

Argomenti unistudium

Tecniche di valutazione del rischio

La norma IEC 31010 serve come supporto per la Iso 31000 e fornisce una guida alla selezione e applicazione delle tecniche sistematiche per la valutazione del rischio ed il suo **scopo** è quello di fornire informazioni per poter prendere decisioni su come trattare particolari **rischi**. La norma riguardo alla valutazione del rischio presuppone che l'organizzazione abbia una politica per decidere quando e come i rischi debbano essere valutati e per fare ciò vanno considerati i seguenti elementi:

comunicazione: ci dev'essere un efficace comunicazione con le parti interessate così da assicurarsi l'**identificazione** in modo adeguato

determinare il contesto: vanno fissati gli obiettivi della valutazione del rischio, i criteri e il programma di valutazione considerando i parametri interni ed esterni dell'organizzazione

valutazione del rischio: fornisce una comprensione dei rischi e delle loro cause

trattamento dei rischi: vanno selezionate una o più opzioni volte a modificare la probabilità di accadimento dei rischi

monitoraggio: i rischi e il loro controllo vanno monitorati per assicurarsi che i trattamenti siano efficaci

L'output che restituisce il **processo di valutazione** del rischio è un input ai processi decisionali dell'organizzazione. Il processo è **diviso in 3 fasi**

Identificazione dei rischi: processo per individuare e riconoscere i rischi attraverso per esempio una **check list**

Analisi dei rischi: determina le **conseguenze e le loro probabilità** così da comprendere meglio i rischi

Selezione delle tecniche di valutazione: va scelta la **tecnica adatta in base al grado di applicabilità** rispetto la fase di valutazione in cui ci troviamo ed **in base** poi alle **risorse** che essa richiede

Il giurista e la comprensione dell'analisi del rischio

Cosa è il rischio? In ambito giuridico molto spesso il concetto di rischio e pericolo vengono equiparati anche se nelle più recenti normative nazionali ed europee si attribuiscono concetti ben distinti infatti il **pericolo** è la **capacità di un fattore di provocare danno** mentre il **rischio** è la **probabilità di realizzazione di un danno causato da un determinato fattore** e quindi si può dire che il **pericolo si misura in base al rischio** perché la capacità di procurare effettivamente un danno dipende dalla probabilità. Al fine di gestire il **rischio** accomunando le differenti discipline relative è stato fatto un standard internazionale l'**ISO 31000** che mostra il rischio anche come opportunità e che un suo azzeramento è praticamente impossibile per questo motivo vanno effettuate delle **attività ricorrenti** (ciclo di deming Plan Do Check Act), fornisce anche una **formula R=P*G** (probabilità*gravità)

Differenti tipologie di interessi sulle quali incide il rischio affrontato: chi si occupa della gestione del rischio deve dargli uno scopo e normalmente è quello di garantire il perseguimento degli obiettivi, un esempio lo si può fare con il GDPR in cui il rischio è un data breach che limiterebbe il perseguimento degli obiettivi ed ecco perché viene effettuata una gestione del rischio

Le fasi del risk management: Il processo di gestione del rischio può essere suddiviso in differenti fasi: **comunicazione, definizione del contesto interno ed esterno, gestione e monitoraggio del rischio** e ciascuna fase dovrà essere documentata in questo senso lo prevede anche la legge per prevenire i

fenomeni corruttivi. La **prima fase** ovvero la comunicazione è essenziale per **raccogliere informazioni** poi la **seconda** serve a **definire il contesto** interno ed esterno così da poter fare una gestione su misura del rischio

Valutazione del rischio: La fase di **valutazione** si compone in **tre sotto fasi: identificazione, analisi e valutazione.** L'**identificazione** ricerca i **pericoli che possono incidere in modo più o meno significativo sul rischio**, una tecnica usata è quella basata su check list sviluppate da terzi e l'output atteso da questa sottofase è l'individuazione di quanti più fattori di rischio possibile. Una volta identificati passiamo all'**analisi** del rischio in cui si cerca di comprendere **quale peso attribuire alla probabilità e alla gravità del rischio tenendo in considerazione i fattori di contrasto già attivi**, una metodologia applicata è quella di dare un valore numerico alla gravità e all'impatto del rischio ed agli elementi di contrasto. Nell'ultima sottofase quella di **valutazione** si **confrontano i risultati delle analisi** dei rischi per capire se è richiesto un intervento specifico ed è approccio comune classificarli in grave, medio e trascurabile

Gestione del rischio: Le misure per contrastare il rischio consistono sia in misure proattive e in misure reattive ed in genere l'individuazione e applicazione di queste non è sempre rimessa alla discrezionalità del soggetto obbligato infatti **alcune misure sono individuate dal legislatore che ne impone l'applicazione**

Monitoraggio e aggiornamento: L'ultima fase del processo di gestione del rischio consiste nel **monitoraggio delle misure proattive** individuate infatti il ciclo di gestione del rischio è ben rappresentato dal ciclo di Deming (Plan Do Check Act) infatti la gestione è tesa al miglioramento continuo (filosofia Kaizen)

Conclusioni: I processi di gestione del rischio rappresentano un'opportunità per il **giurista** che ora con l'introduzione di nuove tecnologie dovrà diventare un **ibrido** in grado cioè di comprendere anche le dinamiche intorno alle tecnologie emergenti oltre che i meccanismi di gestione del rischio

IA e sicurezza informatica

Per **sistema I.A.** utilizzando la definizione dell'A.I. act s'intende un **sistema automatizzato che per obiettivi espliciti o impliciti deduce dall'input che riceve come generare output** quali contenuti o decisioni. Ci sono diversi sistemi di I.A. ed ognuno varia in base ai livelli di autonomia e adattabilità, ci sono i sistemi basati su regole che eseguono unicamente gli algoritmi definiti dai propri ricercatori, poi ci sono quelli basati sulle reti neurali che possono imparare da sole a risolvere problemi portando ad un'evoluzione dal machine learning al deep learning in cui la rete gestisce in autonomia i dati e i problemi proposti, un esempio di questa categoria è chat GPT.

L'**A.I. act** oltre a dare una definizione **impone misure di protezione** per evitare impatti negativi ai diritti fondamentali **adottando un principio basato sul rischio**. Definisce il **divieto di alcuni sistemi** in quando espongono a rischi inaccettabili tra le quali: sistemi di social scoring, sistemi di scraping non mirato, anche se alcuni sistemi possono essere utilizzati in via eccezionale per contrasto. Poi stabilisce **requisiti ed obblighi per i sistemi ad alto rischio** mentre **vincola a requisiti di trasparenza quelli a basso rischio**. Sono ad alto rischio tutti quei sistemi che svolgono una funzione di sicurezza per un prodotto o che abbiano bisogno di una dichiarazione di conformità. Mentre quelli a basso rischio sono tutti quelli che non hanno un rischio significativo ma hanno lo stesso dei vincoli infatti il fornitore deve mettere a disposizione tutta la documentazione e va registrato.

I **requisiti per la messa in mercato di un I.A. ad alto rischio** sono l'**identificazione** e valutazione sia dei **rischi ad uso conforme e non** per poi adottare misure opportune. Un altro requisito è quello di **avere una dichiarazione di conformità nell'ambito della cybersicurezza** implementando misure di sicurezza fin dalla progettazione per evitare per esempio un data poisoning. Parlando poi d'innovazione potrebbe non bastare la soglia massima messa dal legislatore con lo scopo di fissare un punto oltre al quale i modelli che si collocano al di sopra non sono ancora compresi, infatti GPT4 e Gemini l'hanno raggiunta e rientrano nei modelli di IA per finalità generali.