pianificazione della sicurezza

perché pianificare

- razionalizzare gli interventi
  - la fine di ottenere buoni risultati con spesa contenuta
- 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
- mantenere traccia del processo decisionale
  - al fine di individuare dove e perché una certa decisione è stata presa
  - utile in fase di revisione e correzione
- disporre di uno strumento per 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
- predisporre piani finanziari
  - es. allocare i fondi necessari all'implementazione del piano

(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 scale
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

contenuto (tipico) di un piano di sicurezza

- policy
- stato attuale
  - inventario degli asset
  - **analisi del rischio**
- requisiti e vincoli
- **contromisure**
- **piano di rientro** (o roadmap)
  - piano di applicazione delle contromisure per la transizionedalla 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

policy

- criterio adottato dall'organizzazione in merito alla sicurezza, sicuramente contrattato con la direzione
- tipicamente un documento ad un elevato livello di astrazione
- sin dalla policy si deve trovare un compromesso tra..
  - efficacia, costi, disagio agli utenti, ecc.
  - rigidità dei controlli vs. deterrente e recovery
- dovrebbe descrivere
  - obiettivi ad alto livello
    - priorità di certi aspetti rispetto ad altri: es. criticità di certi settori di business, conformità a normative, ecc.
  - responsabilità della gestione della pianificazione
    - es. un gruppo, i manager, ecc.
  - l'impegno
    - quante risorse operative o finanziarie
- una delle parti più critiche e complesse del piano perché fruita dal management e «decision makers»

stato attuale

- 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 e valutazione dei rischi correnti
- 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)
- può essere un risultato da usare per 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 incidente
  - **probabilità**: la probabilità che l'incidente si verifichi
  - **controllabilità o trattabilità**: possibilità di controllarne la probabilità o l'impatto

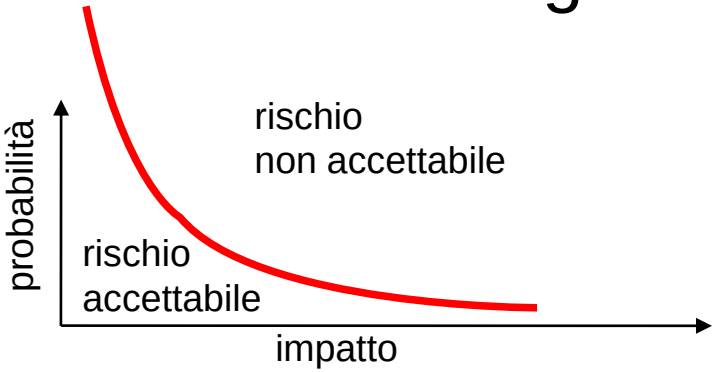
valutazione quantitativa del rischio

- una analisi quantitativa ha come obiettivo la valutazione economica della perdita
- valore atteso della perdita per una data minaccia

  perdita attesa annua =

  valore atteso del numero di incidenti annui *
  impatto del singolo evento avverso

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

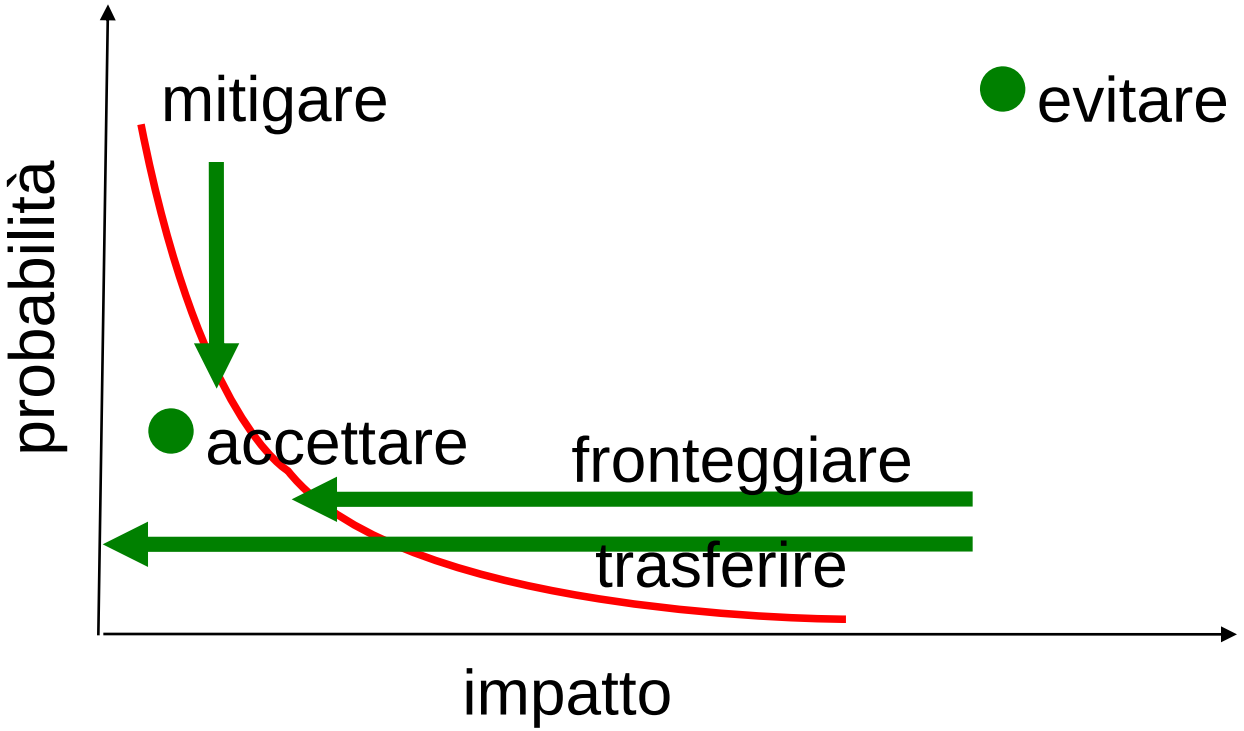


trattamento dei rischi

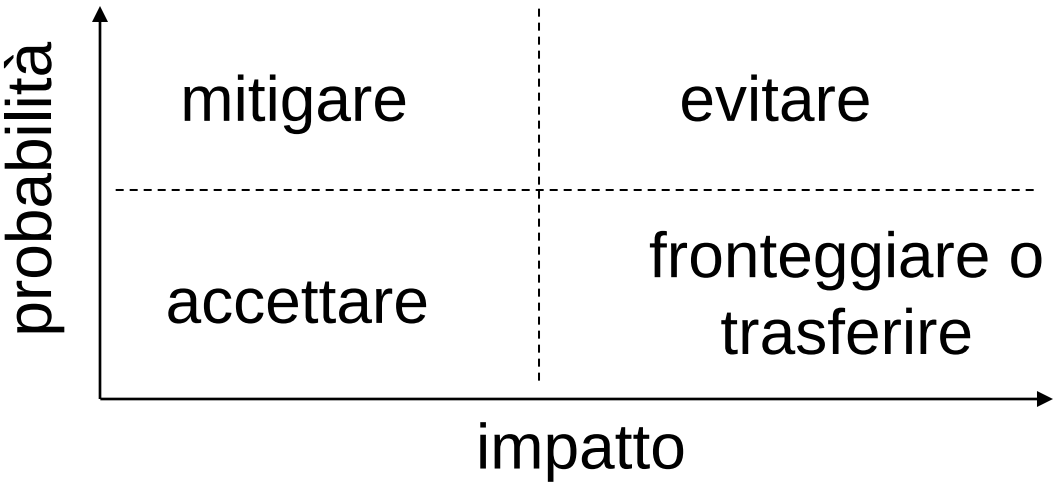
- a fronte di un rischio possiamo...
  - accettare
    - non facendo nulla se il rischio è sufficientemente basso
  - mitigare
    - inserendo delle **contromisure proattive** di tipo tecnologico, procedurale o organizzativo che riducono la probabilità di evento avverso (es. firewall)
  - fronteggiare
    - preparandoci ad affrontare un incidente inserendo delle **contromisure reattive** di tipo tecnologico, procedurale o organizzativo che ne riducono l'impatto (es. backup)
  - trasferire
    - trasferendo la perdita su un altro soggetto (es. assicurazione o accordi 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-probabilità

- i rischi «trattati» si spostano sul piano

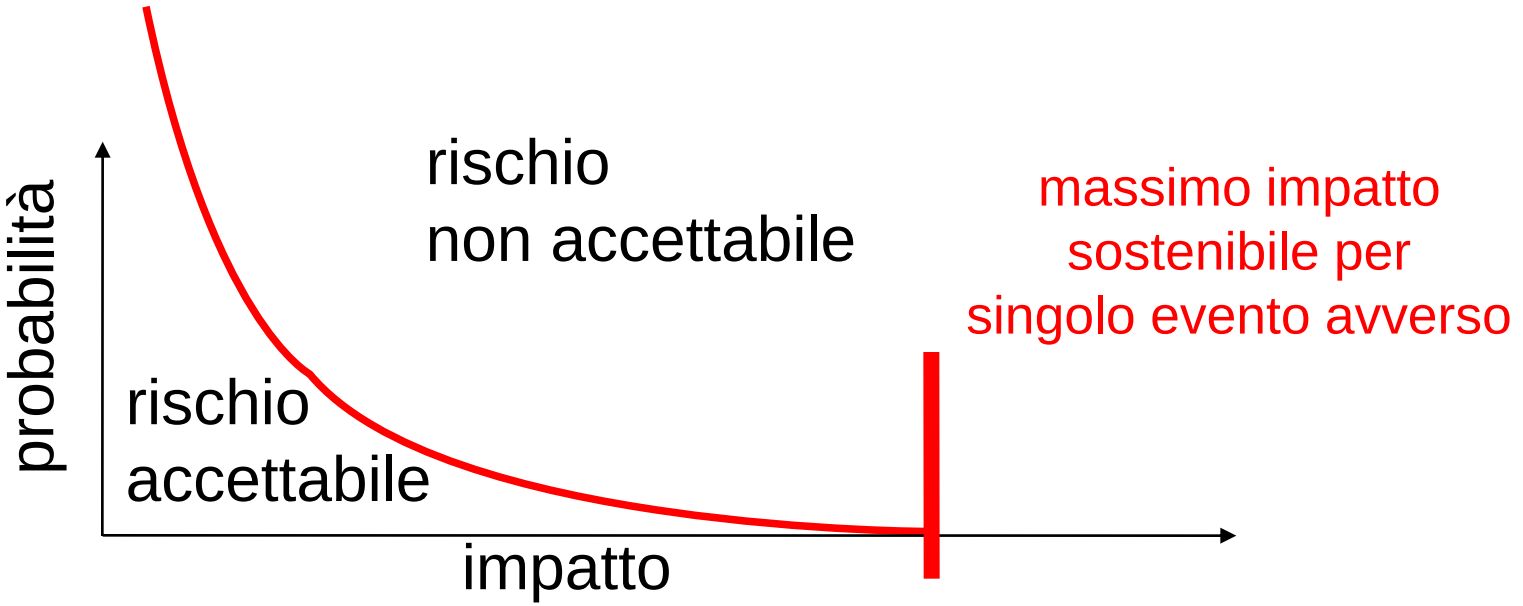


trattamento dei rischi: schema

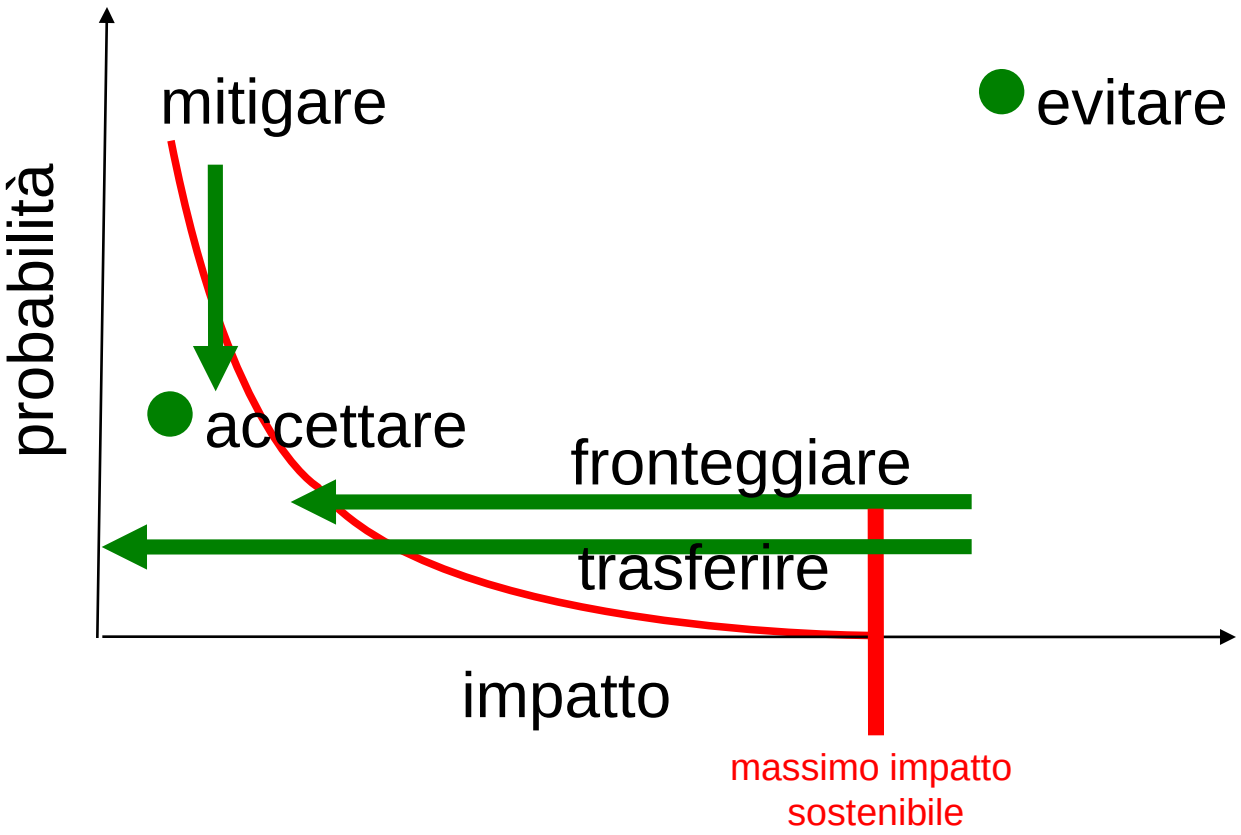


impatto massimo sostenibile

- spesso c'è una soglia oltre la quale non si può sostenere neanche un singolo incidente,
  - pena il “fallimento dell'organizzazione”



trattamento dei rischi e massimo impatto sostenibile



rischi non mitigabili ad alto impatto

- l'evento avverso può non essere mitigabile
  - catastrofi naturali
- se l'impatto del singolo evento avverso è alto non si può sopportare neanche un evento avverso
  - es. per una banca: terremoto con perdita di tutti i dati dei c/c
- ridurre l'impatto prepardosi a fronteggiarlo
  - disaster recovery
  - business continuity

limiti della valutazione quantitativa

- difficoltà nel monetizzare il valore dei beni
  - es. danni di immagine
- necessità di statistiche e stime di probabilità
  - difficilmente applicabile ad eventi con probabilità molto bassa
- spesso sono usati **metodi qualitativi**
  - metriche non monetarie
    - es. alto medio basso o numeriche astratte
  - permettono solo di comparare i rischi tra di loro
- l'analisi del piano impatto-probabilità in questo caso ha solo un valore concettuale

risultato dell'analisi dei rischi

il risultato dell'analisi dei rischi può essere pensato come 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
  - fondamentale per **ordinare la tabella per rischio decrescente**
- 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

- può contenere altre colonne
  - es. dipartimento interessato, responsabilità, ulteriori approfondimenti da fare, ecc.

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
- pianificazione vera e propria per il rientro in sicurezza (piano di rientro)
  - … che di fatto stabilisce i tempi per la **realizzazione** delle contromisure

requisiti e vincoli (analisi)

- requisiti
  - identificano ciò che i meccanismi di sicurezza scelti dovranno fare senza specificare i dettagli
  - è una descrizione molto più concreta rispetto ad una politica
    - es: deve essere possibile valutare l'efficacia della protezione
    - es: tutti gli utenti che accedono a certi dati devono essere autenticati
  - è una descrizione astratta rispetto al progetto poiché non dice come i requisiti verranno soddisfatti
- vincoli di progetto (o di implementazione)
  - la intranet va protetta con un firewall
  - 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.
- **efficacia** (cioè **rischio residuo**)
  - di quanto riduce il rischio? ne introduce altri?

contromisure e valutazione quantitativa del rischio

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	€300
costo annuo totale	€200	€52	€300,4

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

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**

risposta agli incidenti

- può essere parte del piano di sicurezza
- stabilisce procedure in caso di incidente
  - la squadra che si occupa del problema
  - le questioni legali (quando si sporge denuncia)
  - 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