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

FRANCESCO FARINA

SECURITY E PROFESSIONISTI DELLA SECURITY

1

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

DALLA FORMAZIONE ALLA CERTIFICAZIONE AI SENSI DELLA UNI 10459:2017

2

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

Conoscenza

Esperienza

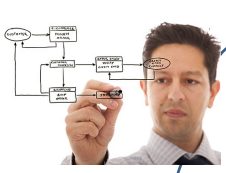
Competenza

Attitudine - Abilita'

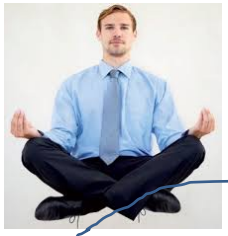
3

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

SENIOR SECURITY MANAGER
LIVELLO STRATEGICO



SECURITY MANAGER
LIVELLO TATTICO



SECURITY EXPERT
LIVELLO OPERATIVO

CONOSCENZE
ABILITA'
COMPETENZE

COMPLESSITA'
AZIENDALE

4

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

IL NUOVO ORIENTAMENTO DEL PROFILO DEL SECURITY MANAGER: I REQUISITI DI ACCESSO

	TITOLO DI ACCESSO/ESPERIENZA PROFESSIONALE	COMPITI/CONOSCENZE/ABILITA'	FORMAZIONE BASE	AGGIORNAMENTO ANNUO
I LIVELLO: SECURITY EXPERT	- Diploma di Scuola Media Superiore: 8 anni di esperienza professionale continuativa di security, nel privato, anche come consulente, e/o in organismi pubblici di sicurezza, di cui almeno 4 anni in incarichi di livello non meramente esecutivo. - Laurea di I livello di una classe che includa discipline almeno in parte afferenti alle conoscenze del Professionista della Security. Minimo 4 anni di esperienza professionale continuativa di security, nel privato, anche come consulente, e/o in organismi pubblici di sicurezza, di cui almeno 2 anni in incarichi di livello non meramente esecutivo. - laurea di II livello: esperienza professionale DI 2 anni, in incarichi non meramente esecutivi.	OPERATIVI IN CONTESTO AZIENDA COMPLESSA	Un Master Universitario (60 crediti formativi) oppure un Corso di livello universitario di almeno 120 ore; entrambi aventi per argomento la gestione della security per materie afferenti alle competenze del profilo.	OBBLIGATORIO: SEMINARI/CONVEGNI/DOCENZE
II LIVELLO: SECURITY MANAGER	- Diploma di Scuola Media Superiore: 12 anni di esperienza professionale continuativa di security nel privato, anche come consulente, e/o in organismi pubblici di sicurezza di cui almeno 4 anni in incarichi di livello manageriale. di security nel privato, anche come consulente, e/o in organismi pubblici di sicurezza di cui almeno 4 anni in incarichi di livello manageriale. - Laurea di I livello di una classe che includa discipline almeno in parte afferenti alle conoscenze del Professionista della Security. Minimo 8 anni di esperienza professionale continuativa di security nel privato, anche come consulente, e/o in organismi pubblici di sicurezza di cui almeno 4 anni in incarichi di livello manageriale. - laurea di II livello: CON esperienza professionale 5 anni, di cui 3 anni in incarichi di livello manageriale.	MANAGERIALI IN CONTESTO AZIENDA COMPLESSA	Un Master Universitario (60 crediti formativi) oppure un Corso di livello universitario di almeno 120 ore; entrambi aventi per argomento la gestione della security per materie afferenti alle competenze del profilo	OBBLIGATORIO: SEMINARI/CONVEGNI/DOCENZE
III LIVELLO: SENIOR SECURITY MANAGER	- Diploma di Scuola Media Superiore: 20 anni di esperienza professionale continuativa di security nel privato, anche come consulente, e/o in organismi pubblici di sicurezza di cui almeno 8 anni in incarichi di livello manageriale. (esperienza maturata entro la data pubblicazione della norma). - Laurea di I livello di una classe che includa discipline almeno in parte afferenti alle conoscenze del Professionista della Security. Minimo 12 anni di esperienza professionale continuativa di security nel privato, anche come consulente, e/o in organismi pubblici di sicurezza di cui almeno 6 anni in incarichi di livello manageriale. - laurea di II livello: CON esperienza professionale 18 anni, di cui 8 anni in incarichi di livello manageriale.	ALTO LIVELLO MANAGERIALE IN CONTESTO AZIENDA COMPLESSA	Un Master Universitario (60 crediti formativi) oppure un Corso di livello universitario di almeno 120 ore; entrambi aventi per argomento la gestione della security per materie afferenti alle competenze del profilo	OBBLIGATORIO: SEMINARI/CONVEGNI/DOCENZE

5

LIVELLAZIONE REQUISITO FORMATIVO PER I TRE PROFILI DEL "PROFESSIONISTA DELLA SECURITY"	EQF SECURITY EXPERT	EQF SECURITY MANAGER	EQF SENIOR SECURITY MANAGER
Sistema organizzativo, dei processi, delle politiche, delle linee guida e delle normative interne dell'Organizzazione	5	6	7
Principi di sostenibilità, di responsabilità sociale e di diritti umani	5	6	6
Legislazione di riferimento	5	6	7
Materie giuridiche	5	6	7
Problematiche di security delle Infrastrutture critiche e relativa legislazione	5	5	7
Norme tecniche di "security risk management"	5	6	7
Criteri di classificazione delle informazioni e di tutela delle informazioni classificate	5	6	7
Disciplina giuridica in materia di crimine informatico e di protezione dei dati	5	6	7
Metodologie di identificazione dei pericoli, di quantificazione e valutazione dei rischi di origine criminosa, di definizione dei criteri di accettabilità, di identificazione delle misure di mitigazione	5	7	7
Procedure, linee guida, norme tecniche per la gestione del rischio nel proprio ambito operativo	5	7	
Modalità di impostazione di procedure, linee guida, norme tecniche per la gestione del rischio nel proprio ambito operativo			7
Metodologie per la valutazione del grado di security nel territorio e nelle comunità ospitanti	6	7	7
Identificazione del rischio prevalente nell'area	7	7	7
Strumenti per valutare l'impatto delle attività di security sul contesto sociale ed economico di riferimento	5	6	7
Tecniche di identificazione delle sorgenti informative, integrazione delle informazioni, categorizzazione e analisi dell'informazione	5	6	7
L'Organizzazione e le sue strutture fisiche	7	7	7
Modelli e tipologie di organizzazione e gestione della security	5	6	6
Principi di prevenzione dei rischi di origine criminosa attraverso la progettazione ambientale e urbanistica	5	6	7
Tecnologie di prevenzione e protezione di security	6	7	7
Ingegneria di security			6
Gestione dei servizi integrati di sicurezza	5	5	7
Problematiche di indagine difensiva all'interno dell'Organizzazione e relativa legislazione e possibili soluzioni	6	7	7
Elementi di coordinamento della continuità operativa ("business continuity" e "disaster recovery")	5	6	7
Elementi di coordinamento della gestione della crisi ("crisis management")	5	6	7
Elementi di psicologia delle masse	5	5	6
Modalità di predisposizione di piani di security	6	7	7
Processi di investigazione ("intelligence" e "due diligence")	5	6	7
Sistemi e tecniche di monitoraggio e "reporting"	5	6	7
Modalità di gestione dei contratti di security	5	6	7
Procedure di security dell'Organizzazione e modalità di rilevamento di eventuali non conformità rispetto alle esigenze della stessa Organizzazione	5	6	7
Tecniche e strumenti di comunicazione (relazione con istituzioni, autorità, Forze dell'ordine, enti locali e stampa)	5	6	
Tecniche e strumenti di comunicazione (relazione con istituzioni, enti locali e stampa)			7
Strumenti e metodi di pianificazione, programmazione e controllo aziendale	5	6	7

6

PROSPETTO DEI DESCRITTORI LIVELLO EQF
Prospetto di sintesi dei livelli EQF così come descritti nella Raccomandazione del Parlamento Europeo e del Consiglio del 23 aprile 2008

	CONOSCENZE Nel contesto del Quadro europeo delle qualifiche, le conoscenze sono descritte come teoriche e/o pratiche	ABILITA' Nel contesto del Quadro europeo delle qualifiche, le abilità sono descritte come cognitive (comprendenti l'uso del pensiero logico, intuitivo e creativo) e pratiche (comprendenti l'abilità manuale e l'uso di metodi, materiali, strumenti e utensili)	COMPETENZE Nel contesto del Quadro europeo delle qualifiche, le competenze sono descritte in termini di responsabilità e autonomia
Liv. EQF 5	Conoscenza teorica e pratica esauriente e specializzata, in un ambito di lavoro o di studio e consapevolezza dei limiti di tale conoscenza.	Una gamma esauriente di abilità cognitive e pratiche necessarie a dare soluzioni creative a problemi astratti.	Saper gestire e sorvegliare attività nel contesto di attività lavorative o di studio esposte a cambiamenti imprevedibili. Esaminare e sviluppare le prestazioni proprie e di altri.
Liv. EQF 6	Conoscenze avanzate in un ambito di lavoro o di studio, che presuppongano una comprensione critica di teorie e principi.	Abilità avanzate, che dimostrino padronanza e innovazione necessarie a risolvere problemi complessi ed imprevedibili in un ambito specializzato di lavoro o di studio.	Gestire attività o progetti, tecnico/professionali complessi assumendo la responsabilità di decisioni in contesti di lavoro o di studio imprevedibili. Assumere la responsabilità di gestire lo sviluppo professionale di persone e gruppi.
Liv. EQF 7	Conoscenze altamente specializzata, parte delle quali all'avanguardia in un ambito di lavoro o di studio, come base del pensiero originario e/o della ricerca. Consapevolezza critica di questioni legate alla conoscenza all'interfaccia tra ambiti diversi.	Abilità specializzate, orientate alla soluzione di problemi, necessarie nella ricerca e/o nell'innovazione al fine di sviluppare conoscenze e procedure nuove e integrare la conoscenza ottenuta in ambiti diversi.	Gestire e trasformare contesti di lavoro o di studio complessi, imprevedibili che richiedono nuovi approcci strategici. Assumere la responsabilità di contribuire alla conoscenza e alla prassi professionale e/o di verificare le prestazioni strategiche dei gruppi.

7

SECURITY:
UNA FUNZIONE «NOBILE» ED IN EVOLUZIONE
DA RISK MANAGEMENT A INTELLIGENCE ECONOMICA

8

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

FUNZIONE SECURITY:
SCENARIO

- SICUREZZA LOGICA
- SICUREZZA FISICA
- SICUREZZA ORGANIZZATIVA

- TUTELA DEL PATRIMONIO TANGIBILE ED INTANGIBILE DI UNA ORGANIZZAZIONE, FATTO DI PERSONE, COSE, KNOW HOW E DATI

SECURITY

- INNOVAZIONE TECNOLOGICA
- INNOVAZIONE ORGANIZZATIVA
- INNOVAZIONE NORMATIVA
- INNOVAZIONE INDUSTRIALE

- PROFESSIONISTI DELLA SECURITY
- ISTITUTI VIGILANZA
- IMPIANTISTI
- PROGETTISTI
- INVESTIGATORI
- INFORMATICI
- PRODUTTORI
- LEGALI
- RISK MANAGER
- FORZE DI POLIZIA
- OPERATORI DELLA SICUREZZA
- HACKER
- DATA PROTECTION OFFICERS
- CERTIFICATORI

9

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

FUNZIONE SECURITY:
SCENARIO

- ***Sicurezza fisica:*** **rappresenta l'insieme di interventi strutturali e tecnico/tecnologici su sedi o materiali di proprietà e/o pertinenza aziendali, avendo per obiettivo la tutela delle risorse materiali, immateriali ed umane di cui disponiamo e di cui abbiamo necessità per garantirci un'adeguata capacità concorrenziale nel breve, medio e lungo periodo**

- ***Sicurezza logica:*** **rappresenta i dispositivi e le funzioni standard atte a ridurre i rischi di aggressioni condotte sui o attraverso i servizi di ICT, congiuntamente ai settori tecnici che li gestiscono, avendo come obiettivo quello di proteggere le informazioni, i dati personali e il know how aziendale**

- ***Sicurezza organizzativa:*** **rappresenta l'organizzazione del lavoro, individuandone i processi "critici" (turni di lavoro, regole contrattuali per l'esercizio) attraverso l'individuazione di modelli flessibili fondati sul "miglioramento continuo" (ciclo di Deming), con l'obiettivo di progettare la più efficiente, solida e flessibile organizzazione di sicurezza a supporto delle *line* aziendali**

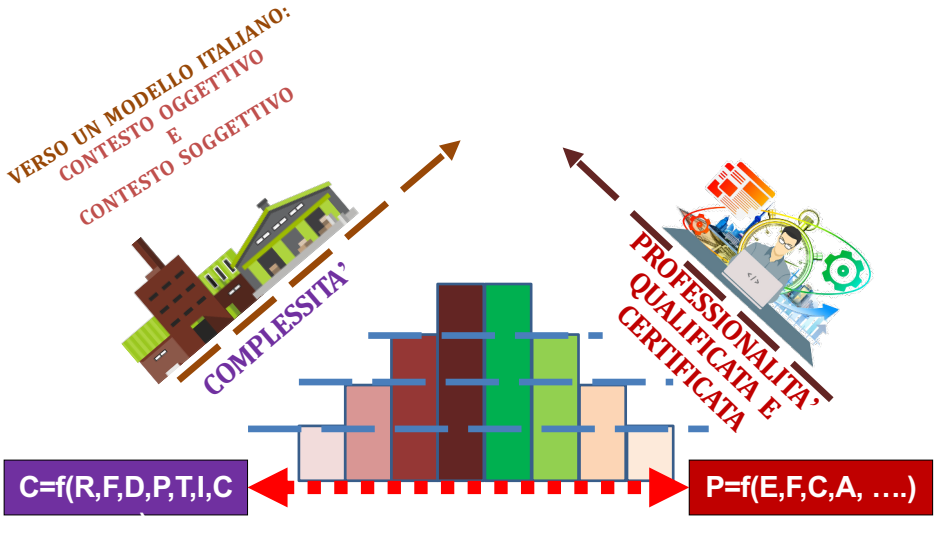
10

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

COMPLESSITA' DELL'ORGANIZZAZIONE E COMPLESSITA' DI SECURITY

11

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



12

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

TRA RISK MANAGEMENT E INTELLIGENCE ECONOMICA

«SECURITY MANAGEMENT»

funzione dedicata al presidio e tutela del patrimonio dell'azienda, tangibile ed intangibile, fatto di proprietà, persone, know how, informazioni, dati, conoscenze, processi e sistemi.

"INTELLIGENCE ECONOMICA"

insieme delle azioni coordinate di ricerca, analisi, distribuzione e protezione delle informazioni, al servizio delle decisioni strategiche

13

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

TRA RISK MANAGEMENT E INTELLIGENCE ECONOMICA

«SECURITY MANAGEMENT»

Il Manager della Security

è il professionista che ha il compito di governare una funzione così complessa e aleatoria, in possesso di conoscenze, competenze e abilità, di attitudine al risk management, di conoscenza del business e delle policies aziendali, di visione e percezione integrata con operatività trasversale nei processi.

"INTELLIGENCE ECONOMICA"

L'Analista di Intelligence Economica

è quel professionista che con conoscenze e competenze trasversali, commerciali come istituzionali, accademiche come politiche, scientifiche come industriali, ricerca e analizza dati e e informazioni per lo sviluppo e la tutela della ricchezza di una nazione, delle risorse naturali, dei suoi investimenti, dei suoi equilibri economici e finanziari, dell'attività di ricerca ed innovazione, della proprietà intellettuale, scientifica, artistica ed industriale

14

SECURITY MANAGEMENT E ENTERPRISE RISK MANAGEMENT

- Approccio integrato, globale e a valenza strategica nella gestione dei rischi di impresa.
- I concetti di ERM si sviluppano a partire da anni '90 nelle moderne teorie di finanza di impresa che assegnano al rischio un ruolo centrale.
- In un contesto economico e finanziario sempre più integrato e competitivo l'ERM deve garantire l'equilibrio e la crescita della singola Impresa che a sua volta concorre all'equilibrio e alla crescita competitiva del sistema Paese.

15

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

SECURITY MANAGEMENT E ENTERPRISE RISK MANAGEMENT

- Introduce le variabili aleatorie nella programmazione strategica di impresa, e nel sistema di budgeting, computando rischi espliciti ed impliciti per l'Azienda.
- E' parte integrante della definizione di scenari difensivi e competitivi.
- Contribuisce alla creazione di valore aziendale:
  - ✓ Ottimizzando il profilo di rischio dell'impresa
  - ✓ Affrontando i rischi in modo proattivo
  - ✓ Gestendo la vulnerabilità aziendale da eventi che alterino l'equilibrio economico, finanziario e patrimoniale
  - ✓ Predisponendo interventi di contenimento volti a garantire la continuità aziendale

16

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

SECURITY MANAGEMENT E ENTERPRISE RISK MANAGEMENT

Rischio=opportunità

si configura come l'insieme degli effetti positivi (opportunità) e negativi (minacce), consequenziali al manifestarsi di un evento rischioso, o imprevisto, o solo parzialmente previsto, sulla situazione economica, finanziaria e patrimoniale di un'impresa.

17

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

TRA RISK MANAGEMENT E INTELLIGENCE ECONOMICA

"le organizzazioni di tutti i tipi e dimensioni si trovano ad affrontare fattori ed influenze interni ed esterni che rendono incerto il raggiungimento dei propri obiettivi. Il rischio è l'effetto che questa incertezza ha sugli obiettivi dell'organizzazione."

……ad ogni azione corrisponda una reazione di pari intensità e direzione ma di verso opposto, ovvero ad ogni azione corrisponda una reazione uguale e contraria…..

Le politiche aziendali o sistemiche possono a loro volta produrre rischi "esternalità", positive o negative, nell'ambiente circostante, fatto di mercati, cittadini e beni pubblici.

18

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

TRA RISK MANAGEMENT E INTELLIGENCE ECONOMICA

- Una nuova autostrada, o una nuova ferrovia, migliora l'accessibilità contribuendo al progresso sociale ed economico, ma crea impatto acustico e visivo, costi di manutenzione e sicurezza da garantire;
- un nuovo gasdotto assicura l'approvvigionamento energetico, ma interferisce in modo significativo con il territorio generando inquinamento atmosferico, acustico, con potenziale rischio ambientale a carico della collettività in caso di incidente;
- una centrale nucleare produce energia elettrica a costi competitivi rispetto alle fonti tradizionali, ma un eventuale incidente ha conseguenze economiche ambientali e sanitarie incommensurabili;

19

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

TRA RISK MANAGEMENT E INTELLIGENCE ECONOMICA

- Un grande evento musicale (azione) movimenta un gran numero di persone, crea beneficio economico, produce esternalità positive sul territorio che lo ospita (settore alberghiero o commercio), ma porta implicazioni sul traffico locale, ordine pubblico, complicazioni medico sanitarie, esposizione ad attacchi terroristici etc. (reazione).
- Le tecnologie IOT, connettono tanti oggetti in rete favorendo comodità e funzionalità, ma produce nuove vulnerabilità cui ci si espone solo per essere connessi ad una rete, deve disporre in maniera continua di energia elettrica perché la tecnologia possa essere attiva

20

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

TRA RISK MANAGEMENT E INTELLIGENCE ECONOMICA

21

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

RESPONSABILITA' E RESPONSABILIZZAZIONE

- ❑ DECRETO 81
- ❑ 231/2001
- ❑ CIRCOLARE GABRIELLI
- ❑ GDPR
- ❑ NIS??

- ❑ RESPONSABILITA' AMMINISTRATIVE E PENALI IN CAPO AGLI AMMINISTRATORI/TITOLARI/ ORGANIZZATORI
- ❑ «BY DESIGN E BY DEFAULT» = DIMOSTRARE PRIMA DI AVVIARE UN PROCESSO, DI REALIZZARE UN EVENTO, DI ATTUARE UN TRATTAMENTO, DI ESSERE IN GRADO DI GESTIRE I RISCHI CHE DA QUESTA ATTIVITA' DOVESSERO GENERARSI
- ❑ RESPONSABILIZZAZIONE ECONOMICA DI CHI HA VANTAGGI ECONOMICI DALLO SVOLGERE INIZIATIVE POTENZIALMENTE GENERATRICI DI RISCHIO
- ❑ RISARCIMENTO ECONOMICO PER GLI ACCADIMENTI GENERATI DAL MANIFESTARSI DEL RISCHIO GENERATO DA QUELLA ATTIVITA'
- ❑ SANZIONI ECONOMICHE PER MANCATA COMPLIANCE

22

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

SECURITY MANAGEMENT
I 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.
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,

23

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

TRA SECURITY MANAGEMENT E INTELLIGENCE ECONOMICA

24

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

TRA SECURITY MANAGEMENT E INTELLIGENCE ECONOMICA

Il blackout ¿½ piombato nel pieno della iniziativa di Veltroni
In migliaia dormono nelle stazioni ferroviarie e della metro

Ore 3.30: stop alla "Notte bianca" 500.000 romani erano in strada

Il sindaco: Veltroni: "In citti¿½ una compostezza esemplare"
La prefettura: "La macchina dell'emergenza ha funzionato bene"

Il Colosseo al buio

ROMA - Gente accampata nelle stazioni della metropolitana e delle ferrovie. Semafori in tilt, macchine incolonnate. Centralini intasati. A Roma come a New York, insomma, durante il grande buio del 14 agosto scorso. In Italia non ¿½ l'ora di punta, ma nella capitale ¿½ come se lo fosse. Alle 3.30, quando in centinaia di migliaia ancora affollano la citti¿½ per assistere agli eventi previsti fino alle 6.30 del mattino, le luci si spengono sulla tanto attesa "Notte bianca". Cosi¿½, complice anche un violento temporale che si era abbattuto sulla citti¿½, la festa si ¿½ trasformata in caos.

Se la maggioranza dei cittadini italiani si sono accorti dell'interruzione di energia elettrica solo al mattino, moltissimi romani hanno invece vissuto lo stop "in diretta". Da settimane il Comune di Walter Veltroni aveva promosso, sul modello di quanto gli¿½ accade a Parigi, l'"apertura" straordinaria della citti¿½: negozi e musei aperti fino al mattino, spettacoli teatrali, mostre itineranti, locali, musica. Ed eccezionale era stata la risposta di capitolini, che in oltre un milione avevano preso d'assalto le strade e le piazze di Roma. Traffico in tilt, naturalmente, ma questo sembrava essere l'unico problema. Invece, ¿½ arrivato il blackout. Mentre ancora mezzo milione di persone erano in giro.

In migliaia, si ¿½ detto, sono rimasti bloccati e hanno perfino dormito nelle stazioni ferroviarie e in quelle del metropolitana, dove centinaia di passeggeri sono rimasti bloccati nei vagoni per quasi un'ora. Intanto, oltre 10.000 telefonate arrivavano alle sale operative, soprattutto dai telefoni cellulari di chi era in strada. Nel mezzo della "notte bianca", i romani che si erano mossi in automobile hanno ripreso la strada di casa, ma ai prevedibili problemi di traffico si ¿½ aggiunto il caos dovuto ai semafori fuori uso. Tra quelli che stavano rientrando a casa proprio al momento dello stop, un centinaio sono rimasti intrappolati negli ascensori, e sono stati "liberati" dai pompieri.

CRONACA 04/10/2021 18:36 CEST | Aggiornato 04/10/2021 20:54 CEST

Fb, Instagram e Whatsapp down. I social di Zuckerberg in tilt dal pomeriggio

Problemi di connessione in tutto il mondo dalle 17.30 di oggi. "Stiamo lavorando per riportare le cose alla normalità" fa sapere Facebook

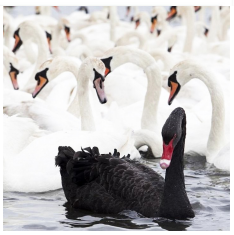
HuffPost

Facebook
@Facebook

We're aware that some people are having trouble accessing our apps and products. We're working to get things back to normal as quickly as possible, and we apologize for any inconvenience.

6:22 PM · 4 ott 2021 · Twitter Web App

31.231 Retweet **14.007** Tweet di citazione **93.943** Mi piace



TENDENZE

"Mi licenzio, basta compromessi". È l'anno d dimissioni (di S. Renda)

Ricciardi: "Rivedere il Gre Pass: concessione solo ai vaccinati, tampone è pun debole"

Il tribunale Ue toglie l'obl di Green Pass al Parlame

25

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

UNI ISO 31000

- Standard pubblicato il 13 Novembre 2009 (Norma internazionale) aggiornato 2018
- Recepisce ed implementa lo standard AS/NZS 4360:2004
- La Versione Italiana si completa con la Guida ISO 73:2009 (Vocabolario), e la ISO/IEC 31010:2009 (Gestione dei rischi –Tecniche di valutazione dei rischi)
- Strutturata in modo analogo ad altre norme ISO (ISO 9000, ISO 14000…)

26

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

UNI ISO 31000:2018

- La nuova versione tiene i concetti chiave rendendoli più chiari e quindi più fruibili. In particolare:
- Punta su Revisione ed aggiornamento dei principi di gestione del rischio come fattore critico di successo
- Da Maggiore enfasi alla leadership del top management ed all'integrazione della gestione del rischio nella governance dell'organizzazione
- Pone maggiore enfasi sull'importanza dell'interattività nella gestione del rischio
- Semplificazione i contenuti per rendere il modello di gestione dei rischi adatto a qualsiasi realtà
- Considera maggiormente gli aspetti positivi del rischio (opportunità), per l'innovazione e la crescita di ogni organizzazione.

27

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

RISK MANAGEMENT E ISO 31000: IL FRAMEWORK DI RIFERIMENTO

- è l'"hardware" all'interno della quale gireranno i vari software applicativi relativi al processo di gestione dei rischi
- È l' immagine copertina per gli stakeholder, l'organizzazione mostra come offre prodotti e servizi di qualità nel rispetto dei propri lavoratori, dell'ambiente e dei consumatori o fruitori.

ESEMPI

- Un Ente locale mostra come garantisce la sicurezza dei cittadini; una casa farmaceutica delle procedure messe in atto a garanzia dell'efficacia e a salvaguarda di medici infermieri e pazienti che utilizzano i suoi prodotti; un gruppo alimentare le politiche di qualità messe in atto a garanzia dei consumatori; una casa automobilistica deve dare sensazione di affidabilità e sicurezza nel guidare le proprie automobili etc.

28

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

RISK MANAGEMENT E ISO 31000: IL FRAMEWORK DI RIFERIMENTO

- La struttura di riferimento dell'organizzazione pone le fondamenta per tutte le sue componenti e gli stakeholders, identificando ed esplicitando la policy aziendale, gli obbiettivi il mandato l'impegno e le disposizioni organizzative che l'organizzazione mette in atto rispetto a:
  - Piani
  - Relazioni
  - Responsabilità
  - Risorse
  - Processi
  - Attività

29

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

RISK MANAGEMENT E ISO 31000: IL FRAMEWORK DI RIFERIMENTO

Contents

Introduction 4
J&J Strategic Framework 5
What is Risk? 7
J&J Approach to Enterprise Risk Management 8
Governance & Oversight 15
Conclusion 17

Our Credo

We believe our first responsibility is to the doctors, nurses and patients,
to mothers and fathers and all others who use our products and services.
In meeting their needs everything we do must be of high quality.
We must constantly strive to reduce our costs
in order to maintain reasonable prices.
Customers' orders must be serviced promptly and accurately.
Our suppliers and distributors must have an opportunity
to make a fair profit.

We are responsible to our employees,
the men and women who work with us throughout the world.
Everyone must be considered as an individual.
We must respect their dignity and recognize their merit.
They must have a sense of security in their jobs.
Compensation must be fair and adequate,
and working conditions clean, orderly and safe.
We must be mindful of ways to help our employees fulfill
their family responsibilities.
Employees must feel free to make suggestions and complaints.
There must be equal opportunity for employment, development
and advancement for those qualified.
We must provide competent management,
and their actions must be just and ethical.

We are responsible to the communities in which we live and work
and to the world community as well.
We must be good citizens–support good works and charities
and bear our fair share of taxes.
We must encourage civic improvements and better health and education.
We must maintain in good order
the property we are privileged to use,
protecting the environment and natural resources.

Our final responsibility is to our stockholders.
Business must make a sound profit.
We must experiment with new ideas.
Research must be carried on, innovative programs developed
and mistakes paid for.
New equipment must be purchased, new facilities provided
and new products launched.
Reserves must be created to provide for adverse times.
When we operate according to these principles,
the stockholders should realize a fair return.

Johnson&Johnson

30

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

RISK MANAGEMENT E ISO 31000: IL FRAMEWORK DI RIFERIMENTO

TABLE OF CONTENTS

Foreword
1. Introduction
2. What is Risk Management?
3. Risk Management Principles
4. The Approach to Managing Risks
5. The Risk Management Process
6. Roles and Responsibilities
7. Recording and Reporting Requirements
Appendices
Appendix 1 - SA Government Risk Management Policy Statement
Appendix 2 – DCSI Risk Management Policy
Appendix 3 - DCSI Risk Management Plan
Appendix 4 - Detailed Risk Management Process
Appendix 5 - Risk Categories and Potential Sources of Risk
Appendix 6 - DCSI Risk Assessment Matrix
Appendix 7 - DCSI Risk Escalation Flowchart
Appendix 8 - DCSI Risk Management Glossary

Risk Management Framework

Government of South Australia
Department for Communities and Social Inclusion

Foreword

The South Australian Government Risk Management Policy Statement 2009 advocates that consistent and systematic application of risk management is central to maximising community outcomes, deriving the benefit of opportunities, managing uncertainty and minimising the impact of adverse events.

Consistent with this policy the Department for Communities and Social Inclusion (DCSI) is committed to protecting itself, employees and others from situations or events that would prevent it from achieving its strategic goals and objectives. Risk management is an integral part of good management practice and the provision of safe workplace environments.

A systematic approach to managing risks and opportunities is more effective and efficient than allowing informal, intuitive processes to operate.

DCSI's adoption of a structured approach to risk management:

- defines a process for systematically managing the risk of all functions and activities in the organisation;
- encourages a high standard of accountability at all levels of the organisation;
- supports effective corporate and clinical governance systems and reporting mechanisms;
- encourages a high standard of efficient and effective client focused care and service delivery by taking advantage of opportunities for improvement; and
- allows the organisation to better meet its client and community demands.

It is everyone's responsibility to be involved in the identification, evaluation and treatment of risks and opportunities that could impact or influence outcomes for the organisation.

We trust this framework is useful in assisting you to integrate risk management into your role within the department.

31

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

- https://www.eni.com/it-IT/investitori/risk-management.html

32

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

RISK MANAGEMENT E ISO 31000: IL FRAMEWORK DI RIFERIMENTO

- Definisce la prima "risk inventory", elenco delle tipologie di rischi che incombono sull'Organizzazione, sulla base di esposizioni, minacce, vulnerabilità, oltre che danno/Impatto che si può generare.
- La risk inventory viene aggiornata con la ripetizione ciclica del processo di gestione, con modifiche intervenute nell'organizzazione e nei suoi processi, di carattere esogeno, conseguenza o interferenza di misure messe in atto per il trattamento di rischi precedentemente individuati.
- Può essere alimentata dall'analisi degli incidenti accaduti ma anche da segnalazioni di organismi istituzionali/indipendenti o osservatori di settore (es CERT (Computer Emergency Response Team"), Polizia, Istituto di Geofisica, Associazioni di categoria).

33

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

RISK MANAGEMENT E ISO 31000: IL FRAMEWORK DI RIFERIMENTO

- l'Organizzazione deve definire le sue politiche di gestione del rischio, i criteri di valutazione e di accettazione dei rischi, ovvero i parametri di riferimento per valutarne i possibili Danni/Impatti.
- Ogni organizzazione ha i suoi parametri, che devono tener conto delle sue peculiarità e delle strategie di lungo e breve termine; il lancio di un marchio piuttosto che la difesa della reputazione, la compliance di una norma o il lancio di un nuovo prodotto sul mercato.
- I criteri di valutazione e di accettazione definiti sono quelli che si andranno ad utilizzare nell'implementazione dei processi di valutazione e nella ponderazione dei rischi, rappresentando l'aspetto quanti/qualitativo della propensione al rischio dell'Organizzazione.

34

UNI ISO 31000:2010: LA STRUTTURA DI RIFERIMENTO PER LA GESTIONE DEL RISCHIO

- La politica, oggetto di comunicazione all'interno ed all'esterno dell'organizzazione, dovrebbe trattare i seguenti punti:
  - il fondamento logico dell'organizzazione per gestire il rischio
  - i legami tra gli obbiettivi dell'organizzazione, le sue politiche e la politica per la gestione del rischio;
  - i vari gradi di responsabilità;
  - il modo in cui sono trattati i conflitti d'interesse;
  - l'impegno a rendere disponibili le risorse necessarie per supportare coloro che hanno i vari gradi di responsabilità;
  - il modo in cui viene misurata e riferita la prestazione relativa alla gestione del rischio;
  - l'impegno a riesaminare e migliorare periodicamente, nonché in risposta ad un evento o ad un cambiamento di circostanze, la politica per la gestione del rischio e la struttura di riferimento.

35

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

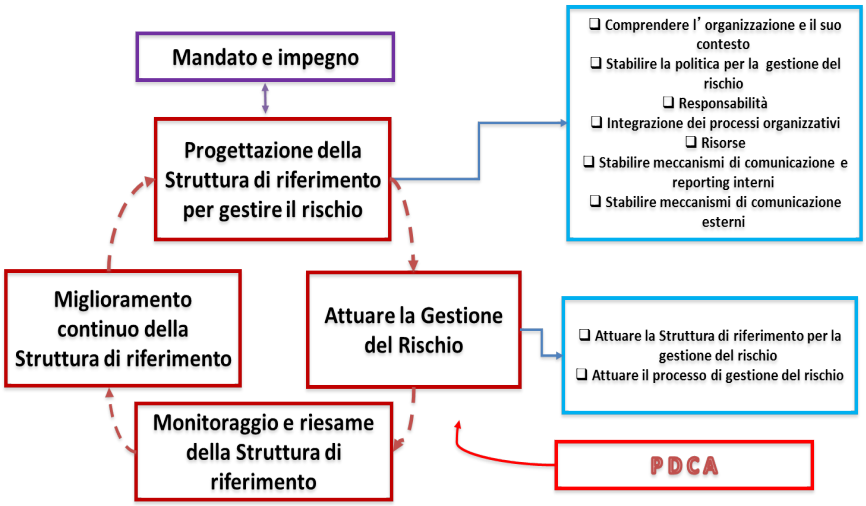
RISK MANAGEMENT E ISO 31000: IL FRAMEWORK DI RIFERIMENTO

- Sulla base degli obbiettivi e dei criteri di accettazione saranno effettuate le scelte strategiche di gestione del rischio da parte dell'organizzazione in merito a:
  - ✓ ELUSIONE O ELIMINAZIONE del rischio decidendo di non iniziare o non continuare l'attività che dà origine ad esso, oppure, ove possibile rimuovere la fonte (Minaccia) del rischio:
  - ✓ TRASFERIMENTO decidendo di trasferire o condividere tutto o parte del rischio con altra(e) parte(i) (contratti e finanziamento del rischio, assicurazioni, esternalizzazioni ecc);
  - ✓ TRATTAMENTO decidendo di investire in attività che permettano di ricondurre il rischio ai livelli ritenuti accettabili attraverso l'individuazione di contromisure (misure di riduzione) atte ad abbassare le probabilità di accadimento o le conseguenze (danni/impatti).
  - ✓ ACCETTAZIONE O RITENZIONE del rischio con una decisione formale ed informata nei casi in cui ciò non è escluso dalle leggi dai regolamenti o dalle obbligazioni assunte.

36

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

RISK MANAGEMENT E ISO 31000: IL FRAMEWORK DI RIFERIMENTO

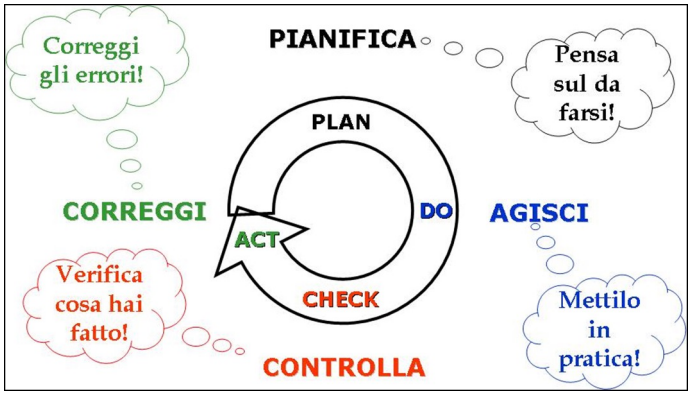


37

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

RISK MANAGEMENT E ISO 31000: IL CICLO DI DEMING

- ***Modello PDCA o Ciclo di Deming:*** strumento operativo molto utile nell'approccio processuale alla Security, che è anche alla base di qualsiasi sistema di gestione



38

RISK MANAGEMENT E ISO 31000: IL CICLO DI DEMING

PLAN

- ***La fase di pianificazione si pone l'obiettivo di fornire tutti gli elementi necessari per:***
  - ***Predisporre una concreta programmazione delle attività di sicurezza***
  - ***Definire gli obiettivi di sicurezza che l'azienda intende perseguire***
  - ***Calcolare il livello di rischio cui le risorse risultano esposte***
  - ***Gestire le opzioni applicabili al rischio residuo***

39

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

RISK MANAGEMENT E ISO 31000: IL CICLO DI DEMING

DO

- ***La fase di implementazione prevede:***
  - ***L'attuazione delle decisioni e delle soluzioni individuate nella fase di pianificazione***
  - ***L'implementazione delle contromisure fisiche, logiche e organizzative***
  - ***La predisposizione degli strumenti tecnici e procedurali atti a rilevare ed analizzare quegli eventi che impattano sulla sicurezza, e che saranno oggetto della fase di verifica e monitoraggio***

40

RISK MANAGEMENT E ISO 31000: IL CICLO DI DEMING

CHECK

- ***La fase di verifica e monitoraggio prevede la valutazione/misurazione delle prestazioni del sistema di gestione, attraverso:***
  - ***La pianificazione di audit periodici***
  - ***Il monitoraggio continuo dell'efficacia delle misure di sicurezza***
  - ***L'investigazione a fronte di incidenti***
  - ***L'analisi dei cambiamenti del contesto di riferimento***

41

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

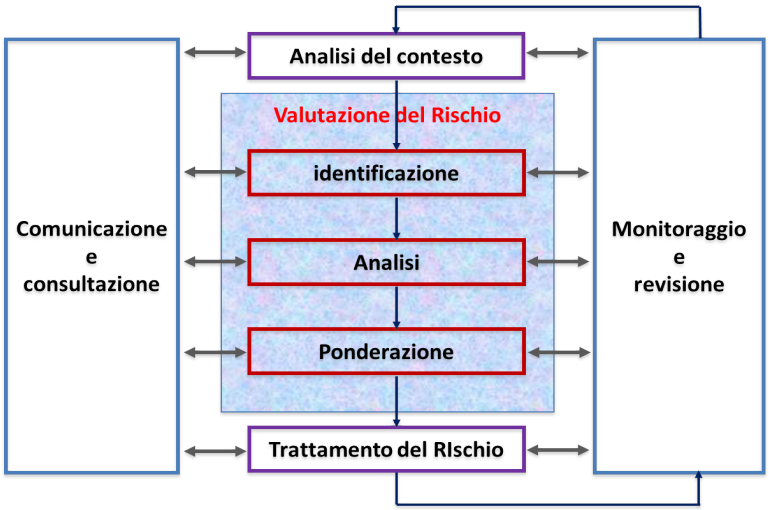
RISK MANAGEMENT E ISO 31000: IL CICLO DI DEMING

ACT

- ***La fase di correzione/miglioramento prevede, sulla base dei risultati delle valutazioni effettuate nel check, l'esecuzione di:***
  - ***Azioni preventive e correttive, in caso di inefficienze***
  - ***Attività volte alla standardizzazione del processo***

42

RISK MANAGEMENT E ISO 31000: IL PROCESSO DI GESTIONE



43

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

UNI ISO 31000:2010: IL PROCESSO DI GESTIONE - TERMINI E DEFINIZIONI

- **Analisi di contesto:**
  - si individuano gli obbiettivi dell'organizzazione, i parametri del contesto interno ed esterno in cui opera per la definizione del processo di gestione del rischio

44

UNI ISO 31000:2010: IL PROCESSO DI GESTIONE - TERMINI E DEFINIZIONI

- Il Contesto Esterno,
  - E' l'ambiente esterno nel quale l'organizzazione cerca di conseguire i propri obbiettivi (culturale, sociale, politico, cogente, finanziario, tecnologico, economico, naturale e competitivo, regionale o locale, internazionale o nazionale),
  - E' il contesto in cui si gestiscono le relazioni con i portatori di interesse (stakeholders) esterni; gli elementi determinanti e le tendenze fondamentali che hanno un impatto sugli obiettivi dell'organizzazione.

45

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

UNI ISO 31000:2010: IL PROCESSO DI GESTIONE - TERMINI E DEFINIZIONI

- Il Contesto Interno,
  - Ambiente interno nel quale l'organizzazione cerca di conseguire i propri obbiettivi attraverso la propria Governance, struttura organizzativa, ruoli e responsabilità; politiche, obbiettivi e strategie adottati per conseguirli;
  - capacità, risorse e conoscenza (capitale, tempo, persone, processi, sistemi e tecnologie);
  - sistemi informativi, flusso di informazioni e processi decisionali (formali e informali); relazioni con i portatori d'interesse interni,
  - cultura dell'organizzazione; norme, Linee Guida e modelli adottati; relazioni contrattuali.

46

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

RISK MANAGEMENT E ISO 31000: IL PROCESSO DI GESTIONE

- il processo di gestione è identificativo del software che gira dentro quella macchina e che le permette di funzionare, alimentarsi ed aggiornarsi
- Si inizia con l'acquisire quelle informazioni strategiche finalizzate a comprendere il contesto, per poi:

1. mappare i rischi
2. analizzare rischi e definirne la magnitudo
3. definire le azioni per il trattamento

47

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

UNI ISO 31000:2010: IL PROCESSO DI GESTIONE - TERMINI E DEFINIZIONI

- **Risk assessment/Valutazione del rischio:**
  - **si realizza tramite:**
    1. **Identificazione del rischio: individuazione, riconoscimento e descrizione (cause, conseguenze – con dati storici, analisi teoriche, opinioni etc.)**
    2. **Analisi del rischio: si creano le basi per la valutazione, inquadramento natura e livello del rischio – decidere come trattarlo, stima del rischio.**
    3. **Ponderazione del rischio: dai risultati dell'analisi a confronto con i criteri di rischio definiti dall'organizzazione si stabilisce se il rischio a seconda della magnitudo è tollerabile o meno.**

48

UNI ISO 31000:2010: IL PROCESSO DI GESTIONE - TERMINI E DEFINIZIONI

LA VALUTAZIONE DEL RISCHIO

- La classificazione del rischio può essere quantitativa, semi-quantitativa o qualitativa in termini di probabilità di accadimento/ o possibili conseguenze/ o impatto.
- Le organizzazioni dovranno definire le proprie misure di probabilità di accadimento e conseguenze e usano spesso valutazioni del tipo "alto, medio o basso"
- a seconda di tipologia e complessità presentano e analizzano i risultati con matrici di rischio 3 x 3 o 4 x 4 o 5x 5.
- Considerando la probabilità e le conseguenze di ogni rischio, danno la priorità o classificare i principali rischi per l'ulteriore analisi.

49

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

UNI ISO 31000:2010: IL PROCESSO DI GESTIONE - TERMINI E DEFINIZIONI

LA VALUTAZIONE DEL RISCHIO

- Di ogni va determinata natura, origine o tipo di impatto attraverso un sistema di classificazione dei rischi.
- non esiste un sistema di classificazione del rischio che sia universalmente applicabile a tutti i tipi di organizzazione.
- Ci sono molti sistemi di classificazione del rischio a disposizione e se ne adotta uno a seconda dalla dimensione, natura e complessità dell'organizzazione.
- La ISO 31000 non raccomanda un sistema di classificazione del rischio specifico ed ogni organizzazione necessiterà di sviluppare il sistema più opportuno in base alla gamma dei rischi che deve affrontare.

50

RISCHIO COME CONCOMITANZA DI ELEMENTI: IL FILO LOGICO

- la "minaccia", intesa come possibilità che venga tentato un attacco o avvenga un incidente o si manifesti un evento naturale (es. terremoto, temporale, attentato, furto etc.),
- la "minaccia" può insistere su di una "esposizione", intesa come quantità misurabile di bene materiale o immateriale potenzialmente soggetto al danno (n. di abitanti, ettari di bosco, n. di vetture, terabyte di dati etc.)
- la "minaccia" sfrutta, ovvero si avvale della debolezza, di una o più "vulnerabilità" di una organizzazione, inducendo il generarsi di un "danno",
- La minaccia, in presenza di una vulnerabilità espone l'Organizzazione al "rischio" riducendone la sua "sicurezza".

51

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

RISCHIO COME CONCOMITANZA DI ELEMENTI: IL FILO LOGICO

- La relazione tra esposizione, minaccia e vulnerabilità genera il rischio che può concretizzarsi in danno.
- un pavimento di 100 metri quadri a parquet di un ufficio è una esposizione, ma l'ufficio non è automaticamente soggetto ad un rischio esplicito;
- la pioggia in sé è una minaccia ma non necessariamente sfocia in un danno;
- una crepa sul tetto è una vulnerabilità ma non per forza genera un allagamento.
- Il rischio di allagamento può generare un danno quando il parquet o parte di esso è esposto alla minaccia pioggia che incontra la vulnerabilità data dalla crepa sul tetto.

52

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

RISK MANAGEMENT E ISO 31000: IL PROCESSO DI GESTIONE
LA MISURAZIONE DEL RISCHIO

- ***Rischio:*** **il rischio è l'effetto di fattori interni ed esterni e di altre influenze che rendono incerto il raggiungimento degli obiettivi delle organizzazioni (di ogni tipo e dimensione). Il rischio è spesso espresso come combinazione degli effetti di un evento e le probabilità associate di accadimento.**

R = P X D

R= rischio P= probabilità D= danno economico

↓

Magnitudo del singolo rischio

↓

Scala delle priorità

53

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

RISK MANAGEMENT E ISO 31000: IL PROCESSO DI GESTIONE
LA MISURAZIONE DEL RISCHIO

- La ***probabilità di accadimento*** a sua volta è funzione della frequenza e della vulnerabilità

P = F(f ;V)

P= probabilità **f**= frequenza **V**= vulnerabilità

↓ ↓

È funzione di:
- **Accadimenti precedenti**
- **Efficacia misure implementate**

È funzione di:
- **Grado adeguatezza procedure**
- **Grado efficienza tecnologie**
- **Grado adeguatezza risorse umane**

54

RISK MANAGEMENT E ISO 31000: IL PROCESSO DI GESTIONE
LA MISURAZIONE DEL RISCHIO

MISURE PASSIVE

Qualunque dispositivo/manufatto che ritarda l'effettuazione del danno attinente il rischio, fornendo quindi un tempo utile per attuare contromisure (strutture e muri, recinzioni, reti, inferriate e cancellate, porte e finestrature, vetri antisfondamento, mezzi forti e di custodia, armadi blindati e corazzati, casseforti a muro e a mobile provviste di serrature singole/doppie, locali di sicurezza e corazzati, ecc.)

Queste, essendo difese fisiche e strutturali, non danno segnalazioni di allarme ma servono per ritardare il tempo di attacco e di superamento delle stesse barriere

55

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

RISK MANAGEMENT E ISO 31000: IL PROCESSO DI GESTIONE
LA MISURAZIONE DEL RISCHIO

MISURE ATTIVE

Le misure attive, o elettroniche, sono le tecnologie basate principalmente sull'elettronica e gestite da una centrale di acquisizione allarmi, che danno una segnalazione di allarme, senza opporsi fisicamente ad attacchi o effrazioni, e quindi sono elemento fondamentale per attivare tempestivamente le contromisure all'evento (sensori volumetrici e a infrarossi, per esterno e per interno, microonde, sistemi interrati, varie tipologie di sistemi di allarme perimetrale, sistemi antitaccheggio, ecc.)

56

RISK MANAGEMENT E ISO 31000: IL PROCESSO DI GESTIONE
LA MISURAZIONE DEL RISCHIO

MISURE ORGANIZZATIVE

Le misure organizzative sono tutte quelle che presuppongono azioni o interventi finalizzati ad evitare il danno conseguente al rischio trattato (norme e procedure, comportamenti e precauzioni, istruzioni e divieti, corsi di informazione e formazione, piano e procedure di intervento emergenza, organizzazione di primo soccorso e intervento, comunicazione e gestione dello stato di emergenza, coinvolgimento delle Forze esterne, gestione dello sfollamento e dell'evacuazione, ecc.)

57

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

UNI ISO 31010 LE TECNICHE DI VALUTAZIONE

1. Brainstorming
2. Interviste strutturata o semi strutturata
3. Metodo Delphi
4. Metodo con le Checklist
5. Analisi preliminare dei rischi (PHA)
6. Hazard and operability study (HAZOP)
7. Hazard analysis and critical control points (HACCP)
8. Valutazione della tossicità
9. Tecnica strutturata "What If"
10. Analisi degli scenari
11. Analisi dell'impatto di business
12. Analisi della radice delle cause
13. Failure mode and effects analysis (FMEA)
14. Analisi dell'albero degli errori
15. Analisi dell'albero degli eventi
16. Analisi causa e conseguenze
17. Analisi causa ed effetto
18. Analisi degli strati di protezione (LOPA)
19. Albero delle decisioni
20. Analisi dell'affidabilità umana (HRA)
21. Analisi della cravatta a farfalla
22. Manuntenzione dell'affidabilità centrata
23. Analisi dei circuiti nascosti
24. Analisi di Markov

58

UNI ISO 31010 LE TECNICHE DI VALUTAZIONE

IMPATTO DELLE MISURE RILEVATE SU VULNERABILITA	TOLLERANZA ORGANIZZAZIONE
FREQUENZA IRRILEVANTE= 1 0<INC≤1	
FREQUENZA BASSA= 2 1<INC≤2	
FREQUENZA MEDIA= 3 2<INC≤3	
FREQUENZA ALTA= 4 3<INC≤5	
FREQUENZA ALTISSIMA 5 5<INC	

DANNO ECONOMICO DA RISCHIO ALLAGAMENTO	
50	PERDITA VALORI DETENUTI AL NETTO DI COPERTURE ASSICURATIVE
5	RIPRISTINO
5	IMMAGINE
10	FERMO ATTIVITA PER INDISPONIBILITA LOCALI
70	TOTALE DANNO POTENZIALE

TABELLA DI VALORIZZAZIONE DANNO DA ALLAGAMENTO				
CLASSIFICAZIONE	CONSISTENZA	QUANTIFICAZIONE RISCHIO DA FURTO	QUANTIFICAZIONE RISCHIO DA ALLAGAMENTO	VALORIZZAZIONE
C	CATASTROFICO	79≤C≤130	43≤C≤70	5
A	ALTO	53≤A≤78	29≤A≤42	4
M	MEDIO	27≤M≤52	15≤M≤28	3
B	BASSO	14≤B≤26	8≤B≤14	2
NS	NON SIGINIFICATIVO	0≤NS≤13	0≤NS≤7	1

	VULNERABLITA	FREQUENZA	PROBABLITA
T0 (PRE PROPOSTA	4	3	4
T1 (POST PROPOSTA)	3	3	3

	MISURA T0			STIMA T1			MISURA T2		
FREQUENZA	N. MEDIO ANNUO ACCADIMENTI AZIENDALI ULTIMI 5 ANNI	N. ANNUO ACCADIMENTI MEDI SETTORE ULTIMI 5 ANNI	FREQUENZA T0	STIMA EFFICACIA LOGICA ACCADIMENTI AZIENDALI RISULTATO ATTESO PIANO TRATTAMENTO	N. ACCADIMENTI MEDI SETTORE ULTIMI 5 ANNI	FREQUENZA T1	N. ACCADIMENTI AZIENDALI ULTIMI 5 ANNI	N. ACCADIMENTI MEDI SETTORE ULTIMI 5 ANNI	FREQUENZA T2
ACCADIMENTO RISCHIO 1	3	3	3	0	3	0,9	1	2	1,3
PESO	0,7	0,3		0,7	0,3		0,7	0,3	

59

RISK MANAGEMENT E ISO 31000: IL PROCESSO DI GESTIONE
LA MISURAZIONE DEL RISCHIO

- ***Trattamento del rischio:*** processo per modificare il rischio:
  - **evitare il rischio decidendo di non iniziare o non continuare l'attività che dà origine ad esso;**
  - **assumere o aumentare l'esposizione al rischio al fine di cogliere un'opportunità;**
  - **rimuovere la fonte di rischio;**
  - **condividere il rischio con altra (e) parte (i) compresi contratti e finanziamento del rischio;**
  - **ritenere il rischio con una decisione informata aumentando il livello delle misure di prevenzione e protezione.**

60

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

RIPARTIZIONE PER FASI TEMPORALI			TIPOLOGIA DI RISCHIO	RIPARTIZIONE PER RESPONSABILITA'		
COMPLETAMENTO	OPERATIVITA'	COMUNE		PUBBLICO	PRIVATO	COMUNE
X			Finanziamento		X	
X			Progettazione			X
X			Costruzione		X	
		X	Incapacità di realizzazione		X	
X			Errata valorizzazionedell'area ceduta come corrispettivo in natura		X	
		X	Politico e amministrativo	X		
X			Stima non corretta dei costi per l'approvazione del progetto tecnico-architettonico		X	
	X		Rischio di Manutenzione		X	
	X		Rischio di Disponibilità		X	
	X		Rischio di Gestione		X	
	X		Rischio di Domanda			X
		X	Rischio finanziario			X
	X		Rischio di completamento		X	
X			Rischio di interruzione o abbandono		X	
	X		Rischio di gestione		X	
		X	Rischio di fornitura		X	
		X	Rischio di superamento dei costi		X	
		X	Rischio di mercato		X	
		X	Rischio di forza maggiore		X	
X			Errore di costruzione		X	
X			Stima errata dei costi o dei tempi		X	
		X	Forza maggiore			X
		X	Modifiche legislative e regolatorie			X
		X	Modifiche della imposizione fiscale		X	
		X	Cattivo project management da parte della società di progetto		X	
	X		Azione sindacale da parte dei dipendenti dell'appaltatore o sub appaltatore		X	
		X	Azione di dimostranti	X		
		X	Performance dei sub appaltatori		X	
X			Insolvenza dell'appaltatore o dei sub appaltatori		X	
	X		Disponibilità delle strutture		X	
	X		Stima errata dei costi		X	
	X		Stima errata del costo del trasferimento del personale da un soggetto giuridico a un altro			X
	X		Stima errata dei costi di riqualificazione del personale che fornisce i sevizi previsti in contratto		X	
	X		Bassa performance dei servizi		X	
	X		Obsolescenza dell'asset		X	
	X		Cambiamenti nella tecnologia		X	

61

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

IL PROFESSIONISTA DELLA SECURITY

Considera l'effetto del rischio sulla componente economica del patrimonio tangibile ed intangibile dell'azienda

Individuare tutte le fonti di pericolo e ne valuta la possibile incidenza;

Gestione delle conseguenze da eventi aleatori di tipo economico, finanziario e patrimoniale dell'Azienda

Elimina alla fonte i fattori di rischio o almeno prova a ridurli;

Predispone tutte le attività necessarie per ottemperare alla vigente normative in materia di salute e sicurezza nei luoghi di lavoro.

Programmare ed attuare i necessari percorsi di informazione e formazione sui rischi;

Qualora il rischio non sia eliminabile, deve fornire adeguati dispositivi di protezione, anche individuale ai singoli lavoratori esposti;

62

SECURITY E INTELLIGENCE: SICUREZZA E COMPETITIVITA'

63

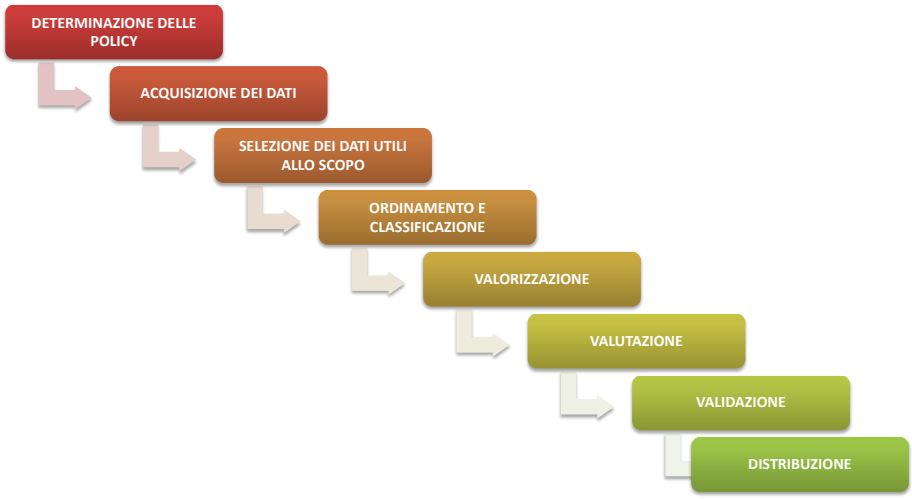
UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL PROCESSO DI INTELLIGENCE

64

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

IL PROCESSO DI INTELLIGENCE



65

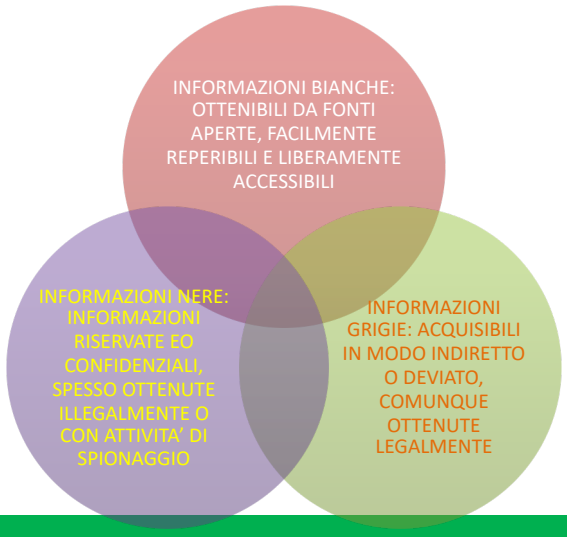
UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL PROCESSO DI INTELLIGENCE: LE FONTI

66

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

IL PROCESSO DI INTELLIGENCE: LE INFORMAZIONI



67

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

IL PROCESSO DI INTELLIGENCE: L'AQUISIZIONE DEI DATI

HUMINT (HUMan INTelligence)

IMINT (IMagery INTelligence): raccolta e analisi di immagini aeree o satellitari

68

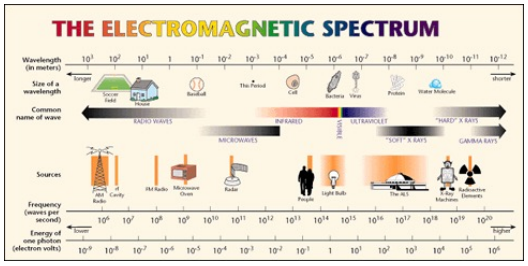
UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

IL PROCESSO DI INTELLIGENCE: L'AQUISIZIONE DEI DATI

MASINT (MeAsurement and Signature INTelligence)

Integrazione di funzioni sensoriali (elettriche, dinamiche, radioattive, elettromagnetiche)

finalizzata a prevenzione e intercettazione di obbiettivi



69

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

IL PROCESSO DI INTELLIGENCE: L'AQUISIZIONE DEI DATI

SIGINT (SIGnal INTelligence)

Spionaggio di segnali elettronici

COMINT (COMmunication INTelligence)

Intercettazione di comunicazioni verbali e scritte

ELINT (ELectronic INTelligence)

analizza tendenzialmente segnali radar (intercettazione posizione di batterie missilistiche rotte aeree etc.).

70

IL PROCESSO DI INTELLIGENCE: L'AQUISIZIONE DEI DATI

OSINT (Open Source INTelligence).

Raccolta informazioni di pubblico accesso

Mezzi di comunicazione — giornali, riviste, televisione, radio e siti web.

Dati pubblici — report governativi, economico finanziari, dati demografici, dibattiti legislativi, conferenze stampa, discorsi, avvisi aeronautici e marittimi.

Osservazioni dirette — fotografie di piloti amatoriali, ascolto di conversazioni radio e osservazione di fotografie satellitari.

71

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

IL PROCESSO DI INTELLIGENCE: LA TECNOLOGIA A SUPPORTO

1. Acquisizione, archiviazione, elaborazione e analisi delle informazioni
2. Semantic Analysis
3. Web Analysis
4. Network Analysis
5. Localizzazione utenti telefonici
6. Elaborazione immagini (Riconoscimento facciale, pacchi sospetti, incidenti, intrusioni)
7. Tracciabilità flussi finanziari

72

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

DA INTELLIGENCE "TRADIZIONALE" A INTELLIGENCE ECONOMICA

73

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

DA INTELLIGENCE "TRADIZIONALE" A INTELLIGENCE ECONOMICA

- Si stravolge ogni vecchia alleanza
- l'alleato in campo militare può essere il peggior "nemico" nell'attingere informazioni strategiche della propria economia e Industria.
- Stati e aziende ricercano vantaggi competitivi o concentrati sulla difesa dallo spionaggio economico del proprio capitale scientifico ed intellettuale.

74

I BENEFICI DELL'INTELLIGENCE ECONOMICA

- la destinazione del beneficio offerto apre alla dicotomia intelligence "istituzionale" - intelligence "aziendale" unite dalla tutela degli interessi economici, scientifici e industriali.
- Istituzionale al servizio dei governi con mission e sfera d'azione direttamente correlati ai fini ultimi che questi si pongono, con beneficio collettivo la sicurezza e competitività economica nazionale.
- La Aziendale sfrutta il beneficio collettivo, e persegue un proprio beneficio "individuale".

75

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

L'INTELLIGENCE ECONOMICA "ISTITUZIONALE"

- Quando è il Governo a commissionare i prodotti informativi:

1. il controllo delle attività dei servizi di intelligence estera e attività clandestine dirette contro i loro interessi economici e commerciali;
2. la tutela dei reati contro la competitività del Sistema Paese;
3. il supporto alle decisioni strategiche di tipo economico-finanziario;
4. la verifica del rispetto degli accordi internazionali, supporto agli accordi commerciali, tutela delle aziende nazionali da pratiche commerciali sleali, corruzione etc.,
5. l'attività di influenza e condizionamento di eventi, comportamenti e politiche di Paesi esteri;
6. la ricerca di informazioni sensibili relative ad aspetti commerciali, organizzativi e tecnologia, per favorire la competitività di aziende nazionali.

76

L'INTELLIGENCE ECONOMICA "AZIENDALE"

- Le aziende, possono sfruttare il beneficio collettivo e mettere in atto proprie attività internamente, o rivolgendosi a servizi di intelligence privata.
- Devono limitarsi quasi esclusivamente alle sole fonti aperte, per il supporto delle decisioni strategiche aziendali relative a produzione, vendite, marketing etc.

- Le informazioni utili sono sostanzialmente quelle relative a:
  - nuovi mercati di approvvigionamento o di sbocco nazionale ed estero;
  - fornitori e clienti nazionali ed esteri;
  - propri competitors nazionali ed esteri.
  - trend in atto, analisi di scenario e prospettiva.

77

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

IL BENEFICIO ECONOMICO DELL'INFORMAZIONE

- Il reperimento dell'informazione cosi come il suo uso possono avere vocazione difensiva come competitiva, ai limiti dello spionaggio con le dovute conseguenze amministrative e penali del caso.
- migliore è la qualità dell'informazione e potenzialmente più efficace sarà la decisione strategica ad essa conseguente, seppur non sempre vi sia una correlazione diretta, ed in nessun caso la decisione strategica è "obbligata" al risultato della attività di intelligence.
- Il beneficio economico, può essere frutto dei maggiori introiti derivanti da operazioni messe in atto da governi ed imprese nazionali, piuttosto che dei costi risparmiati a seguito di azioni competitive o lesive della leale concorrenza da parte di Governi ed imprese estere o da operazioni di spionaggio economico.

78

IL BENEFICIO ECONOMICO DELL'INFORMAZIONE

- Ne consegue che le informazioni ottenute ed elaborate hanno un valore economico oltre che commerciale che deve tener conto:
  - del costo di ricerca ed elaborazione;
  - della sua collocazione temporale;
  - del beneficio economico arrecato alla singola impresa o al Sistema Paese.
- Dato il valore economico generabile, alcuni vedono nell'informazione fornita dai servizi di informazione di uno Stato ad alcune imprese, una forma di sussidio pubblico.

79

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

IL MALEFICIO ECONOMICO DELL'INFORMAZIONE

- Lo spionaggio economico è certamente il tema più caldo delle attività di intelligence, con Stati ed aziende talvolta vittime e altre volte protagonisti.
- Le nazioni più innovative portatrici di capitale intellettuale ed innovazione tecnologica sono quelle più esposte
  - Gli Stati Uniti sono quelli che maggiori risorse impegnano sulla controingerenza.
- Le aziende che beneficiano dell'opera di spionaggio risparmiano sugli investimenti in ricerca e sviluppo, ma il danno sistemico arrecato a Stai ed imprese, sarà sempre superiore al beneficio generato.

80

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

L'INTELLIGENCE ECONOMICA "ISTITUZIONALE"

- i passaggi di informazione passavano per mano di dipendenti o ricercatori complici; l'uso oramai universale della rete ha aperto allo spionaggio elettronico, aprendo alla cyber war.
- Gli importi dei danni causati agli Stati dalle azioni di spionaggio economico sono sempre frutto di interpretazioni e stime, ma di difficile quantificazione.
- L'Ufficio Scienze e Tecnologia della Casa Bianca aveva stimato un danno solo per l'economia americana di oltre 100 miliardi all'anno. La Banca Mondiale afferma che, su un "Prodotto Interno lordo" (PIL) globale di circa 70 miliardi di dollari nel 2001, circa 400 milioni di dollari sono stati persi a causa di atti di cyber crime.

81

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

IL FABBISOGNO DI INTELLIGENCE ECONOMICA:

- Nel contesto italiano sono tendenzialmente le grandi imprese ad avere conoscenza e coscienza dell'Intelligence Economica, sconosciuta invece o del tutto ignorata da parte delle piccole e medie imprese. Va però considerato che le piccole e medie imprese, rappresentano il 99% del tessuto produttivo, di cui il 94,4% è costituito da microimprese.
- Anche nelle grandi però, è difficile individuare, uffici o aree preposte alla intelligence economica; se ne trova piuttosto traccia in attività riconducibili al marketing strategico, o tra le funzioni di security, o su outsourcing ad agenzie o studi di intelligence privata.

82

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

L'APPORTO DEL PROFESSIONISTA DELLA SECURITY ALL' INTELLIGENCE ECONOMICA: VIGILANZA SU COMPETITIVITA' AZIENDA

- Corretto andamento bandi di gara
- Analisi di clienti e fornitori
- Monitoraggio Antifrode
- Spionaggio Industriale
- Compliance
- Sicurezza delle Comunicazioni Aziendali
- Protezione dei dati Aziendali
- Protezione del Know How
- Travel Security
- E-reputation
- Web&social network analysis

83

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

L'APPORTO DEL PROFESSIONISTA DELLA SECURITY ALL' INTELLIGENCE ECONOMICA: PREVENIRE E GESTIRE LE CRISI PER MITIGARNE O ELIMINARNE I COSTI

- Operazioni di emergenza
- Ritiro prodotto
- Crollo del titolo in borsa
- Rimborso vittime
- Comunicazione
- Spese legali
- Esperti e consulenti
- Produzione/distribuzione
- Recupero quote di mercato/spazi espositivi
- Ricostruzione immagine
- Campagne informative
- Investimenti pubblicitari

84