PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3891 di mercoledì 09 novembre 2016

Il comitato ISO/TC 292 sta cercando di migliorare la norma ISO 34001

La norma che offre indicazioni per verificare l'autenticità, l'integrità e l'affidabilità di prodotti e documenti aziendali è in corso di riesame e miglioramento. Di Adalberto Biasiotti.

I lettori sono certo già al corrente dell'esistenza della norma ISO 34001, che offre indicazioni per verificare l'autenticità, l'integrità e l'affidabilità di prodotti e documenti aziendali. Questa norma, alla luce dell'evoluzione dello scenario mondiale su queste critiche situazioni, è in corso di riesame e miglioramento.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

Ecco il titolo esatto della norma*: ISO/DIS 34001.4- Security and resilience ? Security management system for organisations assuring authenticity, integrity and trust for products and documents.*

Ricordo che il prefisso DIS significa DRAFT INTERNATIONAL STANDARD e il documento elaborato dall'ormai noto ISO/TC 292.

La edizione precedente della norma trattava argomenti fondamentali che riepilogo brevemente: la gestione dei rischi legati a beni tangibili e intangibili dell'azienda e l'obiettivo era quello di mettere a disposizione uno strumento, in grado di garantire alla organizzazione l'autenticità, l'integrità e l'affidabilità dei suoi prodotti e documenti.

I rischi che venivano presi in considerazione erano i seguenti:

- atti fraudolenti,
- atti compiuti deliberatamente da un concorrente o un avversario commerciale
- atti criminosi in genere,
- negligenze intenzionali e
- negligenze non intenzionali ma che possono avere conseguenze assai negative per l'organizzazione.

Come di consueto, le indicazioni della norma sono affatto generiche e devono essere tagliate a misura della specifica struttura che intende adottare queste linee guida.

In particolare, l'azienda deve rendersi conto che queste indicazioni coinvolgono le sue relazioni con soggetti terzi, come ad esempio fornitori, appaltatori, aziende di trasporto, clienti, e via dicendo. Quando l'azienda decide di affidare all'esterno un qualunque processo critico, coinvolto dei temi sopra illustrati, deve accertarsi che questo soggetto terzo sia in grado di rispettare la continuità logica delle misure di prevenzione e messa sotto controllo del rischio.

Anche se la norma mette in evidenza i rischi di origine informatica, essi non vengono presi in considerazione da questa norma, perché vengono già analizzati da altre norme specifiche, come ad esempio ISO/IEC 27001.

Infine è bene chiarire ancora una volta che l'obiettivo primario della norma è quella di mettere sotto controllo rischi di origine antropica, sia endogeni, sia esogeni. Rischi di natura accidentale o incidentale non sono presi in considerazione in questa norma.

I lettori, che desiderano saperne di più sull'evoluzione di questa nuovo progetto di norma, devono seguire i lavori del già menzionato comitato tecnico ISO/TC 292.

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.
