Sommario

1. INTRODUZIONE

In un mondo che, giustamente, si sta sempre più concentrando sulla salute e sicurezza dei lavoratori, i sistemi di gestione del rischio diventano conseguentemente fondamentali. Sempre più numerosi studi dimostrano come una visione a 360 gradi dell'impresa porti a risultati, nel tempo, migliori rispetto a quelli delle aziende che non attuano una gestione dei rischi. Per perseguire tali risultati le aziende necessitano di comprendere il livello complessivo di rischio insito nei loro processi e nelle loro attività. Ciò implica il riconoscere e dare priorità ai rischi più significativi, individuare le criticità, arrivando ad attuare un efficace processo di Gestione del Rischio.

la presente documentazione ha lo scopo di illustrare i principi di un sistema di gestione del rischio, di un sistema per la salute e sicurezza sul lavoro e le tecniche necessarie a metterli in atto.

l'elaborato è diviso in 4 parti fondamentali. La prima parte definisce i concetti di gestione del rischio, di prevenzione e di protezione. La seconda tratta la normativa ISO 31000:2018, cioè le linee guida per l'applicazione di un sistema di gestione del rischio. La terza, direttamente collegata alla seconda, elenca le tecniche di valutazione del rischio illustrate nella ISO 31010:2009 ed infine la quarta elenca i principi di applicazione di un sistema di gestione per la salute e sicurezza dei luoghi di lavoro presenti nella ISO 45001:2018.

i capitoli successivi risponderanno, dunque, alle seguenti domande:

- quali sono e cosa illustrano le normative di riferimento per l'applicazione dei sistemi di gestione?
- quali sono le tecniche di valutazione del rischio?
- perché un'organizzazione dovrebbe adottare un sistema di gestione del rischio?

2. GESTIONE DEL RISCHIO

La Gestione del Rischio, o Risk Management, è un processo aziendale volto alla gestione completa ed integrata dei rischi mediante attività sistematiche quali identificazione, misurazione, valutazione e trattamento del rischio[1]. L'UNI 11230 la definisce come "insieme di attività, metodologie e risorse coordinate per guidare e tenere sotto controllo un'organizzazione con riferimento ai rischi".

Esso coinvolge tutti i processi aziendali e, per risultare efficace, deve essere integrato nella cultura dell'organizzazione, diventandone parte integrante dei processi.

Per fare ciò il processo di Risk Management viene suddiviso nelle seguenti fasi[2]:

- Definizione del contesto: valutazione generale dei processi produttivi e delle attività svolte in azienda;
- Identificazione e analisi dei rischi[3]: l'azienda determina e descrive i principali fattori d'incertezza che potenzialmente possono causare una deviazione nel raggiungimento degli obiettivi. Questo punto coinvolge le principali risorse dell'azienda a diversi livelli gerarchici. Poiché l'identificazione dei rischi è multidisciplinare e trasversale all'intera azienda, il processo può risultare complesso e pertanto va affrontato con una metodologia di indagine sistematica e rigorosa. In linea generale viene posta l'attenzione su due aspetti principali: la raccolta di informazioni (volta a raccogliere ed analizzare gli aspetti chiave per gli specifici rischi oggetto dell'analisi) e le tecniche di identificazione (deduttive o induttive, ecc.). Al termine dell'attività di identificazione, i singoli rischi sono descritti lungo le tre componenti chiave: sorgente (pericolo potenziale), evento (trigger che porta al verificarsi degli effetti), effetti (conseguenze del verificarsi di un rischio);

- Valutazione dei rischi: La valutazione dei rischi è la prima misura generale di tutela dei lavoratori**,** l'origine delle decisioni da prendere in materia di salute e sicurezza sul lavoro e dei rischi per la collettività. Per valutazione si intende l'analisi delle possibilità di accadimento degli eventi indesiderati e della loro gravità potenziale. Vene effettuata dal datore di lavoro con la collaborazione del responsabile del servizio di prevenzione e protezione - RSPP e del medico competente e deve considerare: deve contenere: la scelta delle attrezzature di lavoro, le sostanze e i preparati chimici, la sistemazione dei luoghi, lo stress lavoro-correlato, le specificità dovute ad età, sesso, provenienze da altri paesi;
- Preparazione e approvazione Documento Valutazione dei Rischi (DVR): Il DVR, sulla base dei rischi precedentemente identificati e valutati, deve contenere:
    - relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa;
    - l'indicazione delle misure di prevenzione e protezione adottate e dei dpi;
    - l'individuazione delle procedure per l'attuazione delle misure da realizzare e l'individuazione dei ruoli dell'organizzazione aziendale che vi debbono provvedere;
    - I nominativi delle figure della sicurezza RSPP, RLS, medico competente, squadra di emergenza;
    - l'individuazione delle mansioni che espongono i lavoratori a rischi specifici.

- Esecuzione, controllo e modifica del piano: le misure di prevenzione e sicurezza vengono messe in atto, i risultati controllati e valutati. Nel caso in cui le misure messe in atto non portino agli obiettivi prefissati o vi siano modifiche alle procedure aziendali, il piano deve essere riesaminato e modificato.

3. PREVENZIONE E PROTEZIONE

Due concetti fondamentali per la Gestione del Rischio sono quelli di prevenzione e protezione. La prima viene definita come insieme delle azioni e attività che mirano a ridurre gli effetti dei fattori di rischio. Esistono tre livelli diversi di prevenzione:

- Prevenzione primaria: si focalizza sull'adozione di interventi in grado di ridurre a monte l'insorgenza di malattie, o infortuni sul lavoro, combattendo le cause e i fattori predisponenti;
- Prevenzione secondaria: ha come obiettivo la diagnosi precoce di una patologia in modo da intervenire precocemente su di essa;
- Prevenzione terziaria: è volta a ridurre la gravità e le complicazioni di malattie già insorte.

La prevenzione presa in considerazione nel Risk Management è la primaria, definita dal D.Lgs 81/08 come "Il complesso delle disposizioni o misure necessarie anche secondo la particolarità del lavoro, l'esperienza e la tecnica, per evitare o diminuire i rischi professionali nel rispetto della salute della popolazione e dell'integrità' dell'ambiente esterno"[4]. Gli interventi di questo tipo riguardano il lato strutturale e organizzativo dell'attività, come: informazione, formazione e addestramento dei lavoratori, progettazione e costruzione di ambienti, strutture, macchine ed attrezzature, adozione di comportamenti e procedure operative. La protezione invece rientra nel concetto sopraindicato di "prevenzione secondaria" e racchiude le misure volte a ridurre il danno subito a seguito di un evento dannoso. Possiamo differenziare in due tipi la protezione:

- Protezione attiva: riguarda gli accorgimenti messi in atto per ridurre le conseguenze dell'evento dannoso e che richiedono l'intervento dell'uomo.

Per esempio in caso di incendio gli elementi di protezione attiva sono gli idranti, estintori, dispositivi d'allarme, ecc.;

- Protezione passiva: comprende tutte le misure volte a contenere e limitare l'evento dannoso. Per esempio, sempre in caso di incendio, abbiamo i muri tagliafuoco, le vie di uscita, ecc.

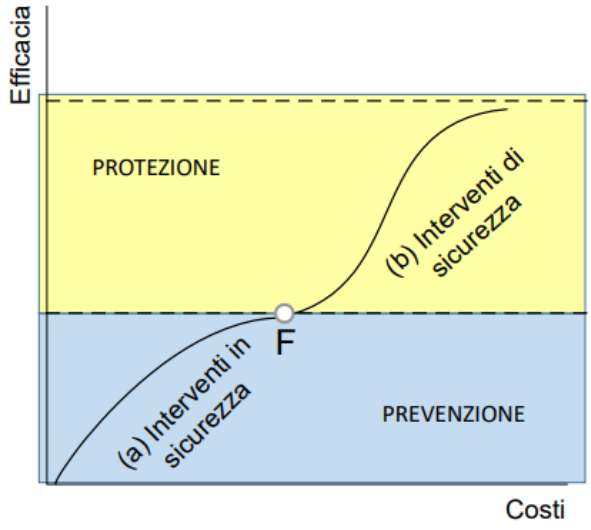
Tra le misure di protezione, inoltre, troviamo i dispositivi di protezione collettiva (D.P.C.) e i dispositivi di protezione individuale (D.P.I). I primi sono volti a proteggere un insieme di persone, come i ponteggi o le porte tagliafuoco. I secondi, invece, proteggono il singolo individuo, qui troviamo, tra gli altri, le maschere facciali, gli elmetti protettivi.

A livello ingegneristico, tramite l'ingegneria della sicurezza, ovvero la disciplina attraverso la quale si studiano, anche in relazione ai presupposti economici, le circostanze di rischio che possono determinarsi durante l'esercizio di sistemi complessi, i concetti di prevenzione e protezione trovano il loro utilizzo nella fase di progettazione dell'attività o di una parte di essa. Il principio ispiratore del progettista deve essere rivolto ad evitare danni non solo agli uomini che attuano i processi, ma anche a coloro che ne sono estranei, con riguardo non meno attento alle cose e all'ambiente. Questo principio fornisce, a chi si occupa di progettazione industriale, due riferimenti fondamentali per lo svolgimento dell'incarico[5]:

- Progettare in sicurezza l'impianto: ossia seguire, durante la progettazione, tutte le regole, i suggerimenti e le indicazioni dettate dall'esperienza, dalle conoscenze tecnico-scientifiche e dalla legislazione, affinché la probabilità che si verificano eventi di rischio siano ridotte ai livelli minimi. (Prevenzione);
- Progettare la sicurezza dell'impianto: organizzare un'efficiente struttura di uomini, mezzi e procedure ed implementare il sistema tecnico-produttivo di cui si vuole aumentare la sicurezza, affinché gli accadimenti, susseguenti a situazioni di pericolo, non abbiano conseguenze dannose. Se ciò non fosse possibile queste devono essere le più limitate possibili. (Protezione).

L’insieme di queste due fasi costituisce il sistema di sicurezza aziendale (fig. 1) e la curva risultante dagli interventi in sicurezza (a) + gli interventi di sicurezza (b) rappresenta la curva di efficacia del sistema di sicurezza aziendale. La posizione del punto di contatto F è importante ai fini della minimizzazione del costo globale degli interventi rapportato all’efficacia dei risultati, in quanto (a) tende ad un asintoto che rappresenta il limite di convenienza degli interventi in sicurezza. La curva (b) ha come origine tale punto ed il suo andamento è influenzato dalla sua ordinata di origine. Piccole spese per la sicurezza che non vengono sostenute in fase di realizzazione, vengono amplificate da un successivo progetto di sicurezza di adeguamento, fino a rendere non conveniente la modifica dell’impianto e consigliarne la dismissione. Inoltre, a mano a mano che la qualità in sicurezza della realizzazione scade, le aree che dovranno essere oggetto di interventi di sicurezza aumenteranno e comporteranno una spesa maggiore di quella dei singoli interventi non effettuati precedentemente[6].

Fig. 1 – Curva risultante



4. ISO 31000:2018 –GUIDE LINEA RISK MANAGEMENT

4.1. Scopo

La ISO 3100:2018 si pone come obiettivo di creare e proteggere il valore nell'impresa. Per fare ciò essa fornisce delle linee guida, da personalizzare per ogni contesto, sulla gestione dei rischi affrontati dalle organizzazioni. Essa tiene conto sia del contesto esterno sia di quello interno dell'organizzazione, comprendendo anche i comportamenti umani e i fattori culturali presenti. All'interno della normativa vengono discussi i principi, il framework e i processi su cui si basa la gestione del rischio. Questi tre componenti possono già essere presenti in azienda ma potrebbero necessitare di miglioramenti o adattamenti per far si che la gestione del rischio sia efficiente, efficace e coerente.

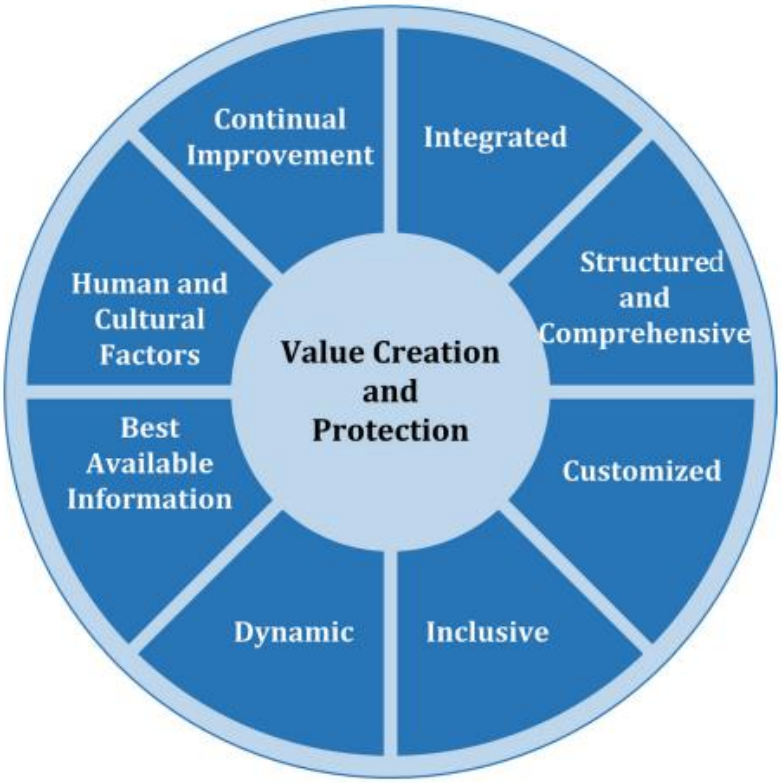
4.2. Principi

La norma delinea dei principi (fig.2) che forniscono indicazioni sulle caratteristiche di una gestione del rischio efficace ed efficiente. I principi, che costituiscono la base della gestione del rischio, sono[7]:

- Integrazione nell'ambito di tutti i processi dell'organizzazione: non è un'attività indipendente, deve essere parte integrante di tutti i processi aziendali;
- Struttura ben definita: un approccio sistematico, strutturato e dinamico contribuisce all'efficienza e a risultati coerenti;
- Personalizzato: in linea con il contesto esterno ed interno e con il profilo di rischio dell'azienda;
- Inclusivo: il coinvolgimento, a tutti i livelli aziendali, assicura la pertinenza e l'aggiornamento della gestione del rischio. Inoltre, permette che tutti siano opportunamente rappresentati e che i loro punti di vista siano presi in considerazione;

- Processo dinamico: la Gestione del Rischio deve rispondere continuamente al cambiamento a fronte di cambiamenti interni ed esterni del contesto di riferimento;
- Basato sulle migliori informazioni disponibili: fonti di informazione come dati storici, esperienza, osservazioni sono elementi fondamentali per il processo di gestione del rischio;
- Fattori umani e culturali: i comportamenti umani e culturali influenzano significativamente tutti gli aspetti della gestione del rischio, a tutti i livelli e processi;
- Continuo miglioramento: sviluppo e attuazione di strategie per ottimizzare la gestione del rischio.

Fig. 2 – Principi ISO 31000:2018



4.3. Framework

Una corretta integrazione nella governance è fondamentale per l'efficacia della gestione del rischio, ciò comporta il supporto degli stakeholder, compresa l'alta dirigenza. Per fare ciò la ISO 31000 fornisce un framework (fig. 3), il cui sviluppo comporta l'integrazione, la progettazione, l'implementazione, la valutazione e il miglioramento della gestione del rischio in tutta l'organizzazione.

Fig. 3 - Framework

Tutti i componenti del framework, in seguito a un'attenta valutazione delle pratiche di gestione del rischio esistenti, dovrebbero essere personalizzati in base alle esigenze[8].

4.3.1. Leadership and Commitment[9]

Dove applicabile, la gestione del rischio dovrebbe essere garantita dalla direzione generale e dagli organi deputati al controllo. Inoltre, dovrebbero dimostrare leadership e impegno a raggiungere gli obiettivi mediante:

- Personalizzazione e implementazione di tutti i componenti del framework;
- Allocazione delle giuste risorse per gestire il rischio;
- Stabilire un approccio o un piano di gestione del rischio mediante una dichiarazione ufficiale;
- Assegnare diversi livelli di autorità, responsabilità e responsabilizzazione all'interno dell'organizzazione.

Questi punti saranno fondamentali per:

- Allineare gestione del rischio ed obiettivi tramite una chiara strategia;
- Riconoscere ed affrontare tutti i rischi;
- Stabilire il numero e i tipi di rischio presenti che serviranno per guidare lo sviluppo dei criteri di rischio, garantendo la loro comunicazione alle parti interessate;
- Promuovere un sistematico monitoraggio dei rischi;
- Assicurarsi che il framework di gestione del rischio sia appropriato all'organizzazione.

Gli organi di controllo, deputati alla supervisione della gestione del rischio, sono tenuti a:

- Assicurarsi l'adeguata considerazione dei rischi durante la definizione degli obbiettivi aziendali;
- Comprendere i rischi affrontati dall'organizzazione al fine di raggiungere i propri obiettivi;
- Garantire la corretta ed efficace implementazione dei sistemi di gestione del rischio;
- Garantire la corretta comunicazione dell'informazione e gestione dei rischi presenti.

4.3.2. Integrazione[10]

Ogni struttura differisce dalle altre a seconda dello scopo, degli obiettivi e della complessità della stessa, una corretta integrazione della gestione del rischio, presente in ogni parte dell'organizzazione, è basata sul conoscimento di questi contesti.

La governance guida le relazioni sia interne che esterne, i processi e le pratiche necessarie al raggiungimento dello scopo, il management, invece, trasforma essi nella strategia per raggiungere gli obiettivi di sostenibilità a lungo termine. Fondamentale quindi, all'interno di un'organizzazione, determinare i ruoli di responsabilità e supervisione della gestione del rischio.

Integrare la gestione del rischio è un processo dinamico ed interattivo, da personalizzare in base alle esigenze. Essa dovrebbe essere parte dell'organizzazione, della governance, leadership e commitment, strategia, obiettivi e operazioni.

4.3.3. Design[11]

La progettazione della gestione del rischio si può dividere in cinque punti fondamentali:

1. Comprensione dell'organizzazione e del suo contesto. Quest'ultimo si può dividere in esterno o interno. Il primo rappresenta tutti i fattori (sociali, culturali, politici, ecc.) che influenzano il mondo esterno, ma anche le relazioni con stakholder esterni, le loro esigenze e aspettative. Il contesto interno, diversamente, include tutti i componenti dell'organizzazione, quali, per esempio la strategia, gli obiettivi, le risorse e conoscenze disponibili[12];
2. Articolare l'impegno alla gestione del rischio attraverso una chiara politica, l'alta dirigenza e gli organi di controllo dovrebbero dimostrare ed articolare il loro continuo impegno riguardante la gestione del rischio. Per fare ciò l'organizzazione potrebbe rinforzare la necessità di integrare la gestione del

rischio in tutte le attività, far si che tutte le risorse necessarie siano disponibili[13];

3. Assegnare ruoli organizzativi, autorità e responsabilità. Importante che l'assegnamento di ruoli e responsabilità sia comunicato a tutti i livelli dell'organizzazione, sottolineando che gestire il rischio è una responsabilità fondamentale[14];
4. Allocare risorse appropriate. Esse possono includere persone, competenze ma anche metodi, strumenti per la gestione del rischio. Tutto questo considerando capacità e vincoli delle risorse esistenti[15];
5. Stabilire comunicazione e consultazione per facilitare l'effettiva applicazione della gestione del rischio. La comunicazione riguarda la condivisione di informazioni ai diretti interessati. La consultazione si occupa di raccogliere il feedback dei partecipanti al fine di contribuire al miglioramento[16].

4.3.4. Implementazione[17]

Per affrontare le incertezze del processo decisionale, sia che esse siano presenti o che si manifestino in seguito, l'efficace attuazione del framework richiede l'impegno e la consapevolezza di tutte le parti interessate. Ciò garantirà che il processo di gestione del rischio sia parte di tutte le attività dell'organizzazione e i cambiamenti, interni od esterni, verranno adeguatamente gestiti.

Il framework di gestione del rischio dovrebbe quindi essere implementato tenendo conto di:

- Un piano adeguato che includa tempo e risorse;
- Identificare chi, quando, come e dove prende decisioni all'interno dell'organizzazione;
- Modificare processi decisionali;
- Garantire che le disposizioni riguardanti la gestione del rischio siano correttamente capite e praticate.

4.3.5. Valutazione[18]

Misurare periodicamente le performance del framework rispetto al suo scopo e attuazione e determinare se rimane idoneo al fine di conseguire gli obiettivi prefissati è fondamentale per valutare l'efficacia di esso.

4.3.6. Miglioramento[19]

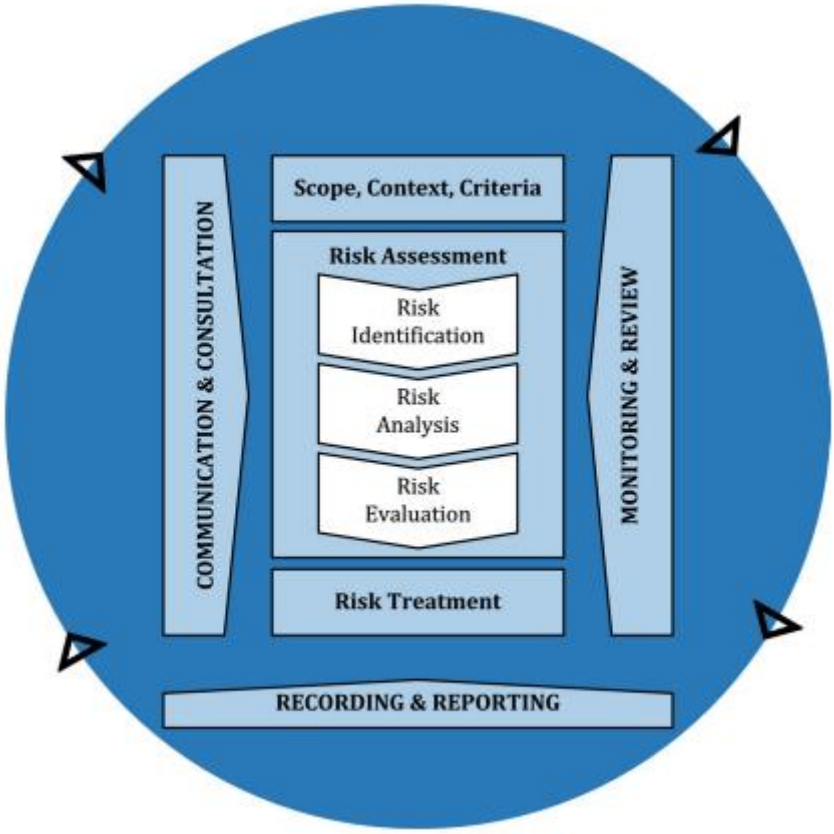
L'organizzazione dovrebbe continuamente monitorare e adattare il framework ai cambiamenti esterni ed interni, migliorando così il suo valore.

Il miglioramento dovrebbe riguardare l'idoneità, l'adeguatezza e l'efficacia della gestione del rischio. Man mano che vengono identificate lacune od opportunità di miglioramento dovrebbero essere sviluppati piani e compiti da assegnare ai responsabili dell'attuazione.

4.4. Processi[20]

Come illustrato in figura (fig. 4) i processi della gestione del rischio comportano l'applicazione delle politiche, procedure e pratiche alle attività di comunicazione e consulenza, definizione del contesto e valutazione, trattamento, monitoraggio, revisione, registrazione e segnalazione dei rischi.

Fig. 4 - Processi



4.4.1. Comunicazione e consultazione[21]

Lo stretto coordinamento tra comunicazione e consultazione facilita lo scambio tempestivo, pertinente e accurato delle informazioni. La prima promuove la consapevolezza e la comprensione del rischio, mentre la seconda ottiene ed elabora feedback e informazioni per supportare il processo decisionale. Tutto ciò per assistere gli stakeholder alla comprensione della gestione del rischio, come vengono prese determinate decisione e la ragione per cui alcune azioni sono necessarie.

Esse mirano a:

- Riunire divere aree di competenza per ciascuna fase del processo di gestione del rischio;

- Prendere in considerazione diversi punti di vista per la definizione dei criteri di valutazione del rischio;
- Facilitare supervisione dei rischi e il processo decisionale fornendo sufficienti informazioni.

4.4.2. Scopo, contesto e criteri[22]

Al fine di personalizzare il processo di gestione del rischio in base al contesto dell'organizzazione bisogna definire:

- Scopo delle attività di gestione del rischio. Essendo esso applicabile a diversi livelli (operativo, strategico, ecc.) bisogna avere chiaro l'ambito in esame e che gli obiettivi da considerare siano allineati a quelli dell'organizzazione. Pianificando l'approccio bisogna tener conto di vari fattori come:
    - Obiettivi e decisioni;
    - Risultati attesi;
    - Tempo, luogo, inclusioni ed esclusioni;
    - Strumenti e tecniche di valutazione del rischio;
    - Risorse necessarie;
    - Relazioni con altri processi dell'organizzazione.
- Contesto interno ed esterno. Per contesto si intende l'ambiente in cui l'organizzazione cerca di raggiungere i propri obiettivi, comprenderlo è importante per vari motivi, in quanto la gestione del rischio avviene all'interno di esso e lo stesso può essere una potenziale fonte di rischio;
- Definizione dei criteri di rischio, specificando quanti e quali tipi di rischi l'organizzazione può permettersi di assumere. I criteri dovrebbero essere allineati con il framework di gestione del rischio. Per stabilirli è quindi importante considerare:
    - Incertezze che influenzano risultati ed obiettivi;
    - Come verranno definite e misurate le conseguenze;
    - Coerenza delle misurazioni;

- Determinazione livello di rischio;
- Considerare combinazioni e sequenze di rischi multipli.

4.4.3. Valutazione del rischio[23]

La valutazione del rischio dovrebbe essere condotta in modo sistematico e collaborativo, attingendo alle conoscenze e ai punti di vista degli stakeholders e utilizzando le migliori informazioni disponibili raccolte tramite indagini.

Essa è divisa in tre step:

- Identificazione del rischio: si basa sul trovare, riconoscere e descrivere i rischi, utilizzando informazioni pertinenti, appropriate e aggiornate. L'organizzazione può servirsi di diverse tecniche, tenendo in considerazione vari fattori come:
  - Fonti di rischio materiali e non;
  - Cause ed eventi;
  - Mutamenti del contesto;
  - Indicatori di rischi emergenti;
  - Limitazioni della conoscenza e affidabilità delle informazioni.
- Analisi del rischio: lo scopo è comprendere la natura dei rischi e le loro caratteristiche. L'analisi può avere vari gradi di dettaglio a seconda dello scopo, disponibilità e affidabilità informazioni e risorse disponibili. Si avvalere di tecniche di analisi qualitative, quantitative o, in alcuni casi, una combinazione di esse. L'analisi può essere influenzata da diversi fattori (qualità informazioni, divergenze d'opinioni, pregiudizi, ecc.) che dovrebbero essere documentate e comunicate ai decisori. I risultati forniscono informazioni per decidere se il rischio deve essere trattato, come e i metodi più appropriati;
- Valutazione del rischio: comporta un confronto tra le due voci precedenti al fine di determinare dove è necessario agire. Le azioni possibili sono diverse:
  - Non agire;

- Trattare il rischio;
- Analizzare ulteriormente il rischio;
- Riconsiderare gli obiettivi.

La decisione finale deve considerare il contesto più ampio e le eventuali conseguenze su di esso.

4.4.4. Trattamento del rischio[24]

Per affrontare il rischio è necessario selezionare una o più azioni di trattamento bilanciando i benefici derivati da esse a fronte di costi, sforzi e svantaggi di implementazione. Le possibilità di trattamento del rischio, in quanto non si escludono a vicenda, possono essere una o più delle seguenti:

- Evitare il rischio, non iniziando quindi l'attività di origine di esso;
- Assumersi il rischio;
- Rimuovere la fonte;
- Cambiare la probabilità;
- Cambiare le conseguenze;
- Condividere il rischio, per esempio con l'acquisto di assicurazioni;
- Mantenimento del rischio mediante decisione informata.

Non dovrebbero essere le sole condizioni economiche a giustificare il trattamento del rischio ma bisognerebbe tener conto di tutte le opinioni delle parti interessate, degli obblighi e degli impegni volontari.

Una corretta progettazione ed implementazione dei metodi di trattamento del rischio non implica il raggiungimento dei risultati desiderati, producendo conseguenze indesiderate. Devono quindi essere presenti fasi di monitoraggio e revisione per garantire che i trattamenti del rischio siano e rimangano efficaci nel tempo.

Nel caso in cui non siano presenti metodi di trattamento del rischio o che essi non lo modifichino sufficientemente, il rischio dovrebbe essere registrato e tenuto sotto

controllo, informando i decisori e gli stakeholders della natura e dell'esistenza di rischi residui al seguito dei trattamenti.

Un piano di trattamento del rischio dovrebbe specificare come verranno implementate le opzioni di trattamento scelte, identificando chiaramente l'ordine in cui esse dovrebbero essere attuate. Il piano va integrato nei piani di gestione e nei processi dell'organizzazione.

Le informazioni che il piano di trattamento del rischio dovrebbe contenere includono:

- Motivazioni della selezione delle opzioni;
- I responsabili dell'approvazione e dell'attauzzione;
- Azioni proposte;
- Risorse necessarie;
- Misure di performance;
- Vincoli;
- Comunicazione e monitoraggio.

4.4.5. Monitoraggio e revisione[25]

Al fine di garantire e migliorare la qualità e l'efficacia del processo di gestione del rischio è necessario pianificare una fase di monitoraggio e revisione di esso che deve avvenire in tutte le sue fasi. Monitoraggio e revisione includono:

- Pianificare, raccogliere e analizzare informazioni;
- Registrare i risultati;
- Fornire feedback.

4.4.6. Registrazione e rendicontazione[26]

Si dovrebbero documentare, attraverso appropriati meccanismi, i processi e i risultati della gestione del rischio. La documentazione serve a:

- Comunicare attività e risultati in tutta l'organizzazione;
- Fornire informazioni per processo decisionale;

- Migliorare gestione del rischio;
- Assistere interazioni con gli stakeholders

5. ISO 31010:2009 – TECNICHE DI GESTIONE DEL RISCHIO

La normativa ISO 31010:2009 è di supporto alla ISO 31000:2018 (punto 4.) e fornisce indicazioni sulla selezione e l'applicazione dei sistemi di gestione del rischio.

5.1. Selezione delle tecniche di valutazione del rischio[27]

La valutazione del rischio dovrebbe essere coerente con i criteri di rischio sviluppato nella definizione del contesto, in quanto essa può essere svolta con diversi gradi di profondità e dettaglio, utilizzando metodi semplici o complessi.

Tecniche adeguate dovrebbero presentare le seguenti caratteristiche:

- Giustificate e appropriate al contesto dell'organizzazione;
- Fornire risultati che aiutino alla comprensione della natura del rischio e a come dovrebbe essere trattato;
- Poter essere utilizzate in modo rintracciabile, ripetibile e verificabile.

Una volta definiti obiettivi e portata della gestione del rischio, i fattori applicabili sulla quale base le tecniche dovrebbero essere scelte sono:

- Gli obiettivi dello studio;
- Esigenze dei decisori, in quanto un elevato livello di dettaglio potrebbe essere necessario per una corretta decisione;
- Tipologia e ambito dei rischi presi in esame;
- Potenziale magnitudo delle conseguenze;
- Grado di competenze, risorse umane e risorse necessarie;
- Disponibilità di informazioni e dati, in quanto alcune tecniche richiedono molte informazioni;

- Necessità di modifica e aggiornamento. Alcune tecniche sono più modificabili di altre;
- Obblighi normativi e contrattuali.

Sono presenti però fattori che influenzano la scelta di un approccio alla gestione del rischio, come:

- Disponibilità delle risorse[28]: come, per esempio, le competenze dei responsabili della valutazione dei rischi oppure i vincoli di tempo e le altre risorse disponibili nell'organizzazione;
- La natura e il grado di incertezze[29]: questo richiede la conoscenza della qualità, quantità e l'integrità delle informazioni disponibili sui rischi presi in considerazione. L'incertezza può essere data dalla mancanza di una o più delle informazioni sopra elencate. Inoltre, i dati non sempre forniscono una base affidabile a causa di dati non sempre disponibili, come per i rischi unici, o per un'interpretazione sbagliata da parte degli stakeholders;
- Complessità[30]: non sempre i rischi devono essere valutati separatamente. In alcuni casi, come nei sistemi complessi, va valutato nella sua integrità oppure, quando un singolo rischio può avere impatto su altre attività. Comprendere la complessità dei rischi presenti nell'organizzazione è quindi cruciale per la scelta delle tecniche appropriate.

Molte attività, progetti o prodotti hanno un ciclo di vita diviso in varie fasi con. In ognuna di esse la valutazione del rischio deve essere applicata con diversi livelli di dettaglio, utilizzando tecniche diverse, per assistere nella presa di decisioni e fornire informazioni utili per lo sviluppo di procedure per condizioni normali e di emergenza.

5.2. Tipi di tecniche di valutazione del Rischio

La normativa ISO 31010:2009, nel suo allegato B "Risk Assessment Techniques" cita e descrive 31 tipi di tecniche che verranno trattate nei punti seguenti.

Esse sono di tre tipologie[31]:

- Qualitative: viene utilizzato un metodo descrittivo per stimare effetti e probabilità del verificarsi del rischio;
- Semi-quantitative: vengono assegnati dei valori numeri a categorie descrittive che però non rappresentano una quantificazione degli effetti economici o delle probabilità;
- Quantitative: consentono un ordinamento per importanza delle diverse tipologie di rischi.

5.2.1. Brainstorming[32]

Consiste nell'organizzare un gruppo di persone competenti, incoraggiando la conversazione tra i membri al fine di identificare pericoli, rischi, criteri decisionali e opzioni di trattamento. Pone al centro l'immaginazione ed è quindi utile soprattutto per identificare rischi legati a nuove tecnologie, quando non esistono già dati disponibili o per trovare soluzioni originali.

Può essere utilizzato sia singolarmente sia in combinazione con altri metodi che verranno successivamente descritti. Nel primo caso per favorire il pensiero creativo in qualsiasi fase del processo o di ciclo di vita del sistema.

Gli inputs sono, appunto, un gruppo di persone con profonda conoscenza del processo o sistema preso in esame.

Il processo di valutazione può essere formale, più strutturato, in cui i partecipanti hanno ben in mente lo scopo e il risultato da raggiungere, con un metodo definito per la valutazione delle idee proposte, oppure informale, meno strutturato e più improvvisato.

Gli outputs dipendono dalla fase del processo di gestione del rischio in cui viene applicato.

Si può dedurre che i punti di forza della tecnica sono:

- Stimolazione dell'immaginazione, il che aiuta ad identificare nuovi rischi e soluzioni originali;
- coinvolgere le persone chiave del processo, favorendo la comunicazione complessiva;
- Rapido e facile da organizzare.

Mentre le limitazioni che si possono riscontrare sono:

- Mancanza di competenze e conoscenze dei partecipanti;
- Essendo poco strutturato è difficile dimostrare che il processo sia completo;
- A causa di alcune dinamiche potrebbe accadere che non tutti i componenti del gruppo siano ascoltati alla stessa maniera, con il rischio di perdere idee preziose.

5.2.2. Interviste strutturate e semi strutturate[33]

Nelle interviste strutturate vengono poste agli intervistati una serie di domande già preparate al fine di far valutare le situazioni da una prospettiva differente in modo tale da identificare vari rischi che rischiano altrimenti di passare inosservati. Similmente, ma concedendo maggiore libertà alla discussione, funzionano le interviste semi-strutturate.

Esse possono essere utilizzate in sostituzione alla tecnica di Brainstorming qualora sia difficile la formazione del gruppo di lavoro. Sono utilizzabili in qualsiasi momento del progetto o del processo e forniscono un importante contributo degli stakeholder.

Gli inputs includono:

- Una chiara definizione degli obiettivi dell'intervista;
- Una lista degli intervistati;
- Una serie di domande già preparate.

Quest'ultimo punto è fondamentale in quanto le domande devono essere utilizzate come guida per l'intervista. Importante che esse siano aperte, dove possibile,

semplici, formulate con un linguaggio appropriato all'intervistato e che riguardino un solo problema.

Al termine dell'elaborazione di tutte le risposte si avrà la visione degli stakholders riguardo ai problemi presi in esame.

I punti di forza di queste tecniche sono:

- Permettono alle persone di ragionare su un problema per il tempo necessario;
- La conversazione "one to one" permette di ragionare in modo più profondo su un problema;
- Permettono di prendere in considerazione le idee di un maggior numero di persone rispetto a quelle del brainstorming.

Le limitazioni, invece, possono essere:

- Il lungo tempo di ottenimento delle opinioni di più persone;
- Il "bias" di ogni singolo individuo non viene rimosso dalla discussione di gruppo;

5.2.3. Tecnica Delphi[34]

In questa tecnica, come nel brainstorming, si ottengono le opinioni di un gruppo di esperti. I due metodi possono sembrare la stessa cosa ma la tecnica Delphi ha come caratteristica principale il fatto che gli esperti forniscano il loro punto di vista in modo anonimo e, mano a mano che il processo progredisce, abbiano accesso alle opinioni degli altri.

Può essere utilizzata in qualsiasi momento del processo di gestione del rischio in quanto è un consenso, da parte di esperti, di come si sta procedendo.

Formato il gruppo di esperti, viene fornito a questi ultimi, individualmente, il primo "round" di domande. Le risposte vengono analizzate, combinate e fatte ricircolare tra i membri del gruppo i quali dovranno fornire altre risposte. Il processo si ripete fino a quando non si avrà il consenso di tutti i membri.

I punti di forza includono:

- Maggior numero di opinioni impopolari in quanto le risposte sono anonime;
- Tutti i punti di vista hanno lo stesso peso, raggirando il problema delle personalità dominanti;
- Le persone non devono essere presenti nello stesso posto allo stesso momento.

Le limitazioni sono:

- L'elaborazione delle risposte richiede molto tempo;
- I partecipanti devono essere in grado di esprimere chiaramente la loro visione scrivendo.

5.2.4. Check-lists[35]

Le check-lists sono delle vere e proprie liste, create tramite l'esperienza acquisita, di rischi o errori di controllo.

Possono essere utilizzate in qualsiasi momento del ciclo del prodotto, sistema o processo. Permettendo di indentificare pericoli, rischi o il corretto funzionamento dei controlli effettuati.

Possono essere utilizzate come tecnica di valutazione del rischio ma sono più utili se applicate per controllare che, a seguito dell'utilizzo di un'altra tecnica, tutto sia stato correttamente valutato.

Per l'utilizzo bisogna, innanzitutto, avere ben chiaro lo scopo dell'attività, solamente in seguito verrà selezionata la check-list adeguata. L'utilizzatore o gli utilizzatori "step by step" controlleranno che ogni elemento della check list sia presente nell'attività presa in esame.

Possiamo quindi identificare i seguenti punti di forza:

- Può essere utilizzata anche da personale non esperto;
- Se ben progettata combina un largo range di esperienza con un sistema facile da utilizzare;
- Aiuta a non dimenticare i problemi comuni.

D’altro lato gli svantaggi sono:

- Inibisce l’immaginazione di identificazione dei rischi;
- Basandosi sull’esperienza si limita al già conosciuto;
- Tende a basarsi sull’osservazione, con la possibilità di mancare i problemi non facilmente visibili.

5.2.5. PHA – Preliminary hazard analysis[36]

PHA è un semplice metodo di analisi che ha come obiettivo l’identificare pericoli, situazioni pericolose ed eventi che possono causare danni. È utilizzato soprattutto nel primo sviluppo di un progetto di cui sono presenti poche informazioni o procedure operative e può essere un precursore per futuri studi del sistema.

Fornendo informazioni e dettagli sul sistema preso in esame, esso formula una lista di rischi generici considerando caratteristiche come attrezzature utilizzate, layout, ambiente operativo, ecc.

Il metodo può essere aggiornato durante le fasi di vita iniziali del sistema per scovare nuovi rischi e apportare correzioni.

Ha come vantaggi:

- Essere utilizzato quando le informazioni sono limitate;
- Considerare i rischi nella fase iniziale del ciclo del sistema.

Ha come svantaggio il fatto di utilizzare solo le informazioni preliminari non fornendo quindi informazioni dettagliate sui rischi e i migliori modi con cui prevenirli.

5.2.6. HAZOP[37]

Acronimo di “Hazard and Operability study” è un strutturato e sistematico esame di un processo, prodotto o sistema esistente, il quale identifica rischi per persone, equipaggiamenti e obiettivi dell’organizzazione.

Informazioni necessarie alla tecnica HAZOP sono quelle riguardanti il sistema, il processo o le procedure da rivedere e le intenzioni e prestazioni del progetto. Parte di esse sono disegni, procedure operative e di manutenzione, logica dei diagrammi, ecc.

Fornito ciò, ogni parte viene revisionata per scoprire quali deviazioni dalla prestazione prevista possono capitare, le potenziali cause e le probabili conseguenze di essa. Ad ogni parte del sistema, processo o procedura che risponde ai cambiamenti viene assegnata una parola chiave (Tab. 1).

Tab 1 – Esempi di parole chiave

Terms	Definitions
No or not	No part of the intended result is achieved or the intended condition is absent
More (higher)	Quantitative increase in output or in the operating condition
Less (lower)	Quantitative decrease
As well as	Quantitative increase (e.g. additional material)
Part of	Quantitative decrease (e.g. only one or two components in a mixture)
Reverse /opposite	Opposite (e.g. backflow)
Other than	No part of the intention is achieved, something completely different happens (e.g. flow or wrong material)
Compatibility	Material; environment
Guide words are applied to parameters such as	
	Physical properties of a material or process
	Physical conditions such as temperature, speed
	A specified intention of a component of a system or design (e.g. information transfer)
	Operational aspects

Al termine dell'utilizzo della tecnica il gruppo deve redigere un verbale con la descrizione degli elementi di ogni punto revisionato. Per ogni deviazione che non può essere corretta bisogna valutare il rischio della stessa.

I vantaggi della tecnica sono i seguenti:

- Fornire i mezzi per esaminare in modo approfondito un sistema o processo;
- Coinvolgere un team multidisciplinare;
- Generare soluzioni per la gestione del rischio;
- Applicabile a una vasta gamma di sistemi o processi;

a fronte dei rischi sopra elencati, gli svantaggi sono:

- Il tempo richiesto per una dettagliata analisi;
- Richiesta di molta documentazione del processo o del sistema;
- Ci si potrebbe concentrare troppo su dettagli di design piuttosto che questioni più problematiche o a problemi esterni.

5.2.7. HACCP – Hazard Analysis and Critical Control Point[38]

Utilizzato soprattutto nell'industria alimentare, questo metodo, come si può intuire dall'acronimo, identifica i rischi e inserisce punti di controllo i punti rilevanti del processo al fine di proteggerlo contro gli stessi. HACCP mira a minimizzare i rischi mediante il controllo durante tutto il processo piuttosto che a prodotto finito.

Partendo dal diagramma di processo il metodo HACCP consiste nel seguire 7 principi:

- Identificazione e analisi dei pericoli;
- Individuazione dei Punti Critici di Controllo (CCP);
- Definizione dei limiti critici;
- Definizione dell'applicazione delle procedure di monitoraggio;
- Pianificazione delle azioni correttive;
- Definizione delle procedure di verifica;
- Definizione delle procedure di registrazione.

Al termine di ciò si avrà un piano HACCP e dei documenti di registrazione per l'analisi dei pericoli. Il primo delinea le procedure da seguire per assicurare il controllo di un prodotto, processo o procedura. I secondi sono un elenco di pericoli e misure da attuare in ogni fase del processo.

I punti di forza sono quindi:

- Processo strutturato che fornisce prove per il controllo della qualità e l'identificazione dei rischi;
- Dove e come i pericoli possono essere prevenuti e rischi controllati;
- Migliorare controllo del rischio durante il processo;

Le limitazioni includono:

- Potrebbe essere necessario combinare la tecnica con altre al fine di identificare i pericoli e definire i rischi che ne derivano.

5.2.8. Valutazione della tossicità[39]

In questo metodo, a seguito di un'esposizione di piante, animali ed esseri umani ad una serie di pericoli ambientali (quali prodotti chimici, micro organismi od altre specie), viene utilizzata la valutazione del rischio ambientale. Ciò comprende l'analisi dei rischi o delle sorgenti di danno, del modo in cui esse influiscono sulla popolazione bersaglio e le varie vie attraverso le quali il pericolo può giungere a una popolazione bersaglio suscettibile. Queste informazioni vengono poi combinate per fornire una stima dell'entità e della natura del danno.

Conoscendo bene la natura e le proprietà del rischio, la suscettibilità della popolazione e i modi in cui le due interagiscono, il processo segue 5 fasi:

- Formulazione del problema: impostare lo scopo definendo il range di target della popolazione e i tipi di rischio d'interesse;
- Identificazione dei rischi: identificare tutte le sorgenti di danno per la popolazione target;
- Analisi dei rischi: capire la natura del danno e come interagisce con il target. Come per esempio l'esposizione del corpo umano ad agenti chimici o biologici;
- Analisi dell'esposizione: esaminare come e in che quantità le sostanze pericolose, o i loro residui, raggiungono la popolazione suscettibile. In questa fase è importante considerare tutte le differenti strade che il rischio potrebbe prendere;
- Caratterizzazione del rischio: le informazioni dei due step precedenti vengono unite per stimare la probabilità delle conseguenze quanto tutte le vie percorribili sono combinate.

Al termine si avrà un'indicazione del livello di rischio dall'esposizione di un certo target ad un certo rischio in un determinato contesto.

Si può dedurre che i punti di forza sono:

- Fornire una profonda conoscenza della natura del problema e dei fattori che ne aumentano il rischio;
- L'analisi di tutte le vie percorribili è un ottimo strumento per capire come e quando migliorare i controlli o introdurne di nuovi.

Il limite principale invece è che necessita di ottimi dati iniziali che non sempre sono disponibili o sono associati ad un alto livello di incertezza.

5.2.9. SWIFT – "Structured What-If Technique"[40]

Inizialmente nasce come alternativa semplice al metodo HAZOP. Utilizza una serie di frasi "what if" standard in combinazione con i "prompts" per indagare su come un sistema, elemento, un'organizzazione o una procedura saranno influenzati da deviazioni dal normale funzionamento. Generalmente il metodo SWIFT viene applicato su più livelli del sistema preso in esame, ma con un livello di dettaglio inferiore rispetto ad HAZOP.

Il sistema, la procedura, l'elemento presi in esame devono essere ben definiti prima che lo studio possa incominciare e il contesto, sia interno che esterno, è stabilito attraverso interviste e lo studio di documenti, piante e disegni. Altro elemento importante è la competenza e l'esperienza del gruppo di studio, il quale deve essere selezionato accuratamente.

La prima fase, prima dell'inizio dello studio, è la preparazione di un elenco di parole o frasi basate su un set standard o create per consentire una visione completa dei pericoli o rischi. Successivamente al tavolo di lavoro vengono discussi e concordati i contesti, i cambiamenti e lo scopo dello studio. A questo punto il facilitatore chiede ai partecipanti di discutere dei rischi e pericoli noti, precedenti esperienze e incidenti, controlli noti ed esistenti ed infine dei requisiti e vincoli normativi. Il tutto è facilitato da frasi tipo "cosa accadrebbe se", le quali hanno l'intento di stimolare il gruppo ad esplorare potenziali scenari con le loro conseguenze. I rischi, le loro cause e le loro conseguenze vengono dunque riepilogati, descritti e registrati. Il team poi valuta se i controlli già in atto sono

adeguati ed efficaci e se non soddisfano i requisiti vengono considerati altri potenziali controlli e metodi di trattamento del rischio.
Al termine del processo si avrà un registro dei rischi con la classificazione delle azioni e degli obiettivi concordati. Questi obiettivi saranno le basi per il piano di trattamento del rischio.

Alcuni dei punti di forza del metodo SWIFT sono:

- Possibile applicazione a tette le forme di impianto, sistema od organizzazione;
- Rapidità di identificazione dei rischi maggiori;
- Studio orientato ai sistemi, che consente di esaminare la risposta del sistema alle deviazioni piuttosto che limitarsi ad esaminare le conseguenze;
- Identificazione di opportunità di miglioramento;
- Coinvolge coloro che sono responsabili dei controlli già esistenti;
- Creazione di un registro dei rischi e un piano per il loro trattamento;

Al contrario, le limitazioni sono:

- Necessità di un facilitatore espero e capace;
- Attenta preparazione in modo di evitare perdite di tempo durante il tavolo di lavoro;
- Se il gruppo non ha un'ampia esperienza alcuni rischi potrebbero non essere identificati;

5.2.10. Analisi dello scenario[41]

Questo metodo può essere utilizzato per considerare i possibili sviluppi futuri ed esplorarne le implicazioni. Scenari come, per esempio, "caso migliore" "caso peggiore" possono essere utilizzati per analizzare le possibili conseguenze e stimare le loro probabilità di accadimento.

I casi d'uso dell'analisi dello scenario sono diversi: prendere decisioni e pianificare le future strategie così come prendere in considerazione le attività già esistenti, può prendere parte in tutte e 3 le componenti dell'analisi del rischio, essere usata per

anticipare come minacce e possibilità si potrebbero sviluppare e molto altro ancora.

Prerequisito fondamentale per una corretta analisi dello scenario è la composizione del team. I componenti devono comprendere la natura dei cambiamenti rilevanti e l'immaginazione per pensare al futuro senza farsi condizionare dal passato. Tutto ciò unito all'accesso alla letteratura e ai dati sui cambiamenti già in atto.

Stabilendo a priori il team, il canale di comunicazione e definendo il contesto dei problemi e le condizioni da considerare, si dovrà successivamente identificare la natura dei cambiamenti che potrebbero verificarsi. Per fare ciò è necessario effettuare ricerche sulle principali tendenze e sui tempi in cui esse possono cambiare. I cambiamenti da considerare sono quelli esterni (cambiamenti tecnologici), quelli riguardanti le decisioni da prendere che possono avere una varietà di risultati, esigenze degli stakeholder e cambiamenti macroambientali (normative, demografiche, ecc). I fattori e le tendenze, sia locali che macro, devono poi essere classificati in base all'importanza e all'incertezza, prestando particolare attenzione a quelli più importanti e quelli più incerti. Viene quindi proposta una serie di scenari ognuno riguardante un possibile cambiamento. Per ognuno di essi viene scritta una storia che racconta come è possibile arrivare dal presente allo scenario preso in oggetto. Ora gli scenari vengono testati per valutare la domanda iniziale ed esplorare come le attività intraprese abbiano successo in quel specifico contesto.

Valutando ogni scenario potrebbe risultare che nessuno di essi sia ottimale ma si dovrebbe avere una percezione più chiara della gamma di opzioni e di come modificare le azioni intraprese man mano che gli indicatori si muovono.

L'analisi dello scenario tiene conto di vari possibili futuri, il che potrebbe essere preferibile all'approccio tradizionale, soprattutto in situazioni in cui sono disponibili pochi dati su cui basarsi. Tuttavia questo metodo ha una debolezza associata all'alta incertezza in quanto non tutti gli scenari possono essere realistici.

5.2.11. BIA – Analisi dell'impatto aziendale[42]

L'analisi dell'impatto aziendale valuta in che modo i principali rischi di interruzione potrebbero influire sulle operazioni di un'organizzazione identificando e quantificando le risorse necessarie per gestirli. Il metodo determina le criticità e i tempi di ripristino dei processi e delle risorse associate (persone, tecnologie, ecc.) per garantire il raggiungimento continuo degli obiettivi. Inoltre, fornisce le interdipendenze e interrelazioni tra processi, soggetti interni ed esterni e collegamenti di filiera.

Una BIA ha diversi metodi di sviluppo, tra essi troviamo i questionari, le interviste, workshop strutturati o anche una combinazione dei tre metodi, tutti con il fine di ottenere una comprensione dei processi critici, gli effetti della perdita di essi e i tempi di ripristino di tali processi. Altri punti chiave di tale metodo sono l'individuazione delle interdipendenze con i principali stakeholder interni ed esterni, determinazione delle risorse attualmente disponibili e di quelle necessarie per continuare ad operare e l'identificazione di soluzioni alternative ai processi in uso.

Analizzato ciò si avrà un elenco di priorità dei processi critici con le relative interdipendenze, gli impatti finanziari e operativi documentati derivati dalla perdita di tali processi e le risorse di supporto necessarie per essi.

I punti di forza della BIA includono:

- Comprensione dei processi critici che forniscono all'organizzazione la capacità di continuare a raggiungere gli obiettivi dichiarati;
- Comprensione delle risorse richieste;
- Opportunità per ridefinire il processo operativo.

I limiti, invece, includono:

- Mancanza di conoscenza dei partecipanti coinvolti;
- Dinamiche che influenzano l'analisi;

- Difficoltà di ottenere un adeguato livello di comprensione dell'organizzazione.

5.2.12. RCA – Analisi delle cause alla radice[43]

Il metodo consiste in un'analisi di una grave perdita per prevenirne il ripetersi. Tenta di identificare le cause profonde o originali invece di occuparsi solo dei sintomi evidenti. Le azioni correttive potrebbero non essere sempre del tutto efficaci e potrebbe essere richiesto un miglioramento continuo. RCA può essere applicato a vari contesti quali indagini sugli incidenti nei luoghi di lavoro, analisi dei guasti nei sistemi tecnologici, controllo della qualità della produzione, processi aziendali e molto altro ancora.

Inizialmente viene formata una squadra di esperti con le competenze necessarie ad analizzare il guasto, la quale stabilirà il campo di applicazione e gli obiettivi da raggiungere. Successivamente si raccoglieranno i dati del guasto da analizzare per determinare la causa e sviluppare soluzioni. Attuate quest'ultime si andrà a verificarne il corretto funzionamento.

I principali punti di forza sono:

- Analisi strutturata;
- Considerazione di tutte le ipotesi probabili;
- Documentazione dei risultati;
- Raccomandazioni finali.

Le limitazioni invece:

- Se gli esperti richiesti non sono disponibili;
- Prove necessarie per lo sviluppo del metodo possono essere distrutte durante il guasto o rimosse con la bonifica;
- Tempo non sufficiente per la valutazione;
- Raccomandazioni attuate non adeguate.

5.2.13. Analisi delle modalità e degli effetti di guasto (FMEA) e modalità ed effetti di guasto e analisi delle criticità (FMECA)[44]

La tecnica FMEA è utilizzata per identificare i modi in cui i componenti, sistemi o processi possono non soddisfare il loro intento progettuale. Alcuni esempi possono essere l'identificazione delle potenziali modalità di guasto di varie parti di un sistema, oppure gli effetti che tali guasti possono avere sul sistema.

FMECA invece estende FMEA classificando le modalità di guasto in base all'importanza o alla criticità.

FMEA/FMECA possono essere applicati durante le fasi di progettazione, produzione o durante il funzionamento del sistema in quanto possono assistere alla selezione di alternative progettuali, assicurare la considerazione di tutte le modalità di guasto o dei loro effetti sul sistema, identificare modalità ed effetti dell'errore umano e altro ancora. Inoltre, possono fornire input ad altre tecniche di analisi come, per esempio, l'albero dei guasti.

Entrambe le tecniche necessitano di informazioni dettagliate per un'analisi significativa, ciò varia se ci si trova in fase di progettazione, il che può richiedere informazioni sui singoli componenti, o se ci si trova a livelli superiori. Le informazioni richieste includono disegni o diagrammi di flusso del sistema, funzione di ogni fase del processo, dettagli ambientali che possono influire e informazioni sullo storico dei guasti.

Il processo da seguire, per una corretta applicazione della tecnica FMEA, è il seguente:

- Definizione degli obiettivi dello studio;
- Formazione della squadra;
- Comprensione del sistema/processo da analizzare;
- Scomposizione del sistema/processo nei suoi componenti o fasi;
- Definizione di ogni componente o fase;

Fatto ciò bisogna identificare per ogni componente o fase come essi possono fallire, cosa potrebbe produrre questo fallimento, quali sarebbero gli effetti, se tali effetti sono innocui o dannosi e i metodi di rilevazione dei fallimenti.

Per l'utilizzo del metodo FMECA, oltre a quanto sopra elencato, bisogna procedere a classificare le modalità di guasto identificate in base alla loro criticità. I metodi più comuni per la classificazione sono l'indice di criticità della modalità, il livello di rischio e il numero di priorità del rischio.

Il tutto deve essere documento in un rapporto contenente i dettagli del sistema, le modalità di svolgimento della tecnica, le ipotesi formulate, le fonti dei dati, i risultati ottenuti e le raccomandazioni per ulteriori analisi o per modifiche da effettuare.

La tecnica FMEA fornisce un elenco delle modalità di errore, i meccanismi che portano a tale errore e gli effetti che essi hanno sul sistema/processo.

La tecnica FMECA, invece, fornisce una valutazione una valutazione di importanza basata sulla probabilità che il sistema fallisca e il livello di rischio derivante dalla modalità di guasto.

I punti di forza, comuni tra le due tecniche, sono:

- Ampiamente applicabile agli errori umani, delle apparecchiature e dei sistemi;
- Presentare in una modalità facilmente comprensibile le modalità di guasto dei componenti, le cause e i loro effetti sul sistema;
- Identificare i problemi all'inizio del processo evitando costose modifiche;
- Fornire input ai programmi di monitoraggio evidenziando le caratteristiche chiave da tenere sott'occhio.

Entrambe però hanno delle limitazioni riguardanti:

- Identificazione delle singole modalità di guasto e non di una loro possibile combinazione;

- Richiesta di tempo per effettuare gli studi;
- Difficoltà per l'applicazione a sistemi multistrato complessi.

5.2.14. FTA – Analisi dell'albero dei guasti[45]

Partendo da un evento principale, il metodo, permette l'identificazione e l'analisi dei fattori che contribuiscono all'avvenimento di esso. I fattori sono identificati deduttivamente e vengono rappresentati in un diagramma ad albero ne specifica anche la loro relazione. Essi possono essere associati ad errori umani, a rotture hardware o altri eventi che portano all'accadimento dell'evento indesiderato.

La tecnica può essere utilizzata in vari modi, qualitativamente per l'identificazione di cause del guasto o quantitativamente per calcolare la probabilità dell'evento, in fase di progettazione per identificare potenziali cause di guasto o nella fase operativa identifica come avvengono gravi guasti oppure, infine, per analizzare le cause del fallimento di un errore che si è verificato.

Per l'analisi qualitativa bisogna comprendere a fondo il sistema, le sue cause di guasto e come esse avvengono. Per l'analisi quantitativa, invece, è richiesta la conoscenza dei tassi di guasto degli eventi di base dell'albero.

Lo sviluppo dell'albero dei guasti è effettuato in più passaggi:

- Definizione dell'evento principale da analizzare;
- Identificazione delle possibili cause immediate o le modalità di guasto;
- Analisi delle cause o delle modalità;
- Scomposizione degli eventi ad un livello inferiore del sistema, fino a quando un'ulteriore scomposizione risulterebbe improduttiva. Per esempio, in un sistema hardware, il livello più basso è rappresentato dal guasto del componente;
- Dove possibile, assegnazione della probabilità di accadimento dell'evento.

È necessario utilizzare l'algebra booleana per capire l'influenza dei singoli errori sull'evento principale.

L’albero finale ottenuto è una rappresentazione pittorica di come l’evento top può verificarsi, dell’interazione degli eventi necessari al suo raggiungimento nonché della probabilità del suo accadimento.

I suoi numerosi punti di forza comprendono:

- Approccio disciplinato, sistematico e flessibile che consente l’analisi di una grande varietà di fattori;
- Approccio “top-down” che focalizza l’attenzione sugli effetti direttamente correlati all’evento principale;
- Facile comprensione del comportamento del sistema grazie alla sua rappresentazione grafica;
- Utilità nell’analisi di sistemi complessi con molte interazioni.

Al contrario tra le limitazioni troviamo:

- Elevati livelli di incertezza quando le probabilità degli eventi base non sono note;
- Eventi causali non legati tra loro con conseguente difficoltà di collegamento;
- Modello statico che non tiene conto delle interdipendenze temporali;
- Difficoltà ad includere effetti domino di guasti condizionali.

5.2.15. ETA - Analisi dell’albero degli eventi[46]

Il metodo consiste in una rappresentazione grafica degli eventi, i quali si escludono a vicenda, a seguito di un evento scatenante, in funzione del funzionamento o non dei vari sistemi presenti, progettati per mitigarne le conseguenze. Anch’esso può essere applicato sia qualitativamente per fare brainstorming su potenziali scenari, che quantitativamente prestandosi a considerare l’accettabilità dei controlli in atto. ETA viene utilizzato principalmente per calcolare e classificare, basandosi sul rischio, gli scenari incidentali conseguenti all’evento scatenante.

Le informazioni necessarie all’utilizzo della tecnica sono un elenco di eventi iniziali, informazioni sui sistemi di controllo in uso e la loro probabilità di

fallimento, nonché una comprensione dei metodi di intensificazione di un errore iniziale.

Partendo quindi da un evento iniziale scelto vengono elencati, in sequenza i sistemi di controllo. Vengono tracciate due linee, una rappresentante il successo del sistema, l'altra il fallimento e ad esse sono assegnate delle probabilità di accadimento. In questo modo vengono modellati diversi percorsi scaturiti dall'evento in esame. Ognuno di essi rappresenta la probabilità che tutti gli eventi di quel "ramo" accadano. Pertanto, la frequenza è data dal prodotto delle singole condizioni e la frequenza dell'evento iniziale.

Al termine si avrà una serie di descrizione qualitative di potenziali problemi, stime delle frequenze e probabilità che essi accadano e raccomandazioni per la riduzione dei rischi.

Tra i punti di forza di ETA troviamo:

- Potenziali scenari a seguito di un evento con la loro analisi;
- Influenza del successo o del fallimento dei sistemi in uso;
- Tiene conto dei tempi e degli effetti domino;
- Rappresenta graficamente sequenze di eventi che non possono essere altrimenti rappresentate con FTA.

Le limitazioni invece:

- Non sempre vengono identificati tutti gli eventi iniziali. Deve essere quindi combinato con altri metodi (Es. HAZOP, PHA);
- Vengono rappresentati solo successi e fallimenti non tenendo conto di eventi di recupero o successi ritardati;

5.2.16. Analisi causa-conseguenza[47]

La tecnica è una combinazione dei metodi FTA ed ETA. Partendo da un evento critico ne analizza le conseguenze mediante la condizione di accadimento o di non

accadimento di essa, condizione rappresentata da guasti di sistema o utilizzo di sistemi di mitigazione delle conseguenze.

Anch'essa, come il metodo FTA, viene utilizzata per rappresentare la logica di errore che porta ad un evento critico ma consentendo, come nel casto del metodo ETA, l'analisi dei guasti sequenziali nel tempo. Inoltre, tiene conto anche dei ritardi temporali. Ogni sequenza, essendo una combinazione di sotto-alberi, permette alla tecnica analisi causa-conseguenza di costruire grandi alberi dei guasti, ma, essendo diagrammi complessi da produrre e utilizzare, tendone ad essere utilizzata quando la potenziale conseguenza ne giustifichi lo sforzo.

Partendo dall'identificazione dell'evento critico viene sviluppato un albero dei guasti per le cause di esso. Vengono quindi costruiti i percorsi per ogni conseguenza a seconda delle diverse condizioni che possono verificarsi. Nel caso in cui i fallimenti, rappresentati da una casella, siano indipendenti, la probabilità di accadimento può essere calcolata moltiplicando le probabilità di ogni singola sequenza che termina in quella particolare condizione. Se più di una sequenza termina con la stessa condizione vengono sommate le probabilità.

Al termine si otterrà una rappresentazione schematica di come un sistema può fallire, di quali siano le conseguenze e una stima delle probabilità di accadimento.

I vantaggi, oltre a quelli delle tecniche FTA ed ETA combinati, sono:

- Analizzare gli eventi che si sviluppano nel tempo;
- Visione d'insieme del sistema.

Lo svantaggio, come già detto in precedenza, è il fatto di essere un metodo complesso da sviluppare.

5.2.17. Analisi causa-effetto[48]

L'analisi causa-effetto è un metodo strutturato che identifica tutte le possibili cause di un evento indesiderato, organizzando tutti i possibili fattori contribuenti in diverse categorie.

A seconda del contesto l'effetto preso in considerazione può essere positivo o negativo e, tramite una visualizzazione grafica di un elenco di cause, il metodo consente la considerazione di tutti gli scenari possibili che portano ad esso. Il che permette al team di stabilire quali siano le cause più probabili potendo poi verificarle e risolverle.

Il grafico utilizzato viene chiamato "fishbone", data la sua somiglianza alla lisca di pesce. Determinato l'effetto da analizzare, vengono diramate dalla linea principale altre linee che rappresentano le principali categorie delle cause. Per ognuna di esse, rispondendo alla domanda "perché" o "cosa lo ha causato", si ramificano le cause e le sottocause le quali descrivono più specificamente le categorie.

Il diagramma risultate deve poi essere testato empiricamente prima di poter far raccomandazioni.

I principali punti di forza sono:

- Coinvolgimento di esperti che lavorano in team;
- Analisi strutturata;
- Considerazione di tutte le possibili ipotesi;
- Facile lettura della rappresentazione grafica;
- Evidenziare le aree dove si necessitano ulteriori dati.

Tra le limitazioni troviamo:

- Team senza le competenze necessarie;
- Tecnica di brainstorming e non di analisi separata;
- Possibili interazioni tra le categorie non considerate.

5.2.18. LOPA – Analisi dei livelli di protezione[49]

Viene utilizzata per stimare i rischi associati ad un evento indesiderato, analizzando la presenza di misure sufficienti per controllare o mitigare il rischio. Selezionando una coppia causa-conseguenza vengono identificati i livelli di protezione che prevengono la causa che porterà alla conseguenza. È un metodo

semiquantitaivo, perciò viene anche effettuato un calcolo dell'ordine di grandezza per determinare se le protezioni sono adeguate a ridurre il rischio ad un livello tollerabile.

La tecnica fornisce una base per la specifica dei livelli di protezione indipendenti (IPL) e dei livelli di integrità della sicurezza (SIL levels). Inoltre, è utilizzata per capire come allocare in modo efficace le risorse per la riduzione del rischio, partendo da quelle presenti e analizzandone l'efficacia.

Un team di esperti, dopo aver identificato le cause scatenanti e la frequenza di accadimento di un evento indesiderato, seleziona una coppia causa-conseguenza da analizzare, identifica e valuta l'efficacia degli strati di protezione che impediscono la causa di diventare una conseguenza e stima le probabilità di fallimento di ogni IPL. In seguito, vengono combinate la frequenza della causa iniziale con la probabilità di guasto degli IPL per determinare la frequenza della conseguenza indesiderata. I livelli di rischi calcolati vengono confrontati con i livelli di tolleranza per determinare se è necessario aggiungere altre protezioni.

Ad analisi conclusa si dovranno fornire raccomandazioni su eventuali altri controlli da effettuare e sull'efficacia di quelli già presenti.

I punti di forza della tecnica includono:

- Identifica e aiuta a concentrare le risorse sui livelli di protezione più critici:
- Identifica sistemi e processi per i quali non sono sufficienti i controlli di sicurezza;
- Si concentra sulle conseguenze più gravi.

Le principali limitazioni invece sono:

- Si concentra unicamente su uno scenario alla volta. Non sono contemplate interazioni tra rischi o controlli;
- I rischi quantificati potrebbero non tener conto dei modi di guasto comuni;

- Non si applica a scenari molto complessi in cui esistono numerose cause-conseguenze.

5.2.19. Analisi albero delle decisioni[50]

Un albero delle decisioni è una rappresentazione che, partendo da un evento iniziale, modella i percorsi conseguentemente alle diverse decisioni che possono essere prese e agli eventi che possono verificarsi. Generalmente questa tecnica viene utilizzata per aiutare a selezionare la migliore linea di azione in caso di incertezza.

Per un corretto utilizzo della tecnica bisogna essere a conoscenza delle informazioni sui possibili esiti delle decisioni e sugli eventi che potrebbero influenzarle. Solo in seguito, partendo da un evento iniziale, si prenderà la decisione di procedere con l'opzione "A" piuttosto che l'opzione "B". Procedendo con le scelte si verificheranno diversi eventi e dovranno essere prese altre decisioni. I costi, l'utilità del percorso e la probabilità degli eventi possono essere stimati e con essi anche il miglior percorso decisionale da prendere che, logicamente, produce il massimo valore atteso. Al termine si otterrò un'analisi logica del rischio che mostra le diverse opzioni adottabili.

I punti di forza sono quindi:

- Possibilità di calcolare il percorso migliore possibile;
- Rappresentazione grafica dei dettagli di un problema.

Le limitazioni invece:

- Grandi alberi posson diventare troppo complessi per una facile comunicazione;
- Tendenza a semplificare la situazione per poterla rappresentare.

5.2.20. HRA – Valutazione dell'affidabilità umana[51]

Quasi tutti i processi contengono un potenziale di errore umano. A volte, tuttavia, l'azione umana è l'unico modo per evitare che un guasto progredisca verso un

incidente. Inoltre, la tecnica è utile per evidenziare gli errori che ostacolano la produttività e rivelare le modalità con cui essi possono essere recuperati dagli operatori.

Il metodo HRA può essere utilizzato qualitativamente per identificare il potenziale errore umano e le relative cause, o quantitativamente per fornire dati sui fallimenti umani da utilizzare poi in altre tecniche.

Bisogna quindi conoscere e definire i compiti che le persone svolgono e i tipi di errori che si verificano nella pratica. Il processo, poi, prevede di porsi varie domande in diversi ambiti, per esempio:

- Definizione del problema: che tipo di coinvolgimento umano deve essere indagato?
- Analisi del compito: come verrà eseguito il compito? Quali ausili saranno necessari?
- Analisi degli errori umani: Come possono verificarsi gli errori? Come si possono recuperare?
- Rappresentazione: Come possono essere integrati questi errori nelle altre attività per calcolare la probabilità di guasto complessiva?
- Screening: Che errori non richiedono una quantificazione dettagliata?
- Valutazione dell'impatto: quali errori o compiti hanno il massimo contributo al rischio?
- Documentazione: Quali HRA devono essere documentati?

Rispondendo a queste domande si otterrà una lista di errori, le modalità di accadimento, le cause e le conseguenze nonché i metodi con cui tali errori possono essere ridotti.

Si può quindi dedurre che i punti di forza includono:

- Meccanismo formale per includere l'errore umano nella considerazione dei rischi nei sistemi in cui gli esseri umani svolgono un ruolo importante;

- Modalità e meccanismi dell'errore umano che può aiutare a ridurre il rischio.

Invece le limitazioni sono:

- Difficoltà a valutare la complessità e variabilità degli esseri umani;
- HRA ha difficoltà ad affrontare fallimenti o insuccessi parziali.

5.2.21. Analisi a papillon[52]

L'analisi a papillon può essere considerata una combinazione del pensiero di un albero dei guasti, che analizza la causa, e un albero degli eventi che analizza le conseguenze. Rappresenta quindi un modo semplice e diagrammatico di descrivere e analizzare i percorsi di un rischio.

È preferibile utilizzare questo tipo di tecnica rispetto all'albero dei guasti quando l'obiettivo è quello di garantire la presenza di una barriera o un controllo per ogni singolo problema.

Il centro del papillon (nodo) è rappresentato dall'evento identificato per l'analisi, alla sua sinistra vengono elencate le possibili cause scatenanti che verranno collegate al nodo tramite delle linee che rappresentano il meccanismo attraverso il quale la fonte di rischio conduce all'evento critico. Invece le barriere che dovrebbero impedire a ciascuna causa di diventare una conseguenza sono rappresentate come barre verticali sulle linee di collegamento. Nel lato destro, al contrario, sono rappresentate le potenziali conseguenze, anch'esse collegate attraverso linee che contengono possibili piani di recupero o di mitigazione rappresentati sempre da barre verticali.

Al termine si avrà quindi un diagramma a forma di papillon che mostra i principali percorsi di rischio con le barriere per prevenire o mitigare le conseguenze.

I punti di forza della tecnica sono:

- Una chiara e semplice rappresentazione grafica del problema;
- Focalizza l'attenzione sui controlli in atto e sulla loro efficacia;

- Non richiede un alto livello di competenza.

Invece tra i punti deboli troviamo:

- Non utilizzabile nel caso in cui più cause si verificano simultaneamente per causare le conseguenze;
- Semplifica situazioni complesse.

5.2.22. Manutenzione centrata sull'affidabilità[53]

È un metodo per identificare le politiche che possono essere implementate per gestire i guasti in modo da raggiungere in modo efficiente ed efficace il livello di sicurezza richiesto e disponibilità ed economia di funzionamento per tutte le apparecchiature. Da ciò si può quindi identificare la manutenzione preventiva applicabile ed efficace per il raggiungimento dell'obiettivo. Il massimo beneficio può essere ottenuto indirizzando l'analisi laddove i guasti avrebbero gravi conseguenze su sicurezza, ambiente, effetti economici o operativi.

Per l'applicazione della tecnica bisogna quindi possedere una buona conoscenza delle attrezzature, della struttura, dell'ambiente operativo e i sistemi associati, dei fallimenti e le loro conseguenze.

Gli step base da seguire sono:

- Avvio e pianificazione;
- Analisi dei guasti funzionali;
- Selezione dei compiti;
- Implementazione;
- Miglioramento continuo.

L'identificazione del rischio è concentrata sulle situazioni in cui i guasti possono essere eliminati o ridotti eseguendo interventi di manutenzione. Viene poi stimata la frequenza di ogni fallimento senza che la manutenzione sia eseguita. Attraverso una matrice di rischio vengono combinate la frequenza e le conseguenze, permettendo di classificare i livelli di rischio. Tutto il processo è documentato per revisione future.

A processo terminato si avranno una serie di manutenzioni da effettuare, che possono includere monitoraggio, ripristino di condizione, manutenzione programmata, ma anche riprogettazione, modifiche alle procedure o formazione aggiuntiva.

5.2.23. SA – Sneak analysis; SCI – Sneak circuit analysis[54]

SA è una metodologia di identificazione degli errori di progettazione. Per "sneak condition" si intende una condizione, hardware o software, latente che potrebbe causare un evento indesiderato, il tutto caratterizzato dalla capacità di sfuggire al rilevamento durante i periodi di test del sistema.

Gli strumenti della "sneak analysis" possono integrare diverse tecniche come l'albero dei guasti, FMEA ed altre ancora, in modo da risparmiare tempo e spese di progetto.

Le tecniche utilizzano diversi strumenti per trovare uno specifico sistema, tra essi troviamo:

- Alberi di rete: rappresenta una sottofunzione. Mostra tutti gli input che possono influenzare gli output;
- Foreste di rete: costruite combinando gli alberi, mostrano l'output di sistema correlando tutti i suoi input.

Al termine del processo, il quale consiste nella costruzione dell'albero della rete e nella valutazione dei suoi percorsi, si otterranno tutte le condizioni latenti che possono portare ad un errore del sistema. Le condizioni sono divise in 4 categorie:

- "sneak paths": percorsi inaspettati lungo i quali la corrente o l'energia scorrono in una direzione non intenzionale;
- "sneak timing": eventi che si verificano in una sequenza inaspettata;
- "sneak indication": visualizzazioni false delle condizioni di funzionamento che potrebbero indurre a compiere un'azione indesiderata;
- "sneak labels": etichettatura sbagliata o imprecisa di funzioni del sistema che potrebbe indurre ad errori.

Tra i punti di forza troviamo:

- Identificazione degli errori in fase di progettazione;
- Funziona meglio se applicato insieme ad HAZOP;
- Utile per sistemi con più strati.

I punti deboli invece sono:

- Processo diverso per diverse applicazioni;
- Dipende dalla creazione di alberi di rete corretti.

5.2.24. Analisi Markov[55]

Comunemente utilizzata per l'analisi di sistemi riparabili in cui l'utilizzo di un'analisi a blocchi non sarebbe adatto ad un'adeguata analisi del sistema.

L'analisi Markov è una tecnica quantitativa e può essere discreta, utilizzando probabilità di cambiamento tra gli stati, o continua, utilizzando i tassi di cambiamento tra gli stati.

La tecnica si presta meglio all'uso di programmi informatici sebbene possa essere anche eseguita manualmente. Viene utilizzata su varie strutture del sistema come componenti indipendenti in parallelo o in serie, sistemi in condivisione.

Per l'utilizzo della tecnica bisogna inizialmente conoscere i vari stati in cui può trovarsi il sistema (completamente operativo, parzialmente operativo, ecc.), le possibili transizioni di sistema da tenere in considerazione e il tasso di cambiamento tra uno stato e l'altro.

Per descrivere le transizioni da uno stato all'altro viene utilizzata una matrice di probabilità, la quale mette in relazione i vari stati di sistema riportando nelle caselle di combinazione le probabilità di cambiamento. Ogni casella della matrice rappresenta quindi la probabilità del sistema di trovarsi in quello specifico stato.

I punti di forza dell'analisi Markov sono:

- Capacità di calcolare le probabilità di stato del sistema.

I punti deboli invece:

- Assunzione di costanti di probabilità di cambiamento;
- Ogni evento è statisticamente indipendente in quanto il futuro non dipende dal passato, ad eccezione di quello immediatamente precedente;
- Conoscenza di tutte le probabilità di cambiamento di stato;
- Risultati difficili da comunicare al personale non tecnico.

5.2.25. Simulazione Monte Carlo[56]

Il metodo considera gli input di sistema come variabili casuali ed esegue N calcoli, chiamati simulazioni, ottenendo N possibili esiti per valutare l'effetto dell'incertezza sui sistemi tenendo conto di una vasta gamma di situazioni. Il tutto può essere sviluppato utilizzando fogli di calcolo o strumenti analoghi.

La tecnica è utilizzata soprattutto nel caso di sistemi troppo complessi da poter analizzare tramite tecniche analitiche.

Il processo prevede una prima fase di sviluppo di un modello, o algoritmo, che rappresenta il più fedelmente possibile il comportamento del sistema in oggetto. Successivamente il modello viene eseguito N volte, utilizzando numeri casuali presi da distribuzioni di probabilità, per ottenere N output che dovranno essere elaborati per fornire informazioni come valori medi, deviazione standard o intervalli di confidenza. I risultati ottenuti sono utili per ottenere i livelli di probabilità in cui si può verificare un determinato risultato.

I principali punti di forza della simulazione Monte Carlo sono:

- Modelli relativamente semplici da sviluppare con possibilità di estensione;
- Possibilità di rappresentare qualsiasi influenza o relazione esistente, anche sottili;
- Modelli facilmente comprensibili;

- Fornisce misura dell'accuratezza di un risultato;

Tra i punti deboli invece troviamo:

- Accuratezza delle soluzioni dipende dal numero di simulazioni eseguite, anche se a velocità dei nuovi computer sta ovviando a questo problema;
- Modelli grandi e complessi possono rappresentare un problema per il modellamento;
- Valutazione non adeguata riguardo eventi con conseguenze elevate o basse.

5.2.26. Statistica bayesiana e reti di Bayes[57]

La premessa della tecnica è che ogni informazione già nota (Prior) può essere combinata con misurazioni successive (Posterior) per stabilire una probabilità complessiva. L'espressione del teorema di Bayes è la seguente:

$$P(A \mid B) = \{P(A)\, P(B \mid A)\} / \Sigma i\, P(B \mid E_i)\, P(E_i)$$

Dove:

- La probabilità di X è indicata con P(X);
- La probabilità che si verifichi X a condizione che si sia verificato Y è indicata con P(X | Y);
- E_i è l'iesimo evento.

La statistica di Bayes differisce da quella classica in quanto si basa sull'interpretazione soggettiva della probabilità. Le reti di Bayes, ottenute dalla statistica, utilizzano un modello grafico per rappresentare un insieme di variabili e la loro relazione probabilistica. Essa è composta da nodi (variabili casuali) e frecce (collegamenti tra nodi genitori e nodi figli).

La tecnica è utilizzata in una vasta gamma di ambiti: si passa dalla diagnosi medica alla modellazione di immagini, all'esplorazione dello spazio fino ai motori di ricerca web utilizzati oggi.

Gli steps iniziali, necessari a sviluppare il metodo, riguardano la definizione di variabili, i nessi causali tra esse, specificare le probabilità condizionali e le probabilità a priori, aggiungere prove alla rete e estrarre credenze posteriori. Ottenute le informazioni si procede applicando l'espressione citata sopra. I risultati ottenuti mettono in relazione le variabili e, tramite il grafico, si possono notare le correlazioni tra esse.

I principali punti di forza sono:

- La regola di Bayes è l'unica cosa che serve al metodo;
- Fornisce un meccanismo per utilizzare credenze soggettive in un problema.

Tra i punti deboli della tecnica invece troviamo:

- Difficile definizione di tutte le interazioni nelle reti di Bayes;
- Richiede una conoscenza di una moltitudine di probabilità condizionali che devono essere fornite da esperti.

5.2.27. Curve FN[58]

Le curve FN sono una rappresentazione grafica della probabilità che si verifichino eventi che causano un danno ad una popolazione specifica. Esse mostrano la frequenza cumulativa (FN) alla quale N o più membri della popolazione saranno influenzati dall'evento. I valori più socialmente e politicamente inaccettabili sono quelli con valori elevati di N ed F.

Gli utilizzi della tecnica sono vari: le curve possono rappresentare i risultati dell'analisi del rischio rapportando probabilità e conseguenza, oppure sono utilizzate per confrontare i rischi, come per esempio confrontando i rischi previsti con i criteri definiti.

Le curve FN sono costruite statisticamente usando numeri reali, provenienti da perdite passate oppure calcolate delle stime di un modello di simulazione. In genere quest'ultime sono più utili a livello di progettazione del sistema, mentre le altre per la gestione di un sistema già presente.

Le curve FN presentano vari punti di forza:

- Utili per presentare le informazioni sul rischio che poi potranno essere utilizzati dai manager o progettisti di sistema per prendere decisioni sui livelli di rischio e sicurezza;
- Utili per rappresentare le informazioni sulla frequenza e sulle conseguenze in modo semplice;
- Appropriate per il confronto dei rischi derivanti da situazioni simili.

Alcuni punti deboli invece sono:

- Non dicono nulla sulla gamma di effetti o esiti degli incidenti. Ad eccezione del numero di persone colpite;
- Non rappresentano una valutazione del rischio ma sono un modo di rappresentare i dati estrapolati da essa.

5.2.28. Indici di rischio[59]

Questi metodi sono utilizzati per valutare una serie di rischi utilizzando criteri simili in modo da poter confrontare i risultati. Un indice di rischio è una misura semiquantitativa del rischio utilizzando una stima derivata dall'assegnazione di un punteggio preso da una scala ordinale. I punteggi vengono applicati ad ogni componente del rischio (fonti, vie di impatto e altro ancora). Ciò può essere utilizzato per determinare quali rischi necessitano di una valutazione più approfondita.

Le informazioni necessarie derivano dall'analisi del sistema, ciò richiede una buona comprensione di tutte le fonti del rischio che può essere ottenuta tramite l'utilizzo di altre tecniche (es. albero dei guasti).

Inizialmente è necessario definire il sistema in oggetto e i punteggi da assegnare ad ogni componente in modo che quest'ultimi possano essere combinati per formare un indice composito. L'incertezza può essere affrontata mediante un'analisi di sensibilità dei punteggi.

Al termine si avranno una serie di indici compositi, riferiti ad una particolare fonte, che possono essere confrontati tra loro.

Tra i punti di forza del metodo troviamo:

- Gli indici sono un valido strumento per classificare diversi rischi;
- Un indice incorpora molteplici fattori che incidono su un rischio.

Le principali limitazioni invece sono:

- Se il modello non è ben validato il risultato potrebbe non essere corretto;
- In alcune simulazioni le scale possono essere non definite correttamente e la valutazione divenire inaffidabile.

5.2.29. Matrice conseguenze/probabilità[60]

La matrice conseguenze/probabilità è utilizzata come classificazione dei rischi o delle fonti di rischio. Comunemente si usa quando sono stati identificati molti rischi e per definire quali di essi non sono accettabili e necessitano di un'analisi più dettagliata.

I livelli di rischio devono essere stabiliti preventivamente e dovrebbero essere in linea con la propensione del rischio dell'organizzazione. Generalmente i livelli si estendono dalla massima conseguenza credibile alla minima conseguenza di preoccupazione, tenendo conto, però, che il livello di probabilità più basso, combinato con il livello di conseguenza più alto, deve essere accettabile, altrimenti tutti i valori più alti saranno di conseguenza intollerabili. Le scale più comuni sono quelle a 3, 4 o 5 punti. L'utilizzo dello strumento necessita di un team con competenze pertinenti e dati disponibili per aiutare i giudizi.

Stabilita la scala, l'utente definisce il livello di probabilità dell'evento e il livello della sua conseguenza, compara i due livelli tramite la matrice e trova il livello di rischio. Procedendo così per ogni evento, al termine si avrà una valutazione per ogni rischio.

I punti di forza del metodo sono:

- Facilità d'uso;
- Rapida classificazione dei rischi in diversi livelli di significatività.

Al contrario, i punti deboli sono:

- Difficoltà ad avere un sistema comune applicabile a tutti i rischi in quanto la matrice dovrebbe essere adeguata alle circostanze;
- Utilizzo soggettivo del metodo;
- Difficoltà confrontare il livello di rischio per diverse categorie di conseguenze.

5.2.30. CBA – Analisi costi/benefici[61]

L'analisi descritta in questo metodo è parte implicita in molti dei sistemi di valutazione del rischio. Essa consiste nel peso dei costi totali previsti rispetto al totale dei benefici attesi, al fine di scegliere l'opzione migliore e più redditizia.

Il valore attuale netto (VAN) è un input per le decisioni da prendere. Un valore positivo associato ad un'azione, normalmente, indica che essa dovrebbe essere fatta. Tuttavia, per i rischi negativi che comportano rischi per la vita, si può applicare il codice ALARP.

I rischi sono perciò divisi in tre livelli:

- Intollerabili: i rischi non dovrebbero essere assunti se non in circostanze straordinarie;
- Trascurabili: i rischi devono solo essere monitorati per garantire il mantenimento di basso livello;
- Fascia centrale: rischi ridotti al minimo ragionevolmente praticabile (ALARP).

Il metodo CBA dovrebbe essere applicato agli ultimi due livelli. Mentre per quelli intollerabili, come già detto, vale il principio ALARP a meno che il costo non sia gravemente sproporzionato rispetto il beneficio ottenuto.

Ci sono più fini d'uso per il metodo come il decidere se un rischio debba essere trattato o meno, trovare la migliore forma di trattamento o decidere tra le diverse linee di azione.

4.2.31. MCDA - Analisi decisionale multicriterio[62]

l'obiettivo principale del metodo è quello di valutare una serie di opzioni, in modo obiettivo e trasparente, per poi sviluppare una matrice criteri che, classificati ed aggregati, forniscono un punteggio complessivo per ciascuna opzione al fine di avere un ordine di preferenza tra esse.

la tecnica viene utilizzata in diversi modi, come per esempio il confronto di più opzioni per determinare quale sia la più appropriata oppure raggiungere il consenso su una decisione in cui diversi stakeholder hanno obiettivi o valori contrastanti.

in generale per l'utilizzo si intraprende il seguente processo:

- definizione degli obiettivi con la determinazione degli attributi di ognuno di essi;
- strutturazione degli attributi in una gerarchia;
- sviluppo di opzioni da valutare rispetto i criteri;
- determinazione dell'importanza dei criteri con l'attribuzione dei relativi "pesi";
- valutazione delle alternative rispetto i criteri tramite l'utilizzo di una matrice di punteggi;
- combinazione dei punteggi dei singoli attributi in un punteggio multiattributo aggregato;
- valutazione dei risultati.

al termine si otterrà la lista delle opzioni ordinata dalla migliore alla peggiore in base al punteggio con la possibilità di eliminare quelle che non soddisfano i criteri prefissati.

i punti di forza della tecnica sono:

- struttura semplice per il processo di presentazione delle ipotesi e per il processo decisionale;
- affronta problemi decisionali complessi non suscettibili ad analisi costi/benefici;
- aiuta a considerare razionalmente problemi per i quali è necessario scendere a compromessi;
- aiuta a raggiungere un accordo tra le parti interessate che hanno obiettivi diversi.

i punti deboli invece sono:

- influenzata da un'errata selezione dei criteri decisionali;
- la maggior parte dei problemi non hanno una soluzione unica;

5.3. Comparazione delle tecniche

La ISO 31010 presenta nell'allegato A due tabelle di classificazione delle tecniche descritte nel punto 4.2. della presente documentazione. La prima (Tab. 2), tramite l'utilizzo dei tre criteri di valutazione fortemente applicabile, applicabile o non applicabile, fornisce indicazioni sull'applicazione delle tecniche in base alla fase della valutazione del rischio in cui ci troviamo.

Tab. 2 – Applicabilità degli strumenti usati per la valutazione del rischio

Tools and techniques	Risk assessment process				
	Risk Identification	Risk analysis			Risk evaluation
		Consequence	Probability	Level of risk	
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA
Structured or semi-structured interviews	SA	NA	NA	NA	NA
Delphi	SA	NA	NA	NA	NA
Check-lists	SA	NA	NA	NA	NA
Primary hazard analysis	SA	NA	NA	NA	NA
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA
Environmental risk assessment	SA	SA	SA	SA	SA
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA
Scenario analysis	SA	SA	A	A	A
Business impact analysis	A	SA	A	A	A
Root cause analysis	NA	SA	SA	SA	SA
Failure mode effect analysis	SA	SA	SA	SA	SA
Fault tree analysis	A	NA	SA	A	A
Event tree analysis	A	SA	A	A	NA
Cause and consequence analysis	A	SA	SA	A	A
Cause-and-effect analysis	SA	SA	NA	NA	NA
Layer protection analysis (LOPA)	A	SA	A	A	NA
Decision tree	NA	SA	SA	A	A
Human reliability analysis	SA	SA	SA	SA	A
Bow tie analysis	NA	A	SA	SA	A
Reliability centred maintenance	SA	SA	SA	SA	SA
Sneak circuit analysis	A	NA	NA	NA	NA
Markov analysis	A	SA	NA	NA	NA
Monte Carlo simulation	NA	NA	NA	NA	SA
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA
FN curves	A	SA	SA	A	SA
Risk indices	A	SA	SA	A	SA
Consequence/probability matrix	SA	SA	SA	SA	A
Cost/benefit analysis	A	SA	A	A	A
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A

Mentre la seconda (Tab. 3) descrive gli attributi dei metodi, tramite la classificazione alto, medio o basso, in termini di:

- complessità del problema;

- natura e grado di incertezza nella valutazione in base all'importo di informazioni disponibili e di cosa è necessario per soddisfare gli obiettivi;
- entità delle risorse in termini di tempo, livelli di competenza, esigenza di dati o costo;
- se il metodo può fornire un risultato quantitativo.

Tab. 3 – Attributi di una selezione di tecniche di valutazione del rischio

Type of risk assessment technique	Description	Relevance of influencing factors			Can provide Quantitative output
		Resources and capability	Nature and degree of uncertainty	Complexity	
LOOK-UP METHODS					
Check-lists	A simple form of risk identification. A technique which provides a listing of typical uncertainties which need to be considered. Users refer to a previously developed list, codes or standards	Low	Low	Low	No
Preliminary hazard analysis	A simple inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system	Low	High	Medium	No
SUPPORTING METHODS					
Structured Interview and brainstorming	A means of collecting a broad set of ideas and evaluation, ranking them by a team. Brainstorming may be stimulated by prompts or by one-on-one and one-on-many interview techniques	Low	Low	Low	No
Delphi technique	A means of combining expert opinions that may support the source and influence identification, probability and consequence estimation and risk evaluation. It is a collaborative technique for building consensus among experts. Involving independent analysis and voting by experts	Medium	Medium	Medium	No
SWIFT Structured "what-if")	A system for prompting a team to identify risks. Normally used within a facilitated workshop. Normally linked to a risk analysis and evaluation technique	Medium	Medium	Any	No
Human reliability analysis (HRA)	Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system	Medium	Medium	Medium	Yes
SCENARIO ANALYSIS					
Root cause analysis (single loss analysis)	A single loss that has occurred is analysed in order to understand contributory causes and how the system or process can be improved to avoid such future losses. The analysis shall consider what controls were in place at the time the loss occurred and how controls might be improved	Medium	Low	Medium	No

Type of risk assessment technique	Description	Relevance of influencing factors			Can provide Quantitative output
		Resources and capability	Nature and degree of uncertainty	Complexity	
Scenario analysis	Possible future scenarios are identified through imagination or extrapolation from the present and different risks considered assuming each of these scenarios might occur. This can be done formally or informally qualitatively or quantitatively	Medium	High	Medium	No
Toxicological risk assessment	Hazards are identified and analysed and possible pathways by which a specified target might be exposed to the hazard are identified. Information on the level of exposure and the nature of harm caused by a given level of exposure are combined to give a measure of the probability that the specified harm will occur	High	High	Medium	Yes
Business impact analysis	Provides an analysis of how key disruption risks could affect an organization's operations and identifies and quantifies the capabilities that would be required to manage it	Medium	Medium	Medium	No
Fault tree analysis	A technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes / sources	High	High	Medium	Yes
Event tree analysis	Using inductive reasoning to translate probabilities of different initiating events into possible outcomes	Medium	Medium	Medium	Yes
Cause/ consequence analysis	A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered	High	Medium	High	Yes
Cause-and-effect analysis	An effect can have a number of contributory factors which may be grouped into different categories. Contributory factors are identified often through brainstorming and displayed in a tree structure or fishbone diagram	Low	Low	Medium	No

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output possible?
FUNCTION ANALYSIS					
FMEA and FMECA	FMEA (Failure Mode and Effect Analysis) is a technique which identifies failure modes and mechanisms, and their effects. There are several types of FMEA: Design (or product) FMEA which is used for components and products, System FMEA which is used for systems, Process FMEA which is used for manufacturing and assembly processes, Service FMEA and Software FMEA. FMEA may be followed by a criticality analysis which defines the significance of each failure mode, qualitatively, semi-qualitatively, or quantitatively (FMECA). The criticality analysis may be based on the probability that the failure mode will result in system failure, or the level of risk associated with the failure mode, or a risk priority number	Medium	Medium	Medium	Yes
Reliability-centred maintenance	A method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment	Medium	Medium	Medium	Yes
Sneak analysis (Sneak circuit analysis)	A methodology for identifying design errors. A sneak condition is a latent hardware, software, or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel	Medium	Medium	Medium	No
HAZOP Hazard and operability studies	A general process of risk identification to define possible deviations from the expected or intended performance. It uses a guideword based system. The criticalities of the deviations are assessed	Medium	High	High	No
HACCP Hazard analysis and critical control points	A systematic, proactive, and preventive system for assuring product quality, reliability and safety of processes by measuring and monitoring specific characteristics which are required to be within defined limits	Medium	Medium	Medium	No

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output possible?
CONTROLS ASSESSMENT					
LOPA (Layers of protection analysis	(May also be called barrier analysis). It allows controls and their effectiveness to be evaluated	Medium	Medium	Medium	Yes
Bow tie analysis	A simple diagrammatic way of describing and analysing the pathways of a risk from hazards to outcomes and reviewing controls. It can be considered to be a combination of the logic of a fault tree analysing the cause of an event (represented by the knot of a bow tie) and an event tree analysing the consequences	Medium	High	Medium	Yes
STATISTICAL METHODS					
Markov analysis	Markov analysis, sometimes called *State-space* analysis, is commonly used in the analysis of repairable complex systems that can exist in multiple states, including various degraded states	High	Low	High	Yes
Monte-Carlo analysis	Monte Carlo simulation is used to establish the aggregate variation in a system resulting from variations in the system, for a number of inputs, where each input has a defined distribution and the inputs are related to the output via defined relationships. The analysis can be used for a specific model where the interactions of the various inputs can be mathematically defined. The inputs can be based upon a variety of distribution types according to the nature of the uncertainty they are intended to represent. For risk assessment, triangular distributions or beta distributions are commonly used	High	Low	High	Yes
Bayesian analysis	A statistical procedure which utilizes prior distribution data to assess the probability of the result. Bayesian analysis depends upon the accuracy of the prior distribution to deduce an accurate result. Bayesian belief networks model cause-and-effect in a variety of domains by capturing probabilistic relationships of variable inputs to derive a result	High	Low	High	Yes

Come si può notare dalle due tabelle non esiste una tecnica unica da utilizzare ma, in base al contesto organizzativo, agli obiettivi e ai dati disponibili, bisogna utilizzare una combinazione di più tecniche complementari tra loro, come per esempio ETA e HAZOP, per eseguire una corretta e totale valutazione dei rischi.

5.3.1. Comparazione tra due tecniche

Mettiamo a confronto due tecniche diverse tra loro: il Brainstorming e RCA.

Possiamo sintetizzare i punti fondamentali delle due tecniche, ampiamente trattate precedentemente, così:

Brainstorming: Gruppo di persone competenti; Nessuna richiesta di dati come input iniziale; Ha come scopo l'identificazione di rischi, pericoli, criteri decisionali ecc.	RCA: Gruppo di persone competenti Utilizzata a seguito dell'avvenimento di un guasto per determinarne la causa; Raccolta dati da analizzare; determinazione e verifica soluzioni

Entrambe prevedono la formazione di un gruppo di figure competenti sull'argomento, sistema o processo da trattare ma, come si può ben notare dai punti precedentemente elencati, le tecniche hanno metodi di utilizzo e obiettivi differenti. nel primo caso, il brainstorming, abbiamo una tecnica più "libera" che svolge meglio la sua funzione in una fase iniziale, quella dell'identificazione dei rischi, che non richiede particolari dati disponibili per essere utilizzata. Mentre nel secondo caso lo scopo è diverso, partendo da una raccolta di dati riguardanti si passa ad un'analisi di essi per determinare le cause del guasto in esame e sviluppare le soluzioni da attuare per non permetterne il ripetersi in futuro. Ne consegue che quest'ultima è più funzionale in un contesto di analisi dei rischi oppure di valutazione del rischio.

Possiamo dedurre da questo breve esempio che ogni tecnica deve essere utilizzata nel corretto campo di utilizzo e nella giusta fase della gestione del rischio. Altro punto fondamentale che possiamo trarre dall'esempio è che una sola tecnica non riesce a coprire tutto il processo di gestione del rischio ma occorre combinarne

diverse per ottenere i migliori risultati possibili e poter incrementare il valore d'impresa.

6. ISO 45001:2018 - sistemi di gestione per la salute e sicurezza sul lavoro

La premessa della ISO 45001:2018 è che un'organizzazione è responsabile della salute e sicurezza sul lavoro (SSL) dei lavoratori. Perciò essa, tramite l'adozione di un sistema di gestione, fornisce un quadro dei rischi e delle opportunità per la SSL al fine di prevenire lesioni e malattie ai lavoratori e di predisporre luoghi di lavoro sicuri e salubri[63].

Il concetto alla base di tutto ciò è il processo iterativo Plan-Do-Check-Act che consiste nel stabilire e valutare i rischi e opportunità per la SSL, attuare i processi pianificati, monitorare e misurare i processi verificandone i risultati ed infine applicare azioni correttive al fine di migliorare le prestazioni del sistema[64].

la normativa fornisce dei punti fondamentali da analizzare e sviluppare per la corretta applicazione di un sistema di gestione per la SSL. Essi sono:

- contesto dell'organizzazione;
- leadership e partecipazione dei lavoratori;
- pianificazione;
- supporto;
- attività operative;
- valutazione delle prestazioni;
- miglioramenti

6.1. Contesto dell'organizzazione[65]

prima di procedere allo sviluppo del sistema bisogna innanzitutto comprendere a fondo l'organizzazione e il suo contesto, determinando tutti i fattori, esterni ed interni, che possono influenzare i risultati attesi. inoltre la stessa deve conoscere

tutte le parti interessate, compresi i lavoratori, le loro esigenze e aspettative e quali tra esse possono diventare requisiti legali.

si passa poi alla definizione dei confini del sistema, cioè qual è il suo campo di applicazione.

6.2. Leadership e partecipazione dei lavoratori[66]

in quanto un sistema di gestione per la SSL, se applicato, deve essere parte integrante dell'organizzazione, l'alta dirigenza deve dimostrare il massimo impegno assumendosi la responsabilità e l'obbligo della prevenzione di lesioni e malattie correlate ai lavori, nonché di predisporre luoghi di lavoro sicuri e salubri. tutto ciò avviene stabilendo una politica e gli obiettivi del SSL compatibili agli indirizzi strategici dell'organizzazione, fornendo le risorse necessarie all'applicazione di esso e in generale sviluppando, garantendo e promuovendo una cultura dell'organizzazione che presti attenzione ai lavoratori assicurando un miglioramento continuo delle condizioni lavorative.

il documento di politica, citato precedentemente, deve essere un punto di riferimento, che comprenda l'impegno ad eliminare i pericoli e ridurre i rischi per i lavoratori, la consultazione e partecipazione attiva dei lavoratori e fissi gli obiettivi da perseguire.

la dirigenza deve inoltre assegnare e comunicare, a tutti i livelli, le responsabilità e i compiti alle figure fondamentali del sistema di gestione, le quali hanno funzione di assicurare la corretta applicazione di esso e riferire a chi di dovere le prestazioni del sistema.

Per ultimo, ma non per importanza, la dirigenza deve stabilire i processi per la consultazione e partecipazione di tutti i lavoratori per la valutazione delle azioni da applicare sia per lo sviluppo del sistema di gestione sia per il miglioramento di esso.

6.3. Pianificazione[67]

Durante questa fase, oltre a considerare i fattori descritti nel punto precedente, l'organizzazione deve determinare i rischi e le opportunità per garantire che il sistema persegua i risultati attesi, prevenire gli effetti indesiderati e conseguire il miglioramento continuo. per fare ciò deve stabilire ed attuare uno o più processi che identificano i pericoli, tenendo conto dell'organizzazione del lavoro, le attività svolte, incidenti rilevanti già accaduti, situazioni di potenziale emergenza, del personale che ha accesso o è nelle vicinanze dei luoghi di lavoro ed altri fattori quali la progettazione degli impianti, luoghi di lavoro e macchinari.

Successivamente si passa alla fase di valutazione dei rischi, in cui vengono valutati sia i rischi connessi ai pericoli individuati sia altri rischi legati alle attività operative e di manutenzione.

nell'attività di pianificazione è compresa anche la valutazione di opportunità di miglioramento di prestazioni della SSL che possono riguardare la modifica dell'organizzazione al fine di adattare al meglio il lavoro al lavoratore e di ridurre o eliminare pericoli e rischi.

infine l'organizzazione deve stabilire gli obiettivi per la SSL al fine di mantenere alti, e di migliorare, le prestazioni del sistema. tali obiettivi devono essere coerenti con la politica, essere misurabili per fornire una valutazione, essere monitorati, comunicati e aggiornati appropriatamente.

6.4. Supporto[68]

l'organizzazione è tenuta a fornire le risorse, come quelle umane, infrastrutturali o tecnologiche, necessarie, non limitandosi solamente a quelle economiche. per fare ciò bisogna:

- determinare le competenze necessarie: valutare le competenze che i lavoratori che influenzano le prestazioni del sistema devono possedere, assicurarsi che le apprendono e conservare le evidenze documentali;

- rendere consapevoli i lavoratori: della politica aziendale, della necessità del loro contributo per l'efficacia del sistema e dei rischi e pericoli presenti in azienda;
- organizzazione della comunicazione: innanzitutto si deve definire l'oggetto della comunicazione, quando e con chi comunicare e come farlo, tenendo conto di tutte le diversità, come genere, lingua, presenti all'interno dell'azienda. Inoltre l'organizzazione deve assicurare la considerazione di tutte le opinioni delle parti interessate. la comunicazione è divisa in: interna, quando avviene tra le figure dell'organizzazione, ed esterna.

tutte le informazioni descritte, utili all'efficacia del sistema di gestione, devono essere documentate, ciò comporta la creazione di documenti specifici che devono essere tenuti sotto controllo per assicurare che siano disponibili per la consultazione ed idonee all'utilizzo.

6.5. Attività operative[69]

si passa poi ad una fase pratica attuando i processi determinati nella fase di pianificazione, mantenendoli sotto controllo e conservando le informazioni affinché sia garantita la corretta applicazione.

questa fase, però, non è statica ma devono essere attuati processi che controllino le modifiche temporanee o permanenti che hanno un impatto sulle prestazioni in termini di SSL, come per esempio l'utilizzo di nuovi prodotti, cambiamenti nelle conoscenze o informazioni, ma anche sviluppi tecnologici. devono poi essere riesaminate le conseguenze dei cambiamenti, ed attuare azioni mitigative per ridurre gli effetti negativi.

un'altra fase importante da attuare è quella della coordinazione dei processi di approvvigionamento con i fornitori o appaltatori, per tenere sotto controllo i rischi derivanti dalle loro attività svolte all'interno dell'organizzazione.

infine, altri processi riguardano la preparazione e risposta alle emergenze, i quali sono utili per stabilire una risposta pianificata alle situazioni di emergenza. è

importante quindi fornire la formazione adeguata ai lavoratori, effettuare esercitazioni per valutare il corretto apprendimento e informare le ditte terze dei servizi di risposta alle emergenze attuati.

6.6. Valutazione delle prestazioni[70]

Per avere la certezza del corretto funzionamento del sistema e del raggiungimento degli obiettivi, i processi messi in atto sono continuamente:

- monitorati: ciò comporta il controllo continuo e la supervisione del sistema, dei processi o dei controlli, al fine di verificare lo scostamento dai livelli di prestazione richiesti;
- misurati: cioè l'assegnazione di un numero agli oggetti o agli eventi. dalla misurazione vengono estrapolati i dati quantitativi che verranno utilizzati per la valutazione delle prestazioni del sistema:
- analizzati: associato direttamente alla misurazione. i dati vengono esaminati per rivelare eventuali relazioni, schemi o tendenze.

oltre ai punti sopra descritti l'organizzazione deve elaborare un programma di auditing interno assicurandosi l'imparzialità dell'auditor.

6.7. Miglioramento[71]

tenendo in considerazione i risultati delle analisi, valutazioni e audit l'organizzazione esegue interventi di correzione sulle parti carenti al fine di un miglioramento continuo del sistema di gestione.

7. Integrazione delle norme ISO 31000 e ISO 45001

Da quello che abbiamo potuto osservare durante l'analisi delle norme ISO 31000 ed ISO 45001 è che entrambe puntano ad un miglioramento dell'efficienza produttiva attraverso una gestione del rischio efficiente ed efficace. La prima, attraverso l'individuazione di principi definiti garantisce la gestione del rischio a tutti i livelli aziendali garantendo la creazione e protezione del valore. Tutto ciò,

inevitabilmente, passa attraverso l'individuazione di quei fattori di rischio che possono produrre inefficienze operative e sprechi di risorse.
La seconda, invece, fornendo uno standard vero e proprio per la creazione di un sistema di gestione per la salute e sicurezza sul lavoro, punta ad un aumento della performance attraverso la riduzione dei rischi e, conseguentemente, degli incidenti in ambito lavorativo.

Possiamo quindi dedurre che in un'organizzazione che punta ad acquisire vantaggi competitivi e al raggiungimento di obiettivi, l'integrazione delle due ISO, seppur richieda una pianificazione ed una strategia ben pianificata, diventa di fondamentale importanza. Un approccio di questo tipo garantisce delle sinergie tra la gestione del rischio e sicurezza sul lavoro. Utilizzando un processo integrato per l'identificazione e valutazione dei rischi, includendo sia quelli operativi sia quelli legati alla sicurezza, si ottiene una visione più completa del contesto aziendale, evitando al contempo una duplicazione di sforzi e risorse che l'applicazione e la gestione separata delle due normative comporterebbe. Inoltre, si avrebbe l'allineamento degli obiettivi di gestione del rischio e della salute e sicurezza, garantendo una coerenza con le strategie aziendali.

Per esempio, con l'applicazione delle tecniche presenti nella ISO 31010, che ha funzione di supporto alla ISO 31000, come l'analisi dell'albero degli eventi (ETA), il quale metodo analizza una serie di eventi derivanti da un evento scatenante, si possono analizzare contemporaneamente i rischi riguardanti l'operatività sia quelli riguardanti la sicurezza dei lavoratori. Ciò implica, di conseguenza, anche la possibilità di organizzare in maniera simultanea delle risposte per le due tipologie di rischio citate prima.

Infatti, un'integrazione di questo tipo consente una risposta coordinata e più efficace agli imprevisti o agli eventi incidentali. La progettazione e la programmazione di procedure di emergenza che tengano conto di entrambi gli aspetti diventano di fondamentale importanza per le organizzazioni, esse

garantiscono che gli interventi preventivi e le eventuali azioni correttive siano tempestive e siano congruenti tra loro.

Non bisogna però dimenticare che un ruolo fondamentale per l'applicazione di un sistema integrato tra ISO 31000 e ISO 45001 è ricoperto dall'alta direzione, in entrambe le norme infatti essa è la figura centrale di tutto il processo. Deve definire una chiara politica di gestione del rischio, coerente in tutte le attività aziendali e che tenga conto del contesto, interno ed esterno, dell'organizzazione. Non deve però operare singolarmente ma, al contrario, è chiaro come il coinvolgimento e la consultazione di tutte le figure chiave, le quali devono essere a conoscenza del loro ruolo aziendale, oltre ad essere informate e formate sui rischi aziendali in modo da saper come agire in ogni circostanza, è parte integrante dello sviluppo del sistema. Chi ha il potere decisionale deve quindi promuovere una cultura aziendale che metta la gestione del rischio al centro delle operazioni, fornendo anche i mezzi e le risorse adeguate all'applicazione del sistema.

Il sistema, dopo la progettazione e l'esecuzione, non è statico ma, anzi, deve essere in continua evoluzione. Il principio base delle due norme è infatti il ciclo di Deming che parla appunto di miglioramento continuo. Il ciclo può essere sintetizzato in quattro fasi: Plan-Check-Do-Act. Le procedure una volta pianificate ed applicate devono essere continuamente monitorate e i risultati devono essere raccolti ed analizzati per capirne le lacune e le conseguenti possibilità di miglioramento, ritornando dunque alla fase di pianificazione.

8. Best practice: collegamento con le ISO

Se, come abbiamo visto, una corretta gestione della sicurezza è un enorme fattore di successo per un'organizzazione, essa passa inevitabilmente dall'applicazione delle best practice in questo ambito. Per best practice si intendono le migliori procedure per la gestione di situazioni che potrebbero causare un evento indesiderato o per la gestione dell'evento stesso, esse si basano sia su indicatori quantitativi o qualitativi sia sull'esperienza pregressa.

Possiamo quindi dedurre che per la scelta delle best practice si deve necessariamente ricorrere ai principi descritti nella ISO 45001, la quale ha come fondamento l'efficace e corretta valutazione e gestione dei rischi che, di conseguenza è direttamente correlata alla ISO 31000, la quale fornisce le linee guida per la gestione del rischio, e alla ISO 31010, che ne fornisce le tecniche per l'applicazione.

Ecco che, ancora una volta, viene ribadita la correlazione tra le norme. Si può dedurre dunque che queste il massimo valore applicativo delle tre si ha tramite l'applicazione di un sistema integrato che ne consideri l'utilizzo simultaneo, evitando, come già detto, spreco di tempo e risorse, nonché una coerente gestione complessiva.

9. Conclusioni

Come abbiamo avuto modo di osservare nella descrizione delle 3 normative ISO 31000, ISO 31010 e ISO 45001 esse sono strettamente collegate e correlate.

Se la prima permette l'integrazione di un sistema di gestione in tutte le attività aziendali, fornendo definizioni ben specifiche, la ISO 45001 si concentra sul campo salute e sicurezza sul lavoro, parte fondamentale per un'organizzazione. infine abbiamo la ISO 31010 che elenca le tipologie di valutazione dei rischi utili a raggiungere gli obiettivi prefissati da entrambe le normative precedenti.

Si capisce di conseguenza che, essendo la 45001 una valutazione di una parte di un'attività aziendale, rientrando direttamente quindi nella ISO 31000, e la 31010 un elenco di tecniche utilizzate dalle altre due, le normative ottengono il massimo valore possibile dall'applicazione solo attraverso una combinazione di tutte e tre.

Se alle prime due domande poste nell'introduzione abbiamo abbondantemente risposto durante lo svolgimento della presente documentazione, la terza, cioè perché un'organizzazione dovrebbe adottare dei sistemi di gestione del rischio, necessita, ancora, di una risposta.

una corretta valutazione del rischio e l'applicazione di idonee misure di eliminazione o, quando non possibile, di mitigazione dei rischi permette nel lungo periodo una riduzione significativa dei costi consentendo una continuità ai processi aziendali ed aumentando di conseguenza i risultati ottenuti dell'organizzazione.

Inoltre, l'applicazione di tecniche di valutazione del rischio permettono di venire a conoscenza dei punti carenti delle attività dell'organizzazione, nonché dei possibili eventi incidentali che possono comportare un pericolo per i lavoratori, permettendo di pianificare una corretta procedura per la gestione delle emergenze in modo da non farsi trovare impreparati in caso di accadimento dell'evento.

Possiamo quindi dedurre che le organizzazioni che vogliono aumentare di valore non possono non tenere in considerazione l'applicazione di uno o più sistemi di gestione visto i numerosi punti di forza che essi comportano.

RIFERIMENTI

[1] Cos'è il Risk Management - ANRA

2Il Risk management - Borsa Italiana

[3] L'identificazione dei rischi - ANRA

[4]art 2, lettera n, D.Lgs. 81/08

[5]La sicurezza sul lavoro, Prof. Mazzuto

[6] La sicurezza sul lavoro, Prof. Mazzuto

[7]ISO 31000:2018, pag. 2-3, Paragrafo 4 "Principles"

[8] ISO 31000:2018, pag. 4, Paragrafo 5 "Framework"

[9] ISO 31000:2018, pag. 5, Paragrafo 5.2 "Leadership ad commitment"

[10] ISO 31000:2018, pag. 5, Paragrafo 5.3 "Integrazione"

[11] ISO 31000:2018, pag. 6, Paragrafo 5.4 "Design"

[12] ISO 31000:2018, pag. 6, Paragrafo 5.4.1 "Comprendere l'organizzazione ed il suo contesto"

[13] ISO 31000:2018, pag. 6, Paragrafo 5.4.2 "Articolare l'impegno alla gestione del rischio"

[14] ISO 31000:2018, pag. 7, Paragrafo 5.4.3 "Assegnare ruoli organizzativi, autorità e responsabilità"

[15] ISO 31000:2018, pag. 7, Paragrafo 5.4.4 "Allocare risorse appropriate"

[16] ISO 31000:2018, pag. 7, Paragrafo 5.4.5 "Stabilire comunicazione e consultazione"

[17] ISO 31000:2018, pag. 7, Paragrafo 5.5 "Implementazione"

[18] ISO 31000:2018, pag. 8, Paragrafo 5.6 "Valutazione"

[19] ISO 31000:2018, pag. 8, Paragrafo 5.7 "Miglioramento"

[20] ISO 31000:2018, pag. 8, Paragrafo 6 "Processi"

[21] ISO 31000:2018, pag. 9, Paragrafo 6.2 "Comunicazione e consultazione"

[22] ISO 31000:2018, pag. 10, Paragrafo 6.3 "Scopo, contesti e criteri"

[23] ISO 31000:2018, pag. 11, Paragrafo 6.4 "Valutazione del rischio"

[24] ISO 31000:2018, pag. 13, Paragrafo 6.5 "Trattamento del rischio"

[25] ISO 31000:2018, pag. 14, Paragrafo 6.6 "Monitoraggio e revisioni"

[26] ISO 31000:2018, pag. 14, Paragrafo 6.7 "Registrazione e rendicontazione"

[27] ISO 31010:2019, pag. 18, Paragrafo 6 "Selezione delle tecniche di valutazione del rischio"

[28] ISO 31010:2019, pag. 19, Paragrafo 6.3 "Disponibilità delle risorse"

[29] ISO 31010:2019, pag. 19, Paragrafo 6.4 "Natura e grado delle incertezze"

[30] ISO 31010:2019, pag. 19, Paragrafo 6.3 "Complessità"

[31] https://www.riskmanagement360.it/risk-analysis/gestione-del-rischio-tutto-quello-che-bisogna-sapere/

[32] ISO 31010:2019, pag. 27, Allegato B, Paragrafo B.1 “Brainstorming”

[33] ISO 31010:2019, pag. 28, Allegato B, Paragrafo B.2 “Interviste strutturate e semi strutturate”

[34] ISO 31010:2019, pag. 29, Allegato B, Paragrafo B.3 “Tecnica Delphi”

[35] ISO 31010:2019, pag. 30, Allegato B, Paragrafo B.4 “Check-lists”

[36] ISO 31010:2019, pag. 31, Allegato B, Paragrafo B.5 “PHA- Preliminary hazard analysis”

[37] ISO 31010:2019, pag. 32, Allegato B, Paragrafo B.6 “HAZOP”

[38] ISO 31010:2019, pag. 35, Allegato B, Paragrafo B.7 “HACCP- Hazard Analysis and Critical Control Point”

[39] ISO 31010:2019, pag. 36, Allegato B, Paragrafo B.8 “Valutazione della tossicità”

[40] ISO 31010:2019, pag. 38, Allegato B, Paragrafo B.9 “SWIFT- Structured What-if Technique”

[41] ISO 31010:2019, pag. 40, Allegato B, Paragrafo B.10 “Analisi dello scenario”

[42] ISO 31010:2019, pag. 42, Allegato B, Paragrafo B.11 “BIA – Analisi dell’impatto aziendale”

[43] ISO 31010:2019, pag.44, Allegato B, Paragrafo B.12 “RCA – Analisi delle cause alla radice”

[44] ISO 31010:2019, pag. 46, Allegato B, Paragrafo B.13 “FMEA e FMECA”

[45] ISO 31010:2019, pag. 49, Allegato B, Paragrafo B.14 “FTA – Analisi dell’albero dei guasti”

[46] ISO 31010:2019, pag. 51, Allegato B, Paragrafo B.15 “ETA – Analisi dell’albero degli eventi”

[47] ISO 31010:2019, pag. 54, Allegato B, Paragrafo B.16 “Analisi causa-conseguenza”

[48] ISO 31010:2019, pag. 56, Allegato B, Paragrafo B.17 “Analisi causa-effetto”

[49] ISO 31010:2019, pag. 59, Allegato B, Paragrafo B.18 “LOPA – Analisi dei livelli di protezione”

[50] ISO 31010:2019, pag. 61, Allegato B, Paragrafo B.19 “Analisi albero delle decisioni”

[51] ISO 31010:2019, pag. 61, Allegato B, Paragrafo B.20 “HRA – Valutazione dell’affidabilità umana”

[52] ISO 31010:2019, pag. 64, Allegato B, Paragrafo B.21 “Analisi a papillon”

[53] ISO 31010:2019, pag. 66, Allegato B, Paragrafo B.22 “Manutenzione centrata sull’affidabilità”

[54] ISO 31010:2019, pag. 68, Allegato B, Paragrafo B.23 “SA – Sneak analysis; SCI – Sneak circuit analysis”

[55] ISO 31010:2019, pag. 69, Allegato B, Paragrafo B.24 “Analisi Markov”

[56] ISO 31010:2019, pag. 73, Allegato B, Paragrafo B.25 “Simulazione Monte Carlo”

[57] ISO 31010:2019, pag. 76, Allegato B, Paragrafo B.26 “Statistica bayesiana e reti di Bayes”

[58] ISO 31010:2019, pag. 79, Allegato B, Paragrafo B.27 “Curve FN”

[59] ISO 31010:2019, pag. 81, Allegato B, Paragrafo B.28 “Indici di rischio”

[60] ISO 31010:2019, pag. 82, Allegato B, Paragrafo B.29 “Matrice conseguenze/probabilità”

[61] ISO 31010:2019, pag. 86, Allegato B, Paragrafo B.30 “CBA – Analisi costi/benefici”

[62] ISO 31010:2019, pag. 88, Allegato B, Paragrafo B.31 “MCDA – Analisi decisione multicriterio”

[63] ISO 45001:2018, pag. 1, Introduzione, Paragrafo 0.1 “Background”

[64] ISO 45001:2018, pag. 1, Introduzione, Paragrafo 0.2 “Ciclo Plan-Do-Check-Act”

[65] ISO 45001:2018, pag. 9, Paragrafo 4 “Contesto dell’organizzazione”

[66] ISO 45001:2018, pag. 10, Paragrafo 5 “Leadership e partecipazione dei lavoratori”

[67] ISO 45001:2018, pag. 12, Paragrafo 6 “Pianificazione”

[68] ISO 45001:2018, pag. 15, Paragrafo 7 “Supporto”

[69] ISO 45001:2018, pag. 18, Paragrafo 8 “Attività operative”

[70] ISO 45001:2018, pag. 19, Paragrafo 9 “Valutazione delle prestazioni”

[71] ISO 45001:2018, pag. 22, Paragrafo 10 “Miglioramento”