PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4850 di Venerdì 15 gennaio 2021

Come sviluppare un'analisi di rischio: una guida preziosa

Il comitato tecnico 262, Working group 6 ha pubblicato alla fine di ottobre 2020 un prezioso manuale, che aiuta i professionisti della security a sviluppare un'analisi di rischio, conforme a ISO 31000.

Ormai tutti i professionisti della security sanno bene che il documento cui fare riferimento, nello sviluppare un'analisi di rischio, è la norma ISO 31000.

Questa norma, pur essendo ben fatta, presenta talvolta delle difficoltà di interpretazione ed applicazione ed ecco la ragione per la quale il gruppo di lavoro 6 del comitato tecnico ISO TC 292 ha ritenuto opportuno sviluppare un manuale, composto di ben 38 pagine, per aiutare i professionisti della security in una corretta applicazione della norma stessa.

Il manuale include informazioni sui principi di gestione del rischio, i processi di pianificazione, comunicazione, monitoraggio e riesame, nonché di continuo miglioramento del documento di analisi del rischio.

Con l'occasione, ricordo ai lettori che un altro documento prezioso, per impostare e gestire correttamente l'analisi dei rischi, è la norma IEC/ISO 31010: 2019 Risk management ? risk assessment, nonché la Guide 73: 2009 Risk management vocabulary.

Particolarmente importante è l'adozione di termini standardizzati per permettere di effettuare un confronto fra documenti afferenti a diverse attività e, soprattutto, per consentire una analisi approfondita in caso di contenzioso tra il committente e l'esecutore dell'analisi di rischio.

Ricordo, con l'occasione, che la norma ISO 31000 offre un approccio standardizzato all'analisi di rischio e non è tagliata a misura di una specifica attività industriale o settore operativo. Questo manuale, sviluppato su ripetute pressioni da parte di tutti i soggetti coinvolti, è strutturato in modo da spiegare l'importanza dei seguenti aspetti:

- l'utilizzo di principi di gestione efficiente ed efficace del rischio, illustrando la maniera in cui il rischio può essere gestito,
- lo sviluppo di un piano che permetta di integrare i rischi nella esistente struttura aziendale,
- il miglioramento della cultura organizzativa nei confronti della gestione dei rischi,
- l'applicazione dei processi di gestione del rischio in fase di identificazione, analisi, valutazione e messa sotto controllo del rischio,
- l'impostazione di un programma di comunicazione e consultazione con i soggetti coinvolti,
- la modalità con cui è possibile tenere sotto controllo ed esaminare il processo di gestione del rischio, ed infine,

- il miglioramento costante del documento, sulla base dell'esperienza.

Il documento prosegue riepilogando gli otto principi di gestione del rischio, che permettono di collegare il quadro di riferimento della gestione del rischio agli obiettivi dell'organizzazione coinvolta.

Di particolare interesse il capitolo 3, dedicato al miglioramento continuo della valutazione dei rischi.

In questo contesto viene offerto un prezioso strumento di rilevazione della qualità del miglioramento del documento, utilizzando gli ormai famosi KPI - key performance indicators.

Infine, un paragrafo è dedicato alle modalità con cui è possibile trarre profitto dalle esperienze maturate, sia in senso positivo, sia in senso negativo.

Questo documento si conclude con due annessi, di cui particolarmente interessante è l'annesso B, dove vengono elencati alcuni esempi di categorie di rischio. Si tratta di un documento prezioso, perché se si dimentica di elencare un rischio, si dimenticherà di trattarlo!

Le categorie di rischi illustrate sono le seguenti:

- i rischi finanziari,
- i rischi operativi, che comprendono i rischi di natura tecnologica, quelli legati a beni ed a processi ed i rischi legati all'ambiente,
- i rischi collegati alla strategia aziendale.

Adalberto Biasiotti

---

www.puntosicuro.it