L'analisi dei rischi. Un approccio con la logica Fuzzy

Author : Lorenzo Schiavina

Date : 19 luglio 2018

Il rischio è il risultato finale, diretto, indiretto o consequenziale ad un'azione volontaria, involontaria o ad un evento accidentale ed è determinato di norma come il prodotto fra la probabilità che un evento pericoloso si realizzi e l'impatto (danno) da questo provocato.

Le aziende devono svolgere una attività continua di analisi del rischio in diversi ambiti:

- **rischi operativi** (quali perdita di beni di qualunque tipo, siano essi tangibili o intangibili...);
- **rischi di conformità** (derivanti dalla violazione di normative...);
- **rischi legali** (quali cause con le controparti, quali clienti, fornitori, dipendenti...);
- **rischi reputazionali** (derivanti da eventi che possono ledere l'immagine dell'organizzazione…).

o come prevede il GDPR:

- **il rischio per i diritti e le libertà delle persone fisiche**

Le varie categorie di rischio non sono fra loro distinte ed autonome.

La violazione di una normativa, ad esempio, può comportare sia una sanzione (e relativa perdita economica), sia un impatto sulla reputazione dell'azienda.

Inoltre, se la sanzione ha conseguenze operative (ad esempio il blocco dei trattamenti di dati personali e la conseguente impossibilità di erogare un servizio) può portare anche a cause con la clientela per mancato rispetto dei contratti di fornitura.

Si creano così catene di relazioni che rendono difficile valutare con precisione il reale impatto di un evento. Questa valutazione può avvenire infatti a diversi livelli e con diversi gradi di complessità.

È possibile ridurre il rischio intervenendo su **impatto** e **probabilità,** adottando adeguate

contromisure che possono ridurre uno o entrambi i fattori.

L'implementazione di contromisure ha ovviamente un costo, che deve essere vantaggioso, rispetto alla riduzione del rischio derivante dalla loro implementazione.

Per tale motivo si effettua in genere un'**analisi del rischio** prima (Rischio inerente) e dopo l'implementazione delle contromisure (Rischio residuo).

In questo modo è possibile valutarne quale potrebbe essere l'efficacia.

La valutazione di dove sia più conveniente intervenire e quali contromisure adottare è uno degli aspetti più importanti che consegue ad una corretta analisi dei rischi.

Esistono anche altre modalità per affrontare un rischio (oltre che gestirlo) quali:

- evitarlo non mettendo in atto le azioni che possono determinarlo;
- trasferirlo a soggetti che istituzionalmente si occupano di gestirlo, come le assicurazioni o tramite opportune clausole contrattuali;
- accettarlo, non mettendo in atto alcuna azione.

È comunque importante notare che il soggetto che effettua l'analisi del rischio non è necessariamente il soggetto che è esposto al rischio stesso.

È il caso sopracitato della valutazione dei rischi del GDPR, dove il rischio valutato non è quello dell'azienda o dei sui asset, ma dei soggetti interessati di cui l'azienda tratta i dati.

Comprendere questo aspetto è fondamentale in quanto si tratta quindi di un rischio non disponibile, che l'azienda dovrebbe in ogni caso ridurre assolutamente al minimo.

Da lì la necessità, nei casi di rischio elevato, di condurre una PIA.

Per condurre un'analisi dei rischi esistono numerosissimi strumenti e relative catalogazioni.

Fra le consigliate quella di ISCOM e quella di ENISA:

http://www.isticom.it/index.php/archivio-pubblicazioni/3-articoli/111-news-pub9

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

Tab. 1 – Tipologie di analisi dei rischi secondo la Linea guida ISCOM – Risk analisys approfondimenti

Qualitativo valutazione del rischio su una scala qualitativa (ad esempio alto, medio, basso).