Università Politecnica delle Marche

FACOLTÀ DI INGEGNERIA

CORSO DI LAUREA IN INGEGNERIA GESTIONALE

Tesi di Laurea

Il nuovo modello Safety Intelligence per la gestione della sicurezza

The new Safety Intelligence model for safety management

Relatore

Prof. Maurizio Bevilacqua

Laureando

Vito Claps

Matricola 1089595

ANNO ACCADEMICO 2020-2021

Sommario

1. Introduzione

Il seguente lavoro di tesi si pone l'obiettivo di illustrare come l'intelligence, nell'era dell'industria 4.0, assume un ruolo sempre più importante in un processo decisionale, in particolare nella gestione della sicurezza.

Da un punto di vista organizzativo, la gestione della sicurezza mira a promuovere un sistema in grado di proteggere da rischi inaccettabili persone e beni, all'interno di organizzazioni. Recentemente, con le crescenti incertezze economiche globali, la gestione della sicurezza nella maggior parte delle organizzazioni, è sottoposta a maggiore pressione per ottenere più risultati con meno risorse. Infatti, vi è una costante ricerca per implementare nuovi approcci in grado di allocare in maniera più efficiente le risorse in modo tale da migliorare le prestazioni in materia di sicurezza organizzativa.

Le informazioni relative alla sicurezza risultano essere fondamentali per gestire in maniera preventiva i rischi e per prendere decisioni informate.

Da questo punto di vista la *"Safety Intelligence"* (SI) svolge un ruolo cruciale, in quanto ha il compito di trasformare i dati e le informazioni sulla sicurezza da uno stato grezzo ad uno stato con maggior valore aggiunto, in modo tale da ottenere un trend che rappresenti le innumerevoli informazioni a disposizione, al fine di essere utilizzate nella gestione della sicurezza.

Di seguito verrà analizzato nel dettaglio i diversi aspetti della gestione della sicurezza supportati dal SI.

2 Quadro generale sulla sicurezza e i suoi aspetti chiave

Prima di procedere con l'analisi della safety intelligence dobbiamo esplicare ad analizzare alcuni concetti fondamentali che permetteranno di comprendere a pieno la necessità di applicare la safety intelligence in ambito della gestione della sicurezza.

2.1 La sicurezza e i suoi sviluppi

La sicurezza è un concetto ampio e astratto, che può essere meglio descritto in termini di "stato" o "situazione particolare". Questo stato è libertà da "qualcosa" che potrebbe avere conseguenze negative, come danni all'uomo o agli animali, perdite economiche o qualsiasi altra forma di danno o perdita. In altre parole, la sicurezza è la condizione per evitare eventi imprevisti come ad esempio incidenti. Per poter raggiungere livelli di sicurezza ottimali e stabiliti dalle normative, è necessario realizzare una valutazione dei rischi.

Attraverso un'analisi e classificazione dei rischi è possibile sostenere il processo decisionale in materia di sicurezza. La valutazione e la gestione dei rischi possono essere visti come un insieme di principi e metodi sviluppati per concettualizzare, stimare e gestire i rischi e le minacce riconosciute.

I campi in cui la sicurezza è un obiettivo primario sono numerosi, così come vari sono i sistemi per raggiungere un grado di sicurezza accettabile.

La gestione della sicurezza può essere considerata come un insieme organico di azioni e compiti che coinvolge tutte le funzioni e le unità lavorative aziendali con l'obiettivo di un continuo miglioramento degli standard di sicurezza, nel rispetto delle normative vigenti.

Da un punto di vista organizzativo, la gestione della sicurezza mira a promuovere un sistema in grado di proteggere persone e beni all'interno di organizzazioni da rischi inaccettabili. Recentemente, con le crescenti incertezze economiche globali, la gestione della sicurezza, nella maggior parte delle organizzazioni, è sottoposta a maggiore pressione per ottenere più risultati con meno risorse. Infatti, vi è una costante ricerca per implementare nuovi approcci in grado di allocare in maniera più efficiente le risorse in modo tale da migliorare le prestazioni in materia di sicurezza organizzativa.

Ad oggi, per l'effetto di un rapido sviluppo di tecnologie che diventano sempre più complesse e progetti industriali su larga scala, la gestione della sicurezza diventa sempre più intricata. Nonostante ciò è ugualmente necessario garantire una buona gestione della sicurezza e per poterlo fare è indispensabile raccogliere, analizzare, valutare e sintetizzare efficacemente le informazioni rilevanti per il rischio di incidenti.

2.2 L'informazione

L'informazione è alla base della gestione della sicurezza, in quanto consente di identificare efficacemente i rischi, prendere decisioni sagge e attuare misure correttive che permettano un miglioramento della salute e della sicurezza stessa.

Nell'ultimo decennio l'informazione ha assunto un ruolo sempre più importante a livello organizzativo, infatti, l'informazione oggi rappresenta una fonte di ricchezza. Attualmente il problema che si sta verificando riguarda l'eccessiva presenza di informazioni inerti, che per essere utilizzate necessitano di metodologie di elaborazione sofisticate in grado di filtrare ed individuare le informazioni veritiere analizzando la fonte.

Una volta che le informazioni sono state filtrate queste vengono utilizzate per effettuare l'analisi dei rischi e consentire una corretta gestione della sicurezza.

In sintesi, l'informazione è la base per un processo decisionale informato in materia di sicurezza a tutti i livelli di un'organizzazione. Informazioni accurate, accessibili e tempestive sono fondamentali per raggiungere gli obiettivi di sicurezza prefissati.

Un ulteriore aspetto riguarda il reperimento delle informazioni che viene effettuato su diversi livelli, tra questi:

i. Persone;
ii. Luogo di lavoro fisico;
iii. L'ambiente esterno.

Quindi per la gestione della sicurezza del sistema, è necessario raccogliere informazioni sui processi, sulle macchine e attrezzature, sull'organizzazione, sulla gestione del lavoro e sul comportamento umano.

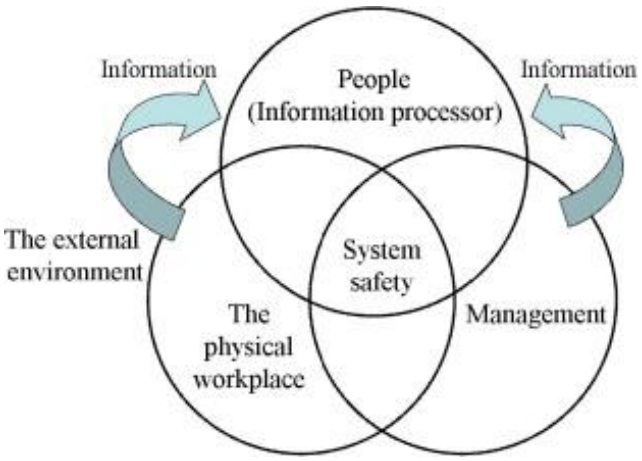


Figura 1

Il tipo di informazioni che si possono estrarre dai diversi livelli di un sistema sono disponibili in molte forme e livelli tecnici, tra questi troviamo: simboli, immagini, comunicazioni verbali, stampe, supporti magnetici, compact disc leggibili al laser e da reti informali, o una semplice comunicazione con colleghi ed esperti di sicurezza.

Quindi potremmo concludere che per garantire una gestione della sicurezza di qualità è necessario analizzare una grande mole di informazioni e per tanto il processo risulta essere complesso.

2.3 Big data

Ad oggi, nell'era dei Big-Data, dell'intelligence e dell'industria 4.0 la quantità di dati che è possibile ricevere è molto elevata ma allo stesso tempo potremmo avere un sovraccarico d'informazioni.
Infatti, le informazioni necessarie per la gestione della sicurezza, hanno un valore se sono pertinenti, aggiornate, accurate e affidabili. I Big-Data sono in grado di strutturare un vero e proprio processo di raccolta e analisi di un grande numero di dati provenienti da diverse fonti a supporto dei processi industriali e dei gestori della sicurezza. Una raccolta di dati molto estesa basata principalmente su tre concetti:

i. Volume: le imprese raccolgono grande mole di dati provenienti da diverse fonti come sensori, dispositivi, video, audio, reti, file di log, applicazioni transazionali,

web e social media. Gran parte di essi viene generata in tempo reale e su vastissima scala.

ii. Velocità: la crescita dell'Internet delle Cose, i flussi di dati verso le imprese devono essere gestiti in modo tempestivo e a una velocità senza precedenti.

iii. Varietà: le organizzazioni si devono confrontare con le differenti tipologie dei dati, da quelli strutturati fino a quelli non strutturati.

La sfida attuale consiste nel trasformare i big data in smart data, ovvero informazioni intelligenti, che diano vantaggio competitivo e siano perfettamente fruibili. Di conseguenza, per ottenere valore dai Big Data si richiedono dei Big Data Analytics, ovvero tecniche per processare ed estrapolare le informazioni utili tramite metodi analitici e tecnologie sempre più sofisticate.

L'analisi dei Big Data permette di aiutare i responsabili dell'azienda nel prendere le decisioni in modo più accurato e veloce, utilizzando dati precedentemente inaccessibili o inutilizzabili.

I processi e le attività di raccolta ed elaborazione di dati e informazioni per sviluppare strategie e prendere decisioni specifiche, portano la scienza della sicurezza ad entrare nell'era di *Safety 4.0* portando così alla nascita della scienza della sicurezza computazionale, dove la sua base e il suo supporto sono l'informatica della sicurezza.

2.4 Safety 4.0

Contestualmente all'evoluzione delle diverse realtà industriali è nata e si è sviluppata la scienza della sicurezza.

Analizzando brevemente il corso della storia possiamo osservare quattro grandi evoluzioni:

i. Industry 1.0, riguardò essenzialmente la meccanizzazione attraverso l'uso della forza del vapore e dell'acqua;

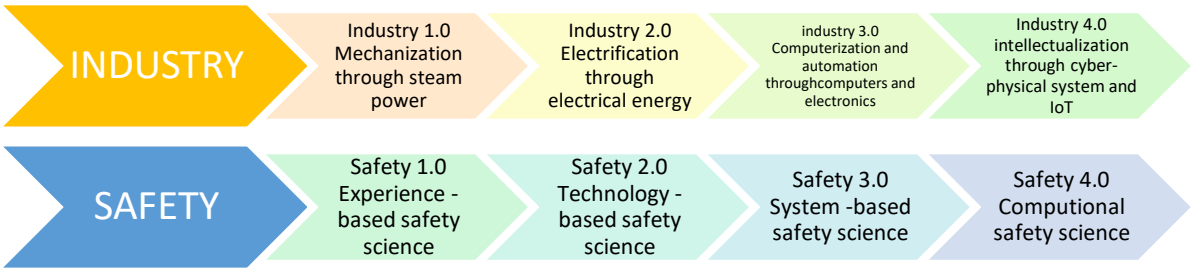
ii. Industry 2.0, caratterizzata dalla produzione di massa grazie all'uso delle linee di montaggio;

iii. Industry 3.0, contraddistinta dall'utilizzo dei computer e da un alto grado di automazione all'interno delle aziende attraverso l'uso dei robot;

iv. Industry 4.0 sta prendendo ciò che è stato avviato nell'Industry 3.0 con l'adozione di computer e automazione e migliorandolo con sistemi intelligenti e autonomi alimentati da sistemi cyber-fisici, Internet of Things e altre reti.

Di pari passo con le evoluzioni industriali possiamo osservare l'evoluzione della scienza della sicurezza e di seguito analizziamo i diversi step che l'hanno caratterizzata:

i. Safety 1.0: scienza della sicurezza basata sull'esperienza;
ii. safety 2.0: scienza della sicurezza basata sulla tecnologia;
iii. Safety 3.0: scienza della sicurezza dei sistemi;
iv. Safety 4.0: scienza della sicurezza computazionale, un nuovo paradigma per la scienza della sicurezza nell'era dei big data e industria 4.0.



Safety 4.0 ottimizza l'informatizzazione di Safety 3.0 e implementa l'informatica di sicurezza come base e supporto per la scienza della sicurezza computazionale, in cui "l'informazione è sicurezza, la sicurezza è informazione" diventa una delle idee e dei concetti di gestione della sicurezza moderni più basilari ed essenziali.

Nella fase di Safety 4.0, varie tecnologie informatiche emergenti come ad esempio, intelligenza artificiale, big data, machine learning, cloud computing, Internet of Things, simulazione, robot autonomi, integrazione di sistema e Internet of Systems vengono gradualmente incorporate nella gestione della sicurezza e possono anche apportare nuove modifiche all'informatica di sicurezza.

3 Safety Intelligence e le sue declinazioni

3.1 Introduzione al SI e definizione generale

Nell'era dei Big Data e dell'Industria 4.0, l'intelligence svolge un ruolo sempre più cruciale in molti settori tanto da introdurre l'intelligence sulla sicurezza.
I processi e le attività di raccolta ed elaborazione di dati e informazioni per sviluppare strategie e prendere decisioni specifiche, generalmente vengono denominati "intelligence". Questo concetto sta assumendo un ruolo sempre più importante in ambito dei Big Data e dell'industria 4.0 per guidare la gestione della sicurezza.
Prima di illustrare come la safety intelligence opera in ambito della sicurezza e quali sono i vantaggi che introduce, è necessario prima definire che cos'è la Safety intelligence.

Potremmo definire il SI come un'informazione sulla sicurezza che è stata elaborata in modo tale che possa essere utile ai responsabili della sicurezza nel prendere decisioni, ma in maniera più accurata ed esaustiva, ma allo stesso tempo, potremmo definire il SI come un approccio che combina metodologie, processi, architetture, strumenti, tecnologie, tecniche, e capacità di trasformare i dati e le informazioni sulla sicurezza grezzi nel prodotto SI, ovvero informazioni sulla sicurezza significative e attuabili, per il processo decisionale in materia di sicurezza.
Pertanto il SI può svolgere un ruolo fondamentale nel promuovere la sicurezza di un'organizzazione e nel migliorarne le prestazioni, individuandone i rischi e nuove opportunità. Osserviamo di seguito, più nel dettaglio, i diversi significati attribuiti al SI.

3.2 Safety Intelligence inteso come "prodotto"

SI è l'informazione sulla sicurezza utilizzabile e attuabile ed è il risultato perseguibile dalle esigenze di gestione della sicurezza prescritte da un'organizzazione. SI è il prodotto derivante dalla raccolta di valutazioni, analisi, integrazioni e interpretazioni di tutti i dati e le informazioni disponibili relative a uno o più aspetti della sicurezza, che ha un'importanza diretta o potenziale per la gestione di un'organizzazione, quali lo sviluppo e l'esecuzione di piani, politiche, decisioni e controlli dei rischi per la sicurezza. In altre

parole, SI è un prodotto di dati e informazioni sulla sicurezza trattati, analizzati e interpretati.

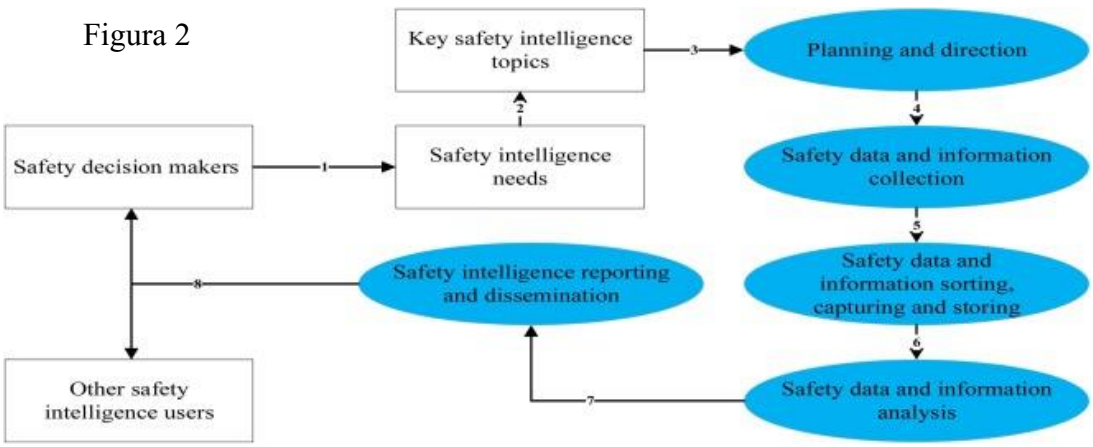
3.3 Safety Intelligence inteso come "processo"

Il SI è un processo che produce e diffonde SI attuabile mediante la pianificazione, la raccolta sistematica, etica e legale, l'elaborazione e l'analisi dei dati e delle informazioni, sulla sicurezza, provenienti dall'ambiente interno ed esterno di un'organizzazione. Le fasi chiave del processo SI possono essere riassunte come segue:

i. *Pianificazione e direzione*, in cui vengono individuate le esigenze e le questioni di sicurezza che hanno la priorità;
ii. *Raccolta dati e informazioni sulla sicurezza*, è necessaria una raccolta mirata di dati e informazioni sulla sicurezza provenienti da varie fonti interne ed esterne dell'organizzazione;
iii. *Smistamento e memorizzazione* dei dati e delle informazioni in materia di sicurezza, ad esempio dividendo i dati e i tipi di informazioni sulla base di determinate norme, utilizzando vari metodi e tecnologie;
iv. *conversione* dei dati e delle informazioni di sicurezza in SI attuabile su cui possono essere prese decisioni in materia di sicurezza;
v. *comunicazione* dei risultati del processo SI o del progetto a coloro che nell'organizzazione hanno l'autorità e la responsabilità di agire sui risultati.

Tutte queste fasi si svolgono in maniera ciclica come possiamo osservare dalla figura 2.

Figura 2



Dal punto di vista della catena dell'informazione, il SI è un processo mediante il quale le organizzazioni, raccolgono dati e informazioni sulla sicurezza che si trovano ad uno stato grezzo, li convertono in informazioni e conoscenze sulla sicurezza utilizzabili e attuabili in modo tale da poter supportare e guidare un'organizzazione nella gestione della sicurezza.
Il processo SI è basato sull'utilizzo di software e tecnologie che consentono di analizzare i dati e le informazioni di sicurezza grezzi, provenienti da più fonti e trarre informazioni che permettano di rendere i processi decisionali più fluidi ed efficaci.
Potremmo quindi concludere dicendo che il SI è una parte significativa del processo di gestione della sicurezza.

3.4 Safety Intelligence inteso come "strumento, tecnologia e tecnica"

È possibile definire il SI come uno strumento efficace o una tecnologia per trasformare i dati in informazioni, le informazioni in conoscenze e le conoscenze in decisioni sulla sicurezza, tutto questo per poter consentire di intraprendere azioni efficaci per la gestione della sicurezza. Nello specifico, SI comprende varie architetture e tecniche come database, data warehousing e data mining, che trasformano i dati di sicurezza grezzi in informazioni e conoscenze utili per fornire supporto alle decisioni in materia di sicurezza.

Una tecnologia utilizzata dal SI è la modalità di apprendimento automatico in grado di identificare le informazioni correlate (ovvero relazioni tra cose che cambiano nel sistema senza un motivo articolato), per prevedere in modo intelligente le informazioni sulla sicurezza, rendendo così le informazioni più chiare. Una notevole spinta all'utilizzo del SI in abito della sicurezza è stata fornita dai rapidi progressi nella gestione dei database ed immagazzinamento dei dati.

Inoltre, le diverse tecnologie abilitanti del SI, consentono di effettuare diagnosi sulla sicurezza ed offrono un vero e proprio approccio basato sull'informazione per collegare, gli obiettivi strategici e le politiche di sicurezza delle organizzazioni, alle procedure tattiche e operative di sicurezza.

Gli strumenti e le tecnologie per l'elaborazione e l'analisi dei dati e delle informazioni sulla sicurezza sono strumenti originariamente sviluppati da molteplici discipline, come

la scienza della sicurezza, la scienza dei dati, la scienza dell'informazione, l'informatica e la scienza dell'intelligenza artificiale.

In sintesi, SI è un insieme di strumenti, tecnologie (figura 3) e tecniche che consentono a un'organizzazione di trasformare i propri dati in informazioni tempestive e accurate per il processo decisionale in materia di sicurezza da mettere a disposizione delle persone giuste nella forma più adeguata.

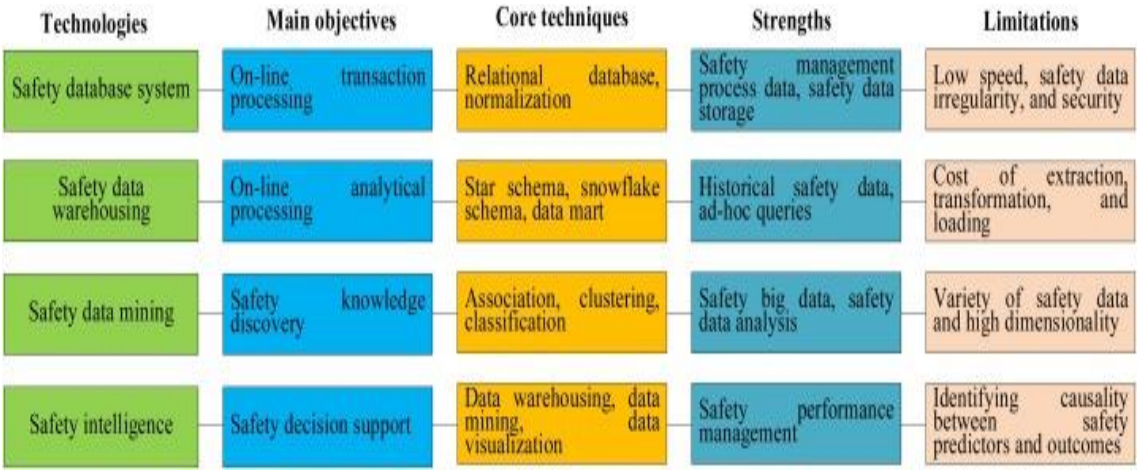


Figura 3

3.5 Safety Intelligence inteso come "capacità"

SI è la capacità di un'organizzazione di raccogliere ed elaborare dati e informazioni sulla sicurezza; è la capacità di un'organizzazione di risolvere i problemi di sicurezza in quanto esso è l'obiettivo primario e il compito della gestione della sicurezza. Inoltre, SI è la capacità di un'organizzazione di comprendere e prevedere i rischi e le modifiche relative alla sicurezza in modo tempestivo, fornendo allo stesso tempo indicazioni utili relative ad azioni da intraprendere al fine di fronteggiare tali situazioni. Infatti il SI può identificare i cambiamenti imminenti in materia di sicurezza in un'organizzazione, che possono essere positivi, quindi rappresentano opportunità di miglioramento della sicurezza, o negativi, che rappresentano minacce o sfide per la sicurezza di un'organizzazione.

SI, inteso come capacità, racchiude in sé le seguenti funzioni:

i. capacità di apprendimento in materia di sicurezza, come ad esempio l'acquisizione di nuove informazioni e comprensione delle più recenti prove di ricerca sulla sicurezza;
ii. capacità di adattarsi e rimodellare l'ambiente di gestione della sicurezza di un'organizzazione;
iii. capacità di comprendere i fattori di gestione della sicurezza quali: pericoli, incidenti, comportamenti non sicuri, cultura della sicurezza e risorse di sicurezza e di agire in modo appropriato sulla base di uno studio e analisi di tali fattori;
iv. capacità di aggiungere maggiore intelligenza all'attività di gestione della sicurezza delle organizzazioni.

In base alle definizioni di SI, come termine di gestione della sicurezza, sopra illustrate potremmo concludere dicendo che SI è un'idea di gestione della sicurezza contemporanea e un approccio che combina metodologie, processi, architetture, strumenti, tecnologie, tecniche, e capacità di trasformare i dati e le informazioni sulla sicurezza grezzi nel prodotto SI, ossia informazioni sulla sicurezza significative e attuabili, per il processo decisionale in materia di sicurezza. Il SI Può svolgere un ruolo fondamentale nel promuovere la sicurezza di un'organizzazione e nel migliorare le prestazioni, individuando i rischi e nuove opportunità di promozione della sicurezza, e migliorare i processi decisionali in materia di sicurezza. Pertanto, l'SI è una priorità assoluta per la maggior parte delle organizzazioni nell'era dei Big Data e dell'intelligence.

4 Modello teorico per SI

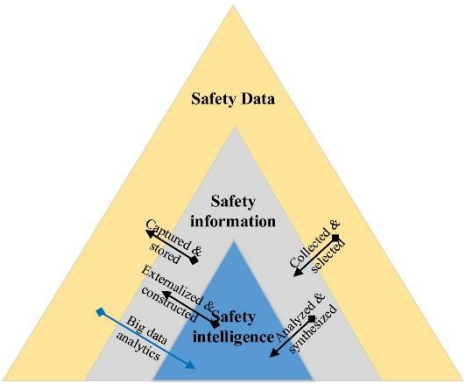
4.1 Obiettivo principale

Il SI si concentra sui dati e le informazioni sulla sicurezza da un punto di vista molto ampio, consentendo alle organizzazioni di prevedere eventi futuri e di utilizzarli per prendere decisioni efficaci, in quanto ogni decisione sulla sicurezza si basa su determinate ipotesi. Pertanto, SI mira principalmente a fornire un supporto decisionale per obiettivi specifici definiti nel contesto delle attività di gestione della sicurezza tenendo conto del quadro organizzativo. In particolare, il SI viene utilizzato dai responsabili delle decisioni per ottenere una conoscenza completa della gestione della sicurezza e dei fattori che li riguardano, nonché per definire e sostenere le loro strategie, politiche, norme, regole in materia di sicurezza e procedure.

Il SI inoltre consente alle persone a tutti i livelli di un'organizzazione di accedere, interagire e analizzare, valutare i dati e informazioni utili per identificare i rischi, migliorare le prestazioni in materia di sicurezza, individuare opportunità e gestire la sicurezza in modo efficace, efficiente e sicuro. In altre parole, SI mira principalmente a formulare un meccanismo decisionale solido, basato sui fatti.

4.2 Base della safety intelligence

Il meccanismo sul quale si basa il SI prende vita a partire dalla raccolta di dati sulla sicurezza di valore grezzo, in quanto al loro stato non forniscono nessun aiuto al processo decisionale. In seguito i dati grezzi vengono trasformati in informazioni sulla sicurezza. In fine si ottiene il SI, ovvero le informazioni di sicurezza elaborate che garantiscono un elevato grado di dettaglio, fondamentale per il processo decisionale sulla sicurezza.



Il tradizionale ciclo di informazioni sulla sicurezza per la realizzazione del SI trasforma i dati di sicurezza in informazioni sulla sicurezza e informazioni sulla sicurezza in SI, che possono guidare i responsabili nel prendere decisioni efficaci in materia di sicurezza.

Ma nell'era dei Big Data, i dati di sicurezza possono anche essere trasformati direttamente in SI effettuando un'accurata analisi.

Le informazioni e i dati relativa alla sicurezza, utilizzati per costruire le fondamenta del SI, provengono sia da ambienti esterni che interni ad un'organizzazione.
In particolare i dati e le informazioni sulla sicurezza che provengono dall'ambiente interno sono, ad esempio, tutti quei dati e informazioni relativi ai processi e ai risultati ottenuti.
Invece, i dati e le informazioni sulla sicurezza provenienti dall'ambiente esterno, includono leggi e regolamenti nazionali sulla sicurezza, standard ufficiali e rapporti sugli incidenti.

4.3 SI strategico, tattico e operativo

La gestione della sicurezza è caratterizzata da una serie di decisioni interconnesse e successive nel tempo dove gli adattamenti e modifiche di queste decisioni vengono fatte in modo continuo e sequenziale al fine di simulare al meglio la realtà. A seconda dell'arco temporale in cui le decisioni vengono prese, potremmo distinguere: decisioni a *lungo termine*, dove i responsabili della sicurezza decidono i possibili investimenti in materia di sicurezza, le strategie, le politiche e i sistemi di gestione della sicurezza da selezionare o adattare per raggiungere al meglio gli obiettivi di sicurezza dell'organizzazione; decisioni a *medio termine*, i responsabili della sicurezza prendono alcune decisioni tattiche come lo sviluppo di piani di sicurezza, procedure, risorse e metodi di prevenzione e controllo per preparare, guidare e ottimizzare la prevenzione e il monitoraggio dei rischi online in un'organizzazione. Tuttavia, le descrizioni delle decisioni tattiche in materia di

sicurezza non sono sufficienti per innescare le attività quotidiane di gestione della sicurezza operativa.
Pertanto, i responsabili della sicurezza devono definire modalità specifiche per eseguire le loro decisioni tattiche. In altre parole, nelle decisioni a *breve termine*, i responsabili della sicurezza devono prendere decisioni operative che possono dar luogo all'esecuzione di ordini operativi di gestione quotidiana della sicurezza.

Un approccio, per ridurre la complessità della gestione della sicurezza, consiste nel definire diversi livelli di gestione:

- Strategica;
- Tattica;
- Operativa

Poiché il supporto SI è richiesto su tutti i livelli di gestione della sicurezza, un'organizzazione deve produrre tre diversi tipi di SI uno per ogni livello di gestione della sicurezza, e metterlo a disposizione del team che necessità di quel tipo di SI specifico. I diversi tipi sono di natura gerarchica con SI strategico in alto come mostrato in figura 4.

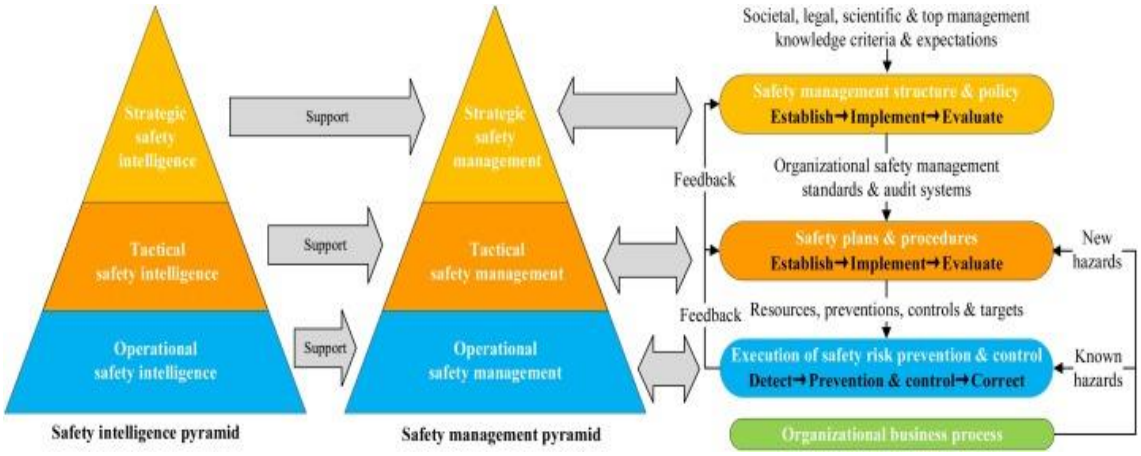


Figura 4

Il *SI strategico* sarà a disposizione dei manager ai più alti livelli di gestione della sicurezza organizzativa. Esso si basa principalmente sulla previsione e la stima della sicurezza, definendo strategie di gestione della sicurezza basate anche sull'esperienza passata e sugli

standard di sicurezza definiti. Il SI strategico è implementato attraverso investimenti, definizione degli obiettivi e delle politiche di sicurezza a lungo termine, mediamente in un arco temporale che va da i tre ai cinque anni.
In questa fase si necessità di responsabili della sicurezza con una profonda esperienza, che siano in grado di comprendere e adattarsi ai cambiamenti in un ambiente dinamico.

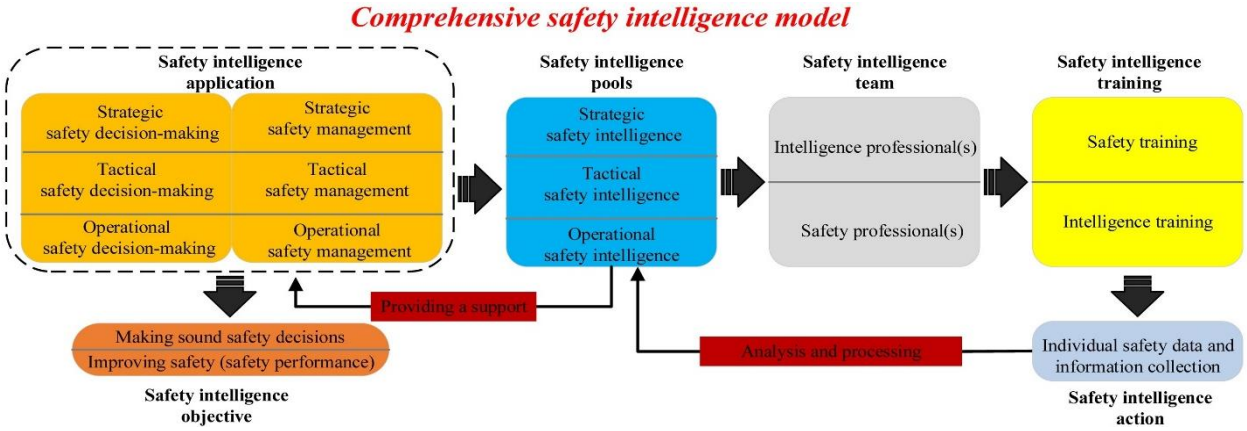
Il *SI tattico* richiede un team con capacità di gestione e valutazione del rischio nonché capace di individuare le debolezze e i punti di forza di un'organizzazione fornendo informazioni relative ai piani di sicurezza, procedure e tecniche da utilizzare per la gestione dei rischi.
Un'efficace valutazione tattica dei rischi per la sicurezza consente, al team in controllo diretto dei rischi per la sicurezza, di allocare risorse nel modo più efficace possibile.
Il SI a livello tattico agisce in un arco temporale di medio termine che va da settimane a mesi.

Il *SI operativo* invece si concentra su tutte le attività quotidiane di gestione della sicurezza delle organizzazioni. Il SI operativo si differenzia dal SI strategico e tattico per lo scopo di gestione e promozione della sicurezza sia a livello di dettaglio richiesto che a livello di tempestività con cui reperire i dati e informazioni sulla sicurezza necessarie. L'immediatezza dell'SI operativo richiede che gli analisti della sicurezza abbiano accesso immediato ai dati e ai sistemi di raccolta delle informazioni in modo tale da poter trasformare i dati e le informazioni di sicurezza in SI in tempi brevi e in un ambiente ad alta pressione. L'arco temporale in cui agisce il SI operativo va da minuti a giorni.

I tre tipi di SI pertanto risultano essere legati tra di loro, fornendo così un approccio basato sui dati per collegare gli obiettivi strategici di sicurezza delle organizzazioni alle politiche tattiche e infine alle azioni di sicurezza operative.

4.4 Struttura della safety intelligence

Il modello concettuale del SI si sviluppa in sei unità:



i. La prima unità, presenta i diversi livelli organizzativi di gestione della sicurezza, sopra argomentati;
ii. La seconda unità del modello comprende i pools SI, ovvero tutti i dati e le informazioni sulla sicurezza raccolti e suddivisi nei diversi livelli di SI, quindi essi vengono mappati tenendo in considerazione i tre livelli di gestione organizzativa della sicurezza.
iii. La terza unità mostra il team organizzativo di SI. Un team SI ideale dovrebbe includere professionisti sia dell'intelligence che della sicurezza.
iv. La quarta unità è correlata al modo in cui il team può interagire e contribuire alle pratiche e alle attività organizzative del SI.
v. La quinta unità del modello invece è legata all'azione del SI, essa si presenta come una raccolta di dati e informazioni sulla sicurezza per la realizzazione del SI.
vi. L'ultima unità indica gli obiettivi del SI.

5 Modello SI a sostegno della gestione della sicurezza

5.1. Importanza dell'SI nel processo decisionale in materia di sicurezza

Simon, famoso studioso di decisioni e vincitore del premio Nobel per l'economia, ha affermato che l'informazione o più precisamente l'intelligence è fondamentale e influenza ogni decisione. Pertanto, ha proposto di suddividere il processo decisionale in tre fasi principali:

i. L'intelligence: raccolta di informazioni e analisi delle situazioni e identificazione dei problemi;
ii. La progettazione: individuazione, sviluppo e analisi di varie soluzioni possibili;
iii. La scelta: valutazione delle opzioni e selezione delle migliori.

Il modello decisionale di Simon è comunemente accettato e funge come base per la ricerca e la pratica decisionale. Molti ricercatori infatti seguirono il modello di Simon e intrapresero ulteriori studi sul suo punto di vista, definendo un'estensione del modello con l'aggiunta di ulteriori fasi più dettagliate. In particolare il processo decisionale in materia di sicurezza può essere strutturato e ordinato in cinque fasi (figura 5) dal punto di vista SI oltre all'intelligence, progettazione e scelta vengono aggiunte due fasi che riguardano l'implementazione e il controllo.

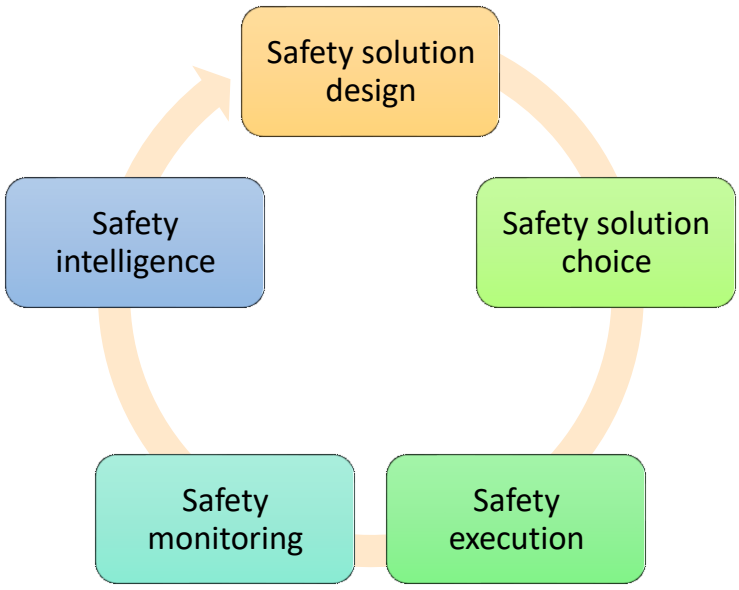


Figura 5

Analizziamo di seguito le diverse fasi:

i. *Safety intelligence*, in questa fase il decisore di sicurezza identifica il problema e la sua causa, raccoglie i dati e le informazioni riguardanti il problema, converte i dati e le informazioni raccolti in SI utile e perseguibile per la risoluzione dei problemi di sicurezza.
ii. *Safety solution design*, la seconda fase comprende lo sviluppo, il riconoscimento e la comprensione di possibili alternative di gestione della sicurezza e delle conseguenze della futura decisione.
iii. *Safety solution choice,* tra le varie alternative verrà scelta la migliore, che in seguito porterà il decisore di sicurezza ad applicarla.
iv. *Safety execution*, la quarta fase si occupa di attuare la decisione presa nella terza fase.
v. *Safety monitoring and review*, nell'ultima fase avviene il monitoraggio e la revisione della sicurezza. L'attuazione della decisione sulla sicurezza, le modifiche dei rischi e la gestione della sicurezza sono monitorati e valutati continuamente e i dati e le informazioni raccolti in questa fase vengono trasferiti alla prima per consentire un adeguamento e miglioramento delle decisioni future in materia di sicurezza.

Inoltre, i flussi e le attività di safety intelligence attraversano l'intero processo decisionale in materia di sicurezza.

5.2 Confronto tra la pratica SI e i processi di gestione della sicurezza

A livello pratico, per fornire un sostegno efficace alla gestione della sicurezza, è necessaria un'integrazione organica della pratica SI e della pratica di gestione della sicurezza ponendo particolare attenzione alle differenze di questi due processi che potrebbero sembrare simili ma in realtà non lo sono. La pratica SI e i cicli di gestione della sicurezza condividono attributi comuni, a causa dei loro obiettivi comuni, come la politica di sicurezza, processo decisionale, analisi dei dati e delle informazioni sicurezza. Pertanto, una maggiore comprensione e conoscenze delle pratiche SI avrebbero come conseguenza un miglioramento della gestione della sicurezza. Analizzando le diverse fasi del processo di pratica SI e del processo di gestione della sicurezza potremmo fare le seguenti osservazioni:

i. La prima fase di entrambi i processi inizia con la definizione del campo di applicazione. Nella fase iniziale del processo di pratica SI, vengono individuate le politiche di sicurezza e le aree di soluzione in cui il SI può operare e ne viene data la priorità. La prima fase del processo di gestione della sicurezza determina i requisiti, i vincoli e le priorità per le decisioni o gli obiettivi strategici che devono essere sostenuti dalla gestione della sicurezza.

ii. La seconda fase si incentra sulla raccolta di dati e informazioni sulla sicurezza. Il processo di pratica SI, in questa fase, è incentrato sulla raccolta di dati e informazioni sulla sicurezza e sulla loro preparazione per l'analisi. Nella seconda fase del processo di gestione della sicurezza, i responsabili della sicurezza raccolgono dati e informazioni per l'identificazione dei problemi con una conseguente catalogazione e classificazione dei vari problemi di sicurezza.

iii. Nella terza fase, l'analisi viene eseguita sia nel processo di pratica SI che nel processo di gestione della sicurezza. Nel processo di pratica SI, i dati e le informazioni sulla sicurezza sono analizzati per la produzione di SI attuabile. La terza fase del processo di gestione della sicurezza mira ad analizzare e valutare le caratteristiche, le cause e le conseguenze dei problemi di sicurezza sulla base dell'analisi sistematica dei dati e delle informazioni raccolte.

iv. L'obiettivo della quarta fase sia del processo di pratica SI che del processo di gestione della sicurezza è quello di produrre vari prodotti per soddisfare le esigenze dei responsabili della sicurezza. Nel processo di pratica SI, vengono individuate soluzioni di sicurezza e raccomandazioni per soddisfare le esigenze stabilite dai decisori di sicurezza che richiedono il supporto SI. L'obiettivo della quarta fase del processo di gestione della sicurezza è formulare soluzioni di sicurezza fattibili dal punto di vista del SI. Nel momento in cui si presentano più soluzioni allora è necessario effettuare, per ogni alternativa, una valutazione dei vantaggi e svantaggi. Le metodologie possono differire tra il processo di pratica SI e quello di gestione della sicurezza; tuttavia, l'obiettivo comune è quello di produrre prodotti analitici che soddisfino le esigenze definite dei gestori della sicurezza.

v. Le fasi finali del processo di pratica SI e del processo di gestione della sicurezza si concentrano sull'applicazione e svolgono funzioni molto simili. In questa fase, i prodotti SI sono distribuiti ai responsabili delle decisioni che li utilizzano per sostenere il processo decisionale e altre attività di gestione della sicurezza. Nella

fase di esecuzione del processo di gestione della sicurezza, i responsabili decidono e attuano soluzioni per affrontare i problemi fornendo una valutazione delle diverse opzioni.

vi. Sia il processo di pratica SI che il processo di gestione della sicurezza sono seguiti da una fase di feedback che comporta il monitoraggio e la revisione della loro efficacia. L'attuazione della pratica SI, la gestione della sicurezza e le modifiche dei rischi sono monitorate e valutate, e i dati e le informazioni sulla sicurezza raccolti sono riportati alla prima fase per adeguare e migliorare le future pratiche di SI e i sistemi di gestione della sicurezza.

In altre parole, gli obiettivi comuni della pratica SI e della gestione della sicurezza comportano l'acquisizione dei dati e delle informazioni sulla sicurezza trattati, la loro fornitura a coloro che ne hanno bisogno e la ricezione di feedback sui prodotti e sulle esigenze aggiuntive. Inoltre, sia la pratica SI che la gestione della sicurezza enfatizzano il miglioramento continuo utilizzando il meccanismo di feedback.

5.3 Modello di gestione della sicurezza guidata dall'intelligence

La gestione della sicurezza guidata dall'intelligence è descritta come una filosofia, un'idea, un approccio e un processo di gestione della sicurezza per trovare e applicare SI utili, per guidare in modo proattivo le decisioni strategiche, operative e tattiche con l'obiettivo di migliorare la gestione della sicurezza.

Alla base, di una gestione della sicurezza guidata dall'intelligence, è necessario disporre di prodotti SI, ossia informazioni relative alla sicurezza sottoposte ad analisi ed elaborazioni, ed inoltre è fondamentale che i responsabili della sicurezza comunichino chiaramente le loro esigenze in materia di SI. Sostanzialmente, la gestione della sicurezza guidata dall'intelligence rappresenta una fusione del processo di pratica SI e del ciclo di pratica di gestione della sicurezza sulla base di ciò è stato realizzato un nuovo modello.

Questo modello è guidato dalla pratica SI ed è utilizzato per sostenere la gestione della sicurezza nell'organizzazione (figura 6).

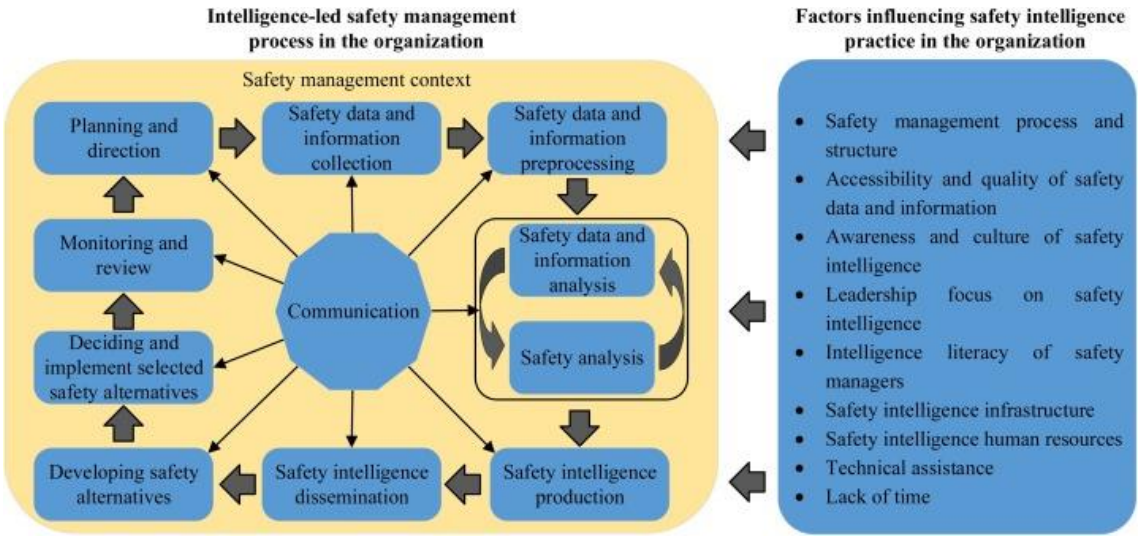


Figura 6

Il processo di gestione della sicurezza guidato dall'intelligence si svolge nel contesto stabilito dalla dirigenza e dai responsabili della sicurezza. Per promuovere l'attuazione della gestione della sicurezza basata sull'intelligence in un'organizzazione, occorre considerare diversi fattori che influenzano la pratica SI, tra questi osserviamo:

i. Obiettivi di gestione della sicurezza come la tolleranza al rischio, criticità della decisione in materia di sicurezza, politiche e procedure .
ii. Disponibilità e qualità dei dati e delle informazioni in materia di sicurezza.
iii. Consapevolezza e cultura dell'intelligence in materia di sicurezza come ad esempio la comprensione dell'importanza della pratica SI, atteggiamento dei responsabili organizzativi e dei responsabili della sicurezza nei confronti della pratica SI e della condivisione delle informazioni sulla sicurezza.
iv. Focalizzazione della leadership sul SI, un'attività di leadership incentrata sulla pratica SI è positivamente associata a capacità di gestione della sicurezza guidate dall'intelligence.
v. Alfabetizzazione dei responsabili della sicurezza riguardo all'uso del SI.
vi. Infrastruttura SI che include hardware, software e rete.
vii. Risorse umane SI intesi come professionisti dell'intelligence con elevate capacità di gestione della sicurezza e i professionisti della sicurezza con competenza in materia di intelligence.

viii. Assistenza tecnica che comprende l'uso della tecnologia dell'informazione nella gestione della sicurezza e delle tecnologie a sostegno della pratica SI.

ix. Condivisione, le informazioni relative a questi fattori devono essere condivise con i soggetti coinvolti nelle pratiche SI e nelle attività di gestione della sicurezza, per migliorare l'efficienza e la qualità della gestione della sicurezza guidata dall'intelligence.

Inoltre, il fulcro del processo di gestione della sicurezza guidato dall'intelligenza è la comunicazione. Una comprensione condivisa della gestione della sicurezza guidata dall'intelligence e dei fattori ad essa associati si ottiene attraverso una comunicazione coerente con i responsabili del processo decisionale in materia di sicurezza, analizzando e producendo giudizi durante tutto il processo.

Una gestione della sicurezza guidata dall'intelligence presenta alcuni vantaggi:

i. La mancanza di informazioni utili nel processo di gestione della sicurezza è evitata il più possibile;

ii. È presente un meccanismo di correzione degli errori;

iii. Viene evidenziata la praticità e la facilita di gestione della sicurezza grazie all'utilizzo di prodotti SI;

iv. È promossa la condivisione di informazioni relative alla sicurezza all'interno di un'organizzazione;

v. Alcuni approcci di gestione della sicurezza già esistenti come gestione della sicurezza basato sugli incidenti, sui rischi, sui dati e gestione delle conoscenze in materia di sicurezza possono essere efficacemente integrati nelle operazioni safety intelligence.

Inoltre, la gestione della sicurezza guidata dall'intelligenza non riguarda solo la prevenzione e il controllo di incidenti, lesioni e altre perdite ma si tratta di un approccio per affrontare tutti i problemi di sicurezza. In altre parole, essa si concentra sui problemi di sicurezza, in particolare le principali minacce e consente di sviluppare strategie di risoluzione.

6 Conclusioni

Nell'era dei big data, dell'intelligence e dell'Industria 4.0, la scienza della sicurezza è entrata nell'era della Safety 4.0, e SI è emersa come un nuovo concetto e termine. Essa presenta vari benefici per la promozione e gestione della sicurezza ed è considerata una prospettiva essenziale nell'era di Safety 4.0. Sebbene sia stato ampiamente proposto il concetto di SI, molte organizzazioni non hanno ancora attuato il metodo in modo efficace.

Ad oggi gli studi per guidare la pratica SI e promuovere ulteriori ricerche esistono a malapena e sono poco incentivati. Nello specifico, manca ancora un quadro universale che guidi le organizzazioni in modo semplice ed esaustivo ad una comprensione del SI in tutte le sue declinazioni, infatti il termine SI viene definito "ombrello", in quanto può essere utilizzato per indicare un prodotto, un processo, uno strumento e una capacità relative alla gestione della sicurezza.

Pertanto il seguente lavoro di tesi tenta di presentare un quadro per SI incentrandosi sulla prospettiva di gestione della sicurezza, infatti come ampiamente illustrato il SI, attraverso un processo di filtraggio ed elaborazione delle informazioni permette di ottenere informazioni significative, che implementate nelle logiche del SI permette di definire metodologie che hanno come fine ultimo quello di ottimizzare efficientemente la gestione della sicurezza.

Bibliografia

1. Creare i legami tra la protezione dell'ambiente, la sicurezza dei processi e l'industria 4.0 - ScienceDirect
2. Sistemi di gestione della sicurezza: un'ampia panoramica della letteratura - ScienceDirect
3. Esplorare l'alfabetizzazione informativo dei professionisti nella gestione della sicurezza - ScienceDirect
4. L'informatica della sicurezza come nuovo, promettente e sostenibile settore della scienza della sicurezza nell'era dell'informazione - ScienceDirect
5. L'informatica della sicurezza come nuovo, promettente e sostenibile settore della scienza della sicurezza nell'era dell'informazione - ScienceDirect