Integrazione dei sistemi di gestione del rischio

Dott. Gabriele Sereni

Dottore Commercialista e Revisore Contabile - Studio MGS

D.lgs.231/2001

Analisi del Rischio

ISO 9001:2015

Analisi del Rischio

D.Lgs.231/2007

Analisi del Rischio

ISO 45001

Analisi del Rischio

SISTEMA AZIENDA

ISO 14001:2015

Analisi del Rischio

ISO 37001

Analisi del Rischio

Regolamento Europeo UE 2016/65 (PRIVACY EUROPEA)

Analisi del Rischio

ISO 9001:2015

- La norma 9001:2015 specifica i requisiti che richiedono all'organizzazione di comprendere il proprio **contesto** e di determinare i rischi, come base per la pianificazione. Ciò rappresenta l'applicazione del ***risk-based thinking*** per pianificare e attuare i processi del sistema di gestione per la qualità ed è di supporto nella determinazione dell'estensione delle informazioni documentate.

ISO 9001:2015

- L'organizzazione deve determinare i rischi e le opportunità che è necessario affrontare per:
  - ✓ Fornire assicurazione che il sistema di gestione per la qualità possa conseguire i risultati attesi
  - ✓ Accrescere e/o rendere solidi gli effetti desiderati
  - ✓ Prevenire, o ridurre, gli effetti indesiderati
  - ✓ Conseguire il miglioramento

ISO 9001:2015

- L'organizzazione deve pianificare:
  - Le azioni per affrontare questi rischi e opportunità
  - Le modalità per integrare e attuare le azioni nei processi del proprio sistema di gestione per la qualità;
  - Valutare l'efficacia di tali azioni

Le azioni intraprese per affrontare i rischi e le opportunità devono essere proporzionate all'impatto potenziale sulla conformità di prodotti e servizi.

ISO 45001

- Il nuovo Punto 4 è dedicato all'"**analisi del contesto**" in cui si opera, nonché dei bisogni e delle aspettative delle parti interessate, quali requisiti "propedeutici" alla corretta impostazione di tutto il SGSS. L'obiettivo è quello di comprendere le questioni più importanti del contesto che possono influenzare, positivamente o negativamente, il modo in cui l'azienda affronta le proprie responsabilità in materia di salute e sicurezza.

ISO 45001

- Il nuovo Punto 6 è dedicato alla "**Pianificazione**" del Sistema. Rispetto ai metodi e alle prassi adottati con il precedente standard, il percorso di analisi dei pericoli risulta molto più approfondito e dettagliato, con un focus sui rischi ed opportunità per l'organizzazione.

GDPR: Regolamento Europeo Privacy

- Tra le attività fondamentali vi è il **rischio** **inerente al trattamento** da intendersi come **rischio** di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione *(si vedano artt. 35-36)* tenendo conto dei **rischi** noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali **rischi**

GDPR: Regolamento Europeo Privacy

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DEFINIZIONE

«Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà

(Linee guida del Gruppo di lavoro Articolo 29 WP248rev.1)

GDPR: Regolamento Europeo Privacy

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

ELEMENTI DA CONSIDERARE NELLA INDIVIDUAZIONE DEL RISCHIO

ISO 14001:2015

- Nel pianificare il sistema di gestione ambientale, l'organizzazione deve determinare i rischi e gli impatti ambientali relativi alle proprie attività
- Nello specifico deve dimostrare che la propria struttura ha un sistema di gestione adeguato a monitorare, migliorare e sostenere tutte le attività necessarie per limitare i rischi di impatto ambientale.

ISO 37001:2016

- La norma UNI ISO 37001, applicabile a qualsiasi organizzazione pubblica o privata, a prescindere dal settore di attività, dimensioni o localizzazione geografica, stabilisce dei requisiti per pianificare, attuare e mantenere un sistema di **gestione e controllo dei rischi di corruzione** secondo un approccio che si articola nelle seguenti fasi: analisi e valutazione dei rischi di corruzione, programmazione e attuazione di misure e controlli anti corruzione, sorveglianza sulla loro applicazione e riesame periodico sull'efficacia e adeguatezza del sistema di prevenzione, in modo da assicurarne il miglioramento continuo.

D.LGS.231:2007 (antiriciclaggio)

- La Banca d'Italia ha pubblicato un nuovo documento recante "Disposizioni in materia di Organizzazione, procedure e controlli interni" per il contrasto al riciclaggio ed al finanziamento del terrorismo da parte degli intermediari finanziari.

- Tra i contenuti più rilevanti vi è un forte richiamo all'approccio basato sul rischio nell'individuare, valutare e gestire i rischi connessi al riciclaggio ed al finanziamento al terrorismo.

D.LGS.231:2001 (Modello di Organizzazione, Gestione e Controllo)

- Il D.Lgs. 231 raccoglie al suo interno gran parte dei processi oggetto di analisi richiesti dagli standard di cui alle certificazioni precedentemente illustrate.

- L'approccio richiesto è quello di definizione dei RISCHI collegati a determinati reati previsti dal Decreto in parola.

- Nello specifico alcuni dei reati oggetto di mappatura dei rischi, sono:
  - ✓ Riciclaggio, Ricettazione e impiego di beni provenienti da attività illecita
  - ✓ Sicurezza sul lavoro
  - ✓ Ambiente
  - ✓ Delitti con finalità di terrorismo
  - ✓ Informatici

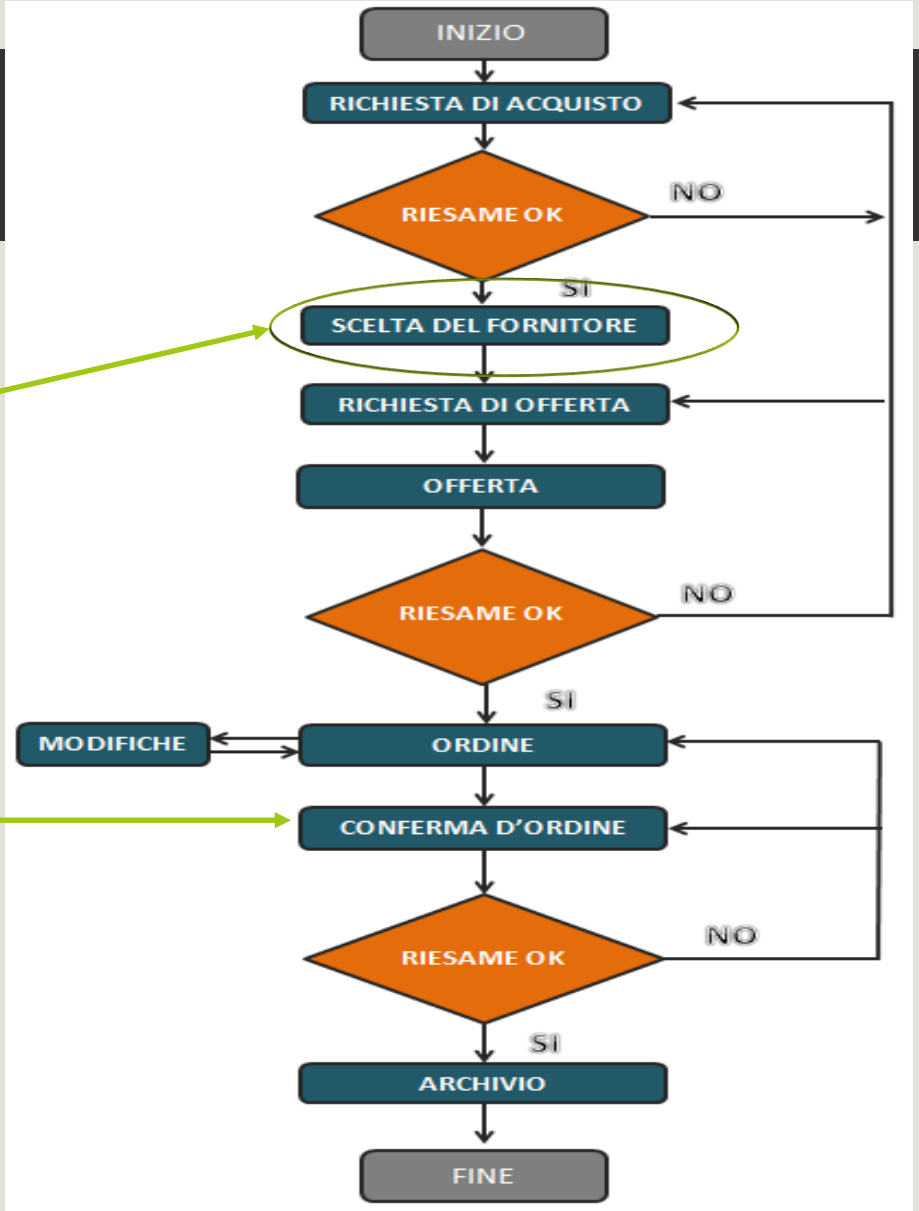
Analisi del rischio

- Per analisi del rischio s'intende l'insieme dei processi di **identificazione** (*risk identification*), di **analisi** in senso stretto (*risk analysis*, a volte *risk evaluation* o anche *risk assessment*) e di **risposta** (*risk response*) al rischio; in alcuni contesti tale insieme viene complessivamente individuato come *processo di gestione del rischio* (*risk management*). In generale, mentre il processo di identificazione definisce i potenziali accadimenti di rischio, l'analisi determina gli effetti degli stessi sul sistema in esame e, infine, il processo di risposta pianifica e mette in opera le azioni di prevenzione e di protezione nonché quelle di monitoraggio e controllo del rischio.

Esempi:

Analisi ai fini 231/2001
- Info ambiente
- Info sicurezza
- Criticità fornitore

Gestione dati privacy contrattualistica



Esempi:

Regolamento Informatico

- Integrazione tra sistema ISO 9001:2015, sistema 231/2001 (reati informatici) e sistema di gestione Privacy.
  - Tutti gli utenti devono essere a conoscenza delle modalità di utilizzo della rete informatica, nonché degli strumenti di controllo a disposizione della Società e, soprattutto delle responsabilità in capo ai singoli soggetti che gestiscono dati "sensibili".

Procedura di selezione del personale

- Integrazione tra sistema ISO 9001:2015, sistema 231/2001 (reati informatici), SGSS (formazione dipendenti) e sistema di gestione Privacy.
  - Vengono disciplinate le modalità di selezione ed assunzione del personale con contestuale consegna del Regolamento Informatico ed illustrazione delle responsabilità dei singoli soggetti coinvolti nel processo anche in relazione ai rischi individuati in sede di analisi ai fini 231/2001 e Privacy (es. Gestione Curricula)

Grazie per l'attenzione

Dott. Gabriele Sereni

Dottore Commercialista e Revisore Contabile - Studio MGS