ma lo scorso aprile è stata pubblicata la ISO 37301 (che verrà adottata in ambito nazionale come **UNI ISO 37301:2021**) che costituisce il primo sistema di gestione certificabile per la compliance: norma che è stata definita non una semplice evoluzione della precedente UNI ISO 19600 del 2016, bensì la pietra angolare di un emergente corpus normativo sulla governance delle organizzazioni.

"*Il tema della compliance, unitamente ad anti-bribery e whistleblowing, è destinato ad aprire inedite e stimolanti prospettive, che possono portare la normazione oltre il consolidato perimetro del management, verso gli ambiti propri di CEO, investitori e consigli di amministrazione, ma anche aprire nuove opportunità per lo sviluppo di Modelli di Organizzazione, Gestione e Controllo (MOG) evoluti e promuovere nuove funzioni e figure professionali.*"(qui – pagina web consultata il 25/10/2022).

Seguendo il concetto di High-Level Structure (HLS) anche un MOG di compliance integrata sarà strutturato con campo di applicazione, riferimenti normativi, termini e definizioni, contesto dell'organizzazione, leadership, pianificazione, supporto, operazione, valutazione delle prestazioni, miglioramento.

L'approccio basato sul rischio, nella definizione del modello integrato, significherà:

1. identificare, coerentemente al contesto aziendale e di mercato, i requisiti, gli obiettivi, i rischi e le opportunità;
2. valutare le priorità;
3. pianificare le azioni;
4. attuare le azioni;
5. verificare l'efficacia delle azioni;
6. mantenere un processo di apprendimento arricchito dall'esperienza e volto al miglioramento continuo.

La redazione di un modello di gestione e controllo integrato che si rifaccia a tali indicazioni, accompagnato da un processo di organizzazione e formazione del personale, è un obiettivo certamente più circoscritto, sostenibile e, in taluni casi, anche in parte finanziabile (investimenti e formazione).

Valletta
RELAZIONI PUBBLICHE

Rassegna Stampa

LEXELLENT
Your partner in law.