

1. Riferimenti

Il D. Lgs. 231/2001 ha introdotto nel nostro ordinamento giuridico la responsabilità degli enti derivante dalla commissione di illeciti penali commessi nell'interesse ed a vantaggio della società. Si tratta del concetto di responsabilità amministrativa delle imprese per reati commessi da amministratori, manager o dipendenti, collegando ad esse pesanti sanzioni pecuniarie o interdittive.

Tale disposizione prevede, infatti, l'attribuzione di alcuni tipi di reati non più solo alle persone fisiche che hanno commesso l'illecito, ma anche e soprattutto alle persone giuridiche quali le società per cui lavorano.

2. Scenario

Il D. Lgs. 231/2001 si applica agli enti forniti di personalità giuridica, nonché a tutte le società e alle associazioni anche se prive di personalità giuridica; restano esclusi soltanto gli enti pubblici non economici. L'ente può esimersi dalla responsabilità dotandosi di modelli di organizzazione, gestione e controllo idonei a prevenire il compimento di reati e dimostrandone un'attenta applicazione, coerentemente con il rispetto di un livello di rischio definito accettabile.

3. Obiettivi

Vigilare sul funzionamento, l'adeguatezza e l'effettiva osservanza del modello organizzativo e di gestione.

Tale compito viene svolto attraverso:

- l'accesso a tutte le informazioni dell'Ente, senza necessità di alcun consenso preventivo;
- l'ausilio di tutte le strutture dell'Ente e/o di consulenti esterni;
- l'utilizzo di risorse con capacità consulenziali in tema di attività ispettiva;
- l'adozione di misure idonee a scoprire ed eliminare tempestivamente situazioni di rischio.

4. Soluzione

La necessità di un costante e dettagliato controllo sul modello organizzativo gestionale adottato in ottemperanza alla normativa in questione, da il via libera ad un nuovo approccio, strutturato ed integrato nell'ambito legale, contabile, gestionale, organizzativo ed analitico, attraverso il prioritario ausilio dell' Information Technology.

Limitandoci ovviamente all'area dei sistemi informativi, il nostro approccio prevede:

Configurazione

- analisi e classificazione delle informazioni che rientrano in quest'ambito: il tipo di reato, ruolo o funzione, modalità ed eventi;

S.P.H.E.R.A.E.S.
"Modello organizzativo 231" (D.Lgs. 231/2001)

- delimitazione dell'ambito di riferimento della rischiosità nelle strutture dell'ente (i.e. unità operative, processi, attività e flussi finanziari);
- definizione dei ruoli coinvolti e formale attribuzione delle responsabilità;
- attivazione del dispositivo di delega per l'estensione di specifiche mansioni da parte dei responsabili;
- implementazione di un processo di verifica continua e periodica dell'adeguatezza e correttezza dei dati evento e delle procedure amministrativo-gestionali definite;
- predisposizione ambiente di controllo del singolo dato e di rilevazione e formalizzazione dei controlli in essere (ruoli, responsabilità, strumenti utilizzati, documentazione, conseguenze, etc...);
- definizione del livello di profondità di analisi atteso (processi, sotto processi, attività, rischi, controlli, responsabilità, ...);
- predisposizione della reportistica;
- predisposizione del Sistema di comunicazione al personale: capillare, efficace, autorevole, chiaro e dettagliato, periodico, completo di tutte le componenti del Modello (Codice Etico, modello, flussi informativi, etc.).

Esecuzione

- trasmissione delle risultanze periodiche dell'attività di controllo e delle anomalie e atipicità riscontrate nelle funzioni a rischio;
- verifica della coerenza dei comportamenti e validazione del modello;
- comunicazione informazioni e condivisione osservazioni con l'organismo deputato al controllo;
- gestione delle sanzioni disciplinari nei confronti di chi per negligenza o imperizia non abbiano saputo individuare, e conseguentemente eliminare, violazioni del modello e perpetrazione di reati.

Analisi

- analisi dei rischi relativi all'informativa identificata e delle connesse procedure amministrativo-gestionali definite/da definire;
- analisi dell'adeguatezza del modello e della reale capacità di prevenire i comportamenti non voluti;
- rivalutazione del modello nel recepimento delle risultanze che rendano necessario correzioni ed adeguamenti, verificandone, successivamente, l'attuazione e l'effettiva funzionalità delle soluzioni attuate.

5. Benefici

- standardizzazione ed automatizzazione del modello organizzativo, gestionale e di controllo più adeguato in ottemperanza con la normativa;
- corretta attribuzione delle specifiche responsabilità;
- facilità di accesso e di analisi dei dati grazie alla rigorosa catalogazione;
- controllo sui più significativi rischi di errori e manipolazioni dei dati associati a importanti volumi di transazioni che sistemi informativi invece gestiscono;
- trasparenza dell'informazione e dei flussi informativi aziendali.