Treviso 25.03.2025

Prof. Gianluigi Lucietto

SETTIMANA DELLA SOSTENIBILITÀ

25-28 MARZO 2025

Come si protegge il futuro? il ruolo del risk management nel governo delle PMI

Avete letto il contenuto della locandina che vi dovrebbe aver convito a partecipare?

Nel **governo "proattivo"** dei rischi aziendali insiste **una leva** di vantaggio competitivo eccezionale per qualsiasi azienda. Se non viene colta ed interiorizzata dalla cultura e dalle strategie aziendali, l'implementazione di qualsiasi processo, sistema o presidio organizzativo di un'attività di risk management verrà però percepito in azienda come un mero "costo", come qualsiasi altro obbligo o adempimento.

La cultura e la strategia aziendale divengono pertanto centrali per affrontare anche il tema del risk management. E' dalla visione dell'organo amministrativo che si deve partire per iniziare ad immaginare la possibile innervatura, all'interno di una organizzazione, di un adeguato sistema di gestione dei rischi. La sfida culturale ed organizzativa investe soprattutto le PMI, nel mondo volatile ed incerto in cui viviamo: organizzazioni spesso de-strutturate o con risorse limitate. Il seminario intende esplorare il significato ed il ruolo nelle PMI del risk management, nonché fornire idee e spunti per concrete e fattive implementazioni organizzative.

Oggi parleremo di…

governo … ruoli … ~~risk management~~ … gestione dei rischi … leve…cultura … strategie … implementazioni organizzative …

… Ma lo faremo in modo diverso

Iniziamo da voi…

- Chi di voi opera in Area IT?
- Chi di voi opera in Area Finanza?
- Chi di voi opera in Area Salute e Sicurezza?
- Chi di voi opera a contatto con qualcuno dell'Area Produzione?
- Chi di voi è nella forma considerato uno specialista in Azienda?
- Chi di voi è considerato uno specialista nella sostanza in Azienda?
- Chi di voi ritiene di essere poco considerato in Azienda dal Top Management?

Chi di voi è «lo specialista» dell'azienda?

Forse è Bill?

… o forse no.
Ma una cosa è certa…

per me <u>ognuno di voi</u> è uno specialista nel suo ambito operativo!

perché lo posso affermare <u>con certezza</u>?

Chi di voi è lo specialista dell'azienda?

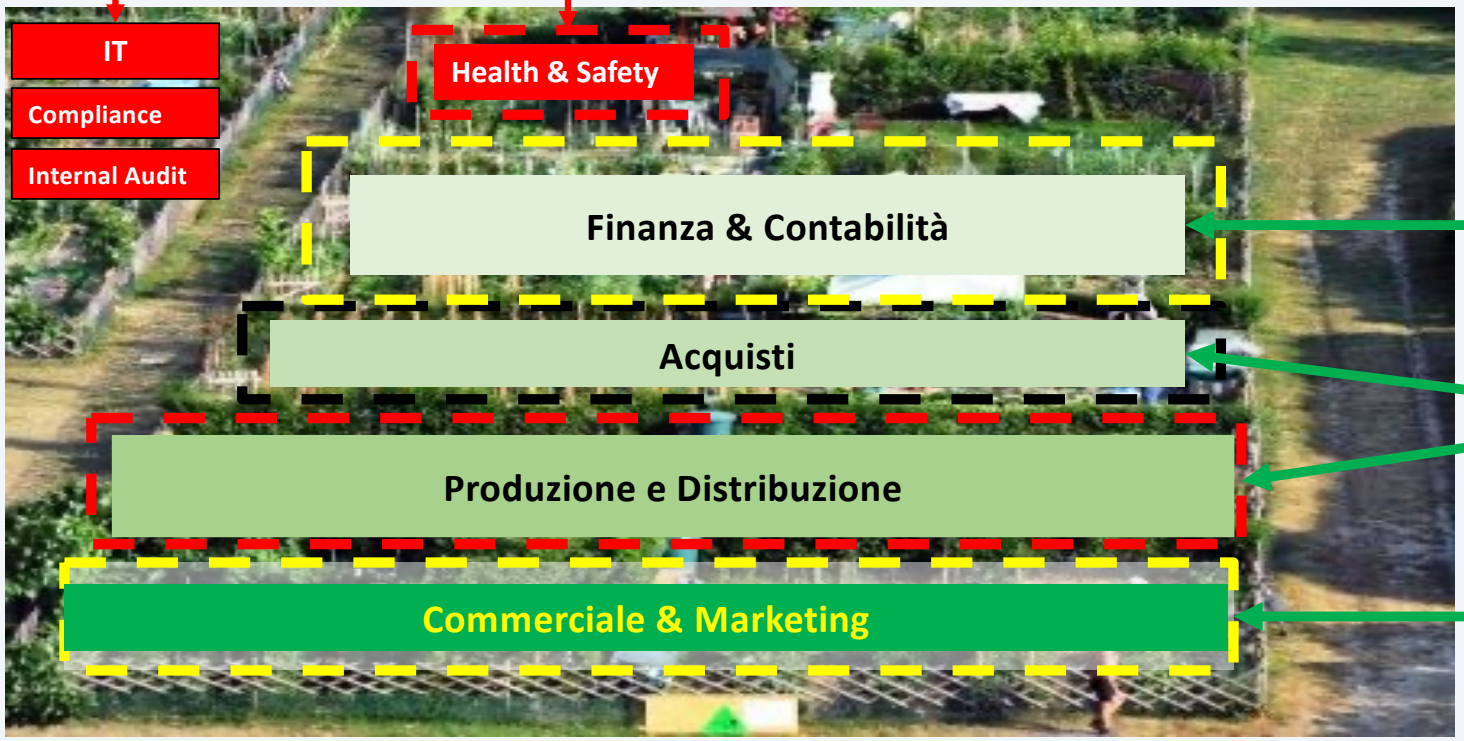
≅ 420.000 imprese

Più del 90% sono micro, piccole e medie imprese

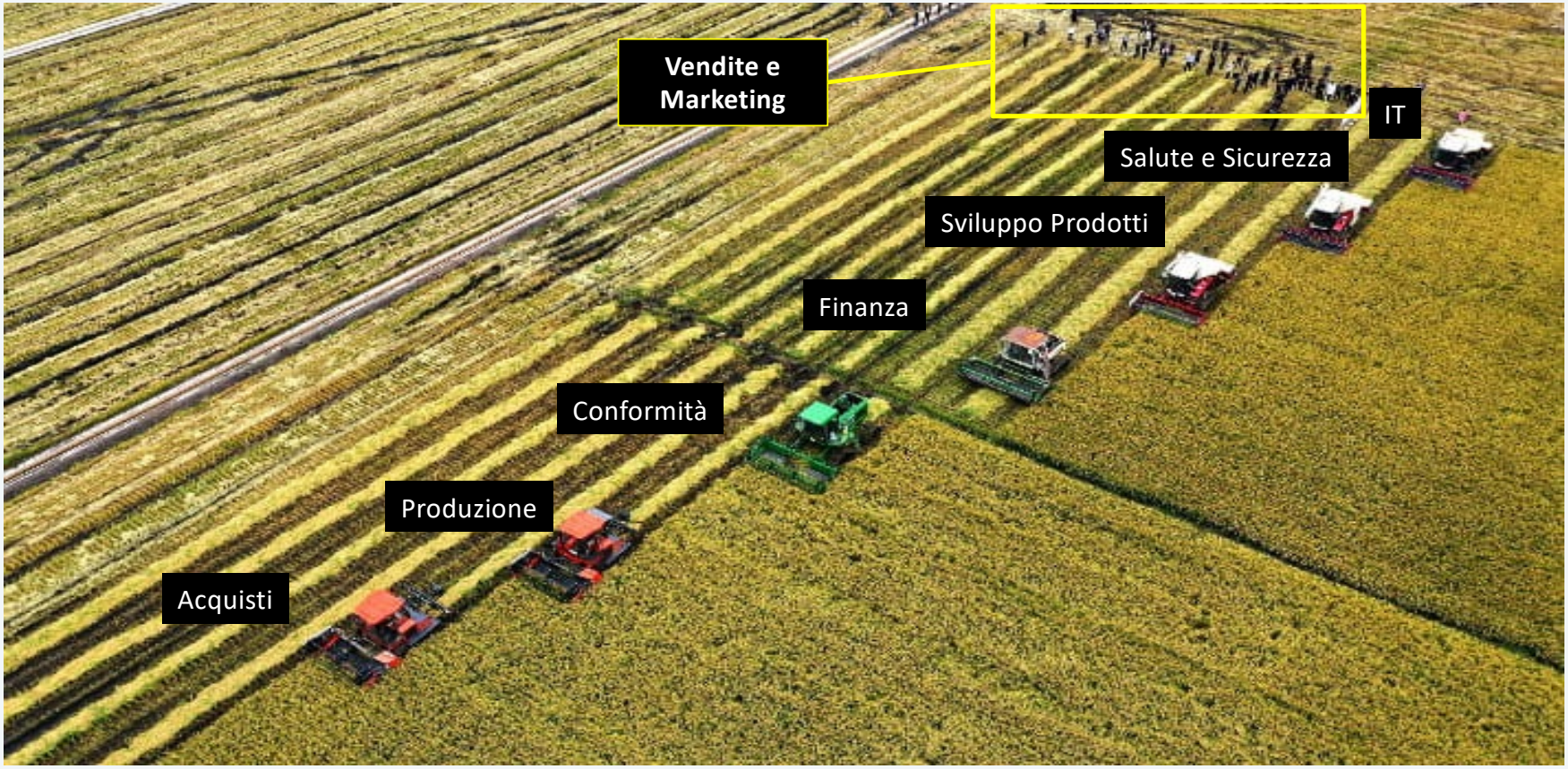
… e come si vedono?

Come si vede l'azienda…

Come è l'azienda «silos» - (senza approccio integrato)



Come dovrebbe essere l'azienda - (integrata)



Perché vi considero «specialisti»?

Cambiamo punto di vista e proviamo con un paradigma in ambito medico…

Come avviene l’accesso in Ospedale

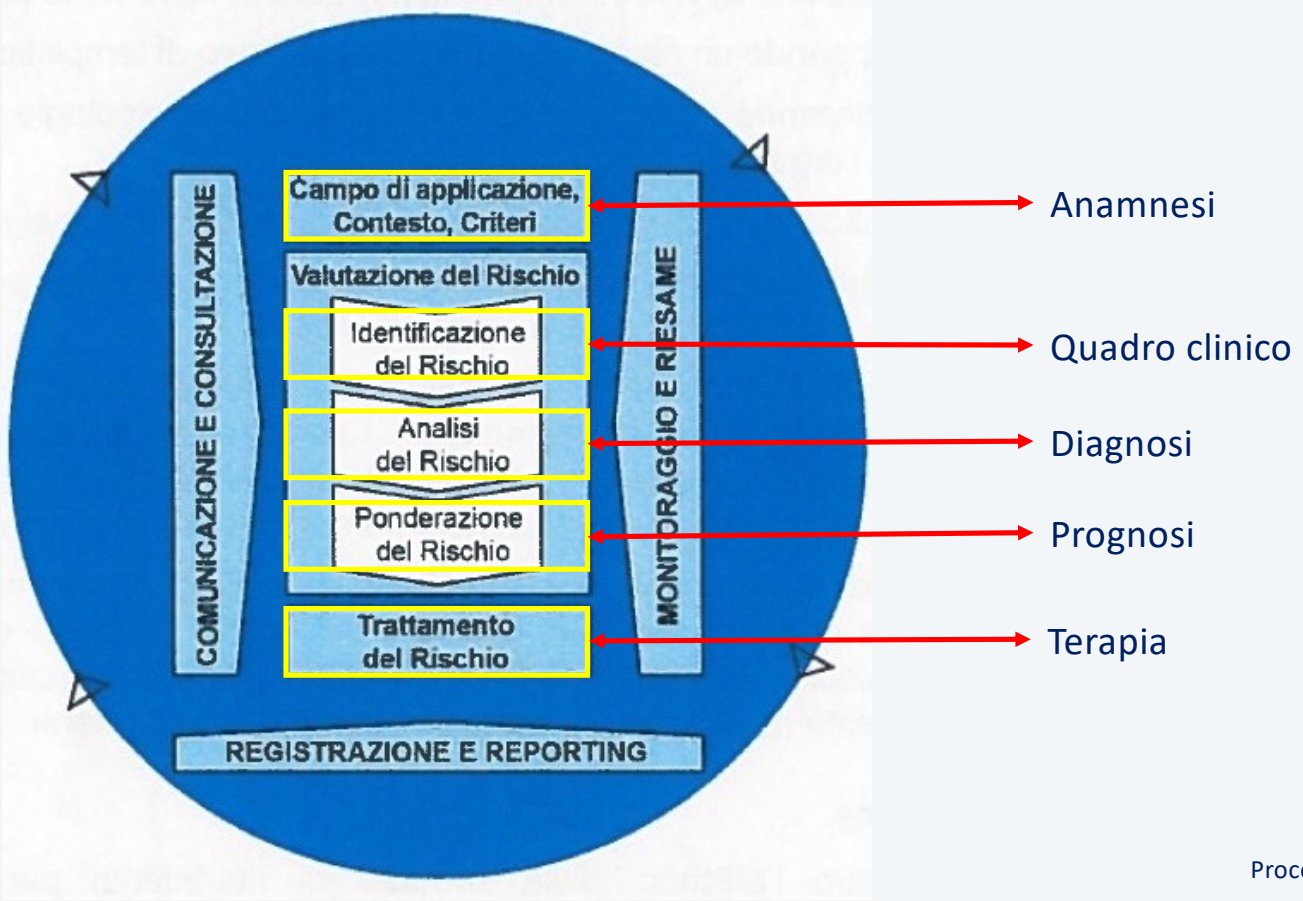
Tramite richiesta di intervento del medico curante

Tramite accesso al pronto soccorso

Come operano i medici?

Fanno domande Visitano il paziente	**Anamnesi**	Storia clinica di un soggetto in esame, raccolta dal medico direttamente o indirettamente come elemento fondamentale per la formulazione della diagnosi; comprende le notizie sui precedenti ereditari e sullo stato di salute dei familiari (*a. familiare* e *personale*), sullo svolgimento dei vari avvenimenti fisiologici, come la dentizione, la crescita, la deambulazione, le abitudini di vita, ecc. (*a. fisiologica*), e la storia delle malattie sofferte dal paziente (*a. patologica*).
Elaborano le info raccolte	**Quadro clinico**	È l'insieme delle manifestazioni, segni e sintomi, con le quali una malattia si presenta all'osservazione del medico. In questo senso contribuisce in maniera decisiva al raggiungimento della diagnosi di una malattia.
Valutano le varie ipotesi	**Diagnosi**	La diagnosi è quel processo di analisi che permette di determinare da quale patologia sia affetto un paziente analizzandone sintomi, segni e storia clinica.
Elaborano una soluzione	**Prognosi**	La prognosi è un giudizio di previsione sul probabile andamento della malattia. Viene formulata una volta fatta la diagnosi, considerando l'usuale tempistica di guarigione, le condizioni del malato, le possibilità terapeutiche e possibili complicazioni o le condizioni ambientali.
Definiscono come intervenire	**Terapia**	Studio e attuazione concreta dei mezzi e dei metodi per combattere la malattia

… Cosa ci ricorda? Qualcuno lo ha già visto?



Processo di Risk Management ISO 31000:2018

Quante sono le specializzazioni mediche?

INDICE DELLE SCUOLE PER AREA, CLASSE E TIPOLOGIA

AREA MEDICA

Classe della **MEDICINA CLINICA GENERALE E SPECIALISTICA**
- Medicina interna
- Medicina d'emergenza-urgenza
- Geriatria
- Medicina dello sport e dell'esercizio fisico
- Medicina termale
- Oncologia medica
- Medicina di comunità e delle cure primarie
- Allergologia ed Immunologia clinica
- Dermatologia e Venereologia
- Ematologia
- Endocrinologia e malattie del metabolismo
- Scienza dell'alimentazione
- Malattie dell'apparato digerente
- Malattie dell'apparato cardiovascolare
- Malattie dell'apparato respiratorio
- Malattie Infettive e Tropicali
- Nefrologia
- Reumatologia

Classe delle **NEUROSCIENZE E SCIENZE CLINICHE DEL COMPORTAMENTO**
- Neurologia
- Neuropsichiatria infantile
- Psichiatria

Classe della **MEDICINA CLINICA DELL'ETÀ EVOLUTIVA**
- Pediatria

AREA CHIRURGICA

Classe delle **CHIRURGIE GENERALI E SPECIALISTICHE**
- Chirurgia Generale
- Chirurgia pediatrica
- Chirurgia plastica, ricostruttiva ed estetica
- Ginecologia ed Ostetricia
- Ortopedia e traumatologia
- Urologia

Classe delle **CHIRURGIE DEL DISTRETTO TESTA E COLLO**
- Chirurgia Maxillo-Facciale
- Neurochirurgia
- Oftalmologia
- Otorinolaringoiatria

Classe delle **CHIRURGIE CARDIO-TORACO-VASCOLARI**
- Cardiochirurgia
- Chirurgia Toracica
- Chirurgia Vascolare

AREA SERVIZI CLINICI

Classe della **MEDICINA DIAGNOSTICA E DI LABORATORIO**
- Anatomia Patologica
- Microbiologia e Virologia
- Patologia Clinica e Biochimica Clinica

Classe della **DIAGNOSTICA PER IMMAGINI E RADIOTERAPIA**
- Radiodiagnostica
- Radioterapia
- Medicina nucleare

Classe dei **SERVIZI CLINICI SPECIALISTICI**
- Anestesia Rianimazione, Terapia Intensiva e del dolore
- Audiologia e foniatria
- Medicina fisica e riabilitativa

Classe dei **SERVIZI CLINICI SPECIALISTICI BIOMEDICI**
- Genetica medica
- Farmacologia e Tossicologia Clinica

Classe della **SANITÀ PUBBLICA**
- Igiene e Medicina Preventiva
- Medicina del Lavoro
- Medicina Legale
- Statistica sanitaria e Biometria

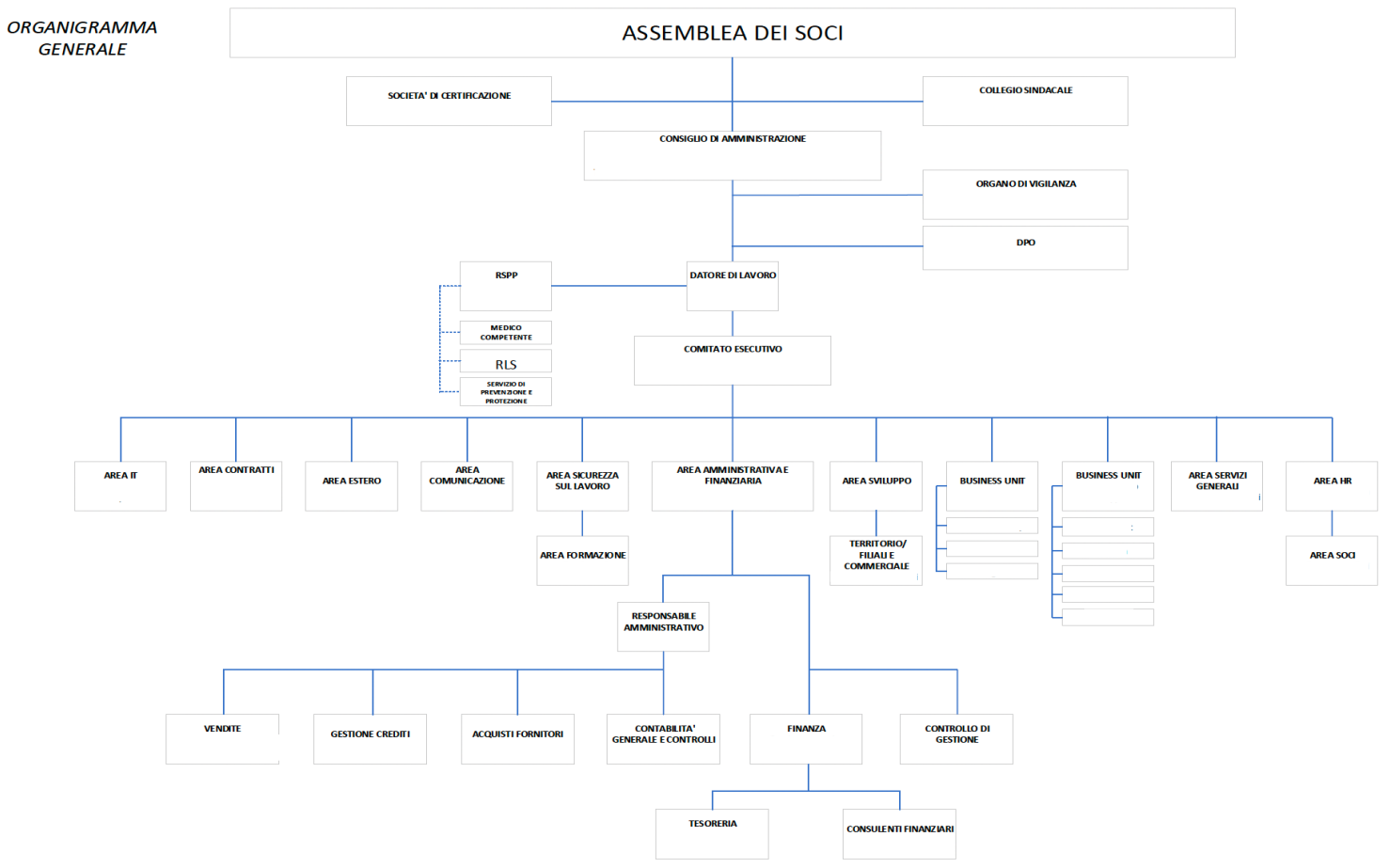
Classe delle **SPECIALIZZAZIONI IN ODONTOIATRIA**
- Chirurgia orale
- Ortognatodonzia
- Odontoiatria Pediatrica

Classe della **FARMACEUTICA**
- Farmacia ospedaliera

Classe della **FISICA SANITARIA**
- Fisica Medica

52

… e quante in azienda?



ANRA
Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali

Facciamo un esempio quante nel settore IT?

oltre 50

ISO 270** 4 macroaree:

norme che descrivono una panoramica e la terminologia:

- ISO/IEC 27000 Sistemi di gestione della sicurezza delle informazioni - Panoramica e vocabolario.

norme che specificano i requisiti:

- ISO/IEC 27001, Sistemi di gestione per la sicurezza delle informazioni – Requisiti;
- ISO/IEC 27006, Requisiti per gli organismi che forniscono audit e certificazione dei SGSI;
- ISO/IEC 27009, Applicazione specifica per settore di ISO / IEC 27001 – Requisiti.

norme che descrivono le linee guida generali:

- ISO/IEC 27002, Codice di condotta per i controlli di sicurezza delle informazioni;
- ISO/IEC 27003, Guida all'implementazione dei SGSI;
- ISO/IEC 27004, Gestione della sicurezza delle informazioni – Misurazione;
- ISO/IEC 27005, Gestione dei rischi per la sicurezza delle informazioni;
- ISO/IEC 27007, Linee guida per la verifica dei SGSI;
- ISO/IEC TR 27008, Linee guida per i revisori dei controlli di sicurezza delle informazioni;
- ISO/IEC 27013, Guida per l'implementazione integrata di ISO/IEC 27001 e ISO/IEC 20000-1;
- ISO/IEC 27014, Governance della sicurezza delle informazioni;
- ISO/IEC TR 27016, Gestione della sicurezza delle informazioni - Economia organizzativa.

norme che descrivono le linee guida negli specifici ambiti/settori:

- ISO/IEC 27010, Gestione della sicurezza delle informazioni per le comunicazioni intersettoriali e inter-organizzative;
- ISO/IEC 27011, Linee guida sulla gestione della sicurezza delle informazioni per le organizzazioni di telecomunicazioni basate su ISO/IEC 27002;
- ISO/IEC TR 27015, Linee guida per la gestione della sicurezza delle informazioni per i servizi finanziari;
- ISO/IEC 27017, Codice di condotta per i controlli di sicurezza delle informazioni basati su ISO/IEC 27002 per i servizi in cloud;
- ISO/IEC 27018, Codice di condotta per la protezione delle informazioni di identificazione personale (PII) in cloud pubblici che agiscono come processori PII;
- ISO/IEC 27019, Linee guida per la gestione della sicurezza delle informazioni basate su ISO/IEC 27002 per i sistemi di controllo del processo, specifici per il settore dei servizi energetici.

Altre norme pubblicate

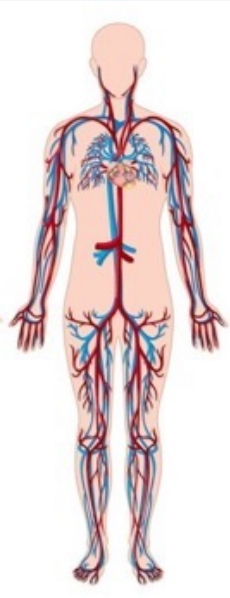
- ISO/IEC 27031 - Linee guida per la disponibilità delle tecnologie dell'informazione e della comunicazione per la continuità aziendale
- ISO/IEC 27032 - Linea guida per la sicurezza informatica
- ISO/IEC 27033-1 - Sicurezza della rete - Parte 1: Panoramica e concetti
- ISO/IEC 27033-2 - Sicurezza di rete - Parte 2: Linee guida per la progettazione e l'implementazione della sicurezza di rete
- ISO/IEC 27033-3 - Sicurezza di rete - Parte 3: Scenari di rete di riferimento - Minacce, tecniche di progettazione e problemi di controllo
- ISO/IEC 27033-4 - Sicurezza di rete - Parte 4: Protezione delle comunicazioni tra reti tramite gateway di sicurezza
- ISO/IEC 27033-5 - Sicurezza di rete - Parte 5: Protezione delle comunicazioni su reti che utilizzano reti private virtuali (VPN)
- ISO/IEC 27033-6 - Sicurezza di rete - Parte 6: Protezione dell'accesso alla rete IP wireless
- ISO/IEC 27034-1 - Sicurezza delle applicazioni - Parte 1: Linee guida per la sicurezza delle applicazioni
- ISO/IEC 27034-2 - Sicurezza delle applicazioni - Parte 2: Quadro normativo dell'organizzazione
- ISO/IEC 27034-6 - Sicurezza delle applicazioni - Parte 6: Casi di studio
- ISO/IEC 27035-1 - Gestione degli incidenti di sicurezza delle informazioni - Parte 1: Principi della gestione degli incidenti
- ISO/IEC 27035-2 - Gestione degli incidenti per la sicurezza delle informazioni - Parte 2: Linee guida per pianificare e preparare la risposta agli incidenti
- ISO/IEC 27036-1 - Sicurezza delle informazioni per le relazioni con i fornitori - Parte 1: Panoramica e concetti
- ISO/IEC 27036-2 - Sicurezza delle informazioni per le relazioni con i fornitori - Parte 2: Requisiti
- ISO/IEC 27036-3 - Sicurezza delle informazioni per le relazioni con i fornitori - Parte 3: Linee guida per la sicurezza della catena di approvvigionamento delle tecnologie dell'informazione e della comunicazione
- ISO/IEC 27036-4 - Sicurezza delle informazioni per le relazioni con i fornitori - Parte 4: Linee guida per la sicurezza dei servizi cloud
- ISO/IEC 27037 - Linee guida per l'identificazione, la raccolta, l'acquisizione e la conservazione delle prove digitali
- ISO/IEC 27038 - Redazione del documento
- ISO/IEC 27039 - Prevenzione delle intrusioni
- ISO/IEC 27040 - Sicurezza dello storage
- ISO/IEC 27041 - Garanzia di indagine
- ISO/IEC 27042 - Analisi dell'evidenza digitale
- ISO/IEC 27043 - Indagine sugli incidenti
- ISO/IEC 27050-1 - Scoperta elettronica - Parte 1: Panoramica e concetti
- ISO/IEC 27701 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO 27799 - Gestione della sicurezza delle informazioni in materia di salute utilizzando ISO/IEC 27002 - guida le organizzazioni del settore sanitario su come proteggere le informazioni sulla salute personale utilizzando ISO/IEC 27002

Perché dobbiamo lavorare tutti insieme?

Che ruolo svolge il sistema informatico in un'Azienda

- ❑ Porta informazioni da un punto ad un altro
- ❑ Processa e archivia informazioni di qualunque tipo

IT



Quindi anche l'IT ha il suo metodo di gestione dei rischi… dalla ISO 27001

6 Pianificare

6.1 **Azioni** per affrontare rischi e opportunità

- 6.1.1 Generalità
- 6.1.2 **Valutazione** del **rischio** relativo alla sicurezza delle informazioni
- 6.1.3 **Trattamento** del **rischio** relativo alla sicurezza delle informazioni

6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli

6.3 Pianificazione delle modifiche

8 Attività Operativa

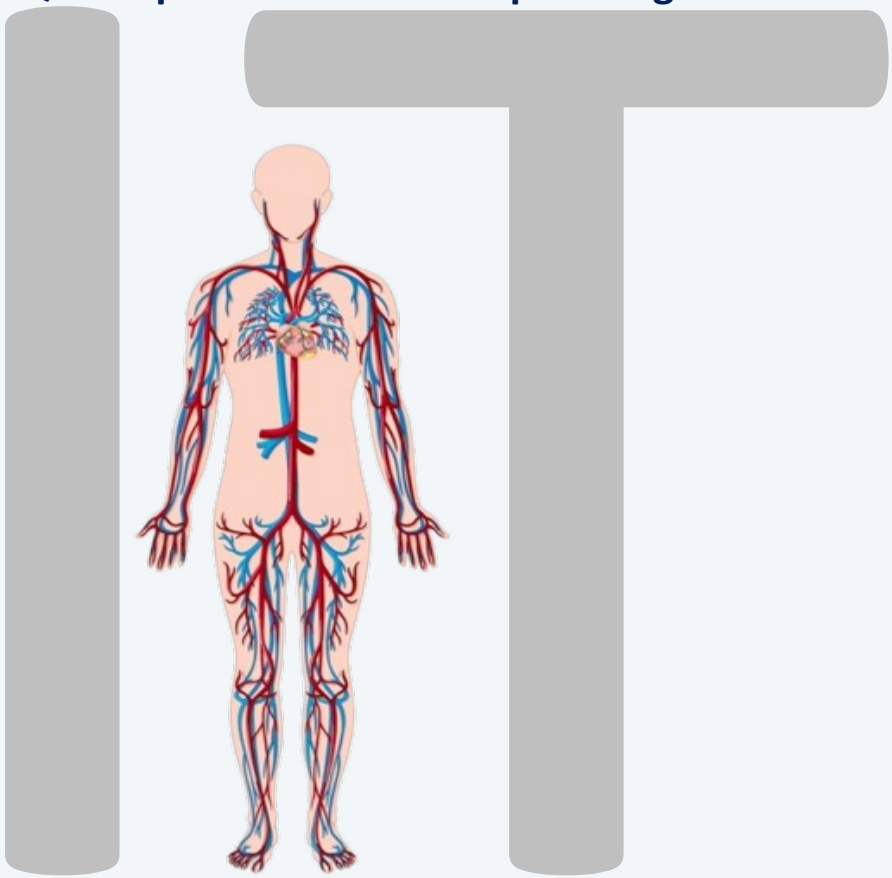
8.1 Pianificazione e controlli Operativi

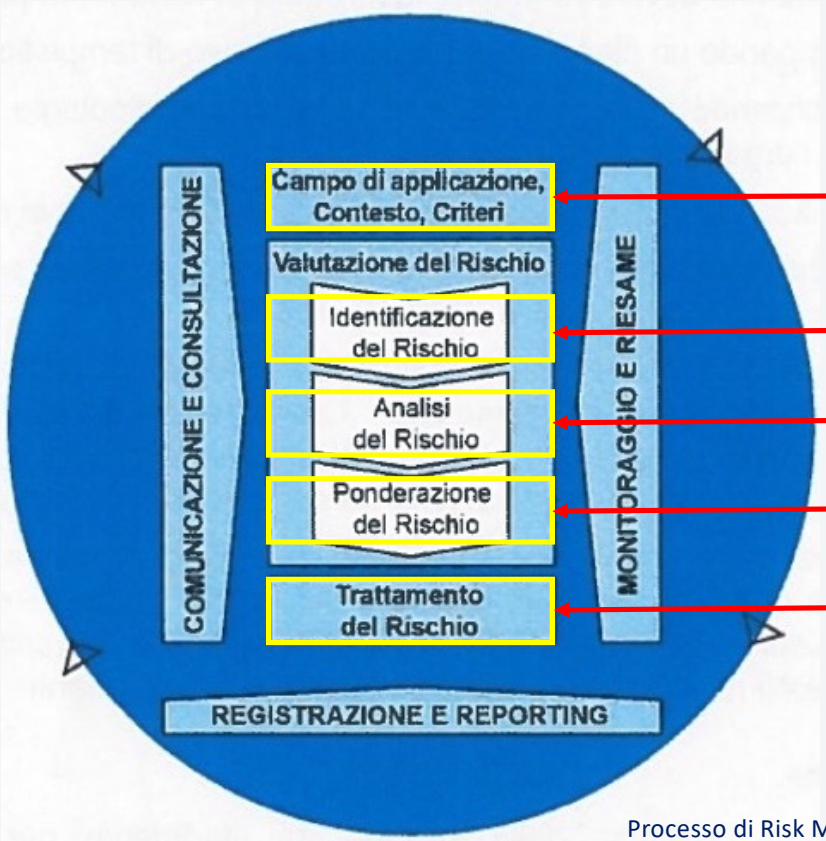
8.2 **Valutazione** del **rischio** relativo alla sicurezza delle informazioni

8.3 **Trattamento** del **rischio** relativo alla sicurezza delle informazioni

Perché dobbiamo lavorare tutti insieme?

Quindi possiamo dire che per la »gestione dell'IT» usiamo lo stesso metodo?





Anamnesi

Quadro clinico

Diagnosi

Prognosi

Terapia

Processo di Risk Management ISO 31000:2018

ANRA
Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali

Possiamo lavorare tutti insieme!

perché la storia insegna… **…. possiamo aiutare Bill!**

Non come se fossimo degli immobili impavidi

Ma come un'unica squadra!

ANRA
Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali

Come arriviamo a collaborare insieme tra specialisti diversi?

Deve «comunicare con semplicità ed efficacia»

Una capacità che lo specialista deve sviluppare …

comunicazione
[co-mu-ni-ca-zió-ne] s.f.
•**1** Trasmissione, partecipazione, diffusione di qlco. agli altri: *c. del messaggio del presidente*; estens. testo che viene comunicato: *c. scritta* || mezzi di
c. (di massa), stampa, radio e televisione
•**2** Relazione presentata a un convegno
•**3** *omissis*
•**4** ling. Scambio di informazioni mediante uno o più linguaggi (verbale, gestuale, musicale ecc.) tra un emittente e un destinatario

dal Sabbatini Coletti

comunicazióne s. f. [dal lat. communicatio - onis]. –
1. a. In senso ampio e generico, l'azione, il fatto di comunicare, cioè di trasmettere ad altro o ad altri
b. In senso più proprio, il rendere partecipe qualcuno di un contenuto mentale o spirituale, di uno stato d'animo, in un rapporto spesso privilegiato e interattivo
Più com., nell'uso corrente, l'atto e il fatto di partecipare, cioè di far conoscere, di rendere noto, e il contenuto stesso di ciò che si partecipa

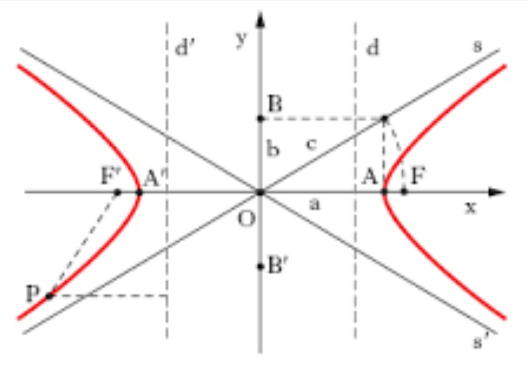
dal dizionario Treccani

ASACERT ISO 9001 UKAS
FERMA
IFRIMA International Federation of Risk and Insurance Management Associations, Inc.
CoLAP Coordinamento Libere Associazioni Professionali

Come arriviamo a collaborare insieme tra specialisti diversi?

Cosa avviene nella testa del vs interlocutore quando gli parlate senza comunicare efficacemente?

Si genera un'Iperbole



Cos'è un'iperbole?

1. Riferimento metaforico volutamente alterato sul piano della quantità sia per eccesso (*è un secolo che ti sto aspettando!*) sia per difetto (*vabbè, speriamo finisca subito!*);

2. In matematica, la curva aperta, composta da due rami, che si ottiene segando un cono con un piano parallelo all'asse o che con esso formi un angolo inferiore a quello fra l'asse e le generatrici; è definibile anche come il luogo dei punti la cui distanza da due punti fissi (*fuochi*) ha differenza costante.

Come arriviamo a collaborare insieme tra specialisti diversi?

Cosa avviene nella testa dell'interlocutore quando gli parlate senza comunicare efficacemente?

Il termine **supercàzzola** (storpiatura dell'originale supercàzzora) è un neologismo (entrato nell'uso comune dal cinema) metasemantico, che indica un nonsenso una frase priva di senso logico composta da un insieme casuale di parole reali e/o inesistenti, esposta in modo ingannevolmente forbito e sicuro a interlocutori che, pur non capendo, alla fine la accettano come corretta. Il termine è utilizzato per indicare chi parla senza dire nulla.

L'obiettivo della supercazzola è di «Sbalordire» 🤯 **& «Confondere»** 🙄

Note: Nel 2015 la definizione di supercazzola è stata inserita nel vocabolario Zingarelli . Termine coniato nel film del 1975 Amici miei, diretto da Mario Monicelli

Fate una prova

Cercate di far comprendere a vostro figlio/figlia di 13 anni che lavoro fate

Un giorno mio figlio mi ha chiesto:
«Papà che lavoro fai?»

Sono impegnato ad aiutare gli Imprenditori nella gestione dei loro rischi

“In che senso?”

«Costruisco muri!!»

“ok, come lo fai e perchè?”

Io: «Prima di tutto capiamo cosa è un muro»

Un muro difensivo è una fortificazione solitamente utilizzata per **proteggere** una città, un paese o un altro insediamento da **potenziali aggressori**. Le mura possono variare da semplici palizzate o terrapieni a estese fortificazioni militari con torri, bastioni e porte di accesso alla città. Le persone, in questo caso gli imprenditori, vogliono avere un muro per proteggere i propri beni dagli aggressori esterni e con beni intendo: **persone, edifici, macchinari, beni e attività**.

Giovanni: «Ho capito. Ma come fai a costruirlo?»

Io: «Ora ti spiego! Fai attenzione!»

Io: «Intanto ascolto l'imprenditore per capire le sue esigenze»

Giovanni: **«come si fa?»**

Io: «Chiedo quali sono i suoi bisogni e di spiegarmeli»

Giovanni : **«ah ok, come fai?»**

Io: «Faccio molte domande perché ho bisogno di essere sicuro di capire correttamente le sue reali esposizioni alle potenziali aggressioni»

Giovanni : **«ah ok, come fai?»**

Io: «Cerco di fare domande sempre più specifiche sul suo lavoro, sulle attività e sul modo in cui opera utilizzando le sue risorse.»

Giovanni : «**ah ok! Come utilizzi tutte queste informazioni?»**

Io: «Comincio a pensare!»

- Mi chiedo quali minacce possono colpire l'imprenditore è come lui è esposto?
- Quali attività potrebbero o sono più sensibili a un'interruzione dell'attività?
- Quali asset sono critici?
- Quali processi sono critici?
- Quali prodotti sono più importanti?
- Chi sono le persone chiave?

«Questo mi aiuta a capire…»

- dove si trovano le sue vulnerabilità
- cosa analizzare

«Così da poter rappresentare un punto di partenza su…»

- possibili minacce ed esposizioni
- vulnerabilità
- impatti

Giovanni: **«E poi, cosa fai?»**

Io: «Preparo il piano d'azione sulla base delle evidenze e delle sue aspettative, questo significa...»

«… questo significa…»

- identificare quanto potrebbe **perdere**…
- quanto è esposto a queste **minacce** (misurazione)
- quali **tecniche** di risk management sono fattibili
- quali di queste tecniche sono quelle **migliori**
- … quindi le vado ad **implementare**
- e **monitoro** i risultati così da **revisionare** l'intero programma di gestione dei rischi!

«È un metodo per pianificare, fare, controllare e agire in aiuto dell'imprenditore»

Giovanni: **«perché tutto questo pensare? Ci vuole molto tempo e un enorme sforzo!»**

Io: «Se non lo facessi, non sarei sicuro di raggiungere lo scopo iniziale del mio lavoro **costruire un muro difensivo resistente»**

Giovanni: **«ma quali minacce consideri per costruire un muro difensivo… e cosa devi proteggere?»**

Io:

«Le minacce hanno molte forme, tante quante sono le conseguenze che potrebbero colpire un'organizzazione.»

Business Interruption

Cyber incident

Pandemic outbreak

Market development

Change in Legislation and Regulation

Climate Change

Natural Catastrophes

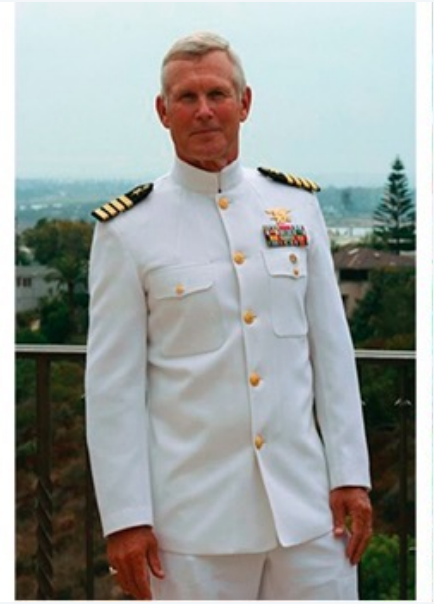
Political Risk and Violence

Si tratta di una singola goccia d'inchiostro in un bicchiere d'acqua

Il moto browniano è il moto casuale di particelle sospese in un mezzo (un liquido o un gas)

… avremo il CHAOS

Analizziamo il termine CHAOS



Bob Schoultz durante i suoi 30 anni di carriera come Navy SEAL

Disorganized

C. Constant
H. Headaches
A. And
O. Ongoing
S. Surprises

Organized

C. Constantly
H. Having
A. An
O. Organizing
S. System

Io: Spero che tu abbia capito perché abbiamo bisogno di costruire un potente muro difensivo e come costruirlo

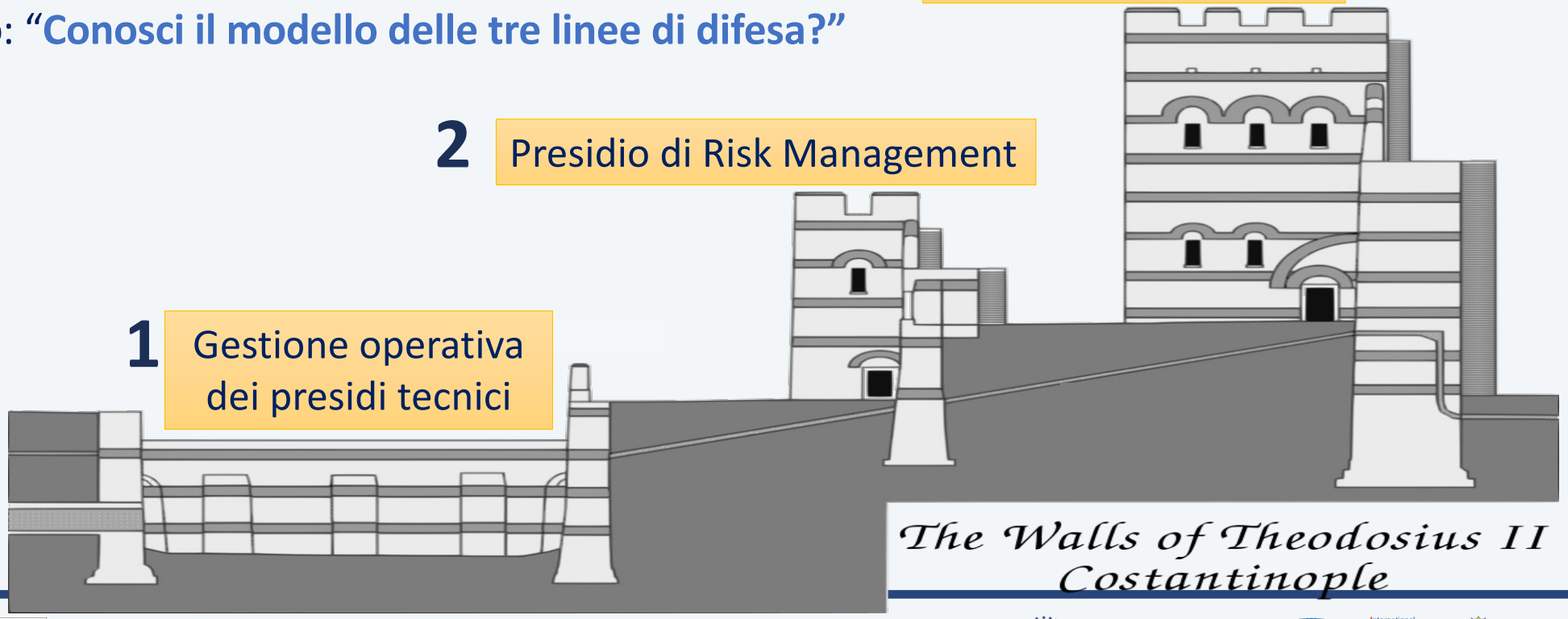
Giovanni: «Ok Papà ma come funziona?»

Io: "Conosci il modello delle tre linee di difesa?"

3 Presidio Internal Audit

2 Presidio di Risk Management

1 Gestione operativa dei presidi tecnici



The Walls of Theodosius II Costantinople

Tutto quello che faccio nella gestione dei rischi è per garantire la continuità operativa

Giovanni: «ma perchè fai tutto questo?»

Io: perché io, come risk manager, so che ci sono elementi che fanno la differenza tra la vita e la morte di ogni attività imprenditoriale!

La gestione dei rischi è un viaggio non una destinazione finale.

Vi lascio con queste ultime immagini prima di entrare nelle metodologie e nelle tecniche che utilizziamo per fare quello che facciamo come specialisti...

Se si comunica efficacemente si gestiscono i rischi

Per ora abbiamo visto un'introduzione alla gestione dei rischi passando dalla medicina all'IT alla costruzione di un muro, tutti abbiamo bisogno di una mano e in questa settimana della Sostenibilità avete la possibilità di raccogliere molte informazioni ricordando che:

lucietto.g@anra.it
mob: + 347 9718840

Quando cambi il modo in cui guardi le cose, le cose che guardi, cambiano

(Dr. Wayne W. Dyer)