pianificazione della sicurezza e analisi dei rischi

(observe)-plan-do-check/study-act cycle

- approccio ciclico alla pianificazione e alla azione
  - è un approccio generale non legato alla sicurezza

- Quattro (o 5) fasi che si ripetono

1. (Observe: osserva la condizione corrente)
2. Plan: stabilisci gli obiettivi obiettivi e le strategie
3. Do: implementa il piano su piccola scala
4. Check/study: verifica I risultati
5. Act: azione su larga scala per gli aspetti di successo e ricomincia.

il piano di sicurezza

- il piano di sicurezza di una organizzazione è un **documento** che descrive come l'organizzazione affronta i suoi problemi di sicurezza

perché pianificare

- capire chi deve fare cosa e quando
- predisporre piani finanziari
  - es. allocare i fondi necessari all'implementazione del piano
- razionalizzare gli interventi
  - la fine di ottenere buoni risultati con spesa contenuta

perché documentare

- per **condividere** gli obiettivi e i processi all'interno dell'organizzazione
  - sinteticamente con i livelli direzionali
  - in forma estesa all'interno del gruppo che si occupa di sicurezza
- **capitalizzare** il lavoro (che di viene un **asset**)
- **tracciare il processo decisionale**
  - al fine di individuare dove e perché una certa decisione è stata presa
  - utile in fase di revisione e correzione
- **verificare il raggiungimento degli obiettivi**
  - se non so quali azioni sono state prese non posso verificarne l'efficacia
  - se non posso verificarne l'efficacia non riesco a capire se le attività legate alla sicurezza stanno andando nella direzione giusta e se le devo modificare

contenuto (tipico) di un piano di sicurezza

- (perimetro)
- policy
- stato attuale
  - inventario degli asset
  - **analisi del rischio**
- vincoli
- **contromisure**
- **piano di rientro** (o roadmap)
  - piano di applicazione delle contromisure per la transizione dalla situazione attuale a quella identificata come ottimale
- **responsabilità**
  - …dell'applicazione del piano
- piano di revisione
  - …del piano di sicurezza
- piano di risposta agli incidenti, business continuity, disaster recovery

(perimetro)

- il piano deve esprimere per cosa si sta pianificando la sicurezza
- esempi:
  - un sistema, una rete, un servizio, un dipartimento, una categoria di dati, ecc.
- il perimetro può essere più o meno facile da descrivere
  - potrebbe essere già chiaro dal titolo
    - es. “pianificazione della sicurezza dei dati personali”
  - potrebbe essere descritto in una apposite sezione

policy

- criterio adottato dall'organizzazione in merito alla sicurezza
  - sicuramente **contrattato con il management**
  - tipicamente un documento ad un elevato livello di astrazione
- una delle parti più critiche del piano perché fruita da manager e "decision makers"
- dovrebbe descrivere
  - gli obiettivi ad alto livello
    - priorità di certi aspetti rispetto ad altri: es. criticità di certi settori di business, normative applicabili, ecc.
      - tipica policy minima: conformità alla normativa (GDPR, NIS, perimetro sicurezza nazionale cibernetica)
    - responsabilità della gestione della pianificazione es. un gruppo, i manager, ecc.
  - l'impegno
    - risorse operative e/o finanziarie
- sin dalla policy si deve trovare un compromesso tra..
  - efficacia, costi, disagio agli utenti, ecc.
  - rigidità dei controlli vs. deterrente e recovery

stato attuale (o inventario)

- inventario delle risorse dell'organizzazione rilevanti per la sicurezza (i cosiddetti asset)
  - dati
  - utenti
  - apparecchiature
  - servizi
  - eventuali contromisure già presenti
  - con indicazione della criticità e del "rapporto" tra di essi
- è sostanzialmente una analisi dello stato attuale

analisi del rischi

- mira ad ottenere una **lista dei rischi correnti** ordinata per **importanza decrescente**
- ciascun rischio descritto testualmente con associata una…
- …valutazione
  - assoluta: es. stimata in perdite $/year attese
  - relativa: ordinamento tra i rischi
    - es. tramite scala numerica astratta
- è fondamentale come **input alla fase di progetto delle contromisure**
- è un risultato intermedio notevole (milestone)
  - è l'input al cosiddetto **decision making**

analisi dei rischi: terminologia

- quando una minaccia si concretizza (in un attacco, virus, fault, ecc) si parla di ***evento avverso o incidente***
- il ***rischio*** è una stima di quanto è importante per l'organizzazione un certo *evento avverso* possibile, cioè una minaccia
- elementi
  - **impatto:** danno, o perdita economica, in caso di un incidente
  - **frequenza**: la quantità di incidente attesi nell'unità di tempo (es. in un anno)
  - **trattabilità**: possibilità di controllarne la frequenza o l'impatto

valutazione quantitativa del rischio

- una analisi quantitativa ha come obiettivo la valutazione economica della perdita
  - o valore atteso della perdita nell'unità di tempo

- valore atteso della perdita per una data minaccia

perdita attesa annua =

valore atteso del numero di incidenti annui

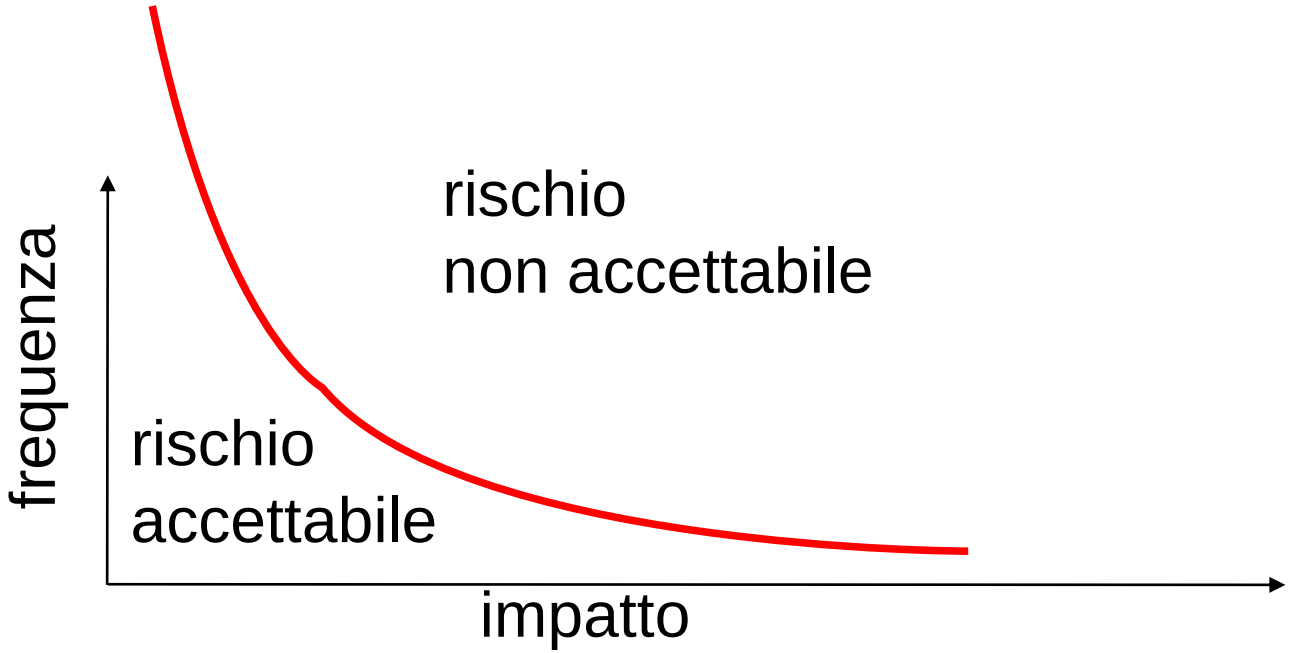
X

impatto del singolo incidente

$$P = f \cdot I$$

accettabilità: interpretazione geometrica

- piano impatto-frequenza
- approccio tipico: la perdita è accettabile se minore di una certa soglia

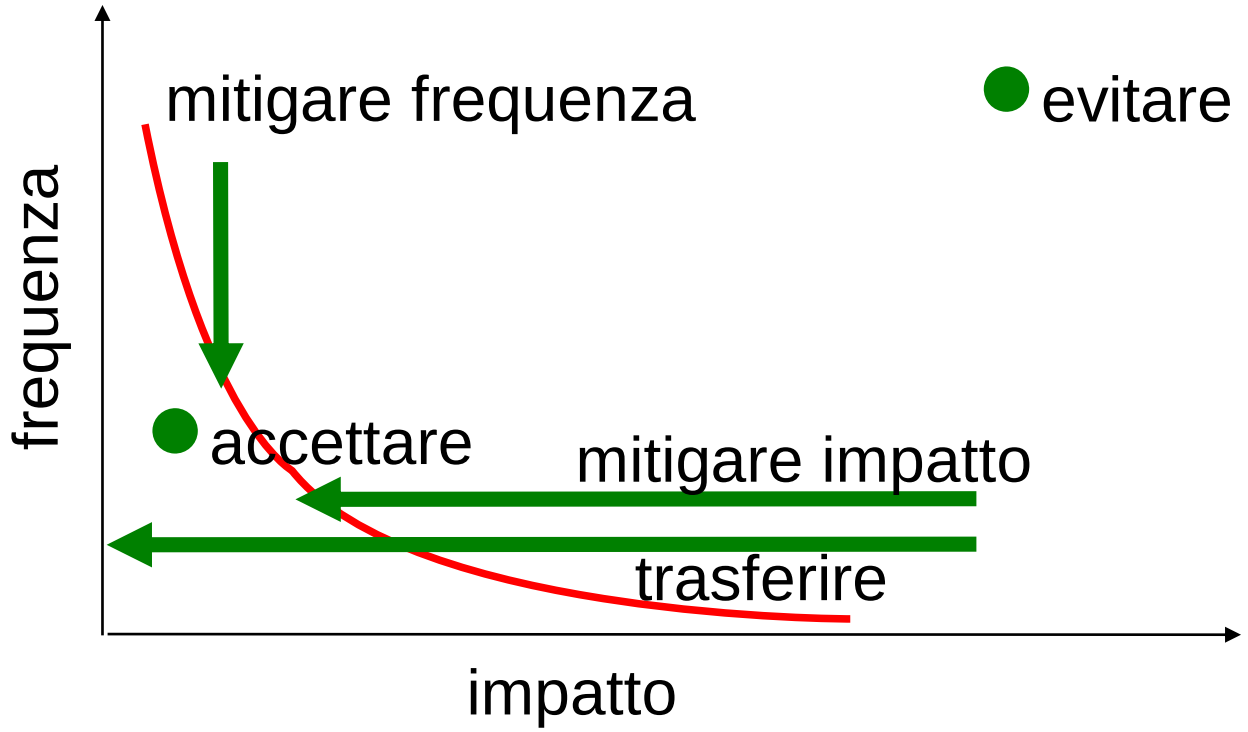


trattamento dei rischi

- a fronte di un rischio possiamo...
  - accettare
    - non facendo nulla se il rischio è sufficientemente basso
  - mitigare sul fronte della frequenza
    - inserendo delle **contromisure proattive** di tipo tecnologico, procedurale o organizzativo che riducono la probabilità di evento avverso (es. firewall)
  - mitigare sul fronte dell'impatto
    - preparandoci ad affrontare un incidente inserendo delle **contromisure reattive** di tipo tecnologico, procedurale o organizzativo che ne riducono l'impatto (es. backup)
    - **trasferendo** la perdita su un altro soggetto (es. assicurazione o consorzi di "mutuo soccorso")
  - evitare
    - non intraprendere l'attività che ci espone al rischio (es. dare l'attività in outsourcing, o cambiare business)

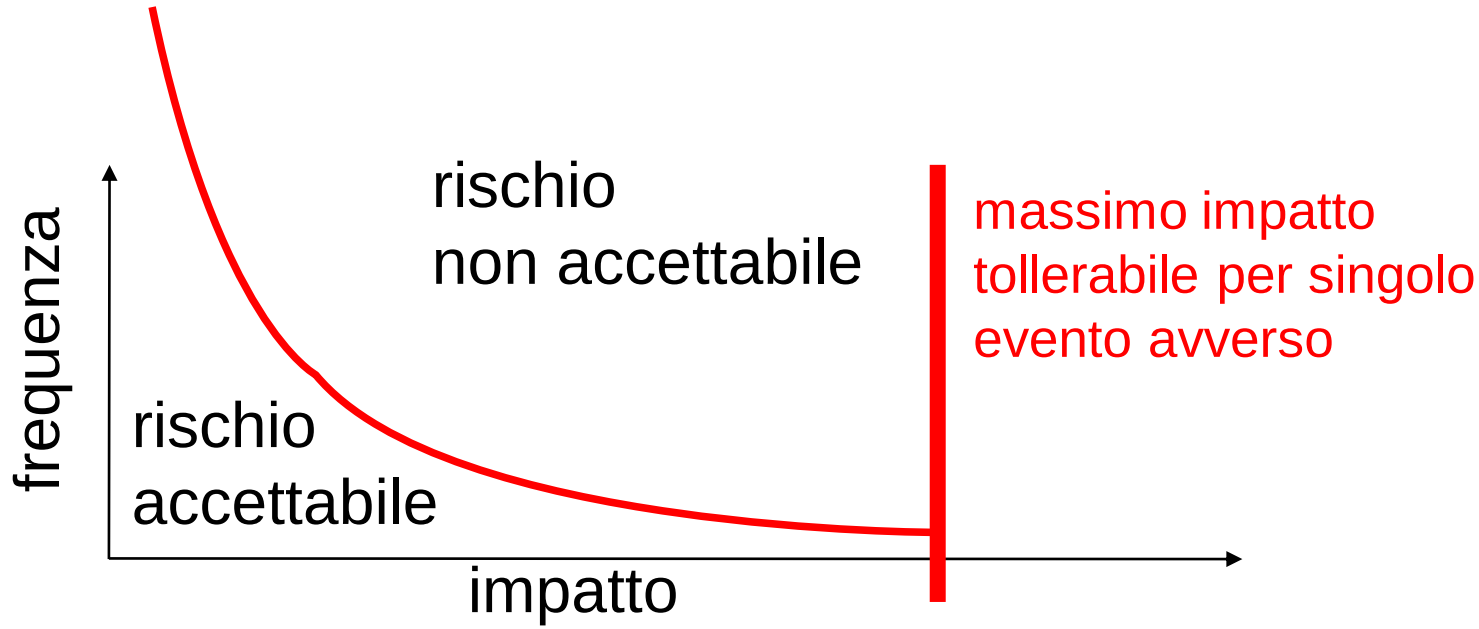
trattamento dei rischi e piano impatto-frequenza

- i rischi «trattati» si spostano sul piano

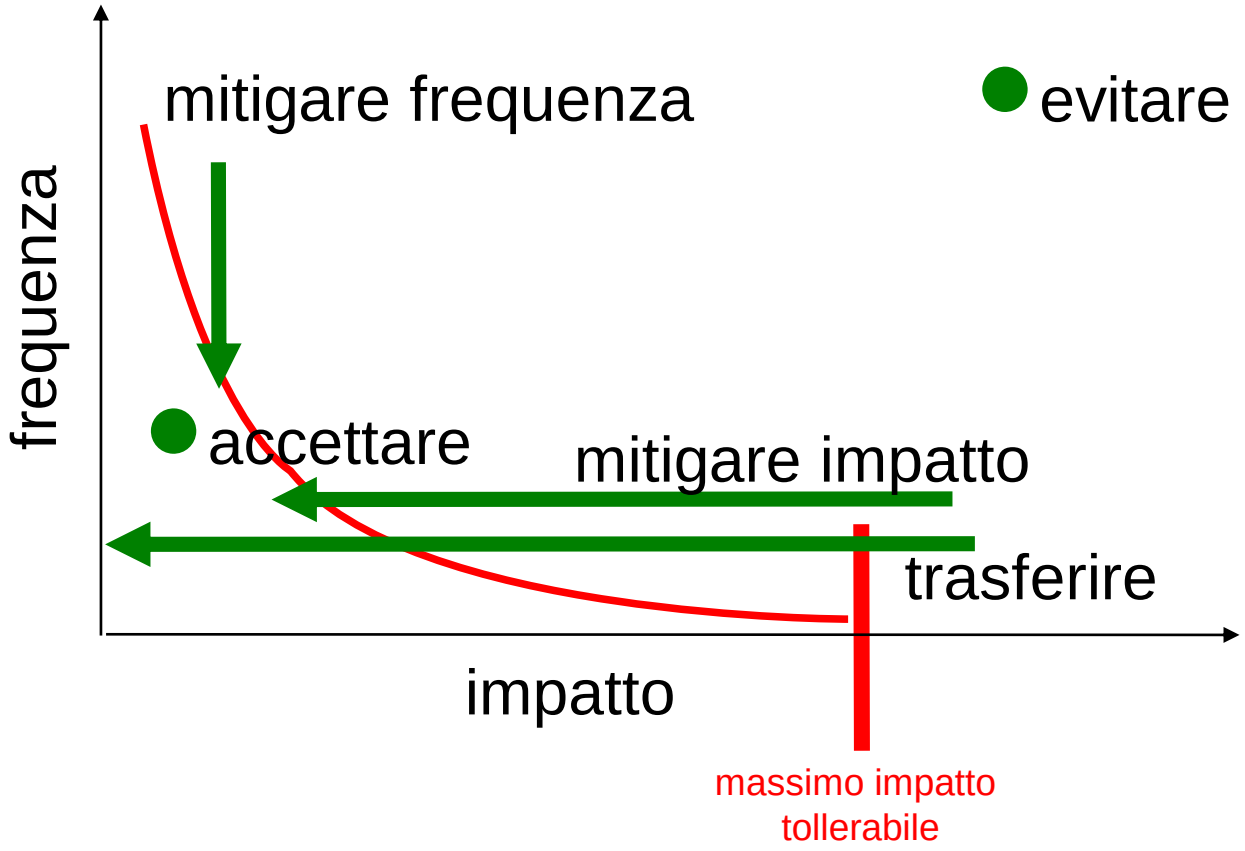


impatto massimo sostenibile

- spesso esiste un massimo impatto che una organizzazione può tollerare senza fallire
  - es. perdita dei dati dei c/c per una banca



trattamento dei rischi e massimo impatto sostenibile



catastrofi

- sono eventi a bassissima frequenza e ad altissimo impatto
  - es. catastrofi naturali
  - l’impatto è maggiore di quello sostenibile
- può essere difficile o troppo costoso trasferire il rischio
  - a causa dell’enorme impatto
  - es. per le banche rispetto a perdite dei dati
- mitigare l'impatto preparandosi a fronteggiare l’incidente
  - disaster recovery
  - business continuity

limiti della valutazione quantitativa

- stimare il rischio come impatto x frequenza è spesso molto difficile
- difficoltà nel monetizzare il valore dei beni
  - es. danni di immagine
- necessità di statistiche e stime di frequenza
  - difficilmente applicabile ad eventi con frequenza molto bassa

valutazione qualitativa

- qualitativa = metriche non monetarie
  - es. alto medio basso o numeriche astratte
- utili per **comparare i rischi tra di loro**
- l'analisi nel piano impatto-frequenza in questo caso ha solo un valore concettuale

oggettività della valutazione qualitativa

- sarebbe bello che persone diverse dessero una valutazione uguale (oggettiva) anche se qualitativa
- il motivo è l'omogeneità di valutazione
  - all'interno di un gruppo
  - nel tempo se il personale cambia
  - possibilità di confrontare risultati di analisi differenti (es. tra organizzazioni diverse)
- può essere utile avere standard per questo
  - interni ad una organizzazione
  - disponibili come prodotti

risultato dell'analisi dei rischi

il risultato dell'analisi dei rischi è una tabella con le seguenti colonne

- **descrizione** del rischio
- **valutazione** del rischio non trattato
  - con metrica monetaria o astratta ma omogenea per tutti i rischi

ordinare la tabella per rischio decrescente

può contenere altre colonne

- es. dipartimento interessato, responsabilità, ulteriori approfondimenti da fare, ecc.

viene poi integrata con le contromisure

- da compilare nella fase di analisi e progetto delle contromisure
- possono essere più di una (alternative tra cui scegliere)
- per ciascuna contromisura: **rischio residuo**, costo, tempi

uso della tabella dei rischi

è input per le fasi di…

- **analisi e progettazione** delle contromisure
  - …che prevede una scelta tra le varie alternative
  - gli strumenti mostrati in questo corso sono «primitive» fondamentali per questa fase
- creazione del piano di rientro in sicurezza (piano di rientro o roadmap)
  - … che di fatto stabilisce i tempi per la **realizzazione** delle contromisure
  - è questo un piano in senso stretto

vincoli

- sono vincoli generici che tutte le contromisure devono soddisfare
- esempi
  - tutti gli operatori che accedono a dati personali devono essere autenticati
  - tutti gli apparati devono essere forniti dal vendor XYZ
  - tutti gli apparati devono essere certificati CC almeno EAL3
  - non si possono usare fingerprint reader

contromisure

- è l'output di una fase di progettazione
- dà i dettagli circa le contromisure scelte
- se gli interventi sono importanti si può prevedere una attività progettuale separata
  - pianificazione indipendente
  - progetti pilota
    - vedi plan-do-check-act
  - interventi importanti possono richiedere una analisi dei rischi dedicata, nota anche come «contingency plan»
  - propria metodologia di sviluppo

contromisure: criteri di scelta

la scelta delle contromisure va fatta in base a

- **costi** della contromisura (più o meno espliciti)
  - acquisto di apparati, acquisizione di competenze, consulenze, gestione, manutenzione, aggiornamento, impatto sulla produttività, usabilità, ecc.
  - total cost of ownership
- **efficacia** (cioè **rischio residuo**)
  - di quanto riduce il rischio? ne introduce altri?

esempio di valutazione quantitativa del rischio e valutazione contromisure

Bene: autovettura, valore € 20.000

Vulnerabilità: trasportabilità **Minaccia: furto**

	senza antifurto	**blocca pedali**	**Stellitare**
furti su 100000 auto	1000	200	2
Valore atteso del numero di eventi avversi annui	0,01	0,002	0,00002
impatto economico annuo atteso	€200 rischio non trattato	€40 rischio residuo	€0,4 rischio residuo
costo contromisura	-	€12 (quota ammortamento)	€300
costo annuo totale	€200	**€52**	€300,4

NOTA: Questa analisi può andar bene per un ampio parco auto in cui **il singolo furto ha un impatto tollerabile**.
Chi possiede una singola auto potrebbe non tollerare l'impatto neanche di un solo furto.
In tal caso, è necessario **trasferire il rischio mediante una polizza assicurativa.**

responsabilità

- tipicamente la responsabilità della attuazione del piano è distribuita, es.
  - amministratori db
    - responsabili della sicurezza dei db
  - capi progetto
    - responsabili dei dati del loro progetto
  - amministratore di rete
    - responsabile della sicurezza di rete
  - manager
    - responsabili indiretti, cioè responsabili della supervisione delle persone che sono direttamente responsabili della sicurezza
- tipicamente basato sull'organigramma aziendale

piano di rientro o roadmap

- mostra quali attività vengono effettuate e quando
- dovrebbe...
  - dare **precedenza** al trattamento dei rischi più importanti
  - **diluire l'impegno** (risorse finanziarie e umane) nel tempo
    - attuazione incrementale delle contromisure più costose e rischiose
  - integrare i piani per le azioni che hanno un piano proprio
- vincoli
  - compatibilità con altri piani aziendali (es. finanziari o di business)

revisione

- il piano dovrebbe prevedere…
  - …quando il piano stesso va revisionato
    - ogni anno
    - ogni volta che si installa un nuovo servizio
    - ogni volta che cambia la normativa
  - …chi deve effettuare la revisione del piano
    - revisione fatta internamente
    - revisione in outsourcing

conflitti di interesse

- la **redazione** di un piano di sicurezza è impegnantiva
  - outsourcing o in-house?
- **l'attuazione** è impegnativa
  - outsourcing o in-house?
- la **revisione** è impegnativa
  - outsourcing o in-house?
- fondamentale evitare **conflitti di interesse**

conflitti di interesse

esempi

- redazione – revisione
  - se il soggetto è lo stesso potrebbe accettare piani cattivi per dimostrare di aver fatto un buon lavoro
- redazione – attuazione
  - se il soggetto è lo stesso potrebbe gonfiare i rischi per poter vendere più contromisure

risposta agli incidenti

- stabilisce procedure in caso di incidente
  - la squadra che si occupa del problema
  - le questioni legali
    - quando e se si sporge denuncia
    - notifiche dovute per legge alla (GDPR, NIS, perimetro sicurezza nazionale cibernetica)
  - le attività per mantenere le prove (computer forensic)
  - il log delle attività di gestione degli incidenti
  - come condurre le relazioni con l'esterno (es. con i clienti)
- stabilisce cosa fare dopo l'incidente
  - revisione del piano di sicurezza
  - revisione del piano di risposta agli incidenti

bussiness continuity plan e disaster recovery plan

- si occupa di minacce il cui rischio a bassa proababilità e ad alto impatto
  - Epidemie
  - Terremoti
  - Incendi
  - Inondazioni
  - Uragani
  - Interruzione dei servizi (elettricità, acqua, ecc.)
  - Terrorismo
  - Cyber attack

bussiness continuity plan e disaster recovery plan

- requisiti
  - insieme minimo di servizi da mantenere
  - finestra temporale nel quale i servizi devono essere di nuovo disponibili
- la soluzione può prevedere...
  - struttura organizzativa di gestione e comando in caso di crisi
  - procedure di backup e ripristino
  - sito secondario (caldo o freddo)
  - comunicazione tra sito primario e secondario
  - replica dei dati tra primario e secondario
  - servizi disponibili sul sito secondario