



Gli eventi di essecome a Sicurezza 2015 (pad. 22, stand M17-N20)

4 novembre 2015 ore 12.00 - Workshop

ISO 31000 Risk Assessment – Applicazioni al mondo del trattamento del denaro

a cura di Vincenzo Pinzolo – ING Progetti

L'idea di base è: come assicurare all'universo bancario e della grande distribuzione il perfetto funzionamento della filiera del trattamento del denaro? Oggi la gestione tradizionale prevede verifiche di parte seconda attuate dagli istituti di credito in un'ottica parziale e poca esaustiva. La risposta arriva invece dalla **norma UNI ISO 31000** "Gestione del rischio-Principi e linee guida".

Il *risk assessment* preso in gestione dalla ISO 31000 può essere esteso, diversificato ed articolato. E tutto ciò in un'ottica di *business continuity* cioè di **continuità del processo produttivo** o di erogazione dei servizi.

I destinatari per l'utilizzo sono rappresentati dai gestori degli aspetti di rischio di qualsiasi attività, sia pubblica che privata, che abbiano bisogno di gestire tutti gli eventi che possano in qualche modo limitare o impattare sulla sua capacità produttiva in modo continuativo, senza blocchi od interruzioni dovuti ad eventi accidentali o imprevisti. Obiettivo finale: offrire uno strumento, una sorta di quadro di riferimento o di schema orientativo, che definisca ed adotti una modalità completa ed efficace di valutazione dei rischi che possono impattare sullo specifico processo e di definire i corrispondenti interventi per prevenire o mitigare gli effetti di tutti gli eventi potenziali ed indesiderati.

La gestione del rischio crea e protegge il valore esprime l'alto concetto di gestione del rischio finalizzato a fare in modo che la filiera trattamento del denaro continui a persistere e svilupparsi nel tempo. La gestione del rischio efficace e strutturata è imprescindibile da una gestione che si prefigga la continuità nel tempo. Immediata conseguenza: **la gestione del rischio è parte integrante di tutti i processi dell'organizzazione.**

La conclusione della corretta applicazione del processo di analisi del rischio è rappresentata dalla certificazione della conformità dello stesso alla ISO 31000 che non può che transitare per un affidabile ente di certificazione.

5 novembre 2015 ore 12.00 - Workshop

Ingegneria della Security – Prospettive di analisi, gestione e trattamento del rischio

a cura di Vincenzo Pinzolo - ING Progetti

Sui temi della Security le aziende e la collettività chiedono risposte all'altezza per quella che viene ormai considerata una vera emergenza culturale. Dedichiamo questo spazio al concetto di "Progettare, realizzare organicamente e monitorare periodicamente la Security" per stimolare il desiderio di contribuire con le proprie conoscenze alla costruzione di un modello di azienda sempre più sicura. Ingegneria della security prende spunto anche dalla ISO 9001 nella revisione 2015 per approfondire un aspetto innovativo qual è la valutazione del rischio finalizzata alla gestione dello stesso. La nuova ISO 9001 introduce infatti come requisito "cogente" il risk assessment quale concetto di valutazione dei rischi esteso a tutto quanto possa minare o comunque limitare la capacità produttiva. Il concetto di valutazione del rischio spazia senza misura, pretendendo che l'azienda affronti e prenda in considerazione tutto ciò che impatta sulla continuità dei processi aziendali.

Ingegneria della security risolve con i seguenti steps:

- osservazione dell'ambiente con esame dell'organizzazione della security on site;
- Analisi di documentazione di supporto;
- Analisi dei rischi suddivisi per area: strutture e tecnologie-risorse strumentali-risorse umane-procedure di gestione ed istruzioni di lavoro.

L'analisi valutativa è suddivisa in:

A) Individuazione di tutti i possibili PERICOLI

B) Valutazione dei RISCHI relativi ad ogni pericolo individuato

- Redazione di una VALUTAZIONE DEI RISCHI correlata con le scelte fatte per luoghi, attrezzature, processi, finalizzata all'individuazione e all'attuazione di idonee misure e provvedimenti. La Valutazione dei Rischi è legata a:
 - location e situazione geo-politico-sociale
 - tipo di attività svolta
 - situazioni determinate da sistemi, strutture ed impianti utilizzati
 - materiali e prodotti coinvolti nei processi.
- Redazione di un PIANO DI PROGETTO (migliorie applicative in termini di strutture, tecnologie, risorse umane e gestione).
- Certificazione da parte di Ente terzo del livello di security raggiunto in funzione di standard di riferimento;
- Monitoraggio continuo.