Gestione del rischio: dagli standard ISO alle applicazioni per i sistemi a supporto delle decisioni (DSS)

Author : Marco Carbonelli

Date : 16 Gennaio 2020

I concetti di *rischio* e di *gestione del rischio* negli ultimi 15 anni hanno trovato applicazione in un numero di settori operativi sempre più ampi, a volte anche non strettamente tecnici, come per il caso nel nostro Paese nell'ambito della **prevenzione della corruzione** [Car1, Car2].

È proprio in questa tipologia di casi che ci si può imbatte in applicazioni piuttosto innovative, non sempre di immediata comprensione, specie quando l'applicazione esula dai settori tradizionali e si propone ad una platea di utilizzatori non prettamente di formazione tecnico-scientifica.

Se, ad esempio, in ambito finanziario e bancario, nell'ambito della protezione civile, dell'*intelligence* e della difesa, della sicurezza sul lavoro e nella protezione delle informazioni e delle reti informatiche, l'applicazione delle metodologie strutturate di *risk management* risalgono già in gran parte al secolo scorso, significative **nuove applicazioni** sono state introdotte nel tempo, anche nell'ambito della valutazione rischio legato a nuove attività imprenditoriali, nuove linee di produzione, così come alla salute delle persone nei luoghi di lavoro, nelle scuole e in ambienti di pubblico accesso e di ritrovo, nell'ambito delle infrastrutture critiche e dei servizi essenziali. In questo lavoro, facendo riferimento alla letteratura tecnica e allo standard di riferimento sul tema dei Principi del *risk management*, la **norma ISO 31000**, si introducono le definizioni fondamentali del rischio e i concetti legati alla sua gestione declinata, come vedremo, nelle fasi di identificazione, analisi, valutazione e trattamento. A conclusione dell'analisi tecnica svolta si evidenziano e discutono sinteticamente le applicazioni sempre più diffuse dei sistemi a supporto delle decisioni (DSS) che hanno, proprio nella fase di valutazione del rischio, un ruolo fondamentale in ausilio ai decisori, sia a livello tecnico sia a livello politico.

La definizione del rischio

Nel campo della gestione dei disastri e delle emergenze la definizione del rischio è da sempre orientata a evidenziare aspetti di natura negativa, i cosiddetti danni o impatti, che si realizzano in termini di conseguenza al verificarsi di un determinato evento di origine naturale o antropica.

Se si fa riferimento alla **letteratura tecnica internazionale** [Sot1], davvero molteplici sono le diverse definizioni di rischio che nel corso del tempo sono state proposte: in Tab.1 sono elencate, nella loro versione originale in lingua inglese e in diversi ambiti tecnici, dieci definizioni ritenute rilevanti, in un percorso storico che parte dagli anni'70 dello scorso secolo fino ad arrivare al decennio scorso.

Se si rimane in questa declinazione (danni e impatti dovuti ad un evento) della definizione di rischio, una declaratoria che cerca di omogenizzare i tentativi riportati in Tab.1 potrebbe essere la seguente [Car3]:

"*il rischio fornisce una misura della potenzialità di un danno dovuto al possibile accadimento di un evento (naturale, dovuto ad attacco terroristico o militare, o ad un'incidente di natura antropica)*".

Proprio nel 2009, però, l'uscita dello standard ISO 31000 [ISO1] ha proposto un approccio più generico per la definizione del rischio, approccio che con flessibilità si può orientare sia in direzione negativa (danno) sia in direzione positiva (vantaggio) per i risultati ottenuti al concretizzarsi di un particolare evento. Per l'ISO 31000 "*il rischio è l'effetto dell'incertezza sugli obiettivi*".

Tab.1 – Diverse definizioni di rischio presenti nella letteratura tecnica internazionale [Sot1].

1. Risk is the measure of probability and the weight of undesired consequences (Lawrence, 1976).
2. Risk equals the product of probability and severity (Wilson & Crouch 1982).
3. Risk is a combination of five primitives: outcome, likelihood, significance, causal scenario and population affected (Kumamoto & Henley, 1996).
4. Risk is a situation or event where something of human value (including humans themselves) has been put at stake and where the outcome is uncertain (Rosa 1998).
5. Risk is the expression of influence and possibility of an accident in the sense of the severity of the potential accident and the probability of the event (MIL-STD-882D, 2000).
6. Risk is a combination of the probability and scope of the consequences (Risk Management Vocabulary ISO 2002).
7. Risk is an uncertain consequence of an event or activity related to something of human value (IRGC, 2005).
8. Risk equals expected damage (Campbell, 2005).
9. Risk is the likelihood of an injury, disease or damage to the health of employees due to hazards (Law on Safety and Health at Work, 2005).
10. Risk refers to uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value (Aven & Renn, 2009).

Nelle prossime sezioni dell'articolo sarà discusso e descritto il concetto di *risk management* così come viene introdotto negli standard ISO 31000 e 31010 [ISO1, ISO2] e nella guida ISO 73 [ISO3], soffermandosi sui concetti di *risk assessment* (Valutazione del Rischio) e *risk analysis* (Analisi del Rischio).

Gli standard e il *risk management*: la ISO 31000 e la ISO 31010

Nel 2009, come detto, l'ISO (*International Organization for Standardization*) ha reso pubblici lo standard ISO 31000 su "Gestione del rischio – Principi e linee guida" (aggiornato successivamente nel 2018) e lo standard ISO 31010 su "Gestione del rischio – Tecniche per la valutazione del rischio".

La ISO 31000 si pone l'obiettivo dichiarato di **armonizzare** i concetti del *risk managemnt* fino a quel momento emersi in diversi campi scientifici, in modo da offrirsi come "standard di riferimento" per il presente e il futuro in questo settore in forte sviluppo da allora in avanti. In questo senso, la ISO 31000 non è da considerarsi uno standard da applicare per ottenere una 'certificazione di conformità', cioè un bollino di qualità rilasciato da terze parti, come in altri casi di standard ISO. La ISO 31000 costituisce solo un approccio di principio, che vuol essere valido per tutti i settori, al tema della gestione del rischio, con lo scopo di uniformare vocabolario, linguaggio d'uso e fasi del processo di gestione (vedi fig.1) fino ad allora piuttosto variegate nei diversi settori.

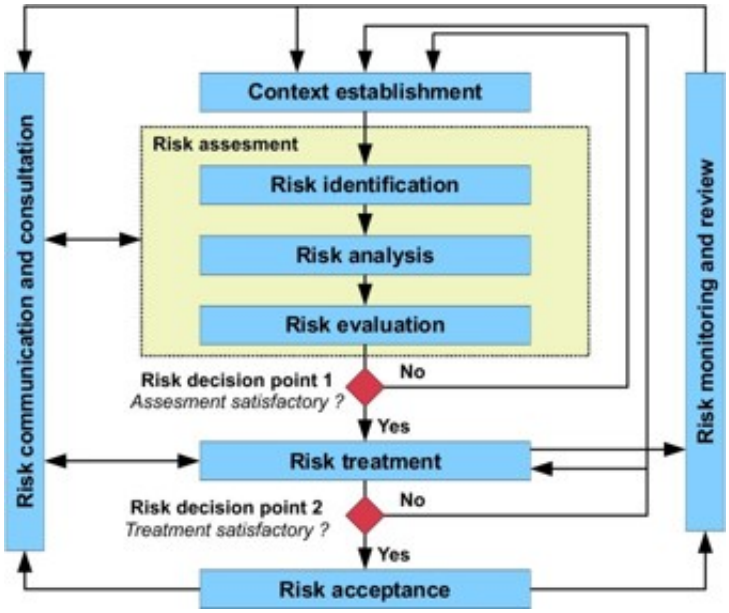

Fig.1 – Rappresentazione grafica delle fasi del processo di Gestione del Rischio in analogia all'approccio della ISO 31000.

Nella ISO 31000 [ISO1] il *risk management* (Gestione del Rischio) è definito come l'insieme di attività coordinate per dirigere e controllare un'organizzazione per quanto riguarda i rischi a cui è esposta. In altre parole, il *risk management* può essere considerato come il **processo sistematico** che consente di identificare, analizzare, valutare e mitigare il rischio.

Nello Standard il rischio, come detto, è definito genericamente come *'l'effetto dell'incertezza sugli obiettivi*', specificando che:

- un **effetto** è lo scostamento rispetto al risultato atteso, sia in senso positivo che negativo;
- gli **obiettivi** possono coprire diversi settori - come ad esempio gli ambiti finanziari, la salute e la sicurezza delle persone, la tutela dell'ambiente - e possono essere applicati a diversi livelli – il livello strategico, il livello organizzativo, l'ambito della produzione e dell'operatività;
- il **rischio** è solitamente caratterizzato dall'accadimento di eventi e di conseguenze di questi eventi, ed è valutato in termini di valore delle conseguenze di un determinato accadimento e probabilità di occorrenza dell'evento;
- l'**incertezza** costituisce la componente non conosciuta associata alla probabilità dell'evento e alle conseguenze che ne derivano nella pratica.

Va anche sottolineato che il concetto di Rischio è applicato in diversi ambiti della società, dall'ambito pubblico (rischio salute, rischio calamità naturali, rischio sicurezza nazionale) al settore privato e produttivo (rischio d'impresa, rischio aziendale, rischio d'investimento…)

Le **istituzioni pubbliche** sono tipicamente interessate a:

- ridurre l'impatto di eventi catastrofici, in termini di:
  - riduzione dei morti e feriti gravi;
  - danno all'economia;
  - mantenimento della qualità di vita della popolazione;
  - danni agli interessi nazionali;
  - danno d'immagine;
- individuare gli 'asset' da proteggere;
- prioritizzare le attività per attuare la riduzione del rischio;
- svolgere azioni di prevenzione e consapevolizzazione;
- coordinare al meglio gli interventi di eventuale soccorso.

In questo caso, dunque, l'approccio è orientato alla riduzione delle conseguenze di un evento sulla qualità della vita dei cittadini.

Invece, gli **operatori privati** e, in generale, gli **investitori**, sono interessati a:

- ridurre l'impatto delle perdite in termini di:
  - danni economici sulle infrastrutture produttive;
  - fatturato;
  - immagine;
  - salute dei dipendenti;
- prioritizzare le attività di riduzione del rischio;
- proteggere la parte *core* del loro business;
- trasferire, dove conveniente, i rischi più rilevanti e non direttamente gestibili su terze parti, con l'intervento di coperture assicurative.

In fig.2 è rappresentato in forma sinottica un confronto tra il settore pubblico e quello privato per quanto attiene le caratteristiche della Gestione del Rischio.

Risk management: istituzioni vs. aziende

Istituzioni	Aziende
Beni da proteggere	
Popolazione Economia nazionale Ambiente/territorio ...	Business Fatturato Immagine ...
Tipo di rischio considerato	
Ambientale (terremoto, inondazione...) Tecnologico Attentati ...	Finanziario Investimento Concorrenza ...
Contromisure	
Legislative Preventive Coordinamento interventi	Assicurative Preventive ...

Fig.2 – Differenze nella Gestione del Rischio tra il settore Pubblico e quello Privato [Car4].

Questi punti di vista diversi, a volte totalmente complementari, hanno imposto nell'ultimo decennio una sempre maggiore necessità di coordinamento tra il settore Pubblico e quello Privato al fine di contrastare pericoli naturali e minacce antropiche di varia natura per ridurre il rischio cumulativo che insiste sulla **popolazione** e sulle **attività produttive** nella complessa società moderna. Proprio questa necessità di coordinamento e integrazione delle vedute ha consentito di avviare, sostanzialmente in tutti gli Stati occidentali, un processo di incremento e ottimizzazione della *robustezza* e della *resilienza* (fig.3) di infrastrutture, servizi essenziali, processi operativi e sistemi tecnologici.

Fig.3 – Settore Pubblico e quello Privato: una integrazione possibile per incrementare robustezza e resilienza [Car4].

Ma cosa si intende precisamente con ***robustezza*** e ***resilienza*** in questo specifico caso?

Con ***robustezza*** intenderemo [Car3,Car4]. la capacità di resistere ad una minaccia - o ad un pericolo naturale - senza sostanziale alterazione del bene o servizio offerto alla popolazione e senza impatto significativo sulla salute delle persone.
La *robustezza*, in sostanza, mira ad evitare che la minaccia abbia effetti su popolazione, sui servizi e sui beni.

Con ***resilienza*** per uno Stato, una Istituzione o una Azienda intenderemo [Car3,Car4] la capacità, di fronte al realizzarsi di una minaccia o pericolo naturale, di recuperare lo *status quo* precedente all'evento, *adattandosi* alla nuova situazione e trovando eventualmente modalità alternative di comportamento, di operatività e di funzionamento.
La *resilienza* mira sostanzialmente ad ottimizzare le operazioni di recupero dopo l'accadimento dell'evento.

Nella fig.4 è riportata una interessante definizione sintetica [Car3] che contrappone le due caratteristiche salienti di *robustezza* e *resilienza*: da un primo lato, si necessita di un rafforzamento delle parti di un sistema, dall'altro lato si necessita di capacità di adattamento, di flessibilità e di riconfigurazione degli elementi del sistema. Due caratteristiche che possono confliggere e che comportano scelte diversificate già in sede di pianificazione delle risorse da usare e delle azioni da intraprendere per ridurre il rischio.

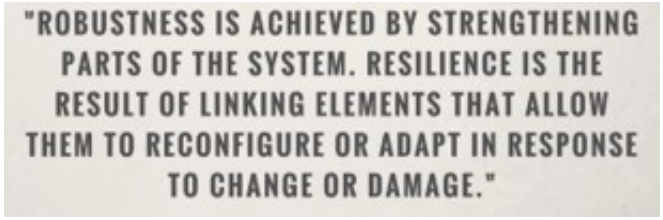

Fig.4 – Settore pubblico e privato: un'integrazione possibile per incrementare robustezza e resilienza.

Tornando ora allo standard ISO 31000, in cui si descrive sostanzialmente come mostrato in fig.1 il processo della Gestione del rischio, si evidenzia come in esso si adotti [Car4] come metodologia quella del ciclo PDCA (Plan/Do/Check/Act). Il ciclo PDCA, sviluppato negli anni 1920 da Walter Shewhart, è stato successivamente reso popolare da W. Edwards Deming e consiste sinteticamente in quattro fasi:

- *Plan* - cosa fare e come farlo (pianificazione) per soddisfare politica e obiettivi che si sono determinati

- *Do* - porre in atto quanto pianificato
- *Check* - verificare se si è fatto quanto pianificato e se quanto fatto risulta efficace al raggiungimento degli obiettivi
- *Act* - come e cosa migliorare?

Fig.5 – Ciclo Plan/Do/Check/Act applicator negli standard ISO.

Tenendo in mente questo approccio metodologico, si può rilevare che la fig.1 rappresenta il dettaglio delle azioni da svolgere in un ciclo di Deming specifico per il *risk management*. In particolare si evidenziano le seguenti fasi/azioni:

- **Definizione degli ambiti, del contesto e dei criteri dell'analisi**, delimitando in modo puntuale il processo/sistema sotto esame.
- **Conduzione della Valutazione del Rischio (*risk assessment*),** che è ripartibile in tre sottofasi distinte (Fig.6):
    - **Identificazione del Rischio** (*risk identification*)
    - **Analisi del Rischio** (*risk analysis*)
    - **Ponderazione del Rischio** (*risk evaluation*)

Lo scopo della valutazione del rischio è quello di determinare nel modo più oggettivo possibile se il rischio sia tollerabile, e quindi accettabile, o se risulti troppo alto e, quindi, necessiti di azioni di mitigazione al fine di ridurne il valore.

Fig.6 – Rappresentazione grafica delle sottofasi della Valutazione del Rischio: identificazione, analisi e ponderazione.

- **Trattamento del Rischio** (Risk Treatment), tipicamente suddiviso in due sotto fasi, mitigazione del rischio attraverso contromisure adeguate, accettazione del rischio residuo.

Come mostrato in fig.1, alle fasi centrali del processo di Gestione del Rischio sin qui esaminate si aggiungono le fasi trasversali di:

- **comunicazione e consultazione** con i soggetti/esperti coinvolti nella gestione/fruizione del processo;
- **monitoraggio e revisione** dei risultati, delle metodologie e delle azioni attuate nelle diverse fasi del processo di gestione.

Tornando alla definizione del rischio, in accordo con la ISO 31000 ma introducendo un punto di vista applicativo e pragmatico da applicare in ambito di disastri naturali, attacchi terroristici convenzionali e non convenzionali, ma anche in disastri di origine antropica, come il caso di incidenti in ambito industriale, possiamo considerare il rischio come una combinazione tra la probabilità di accadimento di un determinato evento e le conseguenze generate dall'evento stesso. In questa visione più applicativa, le conseguenze sono da considerare dei danni, quindi degli effetti negativi, prodotti dall'accadimento dell'evento (si immagini un disastro naturale ad esempio) e possono essere espresse in termini di **diversi punti di vista**: *impatti sulla salute e sulla vita delle persone, impatti economici, impatti ambientali e anche impatti socio/politici*.

La **valutazione del rischio** a questo punto può immaginarsi condotta [ISO1,ISO2] seguendo una delle seguenti tre distinte modalità concettuali:

- in termini **qualitativi** (ad esempio dividendo in tre fasce il rischio: Alto, Medio, Basso), analizzando la combinazione dei danni subiti e della probabilità di accadimento dell'evento, a loro volta valutando anche queste due variabili con criteri qualitativi;
- in termini **semiquantitativi**, cioè usando delle scale numeriche che però non assumono un valore assoluto ma, al contempo, che consentano di tradurre in numeri,

successivamente confrontabili in modo relativo, la probabilità dell'evento, il danno e il rischio. In questo caso le scale numeriche possono essere di tipo lineare o logaritmico, a seconda dei casi specifici considerati e della variazione in *magnitudo* delle due variabili *probabilità dell'evento* e *danno* alla base della valutazione del rischio;
- in termini **quantitativi**, cioè usando delle scale di valutazione numerica con significato assoluto (*probabilità dell'evento* quindi espressa in termini matematici – ad esempio: 1/100; 1/1000 etc; *danni* espressi – ad esempio - in numero di morti e feriti gravi da ospedalizzare, oppure *danni* misurati dal punto di vista economico in termini di migliaia/milioni di euro/dollari, e così via).

Va qui puntualizzato che il più delle volte l'analisi *quantitativa* risulta impossibile da svolgere per la *mancanza di dati puntuali e affidabili* e, più in generale, per le ridotte informazioni disponibili a chi svolge l'analisi. In questi casi, quando comunque una valutazione del rischio risulta necessaria, è opportuno fare riferimento alle prime due modalità, scegliendo come metodo preferito quello *qualitativo* quando le informazioni disponibili sono scarne o quando ci si può accontentare di una valutazione del rischio approssimativa.

È opportuno, dopo il concetto di valutazione del rischio, specificare anche il concetto di *analisi delle conseguenze* (*consequence analysis*), spesso indicata come *analisi d'impatto* (*impact analysis*): con questo tipo di analisi si valutano la natura e l'ampiezza di un *danno* (sinonimo in questo caso di impatto e conseguenza) una volta che l'**evento si sia realmente presentato**. Come detto in precedenza le conseguenze di un evento possono essere osservate da diversi punti di vista: si può essere interessati allo stato di salute delle persone, al numero di morti o ai danni economici e ambientali, fino anche agli impatti socio/politici che si vengono a determinare dopo l'evento.

Minacce, vulnerabilità, esposizione, impatto e rischio: quali relazioni matematiche?

Nella sezione precedente, con riferimento agli Standar ISO, abbiamo introdotto gli elementi fondamentali che contribuiscono a definire il rischio.

Nel prosieguo di questo articolo il *Rischio* (*R*) sarà sistematicamente considerato come una combinazione delle variabili riconducibili ai concetti di *Minaccia* (*M*), *Vulnerabilità* (*V*) e *Esposizione* (*E*) [EuC2,Car3,Car4]. Quindi, queste tre grandezze (*M*, *V*, *E*) risulteranno nella nostra analisi i pilastri per svolgere una valutazione del rischio.

In senso matematico possiamo quindi scrivere questa prima relazione generale di rischio come:

(1) $R = f(M, V, E)$.

Introduciamo ora le seguenti definizioni di *Rischio*, *Minaccia*, *Vulnerabilità* ed *Esposizione* che applicheremo nel seguito [Car3,Car4]:

- il *Rischio* (*R*) fornisce una misura della potenzialità di un danno dovuto al possibile

accadimento di un evento (naturale, dovuto ad attacco terroristico o militare, o a un'incidente di natura antropica);
- una *Minaccia* (*M*) – a volte indicate anche come *Pericolo* (*P*) – rappresenta la probabilità che un evento, accidentale o intenzionale, occorra realmente;
- una *Vulnerabilità* (*V*) rappresenta una possibile debolezza di un sistema, di una procedure, del genere umano, o di una infrastruttura o territorio geografico che può portare a un danno se la minaccia si presenta nella realtà;
- l'*Esposizione* (*E*) rappresenta la massima ampiezza potenziale del danno che una minaccia può provocare. In letteratura questa grandezza è a volte indicata con il concetto di *Bene* (*Asset*) [DHS1];
- la *Conseguenza* (*C*) – o *Impatto* (*I*) – rappresenta il reale danno subito come risultato del presentarsi della minaccia in uno specifico ambito.

Introdotte queste grandezze, con una matematica elementare e sotto ipotesi che verranno discusse nel seguito, si possono scrivere le seguenti relazioni [Car3,Car4,EuC1]:

(2) $R = M \cdot V \cdot E$

(3) $I = C = V \cdot E$

(4) $R = M \cdot I = M \cdot C$.

Queste relazioni matematiche risultano applicabili fino a che le variabili *M*, *V* e *E* si mostrano indipendenti tra loro, e, in generale, questo si realizza in tutti i casi di disastri naturali.

Quando, invece, il valore dell'impatto *I* influenza la probabilità di accadimento della minaccia *M*, come succede per esempio nei casi di **attacchi terroristici** dove l'impatto può condizionare la scelta di luogo e modalità di attacco, il rischio non può più esser espresso come un semplice prodotto delle grandezze qui introdotte ma deve tornare a una formulazione più complessa, del tipo di quella generale introdotta in (1), con la necessità di analisi delle interdipendenze tra le diverse variabili.

Riassumendo possiamo affermare che, tenendo sempre conto del particolare rischio considerato nell'analisi, la valutazione del rischio può essere condotta considerando **diverse variabili e fattori**, che dipendono dalla complessità dei modelli usati per caratterizzare le grandezze e dal livello di precisione delle misure/stime disponibili nel caratterizzarle.

Quando un approccio *quantitativo* incrementa nella sua complessità matematica senza aggiungere 'accuratezza' (in termini di affidabilità e precisione) dei dati considerati nella valutazione del rischio, è fortemente consigliato il suo abbandono, per procedere con un approccio alternativo meno rigoroso quale quello *qualitativo* o *semiquantitativo* che consente una maggiore efficienza nell'uso delle risorse – di tempo e di calcolo - e un livello di trasparenza maggiore nei risultati raggiunti, approssimativi per definizione con questi due approcci.

Seguono quest'ultimo principio di base alcuni importanti per quanto semplici strumenti

matematici che vengono proposti in letteratura, come ad esempio il caso della **matrice conseguenze/probabilità** [ISO2]. Questo strumento consente di combinare a livello qualitativo o semiquantitativo i ‘*livelli*’ di conseguenza e probabilità che caratterizzano una situazione di potenziale rischio per produrre il ‘*livello*’ di rischio da utilizzare in una possibile classifica comparativa di diversi rischi: due esempi di questa matrice sono mostrati in fig.7.

Il formato peculiare della matrice e la definizione dei *livelli* ad essa applicati dipenderà dal contesto nel quale la matrice viene usata e sta all’abilità dell’analista del rischio proporre approcci congruenti con le diverse situazioni analizzate.

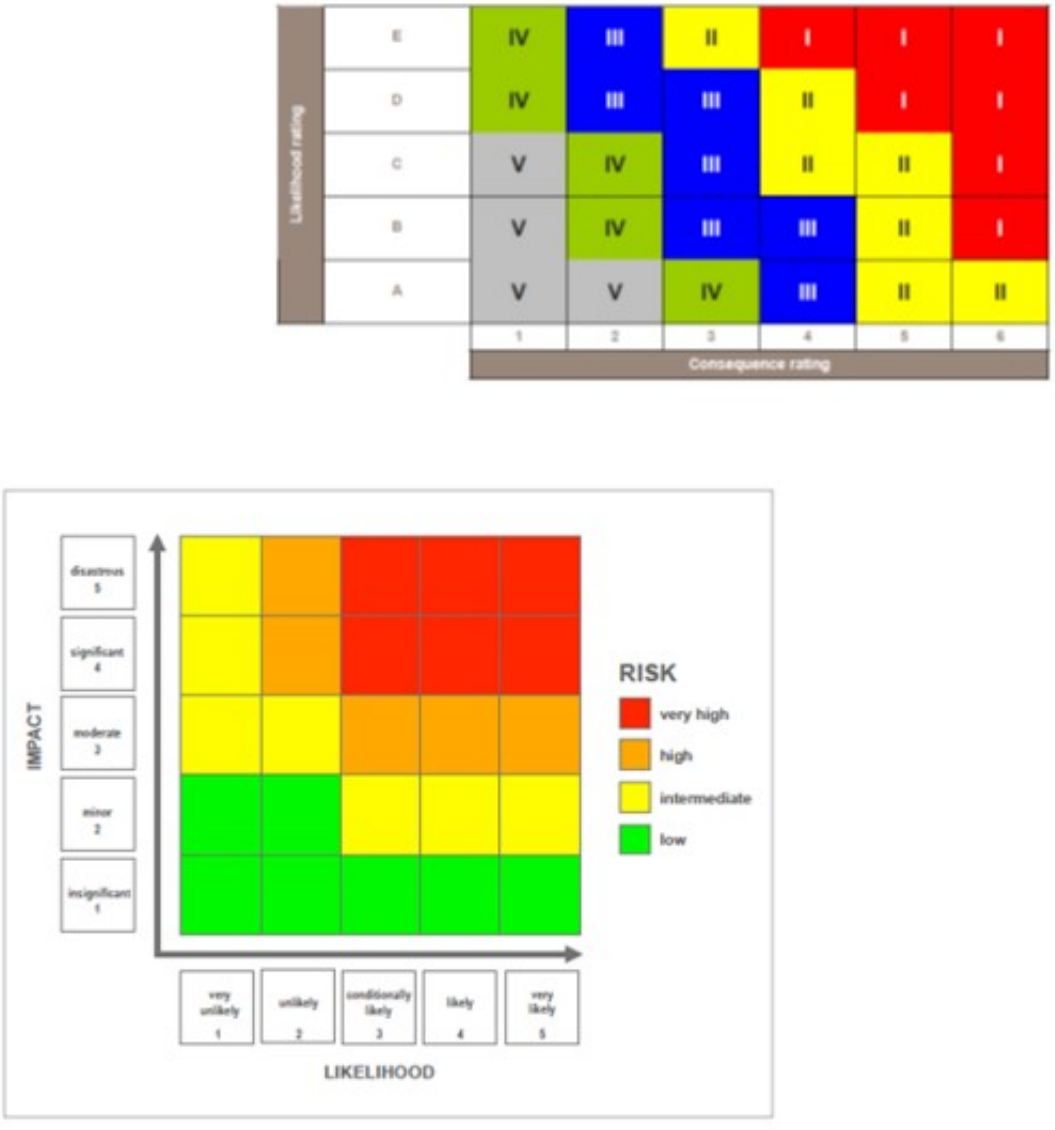

Fig.7 – Due esempi diversi di matrici conseguenza/probabilità: il primo derivante dall’approccio descritto nella ISO 31010 [ISO2], il secondo proposto per applicazioni di protezione civile [Kom1].

Un esempio pratico dell’efficacia di questo tipo di rappresentazione è mostrato in fig.8 dove è

riportata la matrice dei rischi globali prodotta annualmente dal World Economic Forum con un approccio *semiquantitativo*.

Nella fig.8 emerge, ad esempio, come la valutazione degli esperti mondiali posizioni il rischio dell'uso di armi di distruzione di massa (*Weapons of Mass Destruction* o WMD) a un valore di conseguenza (*Impact*) molto alto nella scala dei livelli (intorno a valore 4 su 5), anche più alto dell'impatto dovuto ai cambiamenti climatici e alle condizioni estreme metereologiche, ma con una probabilità di occorrenza (*Likelihood*) più bassa (intorno a valore 2,5 su 5) rispetto a tutti gli altri rischi presenti nella matrice.
Dati questi valori, applicando in prima approssimazione la formula (4) con *M* uguale al valore numerico del livello di *probabilità* e *I* (o l'equivalente *C*) uguale al valore numerico del livello di *impatto*, si può con facilità associare un valore di livello di rischio e costruire una **classifica vettoriale** dei diversi rischi qui considerati [EuC1,Car1, Car2].

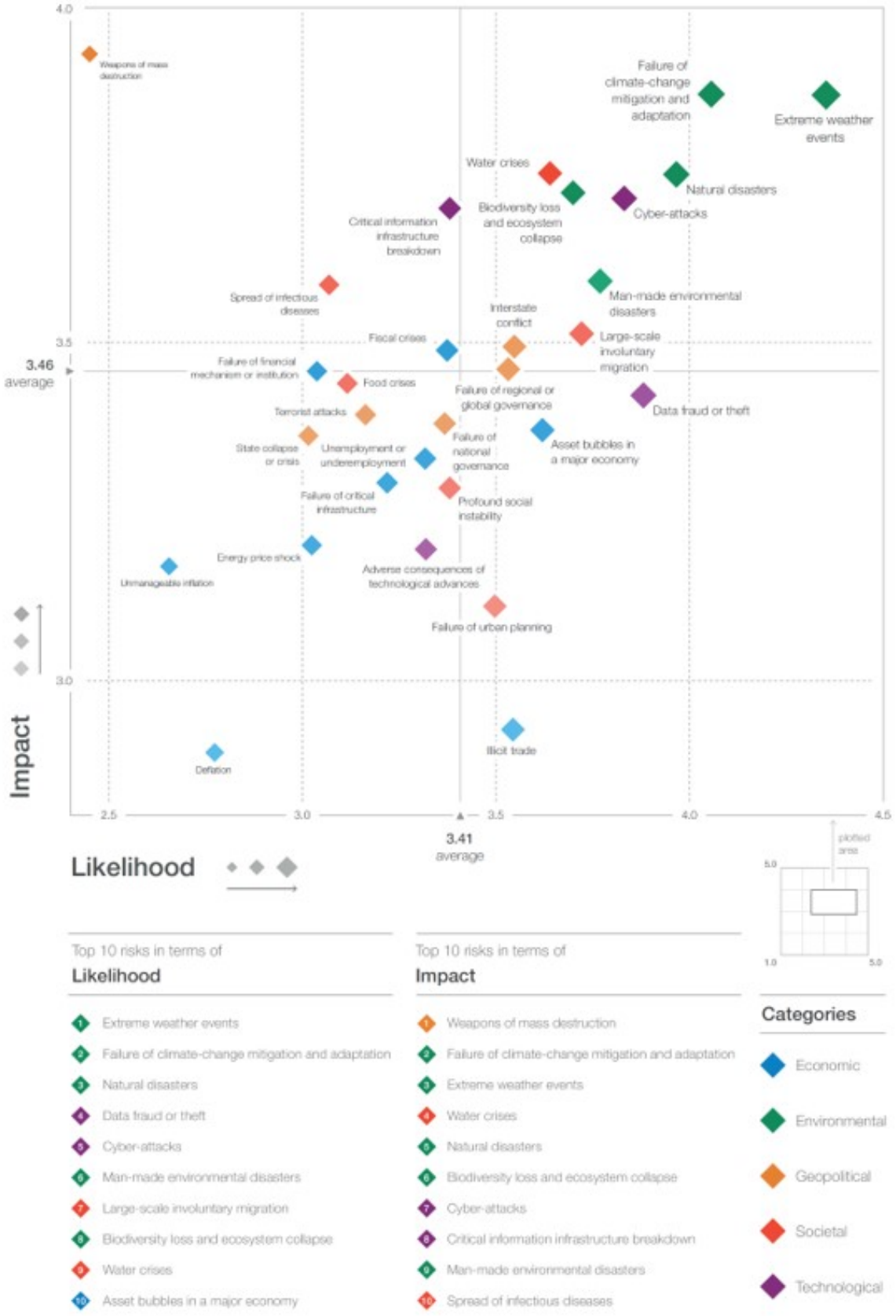

Fig.8 –The Global Risks Landscape 2019 (https://www.climateforesight.eu/global-policy/global-risks-report-2019-environment-related-risks-account-for-three-of-the-top-five-risks-by-likelihood-

and-four-by-impact/).

Decision Support System, risk assessment e applicazioni

In accordo con il l'analisi introdotta da Sprangue e Watson nel 1996 [Sau1], i modelli concettuali risultano cruciali nel comprendere e descrivere i sistemi più complessi.

Proprio questi ricercatori definirono il **sistema di supporto alle decisioni** (Decision Support System – DSS) [Sau1] come *un sistema interattivo basato su un elaboratore (*cioè uno o più computer*) che aiuta coloro che debbono assumere delle decisioni con dati e stime di risoluzione di problemi semi-strutturati, non strutturati o addirittura strutturati in modo parziale e lacunoso*.

In una definizione più pragmatica, un sistema DSS può essere considerato un sistema di calcolo che supporta le attività di decisone degli attori principali di organizzazioni istituzionali o private.

Il sistema DSS può essere utilizzato dal management politico o di vertice di un'azienda, ma anche da chi pianifica le operazioni e gli interventi operativi, cioè figure tecniche anche di livello medio e medio-alto. La sua potenzialità è fornire il **supporto alla decisone** su problemi complessi, caratterizzati da molti aspetti caratteristici, che possono modificare anche rapidamente i loro contorni nel corso del tempo, svilupparsi in modo non prevedibile a priori.

Nella maggior parte dei casi i sistemi DSS forniscono risposte in tempi piuttosto rapidi, includendo ricerche di dati e valutazioni alternative di impatti, cioè informazioni utili agli attori che assumono le decisioni per riepilogare i punti di principale interesse e procedere a scelte consapevoli e basate su tutti i dati disponibili in quella fase del processo.

Per concludere, va sottolineato come un'applicazione di tipo DSS debba fornire funzionalità grafiche in ambito statistico e matematico in senso generale, non intendendo con questo semplicemente le analisi di *trend* e i report *statistici semplificati* per i *top-manager*, ma anche le **capacità più sofisticate di analisi di scenari diversi** di evoluzione in situazioni complesse, capacità che possono essere d'aiuto sia ai *manager d'area* sia agli *advisor tecnici*, con previsioni evolutive che sappiano rispondere rapidamente a domande del tipo "*cosa succede se …*".
Per queste ragioni il DSS, quindi, dovrebbe contemplare tra le sue capacità funzionali anche quelle del *risk assessment*.

Glossario

DSS - Decision Support System

ISO - International Organization for Standardization

PDCA – Plan, Do, Check, Act

Bibliografia e sitografia

[Car1] M. Carbonelli et al., *"Analisi del rischio e anticorruzione: come valutare al meglio i processi lavorativi?"*, Safety & Security, 14 giugno 2018, https://www.safetysecuritymagazine.com/articoli/analisi-del-rischio-e-anticorruzione-come-valutare-al-meglio-i-processi-lavorativi/

[Car2] M. Carbonelli, *"Valutazione del rischio corruzione nei processi lavorativi della PA: come vanno le cose a sei anni dal primo Piano Nazionale Anticorruzione?"*, Safety & Security, 18 giugno 2019, https://www.safetysecuritymagazine.com/articoli/valutazione-del-rischio-corruzione-nei-processi-lavorativi-della-pa-come-vanno-le-cose-a-sei-anni-dal-primo-piano-nazionale-anticorruzione/

[Car3] M. Carbonelli, *"Terrorist attacks and natural/anthropic disasters: Risk Management methodologies fror supporting security decision-making actors"*, Aracne CBRNe Book Series, Roma giugno 2019, IBSN 978-88-255-2565-6

[Car4] M. Carbonelli, L. Gratta, "*Risk Management Part 1: Definitions, standard ISO and application methods*", Lezioni del Master Internazionale di I e II livello CBRNe 2014, Università di Tor Vergata, Roma

[DHS1] DHS, *Risk Steering Committee: DHS Risk Lexicon*, Edition September 2010

[EuC1] European commission staff working paper, *Risk Assessment and Mapping Guidelines for Disaster Management*, Brussels, 2010.

[ISO1] ISO 31000, *Risk management - Principles and guidelines, International Organization for Standardization*, edition 2009, ripubblicato con integrazioni e modifiche nel 2018.

[ISO2] ISO 31010, *Risk management - Risk assessment techniques*. International Organization for Standardization, 2009.

[ISO3] ISO Guide 73, *Risk management - Vocabulary*, International Organization for Standardization, 2009.

[Kom1] N. Komendantova et al., *Multi-hazard and multi-risk decision-support tools as a part of participatory risk governance: Feedback from civil protection stakeholders*, International Journal of Disaster Risk Reduction, Volume 8, June 2014, Pages 50-67, https://www.sciencedirect.com/science/article/pii/S221242091300068X

[Sau1] Sauter Vicky, Decision Support Systems, University of Missouri St. Louis, 2002, http://www.umsl.edu/~sauterv/analysis/488_f02_papers/dss.html

[Sot1] A. Sotic, R. Radjic, '*The Review of the Definition of Risk*', Online Journal of Applied Knowledge Management, Vol.3, Special Issue 2015 - Paper selected from International Conference in Applied Protection and Its Trends, http://www.iiakm.org/ojakm/articles/2015/volume3_3/OJAKM_Volume3_3pp17-26.pdf

Articolo a cura di **Marco Carbonelli**