PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4237 di Mercoledì 16 maggio 2018

Il comitato tecnico 292 non sta mai fermo!

Tutti sappiamo quanto siano preziose le norme per pilotare l'attività dei security manager: due norme che si riveleranno di estrema importanza per impostare correttamente l'analisi di rischio, primo passo verso una vera sicurezza.

I professionisti della security sanno che il primo passo, quando si deve affrontare e risolvere un problema afferente alla security di beni, consiste nell'impostare e sviluppare correttamente una analisi di rischio, identificando tutti i rischi da mettere sotto controllo per poi passare alla fase di attuazione delle misure di mitigazione o prevenzione.

La norma che governa questa attività è l'ormai famosa ISO 31000, che però offre un tracciato, che deve evidentemente essere adattato alle situazioni specifiche.

Ecco la ragione per cui questa norma è accompagnata da altre norme, che affrontano temi più specifici, come ad esempio la gestione della continuità operativa - BCMS, che prende in carico la garanzia che i semilavorati e le materie prime vengano tempestivamente messi a disposizione delle attività produttive.

Desidero ora illustrare due proposte di norme, che indubbiamente potranno attirare l'attenzione dei security manager, in quanto permetteranno di affrontare e risolvere temi affatto peculiari.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[SWGDPR] ?#>

ISO 31050 - Guidance for managing emerging risks to enhance resilience

La resilienza è uno degli aspetti fondamentali che permette all'azienda di fronteggiare situazioni di crisi, mettendo a punto tempestivamente procedure e strutture che permettano, ad esempio, di riprendere al più presto l'attività produttiva.

Per poter garantire un livello soddisfacente di resilienza, occorre sviluppare un'analisi di rischio, che possa prendere in considerazione anche rischi non tradizionali, ma rischi emergenti, dove l'elevato livello di incertezza e il potenziale per la compromissione dell'attività produttiva possono essere drammatici.

L'intento di questa norma è quello che essa diventi parte integrale dell'approccio dell'organizzazione, nei confronti della gestione del rischio.

Questa norma permetterà quindi di ridurre la probabilità che si verifichino questi specifici rischi e metterà sotto controllo eventuali conseguenze negative, legate appunto al verificarsi dell'evento, come ad esempio:

- provvedere ad attrezzare l'organizzazione con la capacità di fronteggiare situazioni inattese in rapida evoluzione,

- sfruttare al meglio ogni opportunità che possa essere legata al verificarsi dell'evento,
- fronteggiare i rischi supplementari con un livello elevato di fiducia,
- offrire una serie di suggerimenti, indirizzati all'alta direzione, legati all'attuazione della norma ISO 31000 alla gestione di rischi emergenti.

È ben chiaro che la gestione di un rischio di questa natura richiede una profonda conoscenza delle modalità di funzionamento dell'organizzazione e dei suoi obiettivi, nel contesto ambientale e operativo.

Per questo motivo, l'obiettivo della norma è quello di definire degli approcci, da concordare a livello internazionale, in grado di mettere sotto controllo questi rischi emergenti e potenzialmente catastrofici, ampliando la gamma dei rischi che attualmente non sono coperti dalle esistenti normative ISO.

Questa norma pertanto rientrerà nella famiglia delle norme ISO 31000 e includerà concetti, principi e metodologie, che potranno assistere l'organizzazione che deve raggiungere i suoi obiettivi.

La struttura della norma, a parte la architettura obbligatoria, come ad esempio lo scopo, i riferimenti normativi, termini e definizioni, simboli ed abbreviazioni, deve coprire numerosi temi, che possono essere illustrati in specifici annessi.

Al proposito, è opportuno far presente che gli eventi che turbano la normale operatività non sempre si verificano in modo drammatico e improvviso, ma possono anche verificarsi come risultato di effetti cumulativi di piccole modifiche, che hanno carattere di progressività.

Le cause che possono portare a situazioni di grave turbamento possono nascere, ad esempio, dalle attese degli azionisti, da nuove strategie adottate dalla concorrenza, da nuove tecnologie, da modifiche del personale addetto, da disponibilità di risorse finanziarie, da requisiti imposti da nuove disposizioni legislative, da atti criminali perpetrati da terzi, dall'impatto di eventi naturali.

È bene ricordare che nessuno di questi elementi sopra elencati è esplicitamente coperto dall'esistenti norme ISO, sviluppate sia dal comitato tecnico 262, sia dal comitato tecnico 292, ed ecco il motivo perché si ritiene opportuno avviare lo sviluppo di una norma con questi contenuti.

ISO 31022 - Risk Management ? Guidelines for the Management of Legal Risk

Passiamo adesso ad esaminare questa seconda famiglia di norme, che viene sviluppata dal comitato tecnico 262.

Anche in questo caso, le organizzazioni operano in un contesto commerciale e sociale oltremodo complesso ed ecco il motivo per cui l'analisi di rischio, condotta secondo la falsariga della norma ISO 31000, ha bisogno di essere costantemente ampliata e spostata su nuovi livelli, sino ad ora mai presi in considerazione.

La norma 31000 è certamente una norma completa, che permette di gestire un gran numero di attività, ma non v'è dubbio che alcune aree richiedano una guida più approfondita; la gestione dei rischi legali è sicuramente una di queste aree.

Oggi le organizzazioni operano in un contesto dove si richiede di essere strettamente conformi a leggi e regolamenti, in tutti paesi in cui l'organizzazione opera. Purtroppo queste leggi e regolamenti possono variare da paese a paese ed occorre che l'azienda abbia una buona conoscenza delle regole del gioco e delle modalità con cui essa deve rispettarle.

Le leggi e regolamenti inoltre sono soggetti a modifiche e anche di questo fatto la direzione aziendale deve tener conto, nell'impostare e mantenere aggiornata l'analisi di rischio.

Ove non si tengano sotto controllo questi fattori, si potrebbero avere conseguenze immediate, significative e negative, che potrebbero avere riflessi sugli aspetti finanziari dell'attività aziendale e perfino portare a possibili responsabilità penali per la alta direzione.

L'obiettivo di questa norma è quello di mostrare come sia possibile utilizzare i principi, illustrati nella norma ISO 31000, per sviluppare una migliore comprensione e miglior gestione degli obblighi legali, regolamentari ed assimilati, che incombono all'azienda.

Queste linee guida intendono quindi aiutare l'organizzazione l'alta direzione nei seguenti campi:

- aiutare l'azienda a raggiungere i suoi obiettivi primari,
- incoraggiare l'adozione di un approccio più strutturato e coerente nella gestione dei rischi legali, laddove questi rischi vengono gestiti in modo proattivo, utilizzando risorse appropriate e facendo ricorso a esperti di adeguato livello,
- comprendere meglio e mettere in evidenza la dimensione e l'impatto dei rischi legali, con conseguente obbligo di attuare procedimenti cautelativi di due diligence,
- identificare e analizzare un più ampio numero di scenari, che possono aiutare nell'assumere decisioni appropriate; infine
- migliorare e incoraggiare l'identificazione di opportunità di continuo miglioramento, che possono manifestarsi nel contesto operativo.

È bene anche sottolineare che l'espressione "rischio legale", che viene usata nella norma, si intende concepita in termini assai allargata e non è solo legata al rispetto di aspetti contrattuali.

Ecco perché tra questi rischi bisogna anche inserire quelli che possono presentarsi nei rapporti con parti terze, anche in assenza di rapporti contrattuali, ma laddove potrebbe nascere la possibilità di contenziosi legali. Ad esempio, lo sviluppo di gas nocivi, in fase di lavorazione di prodotti, può portare alla diffusione di questi gas nelle vicinanze, alla necessità di abbandonare le abitazioni vicine e, di conseguenza, al possibile avvio di azioni legali nei confronti della azienda, da parte dei soggetti che hanno abbandonato la propria abitazione.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.