Giancarlo Butti
ISACA (Information Systems Audit and Control Association)
Capitolo di Milano

Alberto Piamonte
ISACA (Information Systems Audit and Control Association)
Capitolo di Roma

Misurare la physical cyber security

Physical Cyber Security Assessment

Sommario: Che si tratti di sicurezza fisica o di cyber security [1] la capacità di un'organizzazione di resistere ad un attacco può essere oggetto di valutazione attraverso metriche di diverso tipo.

In questo articolo vengono rappresentati alcuni dei possibili strumenti di misura, molto diversi fra di loro, che tuttavia nel loro insieme possono dare preziose indicazioni sul reale livello di resilienza di un'organizzazione

Abstract: Whether it's physical safety or cyber security an organization's ability to withstand an attack can be subject to assessments by different types of metrics.

In this article we are represented some of the possible measuring instruments, very different from each other, which, however, as a whole can give valuable information on the actual level of resilience.

1. Il concetto di rischio e l'analisi dei rischi

Uno dei primi strumenti da analizzare è costituito sicuramente dai modelli per l'analisi del rischio.

Il Dizionario Garzanti della lingua italiana riporta tre diverse definizioni per il concetto di RISCHIO:

- eventualità di conseguenze negative, passive
- esposizione ad un pericolo
- pericolo al quale ci si espone.

Secondo un'altra definizione il RISCHIO è il risultato finale, diretto, indiretto o consequenziale ad un'azione volontaria, involontaria o ad un evento accidentale.

Nelle metodologie di analisi dei rischi la definizione più utilizzata identifica il RISCHIO come prodotto fra la probabilità che un evento pericoloso si realizzi e l'impatto [danno] da questo provocato.[2]

Il RISCHIO è un concetto che pervade ogni aspetto ed ogni momento della vita professionale e privata di ognuno di noi. Il RISCHIO può riguardare la perdita di beni, della salute, degli affetti, del lavoro…

Il RISCHIO può anche riguardare il non ottenere un determinato risultato in termini materiali, economici, morali, affettivi…

Qualunque azione fatta da un individuo o da un'organizzazione di

[1] Una disamina sul significato attribuito al termine cyber security è riportata in Definition of Cybersecurity - Gaps and overlaps in standardisation – ENISA - 2015

[2] E quindi misurabile in perdità (€) per unità di tempo (mese, anno): rischio 10.000€ / anno

qualunque tipo comporta diversi rischi; anche il non fare alcuna azione comporta un'assunzione di RISCHIO.

È quindi ovvio che molto tempo sia stato dedicato alla elaborazione di metodologie che consentano una valutazione del RISCHIO al fine di quantificarlo e, possibilmente, di prevenirlo.

Le aziende devono svolgere una attività continua di analisi del RISCHIO in diversi ambiti, alcuni dei quali obbligatori per legge, quali ad esempio la sicurezza dei lavoratori o il trattamento dei dati personali.

TABELLA 1 – TERMINOLOGIA DELL' ANALISI DEI RISCHI

- Bene - è l'oggetto reale o immateriale da difendere
- Rischio - è il risultato finale, diretto, indiretto o consequenziale ad un'azione volontaria, involontaria o ad un evento accidentale
- Minaccia - è un'azione volontaria, involontaria o un evento accidentale
- Impatto[danno] - è la conseguenza diretta, indiretta, consequenziale ad un evento dannoso
- Probabilità - è il numero di volte che può aver luogo una minaccia in un determinato periodo
- Vulnerabilità - è una caratteristica intrinseca del bene, che viene sfruttata dalla minaccia
- Contromisura - è un fattore che consente di ridurre o annullare l'effetto di una minaccia

Settori particolari, come ad esempio quello bancario, hanno anche codificato la necessità di valutare costantemente la propria posizione rispetto a particolari categorie di rischi, come ad esempio il rischio di credito.

Più in generale i rischi che un'azienda deve affrontare sono molteplici e raggruppabili in diverse aree quali:

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

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.

Nel caso ad esempio di un evento che ha comportato il danneggiamento di un bene, si può valutare come IMPATTO quello subito direttamente dal bene, ad esempio la distruzione di un disco fisso, oppure gli effetti che ne derivano, ad esempio la perdita delle informazioni in esso contenute, o ancora la mancata erogazione di un servizio da parte del server dove il disco era installato e, a catena, ulteriori IMPATTI sui servizi erogati alla clientela.

TABELLA 2 – RELAZIONE FRA RISCHI

Descrizione del bene	Disco fisso
Evento	Distruzione
Costo diretto	Costo del disco
Costi indiretti	Costo dell'intervento tecnico di sostituzione Costo di ripristino dei dati, applicazioni, configurazioni
Costi consequenziali	Mancato guadagno temporaneo per cessazione del servizio Rimborso a clienti Spese legali Spese per il ripristino dell'immagine aziendale Mancato guadagno per perdita di clienti

È possibile ridurre il RISCHIO intervenendo sui 2 fattori che lo compongono, IMPATTI e PROBABILITÀ.

Questo si ottiene adottando adeguate contromisure che possono ridurre uno o entrambi i fattori che concorrono alla determinazione del RISCHIO.

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 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.

Il costo dell'analisi deve essere congruente con i beni da proteggere.

Se la valutazione del rischio viene effettuata secondo una logica minaccia/asset senza tenere in giusta considerazione la relazione fra gli asset, potrebbe esserci una non corretta valutazione del rischio e del rapporto costo beneficio di una particolare contromisura.

Infatti una contromisura che potrebbe apparire non conveniente se rapportata ad una singola minaccia/asset potrebbe risultare conveniente se ripartita su più asset fra loro correlati, ovvero se tutela anche rispetto ad altre minacce.

Ad esempio un impianto antincendio che tuteli un edificio, automaticamente tutela anche i beni in esso contenuti. Considerare queste relazioni è particolarmente importante, ma purtroppo è una caratteristica assente nella maggior parte delle metodologie di analisi del rischio.

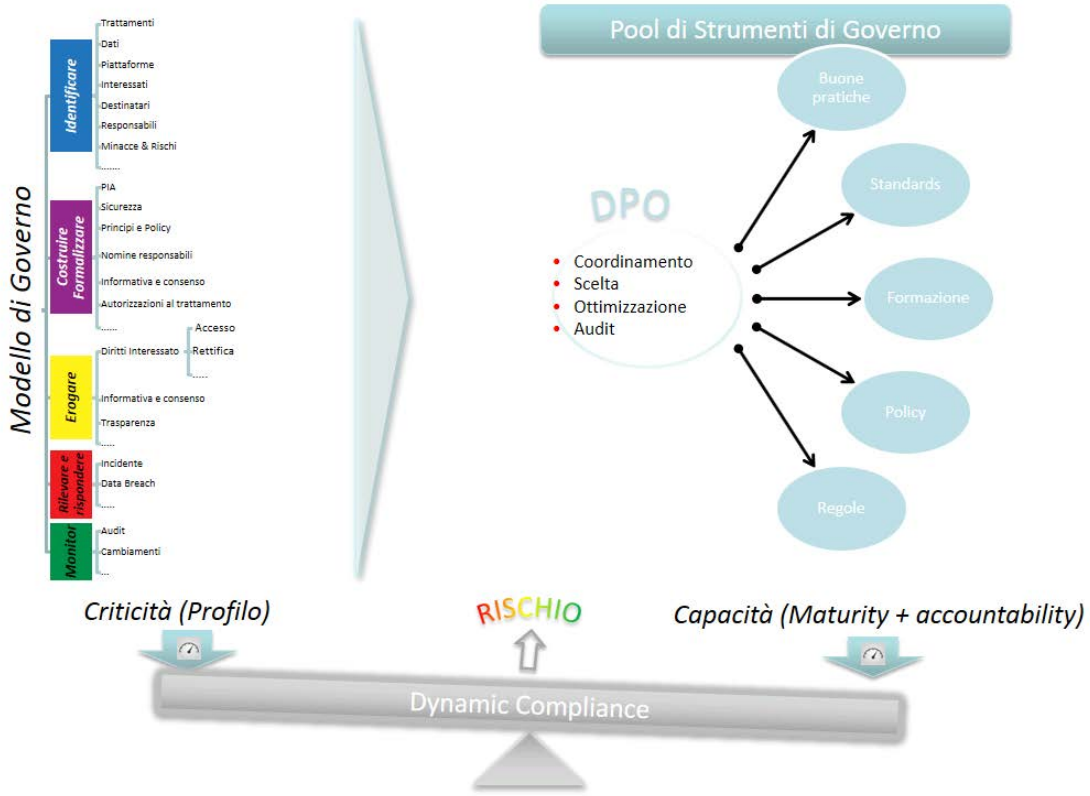


Figura 1. Le azioni da intraprendere devono essere proporzionali ai rischi

Secondo la **Linea guida ISCOM - Risk analisys approfondimenti**

..I diversi metodi e strumenti di analisi dei rischi possono essere distinti, in base al metodo di valutazione dei rischi utilizzato, nelle seguenti tre categorie:

- *qualitativo;*
- *quantitativo;*
- *semi-quantitativo.*

Il primo approccio prevede una valutazione del rischio su una scala qualitativa (ad esempio alto, medio, basso).

Il secondo approccio, invece, riconduce le valutazioni ad un valore numerico puntuale, spesso inteso come la perdita economica derivante dal verificarsi del rischio. Si tratta di un approccio più difficile ed oneroso del primo perché costringe ad un censimento ed una valorizzazione degli asset e ad una valorizzazione delle perdite che si avrebbero in caso di incidente.

Il terzo approccio è un compromesso fra i primi due, nel quale le valutazioni sono effettuate in termini qualitativi e, successivamente, trasformate in numeri per poterle elaborare attraverso algoritmi di calcolo, come se si trattasse di valutazioni quantitative…

La disponibilità di strumenti rigorosi e capaci di effettuare operazioni su valori sia quantitativi sia qualitativi è quindi quanto mai opportuna per affrontare in modo professionale un'analisi dei rischi.

Un approccio QUANTITATIVO, che valuti analiticamente tutti i singoli punti di rischio, può richiedere di trattare insiemi di dati molto ampi (centinaia di migliaia), tale da rendere impraticabile una valutazione "umana" punto-per-punto.

Anche da qui l'esigenza di introdurre metodi rivolti non tanto all'automazione del calcolo (normali fogli di calcolo), ma in grado di automatizzare il processo di valutazione e di sintesi, applicando il metodo appreso con tecniche di più alto livello.

Uno dei possibili approcci nell'affrontare questa problematica è l'uso di tecniche di soft computing, soluzioni applicate di intelligenza artificiale che permettono ad esempio la realizzazione con relativa semplicità di sistemi esperti.

Nel suo complesso il soft computing comprende tre diverse tecnologie:

- **algoritmi genetici**, uno strumento che consente di trovare la soluzione tendenzialmente ottima ad un problema complesso facendo evolvere le soluzioni attraverso generazioni successive che raggiungono il risultato richiesto (solo le soluzioni più promettenti infatti sopravvivono nel processo di evoluzione)
- **logica fuzzy**, che si indirizza al trattamento di un aspetto che normalmente viene rappresentato con difficoltà mediante un elaboratore e cioè l'**incertezza**
- **reti neurali** sono una struttura di calcolo che, semplificandolo, riproduce la logica di apprendimento del cervello.

È importante rilevare che la logica fuzzy e le reti neurali, sotto condizioni abbastanza deboli, sono due facce della stessa medaglia.

La combinazione di queste tre tecnologie è stata implementata in **FuzzyWorld,** uno strumento per la creazione di sistemi esperti realizzato dal prof. Lorenzo Schiavina (già docente di Ricerca Operativa alla facoltà di Matematica all'Università Cattolica di Brescia) e disponibile sul sito della EDOR M.Q. (www.edor.it) azienda che da 30 anni si occupa di logica fuzzy e di programmazione a oggetti.

La realizzazione di un sistema esperto basata su logica fuzzy, o meglio neuro fuzzy ha diversi vantaggi, fra i quali:

- l'uso di valori elementari continui e non discreti
- l'uso di valori espressi sia in forma numerica, sia di tipo letterale e qualitativo

- la possibilità di utilizzare un numero limitato di casi significativi di antecedenti e conseguenti per la generazione automatica della REGOLE utilizzando la tecnica **DI-RO**[3]**.**

È proprio grazie alla tecnica DI-RO che è possibile la creazione di sistemi esperti funzionanti con relativa semplicità (un esempio di applicazione verrà presentato nel proseguo dell'articolo).

Il problema di fondo, che di fatto ha limitato la diffusione dei S.E. è la difficoltà che un esperto ha nel formalizzare la propria conoscenza (non dimenticando inoltre che un esperto potrebbe ragionevolmente non desiderare trasferire la propria conoscenza ad una macchina), traducendola in regole che un'applicazione software sia in grado di gestire.

Nell'esempio che verrà descritto, l'esperto dovrebbe formalizzare 4000 regole solo per definire l'IMPATTO, pur prendendo in considerazione un limitato numero di variabili.

È qui che entrano in gioco le reti neurali, una tecnologia attraverso la quale è possibile "addestrare" un sistema fornendo come informazioni sia i dati di ingresso che i dati in uscita per un determinato problema.

Grazie ad esempio all'uso di semplici fogli Excel è possibile procedere ad un addestramento della rete neurale secondo la logica DI-RO (data in – rules out) se si dispone dello strumento adatto.

Grazie a questa tecnica è inoltre possibile utilizzare un numero limitato di casi significativi di antecedenti e conseguenti per la generazione automatica della REGOLE e di formalizzare competenze che un esperto difficilmente sarebbe in grado di esprimere tramite formule.

SOFT COMPUTING

ALGORITMI GENETICI

Gli algoritmi genetici sono una recente tecnica di ottimizzazione che identificano l'"ottimo" mediante un processo di evoluzione degli individui che si succedono nelle generazioni.

La tecnica utilizzata dagli algoritmi genetici è quella di trovare casualmente una serie di possibili differenti soluzioni di partenza, che rappresentano la generazione iniziale da cui partirà l'evoluzione.

Ogni singolo elemento della soluzione rappresenta un individuo della popolazione evolutiva e come tale sarà caratterizzato dalle proprietà dei suoi cromosomi.

L'algoritmo genetico prevedrà uno schema di accoppiamento fra gli individui atto a selezionare i migliori (cioè le soluzioni più adatte alla sopravvivenza degli individui).

La fase di accoppiamento produrrà una nuova generazione di soluzioni che sarà mediamente migliore della precedente.

[3] *Artificial Intelligence A Guide to Intelligent Systems - Michael Negnevitsky – ADDISON WESLEY*

Questi due passi elementari (accoppiamento e generazione di una nuova popolazione) continueranno per un numero predefinito di generazioni fino a quando sarà trovata la soluzione tendenzialmente ottimale.

Si osservi che la soluzione "matematicamente" ottima può non essere raggiungibile per la natura stessa del problema o può essere una (soddisfacente) soluzione **inferiore** a quella teoricamente raggiungibile matematicamente.

LOGICA FUZZY

La logica fuzzy è una estensione della logica tradizionale (che è un caso particolare della logica fuzzy) nella quale non è valido il principio del terzo escluso (chi è giovane non è vecchio, chi è alto non è basso, chi è bianco non è nero….)

La logica fuzzy è nata per trattare tutte le sfumature di grigio che ci sono tra il bianco ed il nero e che rappresentano l'**incertezza**, cosa del tutto differente dalla probabilità.

Si osservi che tale idea è assolutamente adatta ad affrontare fenomeni di **RISCHIO.**

Per capire i vantaggi della logica fuzzy come strumento di soluzione, si consideri il celebre sillogismo di Socrate:

l'uomo è mortale (precedente)
Socrate è un uomo (precedente)
quindi Socrate è mortale. (conseguente)

Ma non tutti i problemi sono così semplici e diretti; si consideri questo esempio:

l'uomo sano vive a lungo
Socrate ha il raffreddore
quindi Socrate vivrà a lungo oppure no?

A differenza di qualsiasi essere umano che risponderebbe Socrate vivrà a lungo (visto che Socrate ha un semplice raffreddore) una normale applicazioni software non sarebbe in grado di trovare una soluzione.

Infatti il termine "sano" non è direttamente correlabile al "raffreddore" di Socrate, dato che (come si dice tecnicamente) l'appartenenza all'insieme degli esseri sani è soggetta ad **incertezza**.

Nella logica fuzzy l'appartenenza ad un insieme è una questione di grado, espresso in modo continuo, in un intervallo zero-uno.

Utilizzando la conoscenza della natura del raffreddore (cioè una lieve malattia), mediante la logica fuzzy è semplice stabilire che il grado di sanità di Socrate (anche se non è perfettamente sano e quindi non è uno) è assai vicino a quello di un essere perfettamente sano; quindi Socrate (rispetto alla domanda) vivrà a lungo.

Utilizzando il grado di appartenenza, Socrate con il raffreddore è contemporaneamente sano e malato:

- **sano** con un alto grado (ma non completamente **sano** e quindi non con un grado di appartenenza uno, ma lievemente inferiore)

- malato con un piccolo grado.

Tutto questo verrebbe formalizzato in un sistema fuzzy mediante una serie di regole del tipo:

IF Socrate **IS** raffreddato **THEN** Socrate vivrà a lungo.

Si osservi che il "vivrà a lungo" non identifica un grado di probabilità ma una forma di asserzione logica, anche se la probabilità e la logica fuzzy utilizzano valori fra zero e uno

Queste regole sono molto leggibili, ma hanno la contropartita per l'utilizzatore, di dovere scrivere direttamente le regole da utilizzare per ottenere la risposta. Se invece del livello di salute di Socrate si parla di RISCHIO è possibile creare dei sistemi esperti per l'analisi del rischio che congelino l'esperienza e le capacità di un esperto umano.

RETI NEURALI

La rete neurale simula, pur in forma molto semplificata, il funzionamento di neuroni e sinapsi.

Se si considera un bambino che impara a camminare, si capisce immediatamente che il cervello umano impara a gestire una quantità rilevantissima di informazioni per ottenere il risultato desiderato (muoversi senza cadere) grazie a ripetuti tentativi.

Tuttavia nessuno di noi è in grado di formalizzare quali regole il proprio cervello ha ideato per riuscire a camminare, tanto è vero che riuscire a tradurre questa acquisita capacità in formule utilizzabili ad esempio da un robot, è particolarmente difficile. La nostra mente si comporta al riguardo come una **black box** e le reti neurali fanno altrettanto. La buona notizia è che un sistema fuzzy è una rete neurale a 2 strati, senza avere il problema di essere una **black box**, dato che le sue regole di comportamento sono facilmente osservabili.

SISTEMA ESPERTO

Una "applicazione esperta" è un programma informatico in grado di rispondere ad un problema come (teoricamente) risponderebbe un esperto umano.

Rispetto a quest'ultimo ha il vantaggio di essere neutra e non influenzabile in merito alla risposta data ed è inoltre in grado di dare evidenza delle motivazioni che hanno portato a quella specifica risposta.

TABELLA 3 – METODOLOGIE DI ANALISI DEI RISCHI

Linea guida ISCOM ***Risk analisys approfondimenti*** www.iscom.it	**ENISA:** ***Information package for SME*** www.enisa.com
AS/NZS 4360:2004 RISK MANAGEMENT *BSA – Baseline Security Assessment* *Ce.TRA - Continuous e.Business Threat and Risk Analysis* *CRAMM* *Defender Manager* *EBIOS* *ERAM - Enterprise Risk Assessment and Management* *FIRM (Fundamental Information Risk Management)* *ISA – Information Security Assessment* *ISO/IEC 21827 - System Security Engineering, Capability Maturity Model* *NET.RISK* *NORA - Network Oriented Risk Analysis methodology* *OCTAVE® - Operationally Critical Threat, Asset, and Vulnerability EvaluationSM* *OSSTMM – Open Source Security Testing Methodology Manual* *PRA – Psychological Risk Assessment* *RAF - Risk Analyis Facility* *RISKWATCH (versione per l'Italia)* *SARA - Simple to Apply Risk Analysis* *SPRINT – Simplified Process for Risk Identification* *SSM - Scalable Security Model*	*Austrian IT Security Handbook* *Cramm* *Dutch A&K analysis* *Ebios* *ISF methods* *ISO/IEC IS 13335-2 (ISO/IEC IS 27005)* *ISO/IEC IS 17799* *ISO/IEC IS 27001* *ISO 31010* *IT-Grundschutz* *Marion (replaced by Mehari)* *Mehari* *Octave* *SP800-30 (NIST)*

LA VALUTAZIONE QUALITATIVA DEL RISCHIO

PROBABILITÀ

Probabilità	Frequenza	Scala
Nulla	Mai accaduta ed impossibile	0
Bassa	Mai accaduta, ma possibile	1
Medio Bassa	Meno di una volta all'anno	2
Medio Alta	Più di una volta all'anno	3
Alta	Più di una volta al mese	4
Certa	Più di una volta al giorno	5

DANNO (IMPATTO)

Danno	Quantificazione del danno	Scala
Trascurabile	Minimo o nessun impatto	0
Minore	Nessuno sforzo extra richiesto per riparare il danno	1
Significativo	Danno tangibile, sforzo extra richiesto per riparare il danno	2
Dannoso	Significativa quantità di risorse richieste	3
	Grandi quantità di dati, servizi o impianti compromessi, interruzione del servizio o della produzione esteso	4
Grave	Dati, servizi o impianti totalmente compromessi, totale interruzione del servizio o della produzione	5

RISCHIO

Probabilità x Impatto

RISCHIO NORMALIZZATO

Rischio	Non normalizzato	Normalizzato
Nullo	0	0
Minore	1-6	1
Significativo	7-12	2
Dannoso	13-18	3
Serio	19-24	4
Grave	25	5

LA VALUTAZIONE QUANTITATIVA DEL RISCHIO

ANNUAL LOSS EXPECTED

$$ALE = \sum_{i=1}^{n} I(O_i)F_i$$

TABELLA 4 – POSSIBILI FONTI DATI PER ANALISI DI TIPO QUANTITATIVO

Descrizione fonte
Segnalazioni di malfunzionamenti da parte di utenti sia interni che esterni (errori nelle applicazioni e nei sistemi, degrado delle prestazioni, perdite o alterazioni di dati, rotture…);
Rapporti su incidenti
Reclami dei clienti (per ritardi nelle consegne, errate evasioni di ordini…);
Reclami dei fornitori (ad esempio ritardi nei pagamenti)
Reclami dei dipendenti (ad esempio ritardi nei pagamenti degli stipendi, errori nei rimborsi spese).
Rapporti di audit
Analisi dei log

TABELLA 5 – METODOLOGIE DI ANALISI DEL RISCHIO A CONFRONTO

THE MOST IMPORTANT ADVANTAGES AND DISADVANTAGES OF QUANTITATIVE AND QUALITATIVE METHODS OF IT RISK ANALYSIS

Risk Analysis	Quantitative methods	Qualitative methods
Chosen advantages	- They allow for definition of consequences of incidents occurrence in quantitative way, what facilitates realization of costs and benefits analysis during selection of protections. - They give more accurate image of risk.	It allows for putting in order risks according to priority. - It allows for determination of areas of greater risk in a short time and without bigger expenditures. - Analysis is relatively easy and cheap.
Chosen disadvantages	- Quantitative measures depend on the scope and accuracy of defines measurement scale.	It does not allow for determination of probabilities and results using numerical

	- Results of analysis may be not precise and even confusing. - Normal methods must be enriched in qualitative description (in the form of comment, interpretation). - Analysis conducted with application of those methods is generally more expensive, demanding greater experience and advanced tools.	measures. - Costs-benefits analysis is more difficult during selection of protections. - Achieved results have general character, approximate etc.

Tratto da: "IT Risk Assessment:Quantitative and Qualitative Approach" - Artur Rot - Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

SUMMARY OF ADVANTAGES AND DISADVANTAGES OF EACH ELEMENT OF THE PROPOSED TAXONOMY

Risk Analysis	**Quantitative methods**	**Qualitative methods**	Hybrid
Advantages	- Risks levels may be identified in monetary terms - Results can be expressed in management-specific language - Great effort is put into resource value definition and risk mitigation - Cost-benefit assessment effort is possible	- It is not necessary to quantify threat likelihood - Prioritizes the risks and identifies areas for immediate action and improvement - Save time, effort, and expense - Easier to involve people who are not experts on security or computers	- It has the flexibility to change quantitative inputs to qualitative outputs and vice versa
Disadvantages	- Estimating the damage probability of each resource is imprecise - The numerical/monetary results may be difficult for non-technical people	- Does not provide monetary values and probabilities - Making a cost-benefit analysis of recommended	

	to interpret - Calculation can be challenging, expensive, and time consuming	controls is more difficult - Very subjective and prone to errors and imprecision	

Tratto da: "Taxonomy of Information Security Risk Assessment" (ISRA) - JOURNAL OF COMPUTERS & SECURITY – ELSEVIER - Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzega and Mohamed Cheriet

2. Key Indicator

Un'altra modalità con cui è possibile misurare il proprio livello di sicurezza è l'uso di specifici indicatori.

Va però evidenziato che misurare il livello di sicurezza è molto difficile e di per sé anomalo, in quanto sarebbe più opportuno misurare la mancanza di sicurezza.

Non avere mai subito un incidente di sicurezza non è infatti un parametro significativo in quanto non è necessariamente legato al proprio livello di sicurezza quanto piuttosto alla mancanza del verificarsi di eventi dannosi.

Il libro **Linea guida ISCOM - Risk analisys approfondimenti** riporta alcuni esempi di indicatori di natura tecnica:

- *per la sicurezza delle applicazioni:*
  numero pagine vulnerabili al SQL injection/totale pagine applicative, frequenza deploy sorgenti negli ambienti del ciclo di vita software, numero errori applicativi rilevati/mese, numero interventi correttivi/numero errori rilevati;
- *per la sicurezza fisica:*
  numero guasti ai tornelli/anno, numero guasti al sistema di condizionamento delle sale server/anno, numero di black-out, numero furti per anno, numero prove di recovery da disastro, tempo medio di recovery da disastro, numero rilevatori antifumo per metri cubi, numero interventi di manutenzione per anno, tempo medio di intervento di manutenzione;
- *per la sicurezza di rete:*
  frequenza scansioni di rete/anno, numero di sistemi oggetto di scansione/totale sistemi, frequenza di aggiornamento dei pattern delle vulnerabilità, frequenza di revisione delle regole dei firewall, frequenza aggiornamento antivirus, numero di virus rilevati, numero attacchi bloccati/totale attacchi rilevati.

Tali indicatori non sono fra loro omogenei.

Una prima differenza infatti è che alcuni di essi indicano un risultato raggiunto (es. *tempo medio di recovery da disastro)*, cioè una misura a posteriori, mentre altri indicano una serie di interventi di natura

preventiva (…*numero prove di recovery da disastro)*, messi in atto cioè per raggiungere uno scopo.

Questa è la differenza fra i LAG ed i LEAD INDICATORS.

Misurare i risultati tramite dei LAG INDICATORS è relativamente semplice ed i dati rilevati sono precisi e difficilmente confutabili.

I LEAD INDICATORS sono invece degli indicatori predittivi, in quanto non misurano un risultato, ma un processo messo in atto per raggiungerlo; per tale motivo non sono semplici da definire ed inoltre non garantiscono che il risultato atteso sia effettivamente raggiunto (la misura del risultato richiede ovviamente la presenza di un LAG INDICATOR).

Per essere significativi i LEAD INDICATORS devono inoltre essere definiti da qualcuno che ben conosce il processo che porta al risultato atteso e inoltre che qualcuno se ne faccia carico.

Un esempio molto semplice può chiarirne la differenza.

Se si desidera perdere peso è possibile misurare ogni giorno la situazione raggiunta con una bilancia; questa dirà se effettivamente si sono ottenuti i risultati desiderati. Si tratta quindi di un LAG INDICATOR.

Se però si desidera essere certi di ottenere quel risultato si dovranno mettere in atto una serie di azioni, anche queste misurabili, come ad esempio ridurre il numero di calorie introdotte o aumentare il numero di quelle consumate (ad esempio facendo una corsa o andando in palestra). Ecco quindi che è possibile misurare preventivamente la quantità e tipologia di alimenti e calcolare di conseguenza le calorie introdotte ovvero misurare il numero di ore passate in palestra.

Si stanno quindi quantificando gli elementi di un processo pianificato per ottenere il risultato desiderato.

Questi però vanno individuati con precisione; ad esempio le ore passate in palestra non sono in realtà direttamente collegate al numero di calorie bruciate, perché queste sono legate al numero, tipologia ed intensità degli esercizi effettuati.

La formulazione di un LEAD INDICATOR deve quindi essere effettivamente significativa.

Nell'esempio presentato vi è una buona correlazione fra le azioni quantificate ed il risultato atteso, ma non sempre è così.

Ad esempio se si desidera aumentare il fatturato è ipotizzabile aumentare il numero delle visite presso i potenziali clienti per offrire i propri prodotti o presso i clienti già acquisiti per offrire nuovi prodotti.

Il risultato però non è garantito; non vi è una correlazione così diretta fra azione e risultato o meglio, sono molteplici i fattori che si dovranno considerare.

Nel caso specifico della gestione del rischio sono moltissimi i fattori indeterminati che possono influire sul risultato atteso.

È comunque possibile definire a priori una notevole serie di attività misurabili che si possono mettere in atto per aumentare il livello di sicurezza di una organizzazione.

Ad esempio quante prove di ripristino si pianificano per aumentare la propria capacità di risposta ad un incidente di sicurezza che comprometta un server che non operi in alta affidabilità.

Anche in questo caso tuttavia la semplice indicazione di un numero non è significativa se non è seguita da una descrizione di che cosa

comprenda effettivamente una prova di ripristino; se è legata ad esempio alla semplice capacità di lettura dei supporti o alla effettiva ricostruzione e configurazione del server.

Una seconda differenza negli indicatori sopra riportati è che alcuni esprimono un valore assoluto (*numero furti per anno)* mentre altri esprimono un valore relativo (*numero pagine vulnerabili al SQL injection/totale pagine applicative).*

Molti dei LAG INDICATORS hanno infatti significato solo se espressi in valore percentuale; ad esempio quante password sul totale delle password in uso non rispettano i criteri di sicurezza predefiniti, quanti dei server sul totale dei server non sono adeguatamente aggiornati, quanti dei firewall analizzati sul totale dei firewall non sono adeguatamente configurati o hanno ancora la password di default.

Molti indicatori che sarebbe utile avere sono invece difficili o impossibili da misurare.

Ad esempio è possibile misurare i tentativi di attacco intercettati, ma sarà difficile capire quanti attacchi sono stati effettivamente effettuati.

3. Maturity Model

I rischi stanno diventando sempre più "irreversibili".

Ad esempio nel caso di danni all'immagine aziendale la ricostruzione di una reputazione richiede non solo risorse, ma soprattutto tempi, potenzialmente incompatibili con la stessa sopravvivenza di molte iniziative.

In alcuni settori, come l'esplorazione dello spazio o la sanità, le cose devono funzionare al primo tentativo!

Di qui l'esigenza di valutare "preventivamente" la capacità di raggiungere l'obiettivo e di poterla anche dimostrare.

Varie metodologie sono state create nell'ultimo ventennio per dare una risposta formale, possibilmente oggettiva e ripetibile, all'esigenza di:

- valutare preventivamente la capacità di ottenere il risultato desiderato
- confrontare ambienti (fornitori) diversi
- individuare carenze e predisporre piano correttivi.

In tali metodologie sono emersi in particolare due concetti / criteri.

Il primo criterio è quello di "MATURITY" che viene definito come:

La capacità di un'unità organizzativa di raggiungere regolarmente e stabilmente i propri obiettivi in un determinato ambito.

La misura, fatta con metodi codificati e standardizzati corrisponde al: maturity level, valore in una scala discreta che dipende dal metodo utilizzato.

Il secondo è quello di "CAPABILITY", ed in particolare la "Process capability" che viene definito come:

La capacità (prevista) di un processo di raggiungere i suoi obiettivi. Anche questa misurata con una scala di valori discreti.

Si tratta di due prospettive: una, la maturity, che considera aspetti generalmente più ampi (organizzativi e di contesto) ed un'altra più analitica e tecnica (Capability) che si concentra sugli specifici processi.

Si incontra sempre più spesso anche il termine Capability maturity che fa riferimento ad una combinazione dei due approcci.

Anche nell'ambito della sicurezza sono stati definiti dei Maturity Model e dei CMM.

Solitamente un Maturity Model è organizzato in aree omogenee a loro volta suddivise per sottoaree.

Il livello di maturità di un processo misura il quanto bene un'organizzazione lo sta gestendo.

La scala di valori dei livelli di maturità assume una denominazione diversa fra i vari modelli.

Una serie di caratteristiche descrivono per ogni sottoarea i criteri per assegnare il corretto livello di maturità.

Questo permette alle organizzazioni di capire quali sono le aree che presentano maggiori livelli di criticità, definire il livello di maturità desiderato, definire le azioni per raggiungerlo.

Permette inoltre di effettuare comparazioni fra diverse organizzazioni o con benchmark di settore.

Ad esempio nell'ambito della sicurezza il **Cyber Security Capability Maturity Model (CMM) – V1.2**, redatto dal Global Cyber Security Capacity Centre (University of Oxford) è organizzato su 5 diverse aree, dette **Dimension**:

1. devising cyber policy and strategy
2. encouraging responsible cyber culture within society
3. building cyber skills into the workforce and leadership
4. creating effective legal and regulatory frameworks
5. controlling risks through organization, standards and technologies

ognuna delle quali caratterizzata da diversi **Factor:**

Dimension	Factor
Dimension 1 **Cyber Security Policy and Strategy**	D1-1: National Cyber Security Strategy D1-2: Incident Response D1-3: Critical National Infrastructure (CNI) Protection D1-4: Crisis Management D1-5: Cyber Defence Consideration D1-6: Digital Redundancy
Dimension 2 **Cyber culture and**	D2-1: Cyber Security Mind-set D2-2: Cyber security Awareness

society	D2-3: Confidence and trust on the Internet D2-4: Privacy online
Dimension 3 **Cyber security education, training and skills**	D3-1: National availability of cyber education and training D3-2: National Development of cyber security education D3-3: Corporate training & educational initiatives within companies D3-4: Corporate Governance, Knowledge and Standards
Dimension 4 **Legal and regulatory frameworks**	D4-1: Cyber security legal frameworks D4-2: Legal Investigation D4-3: Responsible Disclosure
Dimension5 **Standards, organisations, and technologies**	D5-1: Adherence to standards D5-2: National Infrastructure Resilience D5-3: Cyber Security marketplace

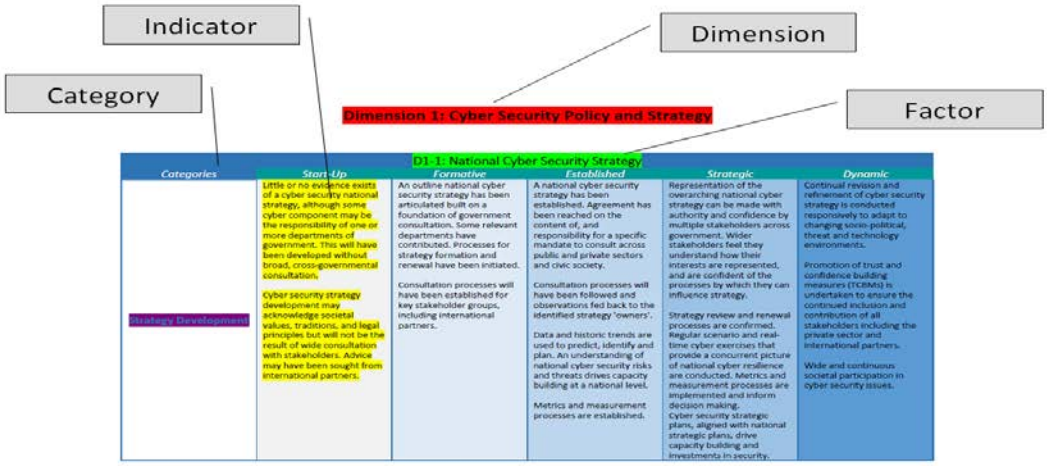
A loro volta i vari **Factor** sono organizzati in **Category**, alle quali è possibile attribuire uno dei 5 diversi livelli di maturità:

Livello	Descrizione
Start-up:	At this level either nothing exists, or it is very embryonic in nature. It could also include initial discussions about cyber capacity building, but no concrete actions have been taken. It also includes a lack of observed evidence in this particular indicator.
Formative:	Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new". However, evidence of this activity can be clearly evidenced.
Established	The elements of the sub-factor are in place, and working. There is not, however, well-thought out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the *relative* investment in the various elements of the sub-factor. But the indicators is functional and defined.
Strategic	Choices have been made about which parts of the indicator are important, and which are less important for the particular organization/nation. Of course, we would all like everything to be as important as everything else, but with finite resources, choices must be made. The strategic level reflects the fact that these choices have been made. They should have been made contingent on the nation/organization's particular circumstances.
Dynamic	At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances: for example, the technology of the threat

	environment, global conflict, a significant change in one area of concern (e.g. Cybercrime or privacy). Dynamic organizations have developed methods for changing strategies in stride, in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this level.

che viene descritto con ciò che il modello definisce **Indicator**.

La struttura del modello è quindi caratterizzata complessivamente dai seguenti elementi:



Una apposita guida, la **CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) - FACILITATOR GUIDE** aiuta una organizzazione nella implementazione del modello per il quale sono disponibili anche dei tool informatizzati (http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity).

Analogamente in ambito privacy il **Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 2.0)** del governo neo zelandese ha una struttura che valuta 9 aree, dette **Elements:**

1. governance, leadership, and accountability
2. culture
3. assurance
4. information management
5. privacy risk assessment
6. privacy programme
7. business processes
8. implementation of the Information Privacy Principles
9. breach and incident management.

Anch'essa utilizza 5 livelli di maturità che vanno da *Ad hoc* a *Optimize***.**

Anche in questo caso è disponibile una **User guide** che guida l'utente di un'organizzazione nella implementazione del modello.

Un ulteriore esempio di modello in ambito privacy è l' **AICPA/CICA Privacy Maturity Model** (based on GAPP and Capability Maturity Model - CMM), che prevede ad esempio i seguenti livelli di maturità:

Livello	Criteri
Ad hoc	procedures or processes are generally informal, incomplete, and inconsistently applied
Repeatable	procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects
Defined	procedures and processes are fully documented and implemented, and cover all relevant aspects
Managed	reviews are conducted to assess the effectiveness of the controls in place
Optimized	regular review and feedback are used to ensure continuous improvement towards optimization of the given process

Relativamente ai Maturity Model sono stati definiti anche alcuni ISO quali ad esempio:

ISO/IEC TR 15504-2:1998(E) [4]

ISO/IEC TR 15504 provides a framework for the assessment of software processes. This framework can be used by organizations involved in planning, managing, monitoring, controlling, and improving the acquisition, supply, development, operation, evolution and support of software.

Livello	Criteri
Level 0: Incomplete	There is general failure to attain the purpose of the process….
Level 1: Performed.	The purpose of the process is generally achieved….
Level 2: Managed.	The process delivers work products according to specified procedures and is planned and tracked…
Level 3: Established.	The process is performed and managed using a defined process based upon good software engineering principles…
Level 4: Predictable.	The defined process is performed consistently in practice within defined control limits, to achieve its defined process goals….
Level 5: Optimizing	Performance of the process is optimized to meet current and future business needs, and the process achieves repeatability in meeting its defined business goals…

[4] *Oggi aggiornata alla serie ISO 33XXX*

ISO/IEC 21827:2008(E)

Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

This International Standard specifies the Systems Security Engineering – Capability Maturity Model® (SSE-CMM®).

The SSE-CMM® is a process reference model focused upon the requirements for implementing security in a system or series of related systems that are the information technology security (ITS) domain. Within the ITS domain, the SSE-CMM® is focused on the processes used to achieve ITS, most specifically on the maturity of those processes. There is no intent within the SSE-CMM® to dictate a specific process to be used by an organization, let alone a specific methodology. Rather the intent is that the organization making use of the SSE-CMM® should use its existing processes, be those processes based upon any other ITS guidance document.

Capability Level	
Level 1 - Performed Informally	Base practices performed
Level 2 - Planned and Tracked	Planning, Disciplined, Tracking and Verifying Performance
Level 3 - Well Defined	Defining a Standard Process, Perform a Defined Process and Coordinate Practices
Level 4 - Quantitatively Controlled	Establishing, Measurable, Quality Goals and Objectively Managing, Performance
Level 5 - Continuously Improving	Improving Organizational Capability and Process Effectiveness

4. Framwork per la sicurezza

Che cosa è un framework di sicurezza?

Un Framework di sicurezza non è uno standard, bensì un quadro di riferimento nel quale possono essere collocati standard e norme di settore, esistenti e future [5.] L'adozione di un Framework di questo tipo è solitamente volontaria. Si tratta fondamentalmente di "modelli" per la creazione di un programma di protezione delle informazioni, per la gestione dei rischi e per la riduzione delle vulnerabilità. È possibile utilizzare tali frameworks per definire e classificare in ordine di priorità le attività necessarie per realizzare la sicurezza in un'organizzazione.

Trattandosi di modelli e non di schemi di approccio o regole precise e rigide, i frameworks sono più facilmente personalizzabili per risolvere

[5] *. Il compito di definire gli standard compete agli organi e agli istituti di standardizzazione nazionali e internazionali, nonché ai regolatori di settore*

specifici problemi di sicurezza informatica (sono personalizzati per soddisfare le specifiche esigenze di sicurezza di un'organizzazione).

Uno degli elementi chiave dei frameworks è la possibilità di adottare un Maturity Model e quindi:

- di misurare quanto ci si avvicini al modello ideale
- di valutare gli scostamenti in termini di rischio
- di individuare e pianificare gli interventi che possono portare dallo stato "attuale" allo stato "desiderato" (che rispecchia il punto d'arrivo della strategia aziendale in ambito sicurezza) secondo i tempi e i modi pianificati dall'organizzazione.

Alcuni esempi di Framework sono:

COBIT - Control Objectives for Information and Related Technology

È stato sviluppato nella metà degli anni novanta da ISACA, un'organizzazione indipendente di professionisti di IT governance. Nella versione attuale COBIT 5 ha come obiettivo principale l'allineamento dell'IT con gli obiettivi strategici del business-aziendale (non solo sicurezza quindi, ma anche efficienza ed efficacia nell'utilizzo dell'IT).

Framework for Improving Critical Infrastructure Cybersecurity (NIST)

Nel 2013 il Presidente Obama ha emesso un ordine esecutivo (13636) e diretto da NIST per sviluppare un framework, non normativo e la cui adozione è volontaria, basato su standard esistenti, linee guida e pratiche, che consentisse di ridurre i cyber risk delle infrastrutture critiche. Il NIST ha rilasciato la versione 1.0 nel febbraio 2014, descrivendolo come un approccio volontario alla gestione dei rischi di sicurezza informatica, per le organizzazioni di tutti i tipi e dimensioni.

Figura 2. Framework for Improving Critical Infrastructure Cybersecurity del NIST

"L'anima" è il nucleo del framework e comprende cinque funzioni che riflettono il ciclo di vita di un programma di gestione dei rischi legati alla sicurezza informatica: identificare, proteggere, rilevare, rispondere e recuperare.

Queste funzioni sono ulteriormente dettagliate in 22 categorie e 98 sottocategorie, sulle quali sono mappati vari riferimenti informativi, quali ad esempio COBIT, ISO 27001 e NIST SP 800-53.

Le organizzazioni possono quindi valutare:

- l'importanza (criticità) che le varie funzioni (categorie/sottocategorie) hanno nel contesto in esame
- il livello (maturità) con il quale una particolare categoria o sottocategoria funzionale è stata implementata
- dal confronto dei due "profili" si possono individuare i principali rischi cui l'organizzazione è esposta e quali interventi vadano pianificati per riportarli ad un livello considerato accettabile

Esempio di Category del Framework NIST

Function	Category	Subcategory	Informative References
IDENTIFY	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9

		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	COBIT 5 APO03.03, APO03.04, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Framework Nazionale per la Cybersecurity italiano

Il Framework italiano si basa sul "Framework for Improving Critical Infrastructure Cybersecurity" emanato dal NIST, riprendendone i concetti base di Framework Core, Framework Implementation Tier and Framework Profiles. Ne eredita quindi il sistema di Function e Category del Framework Core che di fatto rappresenta quel terreno comune che crea il punto d'incontro tra Framework e standard aziendali sia tecnici sia di gestione del rischio.

La scelta di partire dal Framework statunitense è stata fatta ritenendo che la risposta alle minacce cyber debba prevedere un allineamento a livello internazionale oltre che a livello di sistema paese. Questo anche per permettere a imprese multinazionali di allineare i loro processi di gestione della cyber security in modo più semplice su scala internazionale.

Il Framework del NIST propone un quadro d'insieme altamente flessibile che è stato fatto evolvere nella direzione delle caratteristiche del sistema socio-economico del nostro Paese ottenendo un Framework cross-settoriale che può essere contestualizzato su settori produttivi specifici o su tipologie di aziende con determinate caratteristiche. Questo permette di trasferire pratiche e conoscenze da un settore all'altro in modo semplice ed efficace. [6.]

[6] . Tratto da *Un Framework Nazionale per la Cyber Security*

Il framework nazionale fa suoi tre concetti fondamentali del NIST:

I livelli di priorità. I livelli di priorità definiscono qual' è la priorità con cui si deve affrontare ogni singola Subcategory del Framework Core. Da notare che ogni organizzazione è libera di contestualizzare i propri livelli di priorità in base al tipo di business, alla dimensione, al suo profilo di rischio.

I livelli di maturità. I livelli di maturità definiscono le diverse modalità con cui si può implementare ogni singola Subcategory del Framework Core. Il livello di maturità selezionato deve esser valutato attentamente dalla singola azienda in base al suo business e alla sua dimensione nonché al suo profilo di rischio. Tipicamente livelli di maturità maggiori richiedono effort maggiore, sia dal punto di vista economico che di gestione. Per alcune Subcategory non è possibile definire livelli di maturità.

Contestualizzazione del Framework Creare una contestualizzazione del Framework (per un settore produttivo, per tipologie di azienda o per una azienda singola), significa selezionare le Function, Category e Subcategory del Framework Core pertinenti, specificandone livelli di priorità e di maturità adatti al contesto di applicazione.

Figura 3- Framework nazionale per la Cyber Security

Esempio di livelli di maturità per la Subcategory "ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione"

Livello	Descrizione
M1	M1.1. L'azienda ha definito una strategia per la cyber Security.
M2	M2.1. All'interno della strategia sono definiti gli obiettivi e le attività di cyber Security dell'organizzazione. M2.2. La strategia è allineata con gli obiettivi strategici e rischi aziendali. M2.3. La strategia definisce l'approccio per la Governance della cyber security. M2.3. La strategia definisce la struttura e l'organizzazione per la realizzazione del programma. M2.4. La strategia è approvata dal Consiglio di Amministrazione
M3	M3.1. La strategia è aggiornata regolarmente per tenere conto dei cambiamenti di business, cambiamenti nel contesto operativo, e cambiamenti nel profilo di rischio.

5. Sviluppare un sistema esperto per l'analisi dei rischi con Fuzzy World

La logica fuzzy ha numerosi vantaggi in quanto è molto più aderente alla realtà (macroscopica) dei modelli semplificati che necessariamente si è costretti ad utilizzare; è infatti caratterizzata dall'uso di valori continui e non discreti (non ci si limita all'uso di variabili quali ALTO, MEDIO, BASSO, ma ad un insieme "sfumato" e continuo di valori).

Se rappresentiamo l'IMPATTO con una serie di valori che vanno da Trascurabile a Grave, una possibile rappresentazione utilizzando la logica fuzzy è quella rappresentata nella Fig. 4

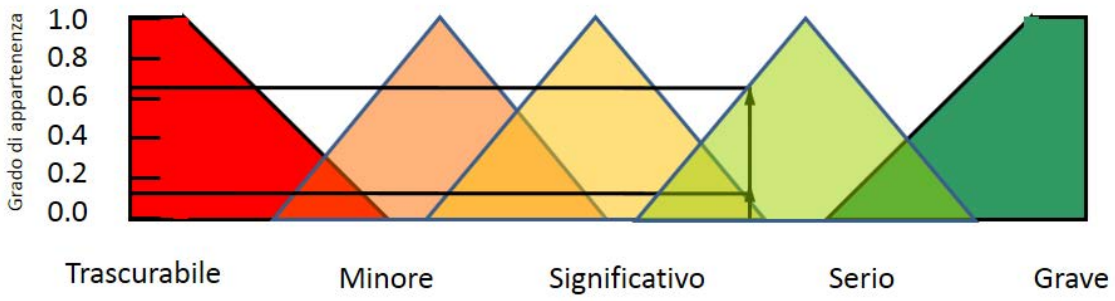
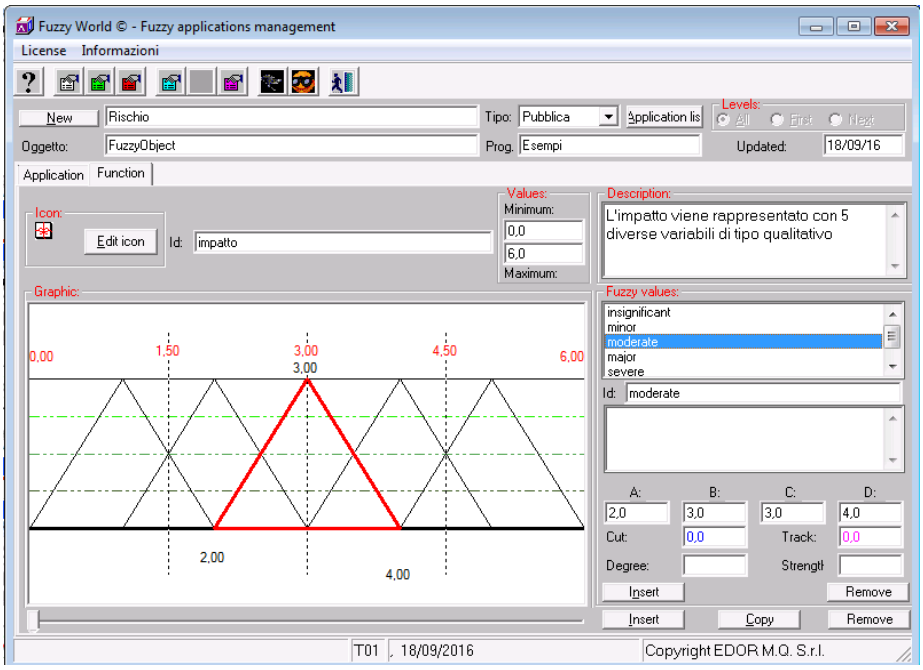


Figura 4. Nella logica fuzzy viene misurato il grado di appartenenza di un elemento ad un insieme

Come applicare queste possibilità all'analisi dei rischi?

Sviluppiamo un esempio di Sistema Esperto per l'analisi dei rischi partendo da una definizione di **RISCHIO** basata su 5 valori qualitativi che vanno da *VeryLight* a *VeryHigh*, derivanti dalla combinazione di 5 valori di **IMPATTO** (Fig. 5) che vanno da *Insignificant* a *Severe* e 5 valori di **PROBABILITÀ** (Fig. 6) che vanno da *Rare* a *Very Likely*.



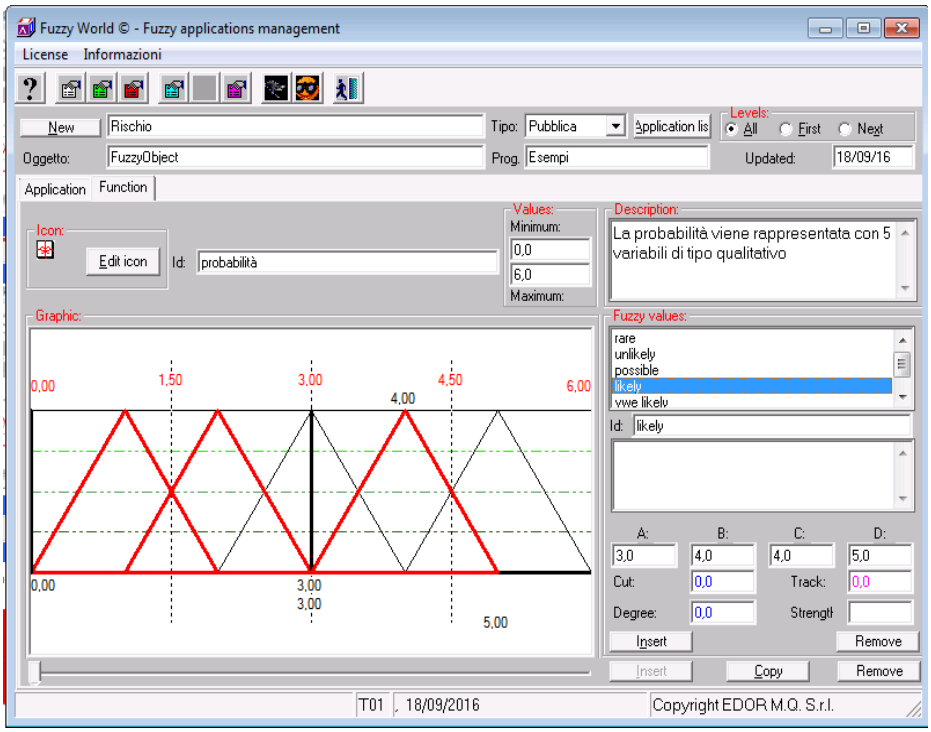


Figura 5 - Definizione di IMPATTO in FuzzyWorld

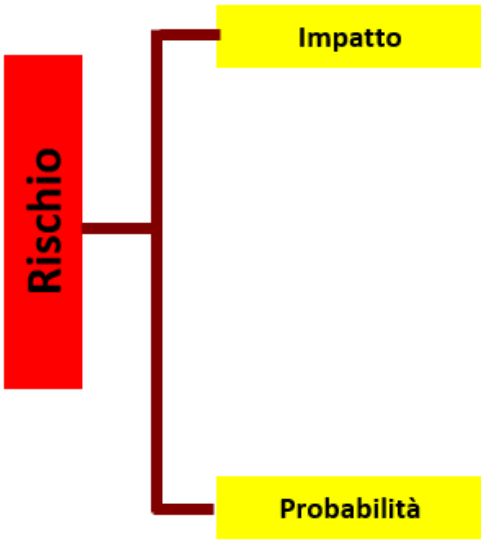
Figura 6 - Definizione di PROBABILITÀ in FuzzyWorld

In termini di regole, la logica applicabile per la determinazione del RISCHIO è la seguente:

IF **PROBABILITÀ** IS xx AND **IMPATTO** IS xx THEN **RISCHIO** IS xx

Per ragioni tecniche, conviene suddividere il nostro Sistema esperto in piccole parti ("*chip di conoscenza*") che modellizzano il sistema in esame.

Nella figura 7 viene presentato un primo chip di conoscenza, composto da 2 ***antecedenti*** (informazioni note) ed un ***conseguente*** (risultato dell'applicazione delle regole agli antecedenti).



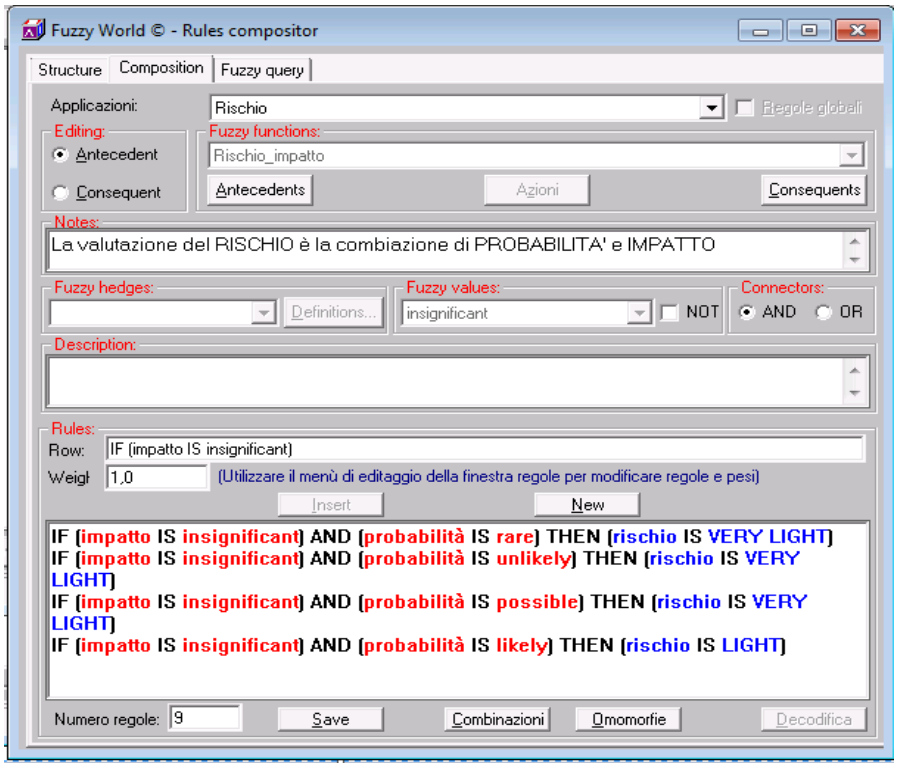


Figura 7. Il S.E. per l'analisi del rischio

Figura 8. Regole per il calcolo del RISCHIO in FuzzyWorld

Fino a qui nulla di particolare, ma iniziamo ora dare delle regole per definire l'**IMPATTO**.

La valutazione dell'**IMPATTO** può derivare da numerosi fattori, quali ad esempio la perdita economica (diretta, indiretta, consequenziale…), ma anche dal numero di servizi o dal numero di clienti impattati dall'evento dannoso o ancora dal fatto che l'evento possa avere delle conseguenze legali (intese come violazioni di norme o contenzioso con vari soggetti) o delle conseguenze sulla reputazione dell'organizzazione. Altri elementi potrebbero essere presi in considerazione, ma in questo esempio ci limitiamo a quelli citati *(Fig. 9).*

Per essere applicabile a qualunque azienda i dati non possono essere espressi in valore assoluto, ma ad esempio in percentuale (sul fatturato, sul totale dei clienti, sul totale dei servizi…).

Analogamente, per quanto attiene alla PROBABILITÀ possiamo considerare ad esempio il numero di avvenimenti nel corso dell'anno per definire se un evento è raro o molto frequente.

Anche in questo caso è necessario definire delle scale di valori per quanto riguarda le variabili espresse in percentuali e parametri di altra natura per quanto attiene l'impatto legale e reputazionale.

Si potrebbe per questi ultimi esprimere solo un SI/NO o dare anche in questo caso una scala di valori.

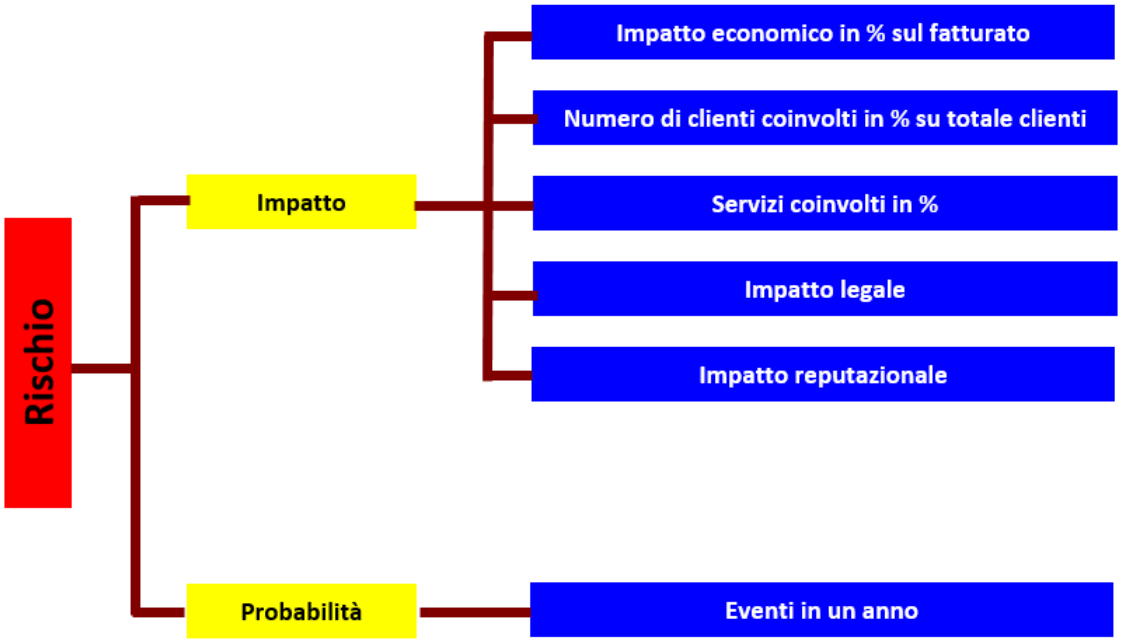
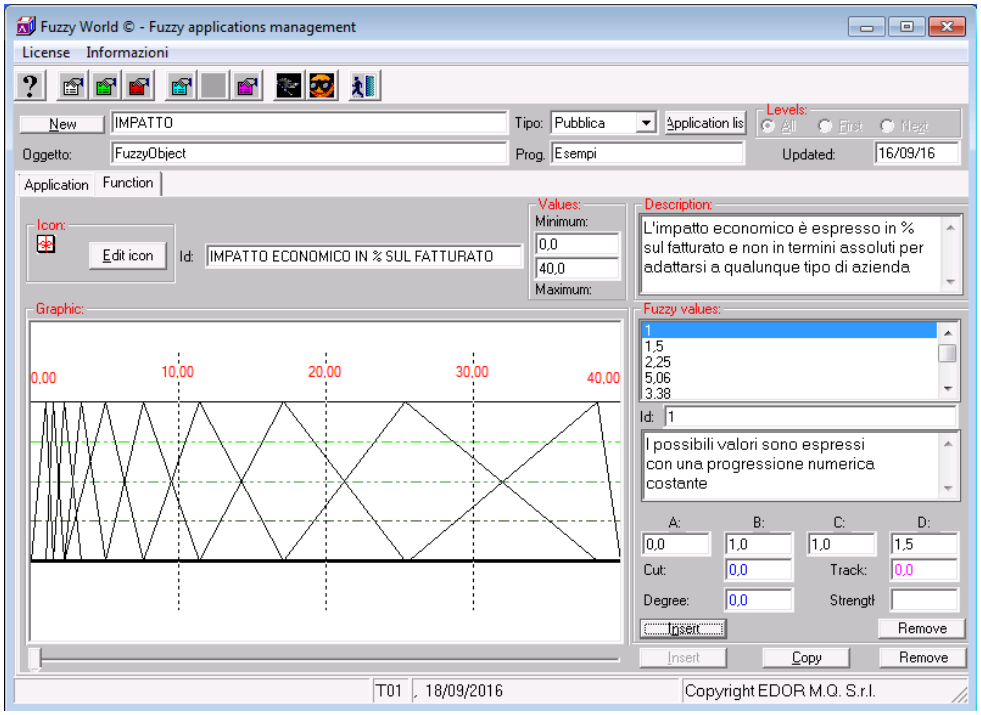


Figura 9 - La declinazione di Impatto e Probabilità

Nell'esempio le variabili economiche usano una scala di 10 valori in progressione *(Fig. 10).*



Per quanto riguarda la frequenza va ricordato che la logica fuzzy opera con un insieme continuo di valori ed è quindi possibile definire direttamente in FuzzyWorld la numerosità degli eventi annuali attribuibili a ciascuna variabile considerata *(Fig. 11).*

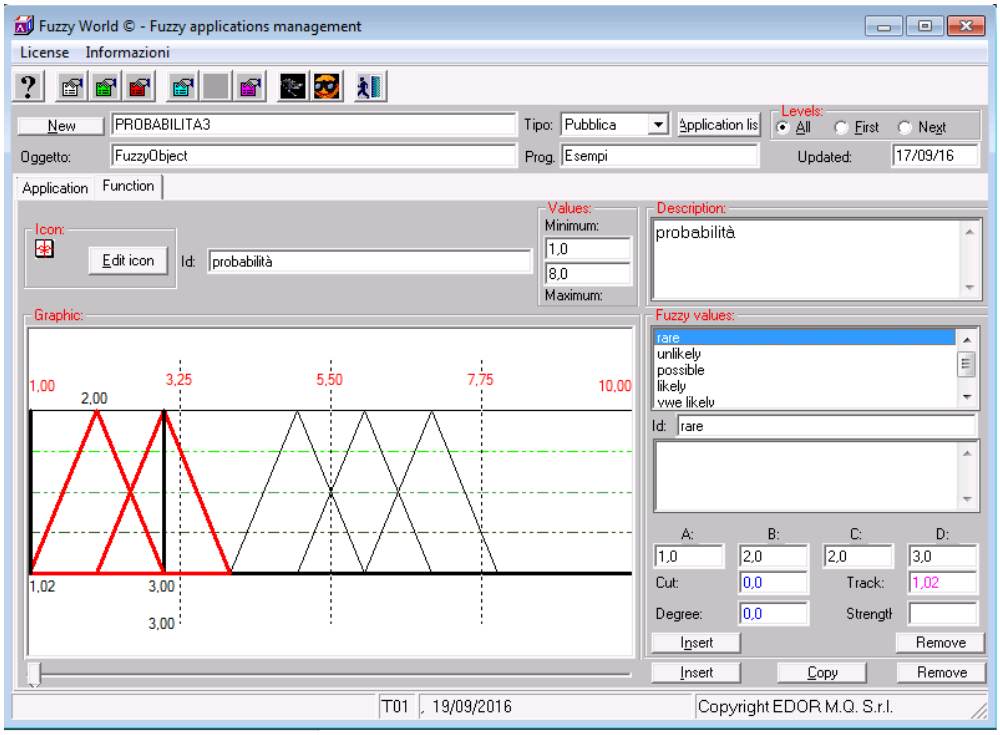


Figura 10. La valorizzazione dell'Impatto Economico nel S.E.

Figura 11. La valorizzazione della probabilità nel S.E.

Le possibili combinazioni di tutte le variabili così introdotte avviene mediante una regola di questo tipo:

IF *impatto economico in % sul fatturato IS x*
AND *impatto economico in % sul fatturato IS <=x+1*
AND *n. di clienti coinvolti in % su totale clienti IS y*
AND *n. di clienti coinvolti in % su totale clienti IS <=y+1*
…
AND *impatto legale IS si/no*
AND *impatto reputazionale IS si/no*
THEN *impatto* **IS** *n*

Che, se volessimo elencarle tutte, porterebbe ad un numero rilevantissimo di possibili combinazioni dove il risultato (n) deve essere attribuito manualmente dall'esperto.

Fortunatamente questo non è necessario in quanto è possibile addestrare la rete neurale mediante la compilazione di fogli Excel sui quali rappresentare i valori di antecedenti e conseguenti *(Fig. 12).*

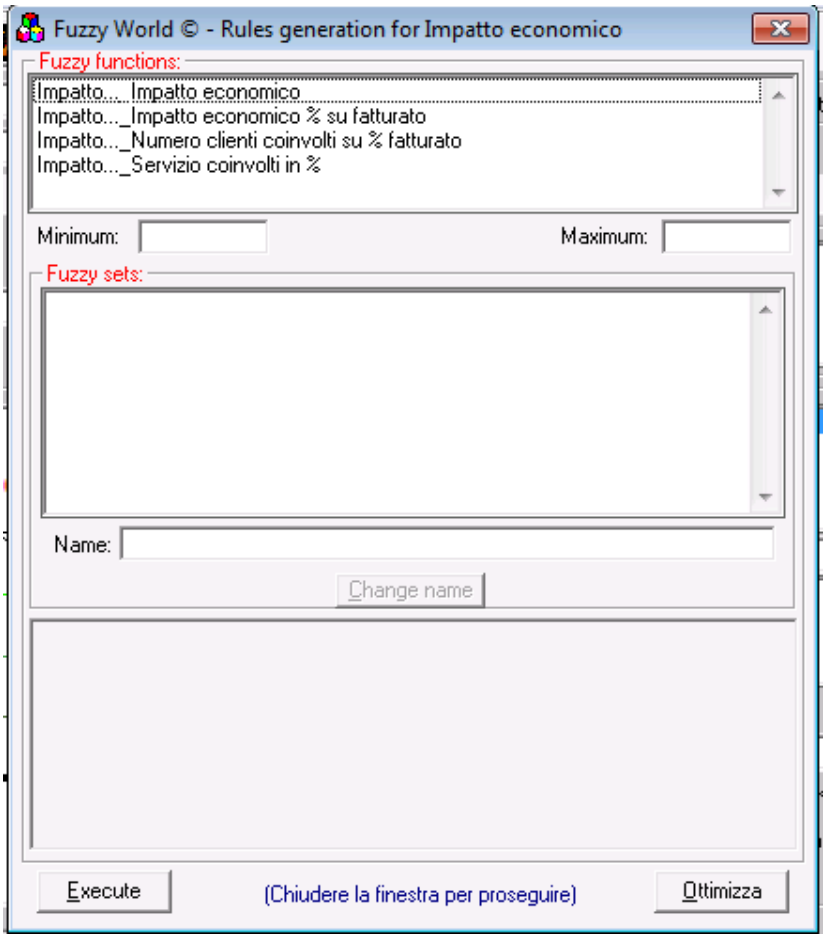
impatto economico in % sul fatturato	numero di clienti coinvolti in % su totale clienti	servizi coinvolti in %	Impatto economico	Pesi
1,00	0,00	0,00	1	1
1,50	0,00	0,00	1	1
2,25	0,00	0,00	1	1
3,38	0,00	0,00	1	1
5,06	0,00	0,00	1	1
7,59	0,00	0,00	2	1
####	0,00	0,00	2	1
####	0,00	0,00	2	1
####	0,00	0,00	3	1
####	0,00	0,00	3	1
1,00	1,00	1,00	1	1
1,50	1,30	1,50	1	1
2,25	1,69	2,25	2	1
3,38	2,20	3,38	2	1
5,06	2,86	5,06	2	1

impatto legale	impatto reputazionale	Impatto sociale	Pesi
0	0	0	1
0	1	1	1
0	2	1	1
0	3	2	1
1	0	1	1
1	1	1	1
1	2	2	1
1	3	2	1
2	0	1	1
2	1	2	1
2	2	2	1
2	3	3	1
3	0	1	1
3	1	2	1
3	2	3	1

impatto economico	impatto sociale	Impatto	Pesi
1	0	1	1
2	0	1	1
3	0	2	1
4	0	2	1
5	0	3	1
1	1	1	1
2	1	2	1
3	1	2	1
4	1	3	1
5	1	4	1
1	2	2	1
2	2	3	1
3	2	4	1
4	2	5	1
5	2	5	1

Figura 12. L'impostazione dei fogli Excel con antecedenti e conseguenti per l'addestramento della rete neurale

Questa modalità operativa presenta enormi vantaggi; il primo è che non è necessario formulare una riga di antecedenti e conseguenti per ogni possibile combinazione di valori. Sarà infatti la rete neurale che determinerà il modo di comportarsi nelle varie situazioni analogamente a quello che fa un bambino che, imparando a camminare, non sperimenta tutte le possibili combinazioni che possono presentarsi nella realtà. La rete neurale elaborerà tutte le possibili soluzioni; eventuali ulteriori regole potranno inoltre essere aggiunte dinamicamente durante l'utilizzo dell'applicazione.



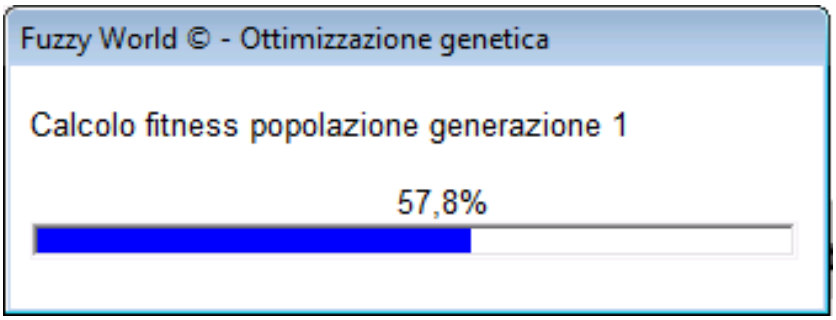


Figura 13. Importazione foglio Excel

Figura 14. Ottimizzazione con algoritmi generici

Il modello finale viene così rappresentato:

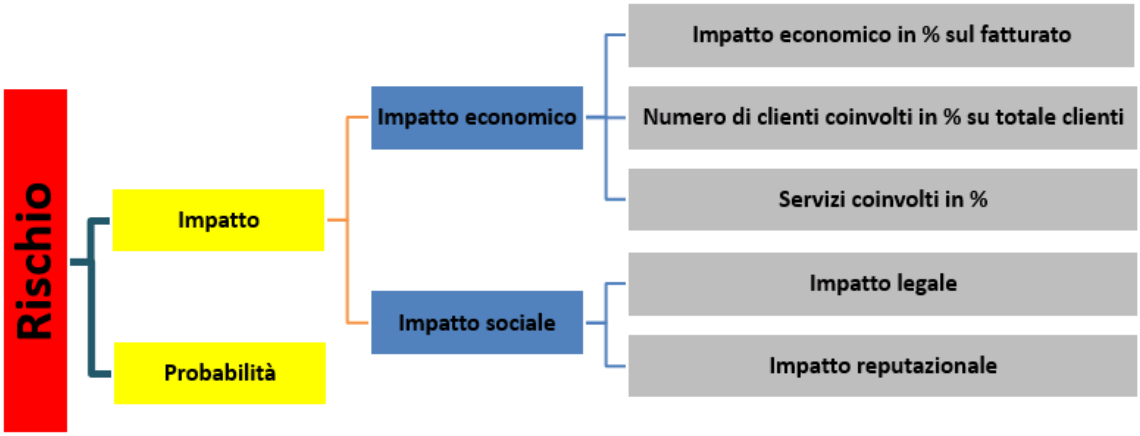


Figura 15. Modello finale

costituito dai seguenti chip di conoscenza:

- Chip di "*impatto economico*", composta da 3 antecedenti
- Chip di "*impatto sociale*", composto da 2 antecedenti
- Chip di "*impatto*", composto da 2 antecedenti
- Chip di "*rischio*", composto da 2 antecedenti (il chip di "*impatto*", a sua volta composto e il chip di "*probabilità*" non sotto livellato)

Il S.E. finale è rappresentato nella Figura 15; il modello può essere articolato ulteriormente, introducendo nuove variabili o dettagliando quelle esistenti. In conclusione, la disponibilità di un adeguato modello e di dati per l'addestramento consente la realizzazione di un S.E. perfettamente operativo in tempi molto contenuti.

NOTA

Le immagini e gli esempi di questo articolo sono tratti dai libri:

- **Intelligenza artificiale e softComputing:** applicazioni pratiche per aziende e professionisti, *L. Schiavina e G. Butti* (in corso di pubblicazione presso FrancoAngeli Editore)
- **GDPR Nuova privacy la conformità su misura**, *G. Butti e A. Piamonte* – ITER (www.iter.it)

Bibliografia.

[1] Definition of Cybersecurity - Gaps and overlaps in standardization -ENISA - 2015

[2] Cyber Security Capability Maturity Model (CMM) – V1.2 – Global Cyber Security Capacity Center - 2014

[3] CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) - FACILITATOR GUIDE – Global Cyber Security Capacity Center - 2014

[4] 2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security – Laboratorio Nazionale CINI di Cyber Security - Consorzio Interuniversitario Nazionale per l'Informatica – 2015

[5] Framework for Improving Critical Infrastructure Cybersecurity – NIST - 2014

[6] CMMI® for Services, Version 1.3 - Software Engineering Process Management Program – 2010

[7] ISO/IEC TR 15504-1:1998(E)

[8] RISK ANALYSIS Approfondimenti – ISCOM – 2006

[9] Privacy Maturity Assessment Framework - Elements, attributes, and criteria (version 2.0) – New Zealand Government – 2014

[10] AICPA/CICA - Privacy Maturity Model - March 2011

[11] Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®) - ISO/IEC 21827:2008(E)

[12] IT Risk Assessment:Quantitative and Qualitative Approach - Artur Rot - Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[13] Taxonomy of Information Security Risk Assessment (ISRA) - JOURNAL OF COMPUTERS & SECURITY – ELSEVIER - Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzega and Mohamed Cheriet

[14] SoftComputing: applicazioni pratiche per aziende e professionisti, L. Schiavina e G. Butti (in corso di pubblicazione presso FrancoAngeli Editore)

[15] GDPR Nuova privacy la conformità su misura, G. Butti e A. Piamonte – (in corso di pubblicazione presso ITER)