UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CORSO DI PERFEZIONAMENTO IN
«SECURITY MANAGER»
CORSO DI FORMAZIONE IN
«PROFESSIONISTA DELLA SECURITY»

26 NOVEMBRE 2021

MASSIMO MARROCCO

Ore 16:00 – 18:00

Il percorso di implementazione di un modello di gestione con riferimento alle best practices

1

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Introduzione

2

INTRODUZIONE

Per prima cosa si ritiene opportuno ricordare che cosa è una norma Uni e come si colloca nel contesto della normazione in generale, andando a cogliere alcune definizioni dal sito ufficiale (http://www.uni.com/index.php?option=com_content&view=article&id=141&Itemid=2422) :

le norme UNI sono emanate dall' Ente Nazionale Italiano di Unificazione - un'associazione privata senza scopo di lucro riconosciuta dallo Stato e dall'Unione Europea che da quasi 100 anni elabora e pubblica norme tecniche volontarie – le norme UNI – in tutti i settori industriali, commerciali e del terziario.

3

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

INTRODUZIONE

Come detto si tratta di norme tecniche volontarie e quindi non prevedono un regime sanzionatorio in caso di mancato rispetto ma descrivono un modello di riferimento elaborato da esperti professionisti del settore, allo scopo di operare al meglio garantendo sicurezza, qualità, rispetto per l'ambiente e prestazioni certe in tutti i settori industriali, commerciali e del terziario.

Recentemente e come nel caso della norma UNI 10459:2017 scopo è anche quello di uniformare i profili professionali al mercato europeo favorendo la circolazione delle professionalità

4

INTRODUZIONE

Scopo della normazione è contribuire al miglioramento dell'efficienza e dell'efficacia del sistema socio-economico, fornendo gli strumenti di supporto all'innovazione tecnologica, alla competitività, alla protezione dei consumatori, alla tutela dell'ambiente, alla qualità di prodotti, servizi e processi.

Le norme UNI sono emanate a livello nazionale e si affiancano e coordinano con norme di pari caratteristiche di livello europeo (CEN) e mondiale (ISO).

5

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

INTRODUZIONE

La volontarietà dichiarata potrebbe trarre in inganno rispetto all'obbligo di rispetto: non operare in linea con i principi contenuti nelle norme UNI o equivalenti, espone comunque il professionista a valutazioni di merito in caso di procedimenti di giudizio, ove il magistrato richiede spesso il parere a periti d'ufficio per operare un confronto tra l'operato dell'indagato e le buone prassi di riferimento.

Diligenza

Diligenza qualificata

6

INTRODUZIONE

Come già anticipato e citato nella stessa norma 10459, operare in rispetto della norma stessa permette di inserirsi nel contesto lavorativo senza frontiere dell'Unione Europea, e rappresenta quindi uno strumento utile alla mobilità delle persone ed all'abbattimento delle barriere alla libera circolazione del capitale umano.

In quest'ottica di omogeneizzazione in visione europea dei livelli di qualifica deve essere intesa anche la previsione insita nella ultima versione della norma di tre diversi livelli del profilo di professionista specialista della security, che compendiano sia il livello di preparazione teorica che gli anni di esperienza sul campo.

7

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

INTRODUZIONE

Nelle lezioni iniziali è stata già descritta la nuova norma UNI 10459:2017 che indica i contenuti della preparazione professionale del security manager aziendale con le rispettive indicazioni dei compiti, competenze e abilità che determinano la figura del SM stesso.

8

Modello di gestione ed UNI 10459:2017

9

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

MG ed UNI 10459:2017

Adesso cominceremo a descrivere i passaggi operativi basilari di approccio metodologico per l'implementazione del « modello a misurazione continua dell'efficacia» che è stato elaborato e pubblicato dal CESINTES e rappresenta una novità del settore perché per la prima volta si è passati dall'erogare conoscenze sul «fare» a quelle sul «come fare» in maniera oggettiva ed in linea con le indicazioni della ISO 31000:2018 ed UNI 10459:2017 in particolare per l'esecuzione dei *compiti* con utilizzo delle *conoscenze* ed *abilità* .

10

MG ed UNI 10459:2017

La valenza di un approccio metodologico OGGETTIVO ricade soprattutto sul professionista che esegue l'incarico perché nel pieno rispetto della norma ISO 31000:2018 , la responsabilità professionale è supportata da una valutazione del contesto che risulta conforme ed uguale per tutti coloro che saranno chiamati allo stesso incarico ed adotteranno lo stesso modello.

11

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

MG ed UNI 10459:2017

Il modello proposto è da intendersi come *preferito* ma non unico in quanto esistono varie scuole di formazione con diversi orientamenti interpretativi in considerazione del fatto che, come già detto, le varie norme UNI, CEN o ISO sono norme volontarie e non tecniche.

Parleremo di ***modello di misurazione continua dell'efficacia (gestione)*** e non di ***sistema di gestione*** per non creare confusione con i ***sistemi certificabili*** perché finalizzati all'ottenimento di una caratteristica organizzativa (per esempio qualità, sicurezza delle informazioni, continuità operativa) mentre il rischio rappresenta un evento da trattare ed il modello di gestione non è certificabile.

12

MG ed UNI 10459:2017

Il modello che proponiamo si sviluppa nelle seguenti fasi principali:

- ✓ *Determinazione del contesto*
  - *Policy organizzazione*
  - *Identificazione dei rischi*
- ✓ *Misurazione e trattamento dei rischi*
  - *Misurazione – priorità*
  - *Trattamento – misure riduzione*
  - *Misurazione aggiornata*
- ✓ *Implementazione del sistema di gestione*
  - *Modello di gestione: responsabilità , procedure, continuo miglioramento*
  - *Rischio residuo e gestione complessità*

13

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Determinazione contestualizzata dei rischi

14

Determinazione contestualizzata dei rischi

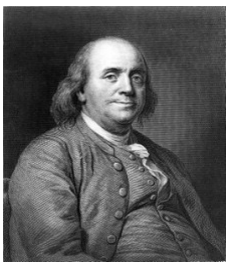
Questa fase iniziale è fondamentale e determinante per l'efficacia del modello di gestione in quanto il SM è chiamato al massimo impegno teorico ed intuitivo per identificare tutti i rischi attinenti il caso in esame perché un rischio non preso in considerazione in questa fase potrebbe avere un impatto devastante sull'intera organizzazione, vanificando l'efficacia del progetto implementato.

15

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Sbagliare a prepararsi significa prepararsi a sbagliare

Benjamin Franklin



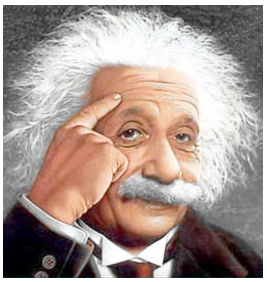
16

La conoscenza è basata sulle osservazioni non sulle opinioni

Albert Einstein

Osservazione: disponibile, misurabile ed uguale per tutti

Opinione: affermazione soggettiva



17

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Rapporto tra Sicurezza e Rischio

La Sicurezza non è un'entità misurabile perché rappresenta una sensazione ed una caratteristica del contesto. Per esempio un alpinista si trova a suo agio (sicuro) appeso con una sottile fune a picco sul vuoto mentre molti altri sarebbero terrorizzati (insicuri).

La Sicurezza però è l'inverso del Rischio in quanto alta Sicurezza = Basso rischio e viceversa.

L'alpinista si sente sicuro perché conosce i Rischi della montagna ed ha adottato adeguate misure di riduzione che non sono percepite dai meno esperti.

18

Rapporto tra Sicurezza e Rischio

A differenza della Sicurezza il Rischio è invece calcolabile e modificabile come vedremo in seguito.

La buona prassi di trattamento del Rischio è la norma mondiale ISO 31000 dove viene descritto «***cosa fare***» in maniera oggettiva.

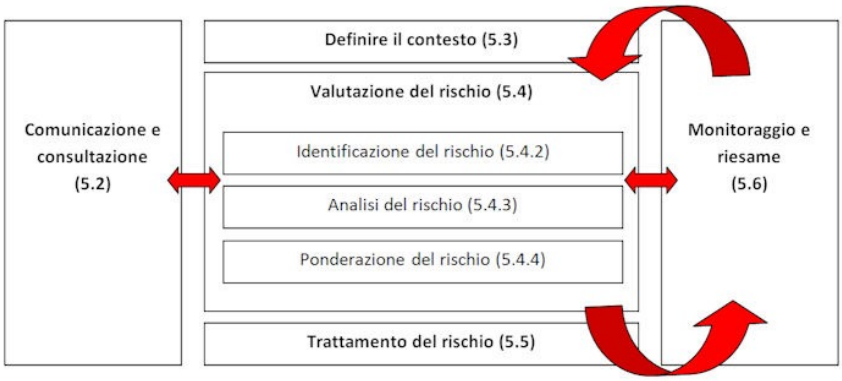
Scopo di questo corso è offrire un modello compliance con la ISO 31000 che indichi « ***come fare»*** sempre in maniera oggettiva.

In sintesi le valorizzazioni di calcolo del Rischio saranno proposte con grandezze disponibili e misurabili da tutti con valori uguali e quindi in maniera oggettiva

19

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Richiami al contenuto della ISO 31000:2018



20

Policy dell'organizzazione

Abbiamo definito ***contestualizzata*** la determinazione dei rischi perché l'analisi deve iniziare con una approfondita conoscenza dell'attività svolta dall'Organizzazione e quindi questa fase è bene che veda affiancato il SM da un elemento interno dell'Organizzazione stessa che conosca tutte le caratteristiche realizzative dei processi di produzione dei beni/servizi ed anche dei relativi stabilimenti intesi come siti ove viene svolta l'attività dell'Organizzazione stessa.

21

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Policy dell'organizzazione

E' bene che tale figura referente , a seconda della dimensione del contesto, sia eventualmente affiancata da un team di esperti dei sottosistemi produttivi.

Qui entra in gioco la "*conoscenza"* di "*tecniche di identificazione delle sorgenti informative, integrazione delle informazioni, categorizzazione ed analisi dell'informazione*" parimenti indicata per tutti i tre i livelli di qualifica del SM.

22

Policy dell'organizzazione

In questa fase di definizione del contesto di riferimento è bene anche ottenere indicazioni da parte dell'organizzazione su:

- messa a disposizione di risorse (generalmente economiche)
- livello di accettazione del rischio che può essere ritenuto
- eventuali piani di sviluppo/riorganizzazione in corso
- eventuali modifiche delle normative di riferimento che potrebbero impattare sull'organizzazione stessa .

Sarà bene prendere in considerazione anche lo storico di riferimento riferito sia al contesto stesso che a contesti simili e verificare l'efficacia di eventuali misure di riduzione già implementate in occasione di episodi passati

23

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Policy dell'organizzazione

Riassumiamo questa prima attività:

1. Abbiamo preso contatto con i vertici dell'organizzazione ed abbiamo focalizzato le caratteristiche dell'attività svolta, gli stabilimenti produttivi ed eventuali piani di sviluppo;
2. Abbiamo avuto indicazioni circa un referente aziendale che ci assisterà nella nostra attività e che ci darà conto anche dello storico tematico;
3. Abbiamo eseguito una primo approccio di ambientazione ed abbiamo preso visione della documentazione tecnica disponibile
4. Abbiamo avuto indicazioni sulle risorse disponibili e sul livello di rischio che l'organizzazione dichiara accettabile
5. Abbiamo avuto indicazioni circa i programmi a breve/medio termine dell'organizzazione (piani industriali)

24

Identificazione dei rischi

- Per quanto attiene l'identificazione dei rischi possiamo far riferimento alla ISO 31000:2018 punto 2.15:

Risk identification:

- **process of finding, recognizing and describing risks**
- **NOTE 1: Risk identification involves the identification of risk sources, events, their cause and their potential consequences**
- **NOTE 2: risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs**

25

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Identificazione dei rischi

- La norma ci dice che il processo di identificazione dei rischi si basa su attività di scoperta (evidenziazione), ricognizione (valutazione contestualizzata) e descrizione (elencazione motivata).
- La Nota 1 ci spiega che l'identificazione dei rischi contempla l'identificazione delle fonti di rischio, gli eventi che potrebbero avere conseguenze, le loro cause e le loro potenziali conseguenze.

26

Identificazione dei rischi

La Nota 2 ci suggerisce di considerare nell'identificazione dei rischi anche episodi accaduti, analisi teoriche, opinioni di persone informate e di esperti, esigenze di parti interessate (dove per parti interessate debbono intendersi tutti coloro – persone fisiche o giuridiche – che siano ad ogni titolo coinvolte con l'Organizzazione)

27

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Sequenza logica Evento-Rischio

Il Rischio rappresenta il risultato della variazione di equilibrio del contesto secondo la ISO 31000 che possiamo così schematizzare:

L'equilibrio di un contesto è modificato da un evento che impatta sulle esposizioni creando delle minacce che si concretizzano a causa delle vulnerabilità.

Per esempio un individuo che cammina all'improvviso sia coinvolto in un terremoto (evento): il rischio che ne deriva è diverso a seconda che l'uomo si trovi in uno spazio aperto (bassa esposizione a lesioni per la minaccia di essere sepolto o colpito da corpi pesanti) oppure all'interno di un edificio. La vulnerabilità è data dalla mancanza di protezione da dette lesioni.

28

Identificazione degli eventi/rischi

E' opportuno che in tale fase il SM effettui sopralluoghi nei vari siti, con presa visione sia delle aree esterne adiacenti, sia delle zone interne ai siti stessi, possibilmente con il supporto di rappresentazioni grafiche aggiornate (planimetrie ed «as built» degli impianti tecnologici).

Parallelamente su fonti di informazioni di riferimento (web, pubblicazioni di enti di statistica, ecc) potrà trovare indicazioni su eventuali rischi ambientali, di contesto sociale e specifici relativi all'attività svolta dall'organizzazione.

(*ricorda: osservazioni più che opinioni*)

29

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Identificazione dei rischi

In questa parte di attività, come suggerito anche dalla Nota 2 sopraindicata, sarà molto importante conoscere la storia dell'organizzazione in quanto ad incidenti o episodi rilevanti accaduti in passato, quali eventuali contromisure sono state adottate e se le stesse sono ancora efficaci. Trascurare un evento già accaduto può significare non considerare l'elevata probabilità che si ripeta l'evento con il susseguente danno.

Analogamente non valutare un evento accaduto ad altre realtà imprenditoriali simili può rappresentare una debolezza .

30

Identificazione dei rischi

La tabella che segue è un esempio dei vari tipi di rischio che potrebbero essere presi in considerazione e valutati nella probabilità di accadimento:

31

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Identificazione dei rischi

Tipologia rischio	Descrizione di riferimento
Legati alla produzione	Rischi di security insiti nella attività dell'Organizzazione intesa come processo di produzione di servizio/prodotto, rischi da obblighi normativi
Contesto locativo	Rischi insiti nella collocazione geografica e tipologia edilizia degli immobili utilizzati dall'Organizzazione: terremoti, allagamenti, fulmini, inondazioni, crolli, smottamenti
Danni al patrimonio	Furti, incendi, sabotaggi, attentati, frodi finanziarie, furto proprietà intellettuali, sequestri e richiesta riscatti.
Danni di compliance ambientale	Emissioni nocive gas , liquidi e solidi , rifiuti, emissione elevate di: rumori, vibrazioni, onde magnetiche,
Danni con azione di malintenzionati	Attacchi informatici, infedeltà dei dipendenti, furto dati riservati, rapimenti di dipendenti, attacchi all'immagine aziendale, attacchi NBC,
Altri danni derivati da	Fermo della produzione, pandemie, modifiche equilibri politici del paese, richieste malavita organizzata, fermo dei vettori di trasporto, blocco della circolazione viaria, scioperi,

32

LA TOP 10 DEI RISCHI IN ITALIA

Fonte: Allianz Global Corporate & Specialty.

Le cifre rappresentano la frequenza con cui un rischio è stato selezionato come percentuale di tutte le risposte per un determinato Paese.
Rispondenti: 47
Risposte: 55
E' stato possibile selezionare più di un rischio e di un settore industriale. Le cifre non raggiungono il 100% perché si possono selezionare fino a tre rischi.

Classifica		Percentuale	2018 classifica	Tendenza
1	Interruzione di attività (anche della supply chain)	47%	1 (51%)	=
2	Rischi informatici (crimine informatico, violazione dei dati, guasti IT)	38%	2 (38%)	=
2	Catastrofi naturali (tempeste, inondazioni, terremoti)	38%	3 (30%)	▲
4	Mancanza di qualità, difetti seriali, richiamo di prodotti NUOVO	22%	-	▲
5	Danno reputazionale o d'immagine	20%	4 (23%)	▼
6	Cambiamenti nello scenario legislativo e regolamentare (sanzioni economiche, protezionismo, Brexit, disgregazione dell'Eurozona)	18%	7 (14%)	▲
6	Cambiamenti nei mercati (volatilità, aumento della competizione/arrivo di nuovi operatori, fusioni e acquisizioni, stagnazione e fluttuazione del mercato)	18%	8 (13%)	▲
8	Cambiamento climatico/aumentata instabilità metereologica	16%	9 (11%)	▲
9	Incendio, esplosioni	13%	5 (17%)	▼
9	Nuove tecnologie (impatto dell'aumento della maggiore interconnettività, delle nanotecnologie, dell'intelligenza artificiale, della stampa 3D, dei droni)	13%	6 (16%)	▼

33

Identificazione dei rischi

Una volta stabilito il contesto da prendere in esame ed il team di supporto il SM può iniziare la fase di identificazione ed elencazione dei rischi con diverse matrici di identificazione. Noi sceglieremo quella generica che divide i rischi in:

- ***endogeni***
- ***esogeni***

in un processo di totale prospettazione intuitiva e di elencazione motivata.

34

Rischi esogeni

- Sismicità e prossimità zone instabili
- Allagamenti, straripamenti, dighe, invasi, rete fognaria
- Vulcani attivi ed emissioni polveri,
- Vicinanza siti sensibili quali fabbriche chimiche o biologiche, centrali elettriche, termovalorizzatori,
- Siti sensibili per attentati o sabotaggi
- Vicinanza aeroporti
- Vicinanza siti militari
- Viabilità mezzi ordinari e pesanti
- Caratteristiche rete servizi primari (energia e TD)
- Attacchi terroristici, intrusioni non autorizzate anche via web, sequestri per riscatto..

35

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Rischi endogeni

- Infedeltà dei dipendenti;
- Rotture macchinari della produzione,
- Incendi materiale stoccato
- Furti di informazioni, copyright,…
- Salute dei lavoratori o terzi presenti nei siti di produzione,
- Personale esterno in appalto
- Danni ambientali per inquinamento aria, acqua o terreno
- ……..

36

Identificazione dei rischi

Le varie tipologie di rischi indicate possono sembrare eccessive rispetto al contenuto della norma UNI 10459:2017 ma si suggerisce di tener conto anche della *ricaduta di eventi non propriamente elencati nella norma* come impatto collaterale.

Per esempio la norma non si sofferma sul rischio incendio ma è evidente che un SM deve considerare tale ipotesi per la probabilità che avvengano incendi che a seconda dell'estensione comportino situazioni di indisponibilità totale o parziale degli impianti di protezione coinvolti, del controllo degli accessi in caso di evacuazione, della possibilità di furti o azioni illecite in situazioni di caos caratteristiche di una evacuazione.

37

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Gestione e trattamento dei rischi

38

Gestione del rischio

Processo per modificare l'impatto del rischio:

Il trattamento del rischio può implicare:

- Evitare il rischio decidendo di non iniziare o non continuare l'attività che da origine ad esso (elusione);
- Rimuovere la fonte del rischio;
- Modificare la verosimiglianza (trattamento);
- Modificare le conseguenze (trattamento);
- Condividere il rischio con altra(e) parte(i) –trasferimento a terzi (compresi contratti assicurazione e simili);
- Ritenere il rischio con una decisione informata, aumentando il livello delle misure di prevenzione e protezione (trattamento)

39

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Gestione e/o trattamento

Pur avendo una terminologia che può trarre in inganno le due azioni si diversificano in quanto:

GESTIONE: è un'attività di tipo manageriale che interfaccia il S.M. all'Organizzazione per le decisioni strategiche di policy legate al livello di rischio accettato ed alle risorse messe a disposizione (scelte che il S.M. può suggerire ma non decidere)

TRATTAMENTO: a valle della decisione di ritenere rischi nasce l'attività del S.M. che progetta misure di riduzione della Magnitudo degli stessi per portarla al livello indicato dall'Organizzazione come accettabile, utilizzando le risorse economiche messe a disposizione

40

Trattamento: misurazione - priorità

Dopo aver identificato i rischi che l'organizzazione intende gestire attraverso il trattamento di riduzione, il S.M. avvia tale attività che prevede tre fasi:

- ✓ ***misurazione*** del singolo rischio
- ✓ realizzazione ***tabella priorità***
- ✓ implementazione ***misure riduzione***

La logica di questa progressione è data dal confronto tra rischi da ridurre e risorse economiche disponibili che suggerisce di iniziare il trattamento dei rischi di magnitudo superiore procedendo con le magnitudo inferiori fino all'esaurimento delle risorse messe a disposizione

41

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Risorse economiche e ISO 31000

Il modello proposto attua il trattamento dei rischi in funzione delle risorse economiche disponibili cominciando a ridurre le magnitudo maggiori fino ad esaurimento della disponibilità. Ciò è considerato più rispondente alle necessità di produrre progetti nell'ambito di gare o confronti di costi.

Comunque il modello è attuabile anche nel caso in cui si dovesse realizzare un piano di trattamento senza limitazioni iniziali di spesa , basterà iniziare sempre dalle magnitudo più elevate e proseguire fino alle magnitudo che rispondono ai criteri di accettazione, relazionando sui costi complessivi invece che sulle risorse disponibili.

42

Perchè il Rischio non può essere azzerato?

Come abbiamo detto il Rischio è l'effetto dell'incertezza nel raggiungimento degli obiettivi . Abbiamo detto che possiamo implementare una misura di riduzione «aggiungendo» un altro asset (anello) alla catena che sostituisca quello mancante nell'effetto voluto. Ma anche questo nuovo asset può venir meno e quindi possiamo aggiungere un altro asset che sopperisca alla venuta meno di entrambi. Portando il discorso all'estremo avremo asset e costi in crescita infinita con il Rischio ridotto ***ma non annullato***.

43

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Misurazione - priorità

Dobbiamo ora introdurre la basilare funzione di misurazione teorica del rischio comunemente indicata come " *equazione del rischio"* utilizzando la funzione che lega il Rischio alla probabilità e Danno*:*

$$R = f(P; D)$$

R = rischio da misurare

P = probabilità di accadimento

D= danno inteso come sommatoria di tutti gli impatti economici

44

Misurazione - priorità

Per poter procedere alla misurazione è necessario omogeneizzare le grandezze in esame per poter calcolare i valori numerici con la funzione

$$R = P \times D$$

Vedremo in seguito che ciò è reso possibile dalla valorizzazione di tutte le grandezze con il sistema semiprobabilistico e semiquantitativo

45

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Misurazione - priorità

Esistono nella letteratura specialistica diverse versioni di tale equazione che come secondo fattore della moltiplicazione indicano “danno” oppure “impatto” oppure “ ricaduta”.

La probabilità di fatto è legata all’ “Incertezza” su quanto potrà verificarsi nel progredire del tempo in un’ottica di equilibrio produttivo dell’Organizzazione ed eventi che possano modificare tale equilibrio.

Il calcolo della probabilità può essere legato a valutazioni storiche, statistiche, su informazioni relative al mutamento del contesto politico-economico-tecnologico, ecc.

46

Misurazione - priorità

La probabilità a sua volta è funzione della frequenza e della vulnerabilità

$$P = f(f ; V)$$

P = probabilità

f = frequenza

V= vulnerabilità che è funzione di:

- ✓ Grado inadeguatezza procedure
- ✓ Grado inefficienza tecnologie
- ✓ Grado inadeguatezza risorse umane

47

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Misurazione - priorità

A seconda della dimensione della Organizzazione in esame e dei rischi individuati è consigliabile operare una semplificazione raggruppando i diversi valori di probabilità o danno in ***parametri di valutazione semiprobabilistici e semiquantitativi***, quindi potremo avere da 2 a più parametri di probabilità e da 2 a più parametri di danno.

ESEMPIO DI PARAMETRAZIONE A TRE VALORI

Probabilita' (P)	Danno (D)
• Alta (3)	Alto (3)
• Media (2)	Medio (2)
• Bassa (1)	Basso (1)

48

Stima della probabilità

Come abbiamo visto la probabilità è funzione della frequenza e quindi si farà riferimento alle fattispecie accadute in un periodo temporale medio (per esempio ultimi 5 anni) che potrebbero causare il rischio preso in considerazione

Alta probabilità : accaduto più volte

Media probabilità : accaduto una volta

Bassa probabilità : mai accaduto

49

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Stima della probabilità

Sulla stima della probabilità abbiamo visto che incide anche la vulnerabilità negli aspetti :

- ✓ Grado inadeguatezza procedure
- ✓ Grado inefficienza tecnologie
- ✓ Grado inadeguatezza risorse umane

Quindi dalla considerazione contemporanea dei vari fattori scaturisce la valutazione di stima da considerare nel calcolo della magnitudo

50

TABELLA STIMA PROBABILITA'						
consistenza	numero eventi negli ultimi 5 anni	Stima frequenza	grado inadeguatezza procedure	grado inefficienza tecnologie	grado inadeguatezza risorse umane	Valorizzazione media tabellare
ALTO	> 1 volta					
MEDIO	1 volta					
BASSO	0 volte					

51

Stima della probabilità

Esempio:

Un evento pericoloso è già accaduto più volte negli ultimi 5 anni (Alta) ma recentemente sono state implementate specifiche soluzioni tecnologiche (impianti monitoraggio) ed emanato procedure di risposta (adeguatezza procedure) che sono state portate a conoscenza con formazione agli addetti in numero sufficiente (adeguatezza risorse umane)

Quindi la probabilità per eventi già accaduti ha un fattore ALTO da moltiplicare con vulnerabilità ora BASSA.

52

TABELLA STIMA PROBABILITA'						
consistenza	numero eventi negli ultimi 5 anni	Stima frequenza	grado inadeguatezza procedure	grado inefficienza tecnologie	grado inadeguatezza risorse umane	Valorizzazione media tabellare
ALTO	> 1 volta	3				
MEDIO	1 volta					
BASSO	0 volte		1	1	1	

53

Stima della probabilità

Nello stesso esempio però se alla implementazione di specifiche soluzioni tecnologiche (impianti monitoraggio) ed emanazione di procedure di risposta (adeguatezza procedure) non avesse avuto seguito anche l'informazione e formazione degli addetti in numero adeguato, la stima della inadeguatezza risorse sarebbe MEDIA= 2

54

Calcolo stima probabilità a valori plurimi

Ci troviamo ora nella necessità di calcolare il valore della probabilità con misura UNICA ma di fatto abbiamo 4 valori in tabella.

Il modello che proponiamo utilizza il sistema di media aritmetica con arrotondamento al valore assoluto superiore (criterio di prudenza) assumendo pari peso per ogni valorizzazione.

55

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Calcolo stima probabilità a valori plurimi

TABELLA STIMA PROBABILITA'						
consistenza	numero eventi negli ultimi 5 anni	Stima frequenza	grado inadeguatezza procedure	grado inefficienza tecnologie	grado inadeguatezza risorse umane	Valorizzazione media tabellare
ALTO	> 1 volta	3				
MEDIO	1 volta					
BASSO	0 volte		1	1	2	**2**

(3+1+1+2) /4= 1,75	**valore assoluto superiore 2**

56

Stima del danno

Per la stima del danno occorre invece far riferimento alle indicazione dell'organizzazione in quanto il danno può avere diverse componenti:

- ✓ Danno per sanzioni penali o amministrative
- ✓ Danno di immagine
- ✓ Danno economico per perdita di patrimonio
- ✓ Danno economico per fermo attività
- ✓ Danno per costi di consulenze
- ✓ ….

57

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Stima del danno

Inoltre a parità di valore espresso in valuta ogni organizzazione ha una propria considerazione. Per esempio un Danno di 100.000 Euro può essere catastrofico per una PMI ma assolutamente tollerabile per una grande multinazionale.

Quindi la stima del Danno non è sulla quantità ma sull'impatto ed è onere dell'Organizzazione indicarlo al SM.

58

Esempio tabella stima DANNO

TABELLA STIMA DANNO ECONOMICO		
consistenza	valore in K Euro	valorizzazione tabellare
ALTO	> 50	3
MEDIO	<50 >10	2
BASSO	<10	1

59

Propensione al Rischio

Anche questo parametro è fornito dall'Organizzazione e rappresenta l'obiettivo del Trattamento del Rischio nel valore accettato della Magnitudo calcolata (da Rischio Preventivo a Rischio Atteso):

Magnitudo inaccettabile	Magnitudo accettabile
9,6,4	3,2,1

60

Tabella priorità

Siamo ora in grado di misurare il singolo rischio

R = P x D

e completare la tabella delle priorità indicando i valori decrescenti delle magnitudo calcolate.

Ricordiamo che Magnitudo e Rischio sono diverse espressioni della stessa entità: Rischio è generico Magnitudo è del singolo contesto

61

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Misurazione - priorità

Poiché abbiamo scelto una valorizzazione tabellare 3-2-1 le magnitudo calcolate avranno i seguenti valori: 9-6-4-3-2-1

Cominceremo quindi dal trattamento delle magnitudo 9 e poi scenderemo fino all'esaurimento delle risorse disponibili.

In questa fase è importante considerare ***la disponibilità di risorse*** messe a disposizione dall'organizzazione perché verosimilmente non tutti i rischi potranno essere trattati.

Abbiamo già detto che parimenti è possibile realizzare un piano di trattamento senza riferimento iniziale alle risorse disponibili attuando la riduzione di tutti i rischi eccedenti i limiti ammessi e poi sommando i costi.

62

Misurazione - priorità

Magnitudo rischio = PxD	Priorità
9	Primi rischi da trattare
6, 4	Fase successiva
3- 2 - 1	Ultima fase (non trattamento)

63

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Misurazione - priorità

Con la stessa metodologia in caso di Organizzazioni più complesse possiamo considerare diverse valorizzazioni tabellari della probabilità o del danno realizzando quindi tabelle 2 x 2 (Alto 2/Basso 1) , 4x4 (Altissimo 4/Alto 3/Medio 2/Basso 1) comunque a discrezione del SM riferite al livello di approssimazione scelto soprattutto in funzione della valorizzazione del Danno e della complessità dell'Organizzazione.

64

Dal cosa fare a come fare

Ricapitoliamo quanto finora detto:

- La Sicurezza non è trattabile il Rischio si
- La norma di riferimento è la ISO 31000:2018
- La ISO 31000 indica «*cosa fare*» ma non « come fare»
- Il modello proposto guida il SM nel fare in maniera oggettiva
- Un modello oggettivo ha un maggior valore esimente per il SM

65

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Trattamento-misure riduzione

Iniziamo ora la fase di progettazione delle misure di riduzione del rischio che serviranno per ridurre la magnitudo.

Ricordiamo che i fattori della misura del rischio sono

Probabilità

Frequenza

Vulnerabilità

Danno

Focalizzeremo inizialmente l'attenzione sulle Vulnerabilità perché sia la frequenza che il danno non dipendono direttamente dalla implementazione delle misure di riduzione: ne sono una conseguenza

66

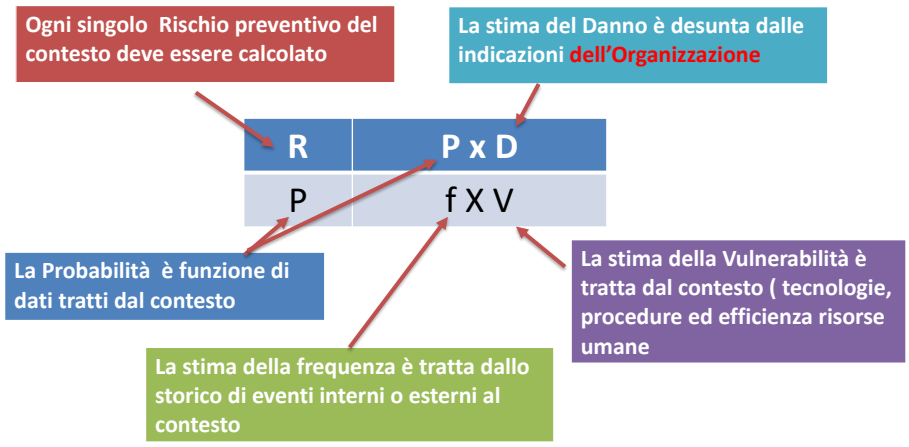
Il Danno come risultato di un evento

La progressione temporale della formazione di un Danno nasce con un EVENTO (indesiderato) calato nel CONTESTO che ha delle ESPOSIZIONI con relative VULNERABILITA'.

Il Danno può essere generato con una progressione temporale o praticamente istantaneo.

67

Riepilogo



68

PAUSA

69

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Implementazione del Modello di Gestione

70

Modello di gestione

Un modello di gestione (MG) è un insieme di regole e procedure, che un'organizzazione o azienda può applicare allo scopo di raggiungere obiettivi definiti, quali ad esempio:

- il monitoraggio continuo delle misure implementate per la riduzione dei rischi
- la gestione dell'ordinario e straordinario con adeguate procedure;
- il miglioramento continuo delle prestazioni dell'organizzazione stessa.

71

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Modello di gestione

Abbiamo detto in apertura che il modello di gestione del rischio non è certificabile ma è liberamente adottabile come prassi esecutiva

L'obiettivo generalmente è quello di attuare strumenti che consentano all'azienda di tenere sotto controllo la consistenza del rischio nei propri processi e nelle proprie attività.

Un modello di gestione rappresenta comunque un valore aziendale in quanto permette di mantenere sempre alto il controllo dei rischi indipendentemente dalle risorse umane sia a livello di disponibilità che di competenza.

72

Modello di gestione

Gli scopi e gli obiettivi del MG possono essere:

- ✓ Verifica della costante efficacia delle misure implementate
- ✓ Assegnazione di responsabilità di controllo/verifica
- ✓ Gestione dell'ordinario
- ✓ Gestione dello straordinario
- ✓ Gestione degli allert
- ✓ Gestione dei cambiamenti
- ✓ Tracing ed audit
- ✓ Continuo miglioramento

73

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Modello di gestione

Un MG è materialmente costituito da un insieme documentale di dimensioni correlate alla grandezza e complessità dell'Organizzazione, ispirato alle indicazioni del ciclo di Deming – Plan- Do- Check – Act -, coordinato con un regolamento funzionale dell'Organizzazione , con i seguenti ***contenuti***:

1. responsabile del Modello di Gestione
2. procedure da intendersi come istruzioni operative di alto livello di dettaglio destinate al responsabile designato della attività inserita in quelle con possibile rischio. Tutto l'insieme delle procedure deve essere tale da considerare tutti gli elementi base costituenti l'implementazione del modello di riduzione del rischio ai livelli approvati e tutti i livelli di coordinamento tra le varie unità organizzative dell'Organizzazione

74

Modello di gestione

3. sistemi di misurazione del rispetto delle procedure attraverso il monitoraggio di elementi caratteristici indicati nella procedura stessa;
4. procedure di svolgimento di audit di vario livello
5. procedure di gestione delle contingency
6. attività di miglioramento continuo affidata al Responsabile MG

75

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Conclusione

Come abbiamo visto il MG si basa sul trattamento dei rischi generalmente considerati singolarmente con l'implementazione delle misure di riduzione passive, attive ed organizzative o combinazione delle stesse.

Un ulteriore miglioramento del MG può essere attuato con uno studio dei possibili impatti di rischi che accadano contemporaneamente ed identificazione delle relative misure di riduzione – gestione delle complessità - .

76

Grazie per l'attenzione

Ing. Massimo Marrocco

77

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

ING. MASSIMO MARROCCO

Università degli Studi di Roma Tor Vergata

ingmarroccomassimo@tiscali.it

78