Sicurezza informatica--> impedire accesso non autorizzato

--> cia "confidendentialy, integrity (riferiscono ai dati), availability" (al sistema).

Data confidentialy--> segretezza dati

Data integrity--> evitare dati alterati

System availability--> garantire sistema operante.

Autenticazione--> riconoscimento credenziali utente

Autorizzazione--> permesso accesso al sistema dopo autenticazione

Riservatezza--> protezione privacy (leggibile per chi ne ha diritto)

Disponibilità--> documento disponibile a chi è autorizzato (availability)

Integrità--> garanzia e certezza documento sia originale

Paternità--> documento associato ad utente

Segretezza--> agire ai livelli pila protocollare

Livello fisico--> impedire intrusi prelevamento informazioni

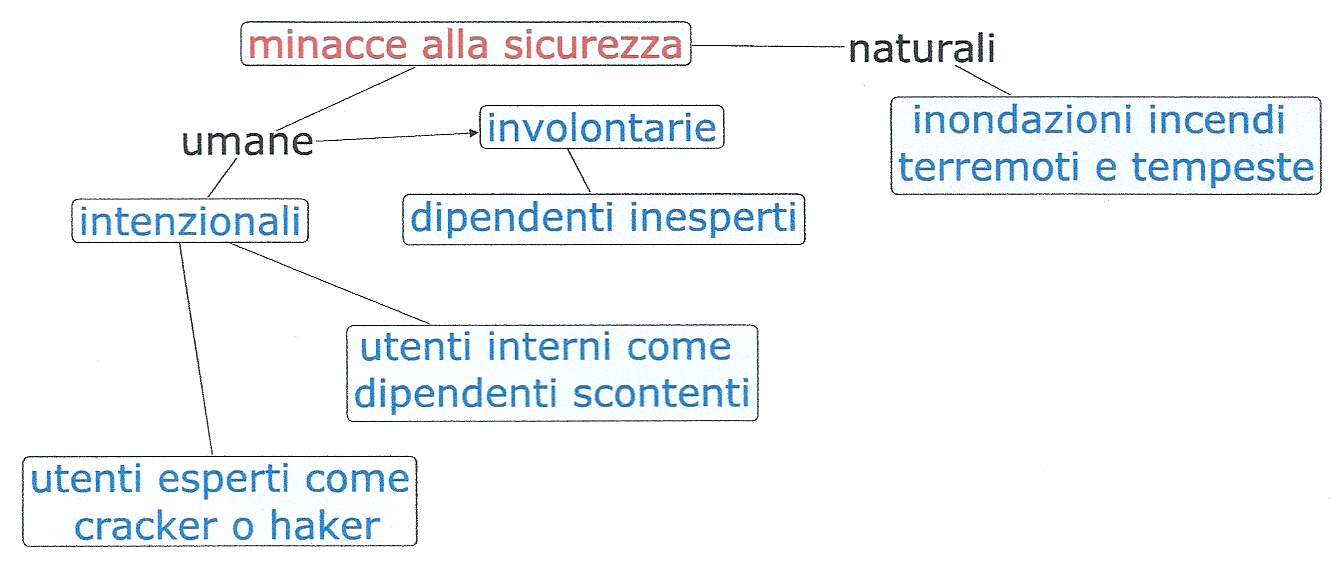
Data link--> introdurre codifiche e cifrature per renderli incomprensibili

Valutazione rischi

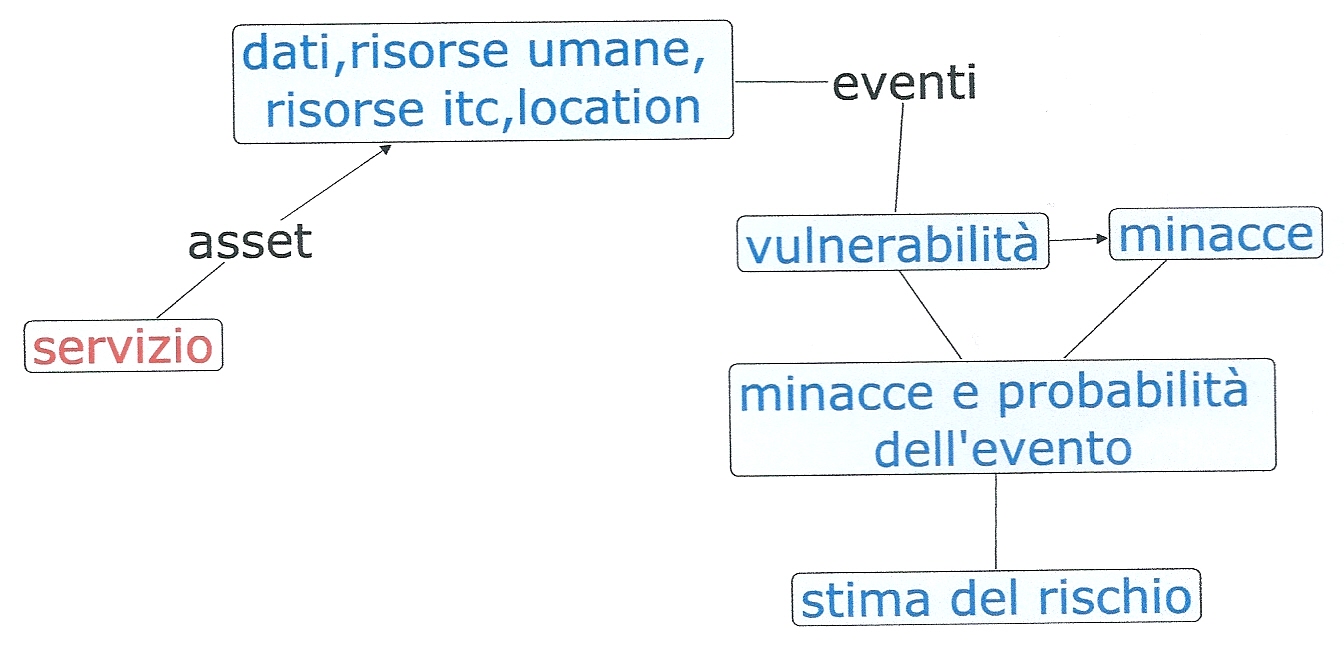
Possiamo individuare 2 fasi essenziali:

Il primo è analisi dei rischi--> situazione di vulnerabilità, elenco possibili minacce, cause perdite di sicurezza.

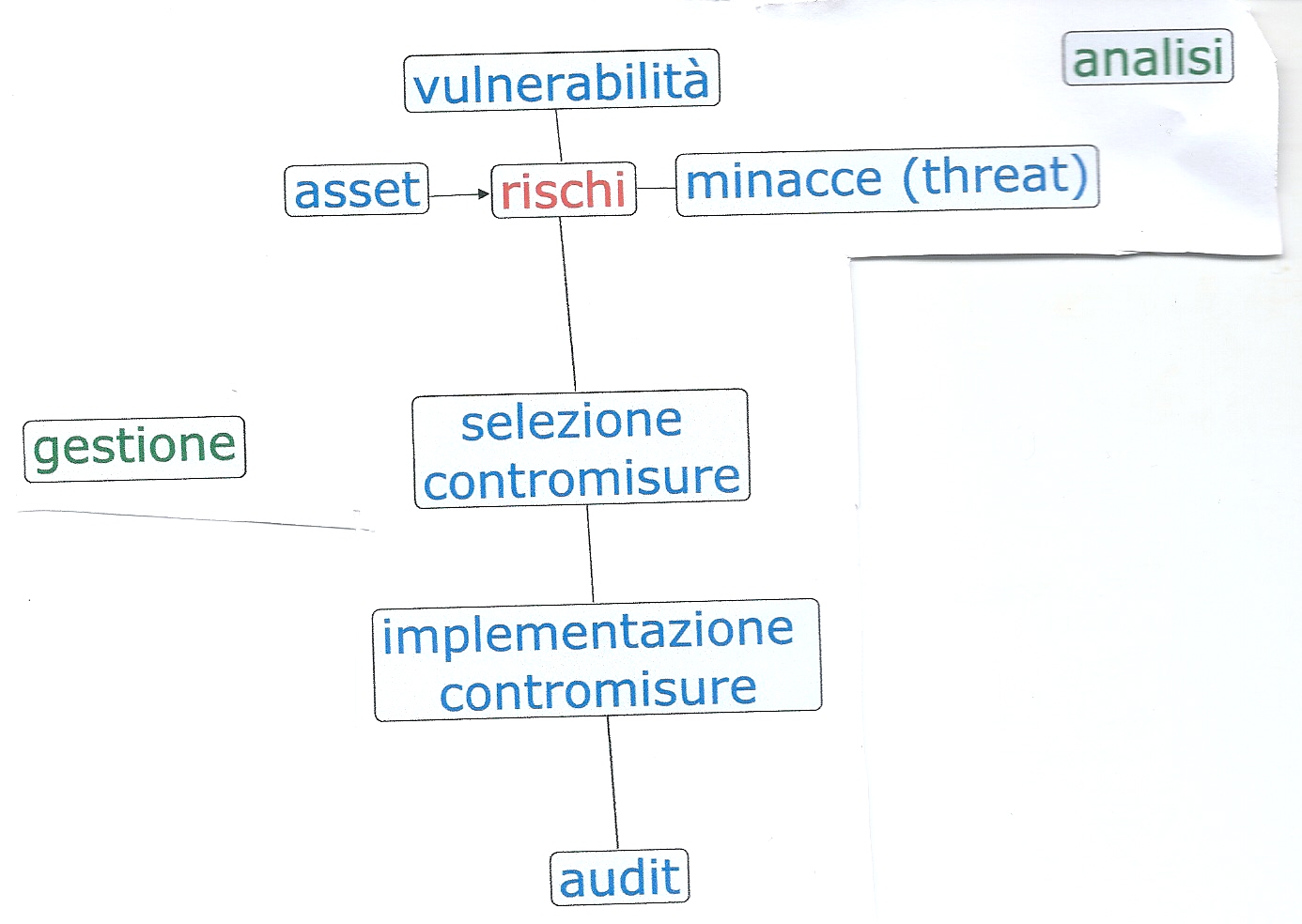
Il secondo gestione della problematica



Per ciascuna situazione di rischio, stima probabilistica evento dannoso e grado di dannosità



Nella figura seguente schema riassuntivo del processo stima dei rischi

la principale tipologie di minacce

Obiettivo + metodo + vulnerabilità = attacco

Attacco rete informatica--> accesso non autorizzato divise in 2 tipologie:

La prima è attacchi dimostrativi--> non pericolosi dimostrazione abilità hacker

La seconda è attacchi criminali--> minacce accesso informazioni

Minacce ai servizi ovvero--> impedire servizio utenti

Attacchi passivi--> lettura del contenuto di pacchetti sulla lan (difficile da rilevare, ed è possibile solo la prevenzione)

Attacchi attivi

Intercettazione--> intercettazione pass pere modifica dati

Sostituzione di un host--> sostituzione host falsificandone l'indirizzo di rete del mittente

Produzione--> inserimento di componenti allo scopo di far danni;

Virus--> attacco agli host per replicarsi

Worm--> provoca danni perchè consuma risorse senza attaccarsi ad un'altro programma

Dos--> tengono occupato l'host per impedire l'accesso alla rete

Intrusione--> accesso non autorizzato ad un host

Sicurezza nei sistemi informativi distribuiti

Serve a proteggere le informazioni sugli host e circolanti sulla rete e le risorse e i servizi offerti agli utenti.

per sicurezza si intende l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza dell'informazioni gestite

distinta in:

sicurezza nella rete--> a livello di sistema operativo (generale sull'host)

sicurezza sugli host--> a livello di applicazione (solo su programmi che necessitano di protezione)

riassunto dei 3 pilastri "sicurezza"

prevenzione--> protezione sistemi e comunicazioni

rilevazione--> controllo degli accessi tramite pass e certificati

investigazione--> controllo interno con confronto e collaborazione utenti

prevenzione tecniche adottate

uso della criptografia--> garantisce la riservatezza delle informazioni e integrità dei dati

autenticazione degli utenti--> permette di riconoscere in modo univoco

l'identità dell'interlocutore

autorizzazione--> parte più complessa dei servizi di integrazione e aziendali

firma elettronica--> garanzia di autenticità e non falsificabile

connessione tcp sicure mediante ssl--> ssl sta per "secure socket layer" offre sicurezza autenticazione in comunicazione, garantisce integrità dati e comunicazione

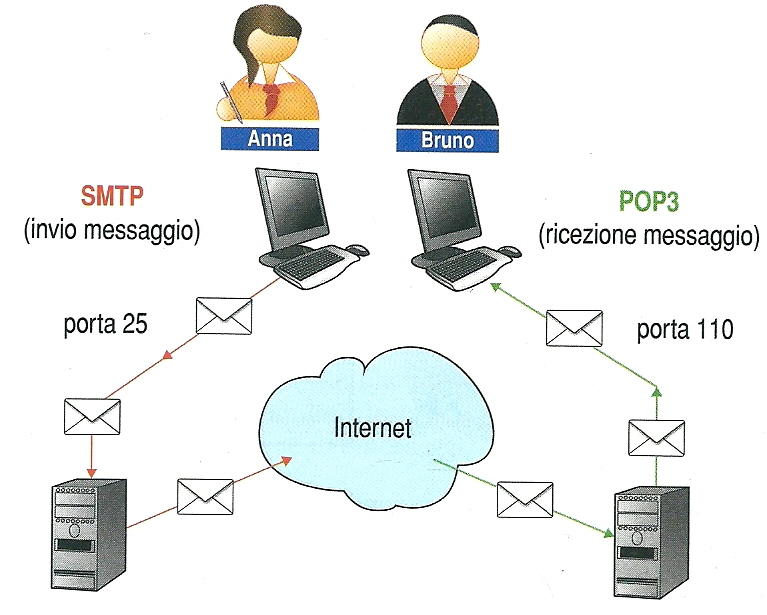
firewall--> difesa di un perimetro di una rete

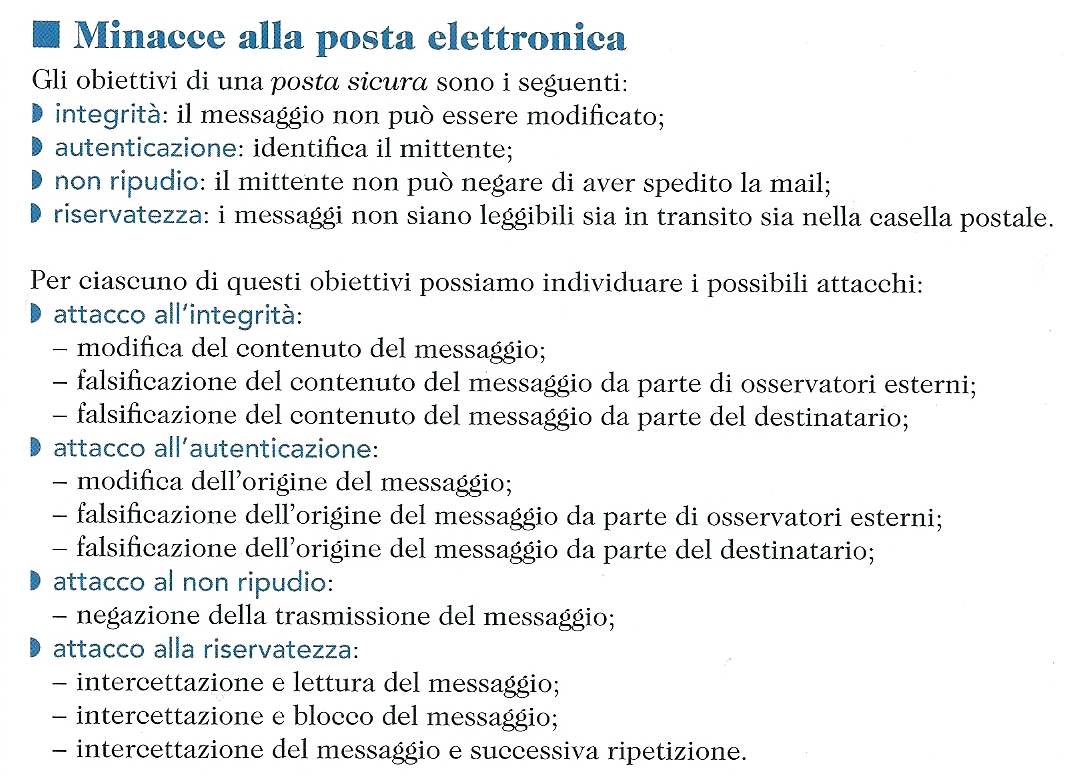
reti private--> acquisto linea uso esclusivo aziendale con costi considerevoli

reti private virtuali--> realizzare una VPN creando tunnel sulle infrastrutture di internet con connessione punto- punto



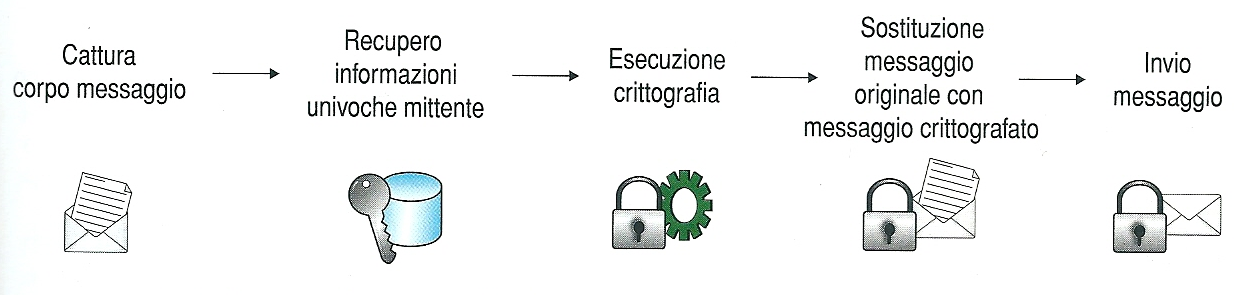
la posta elettronica è il servizio più importante di internet usato da tutto coloro che hanno un account; essendo pubblica è esposta a ogni tipo di attacco informatico.





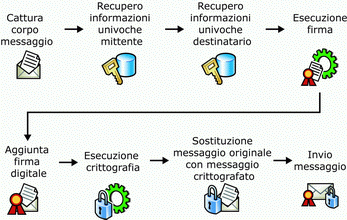
firma digitali--> la procedura per apporre la firma digitale segue lo schema seguente



criptografia dei messaggi--> procedura semplice riportata in questo schema

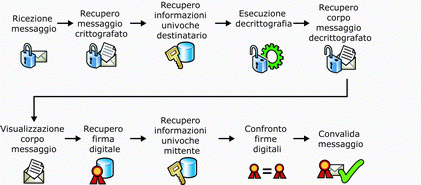
interazione delle firme digitali con la crittografia dei messaggi

schema applicazione di firma digitale con cifratura di un messaggi di posta elettronica.



1. acquisizione del messaggio
2. recupero informazioni che identificano il mittente in maniera univoca
3. recupero informazioni che identificano il destinatario in maniera univoca
4. applicazione al messaggio di una firma generata in base alle informazioni univoche del mittente
5. aggiunta della firma digitale al messaggio
6. crittografia del messaggio in base all'informazione relativa al destinatario
7. sostituzione del messaggio originario con quello crittografato
8. invio del messaggio

operazione di decrittografia e verifica di una firma digitale



1. ricezione del messaggio
2. recupero messaggio crittografato
3. recupero informazioni destinatario in maniera univoca
4. decrittografia del messaggio
5. restituzione del messaggio non crittografato
6. recapito del messaggio non crittografato al destinatario
7. recupero firma digitale del messaggio non crittografato
8. recupero informazione mittente
9. confronto della firma digitale inclusa nel messaggio con quella generata al momento della ricezione
10. se le firme corrispondono il messaggio è valido

ROSSI PATRICK 5I