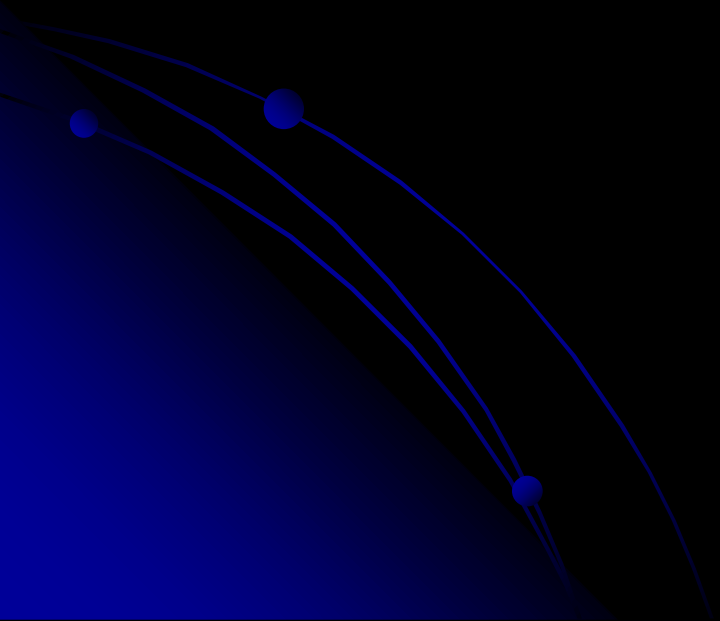


# La sicurezza informatica



# SICUREZZA INFORMATICA

- Sicurezza ATTIVA
- Sicurezza PASSIVA



# SICUREZZA PASSIVA

- Per *sicurezza passiva* :tecniche e gli strumenti di tipo difensivo, il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata.

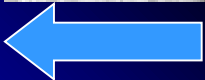


# SICUREZZA ATTIVA

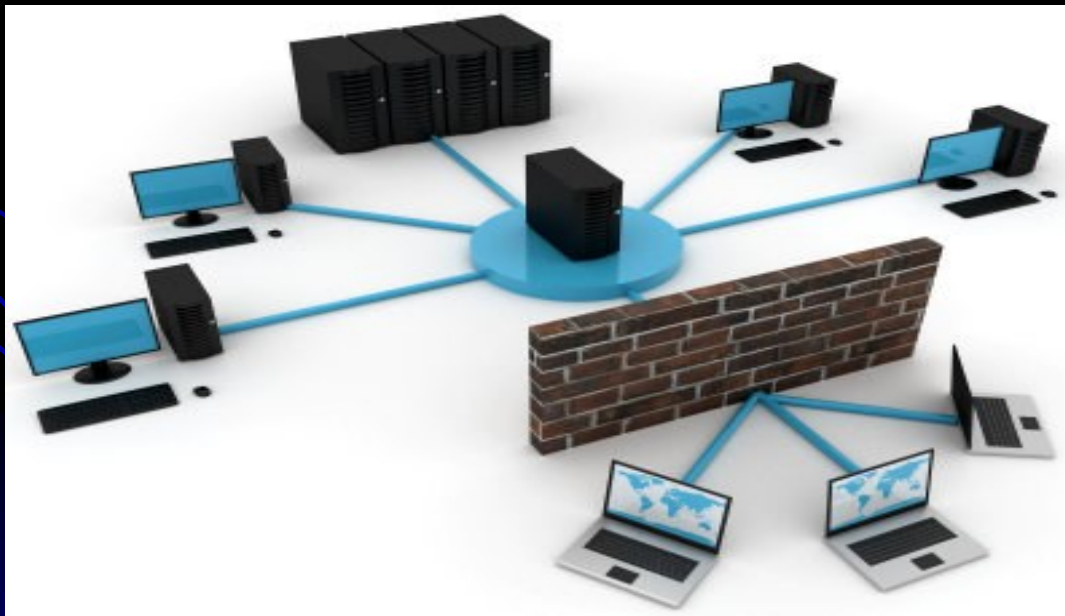
Per *sicurezza attiva* :tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri,



- In questa categoria rientrano sia strumenti **hardware** che **software**.



- Le possibili TECNICHE DI ATTACCO sono molteplici, perciò è necessario usare diverse barriere difensive fra l'attaccante e l'obiettivo.

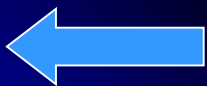


# TECNICHE DI ATTACCO

- Exploit :sfrutta una vulnerabilità di un software per acquisire i privilegi di un computer
- Cracking :per ottenere accesso ad un'area altrimenti riservata; si intende anche la violazione di sistemi informatici collegati ad Internet, allo scopo di danneggiarli, di rubare informazioni



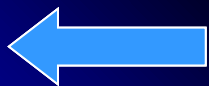
- Backdoor :sono usate per consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.
- Trojan :le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che, inconsapevolmente, lo installa; usato dall'attaccante per inviare istruzioni che il server esegue





# SICUREZZA delle INFORMAZIONI

- Dal momento che l'informazione è un bene aziendale, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.



- Per questo esistono, a carico delle imprese, precisi obblighi in materia di privacy.



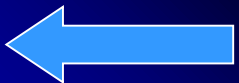
# SICUREZZA DEI DATI

- PARAMETRI DI PROTEZIONE:
- Disponibilità
- Integrità dei dati
- Riservatezza

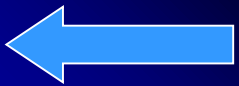


# DISPONIBILITA'

- La **disponibilità** misura l'attitudine di un'entità o sistema ad essere in grado di svolgere una funzione richiesta in determinate condizioni ad un dato istante (es. fornire un servizio ad un utente), o durante un dato intervallo di tempo, supponendo che siano assicurati i mezzi esterni eventualmente necessari.



- Può essere definita come il rapporto tra il tempo effettivo di funzionamento ed il tempo totale  
(dunque minore o uguale ad 1).



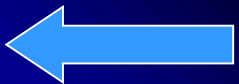
# INTEGRITA' DEI DATI

- Con il termine **integrità dei dati** si intende, la protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, accidentali oppure effettuate da una terza parte, essendo compreso nell'alterazione anche il caso limite della generazione ex novo di dati ed informazioni.

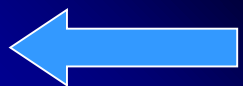


# RISERVATEZZA

- Nella sicurezza informatica per **confidenzialità** si intende la protezione dei dati e delle informazioni scambiate tra un mittente e uno o più destinatari nei confronti di terze



- Tale protezione deve essere realizzata a prescindere dalla sicurezza del sistema di comunicazione utilizzato:



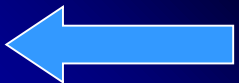
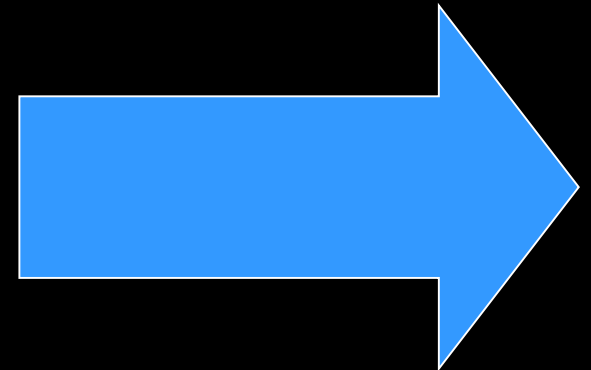


- Assume anzi particolare interesse il problema di assicurare la confidenzialità quando il sistema di comunicazione utilizzato è intrinsecamente insicuro (come ad esempio la rete internet).



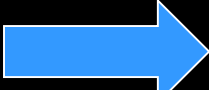
# SICUREZZA

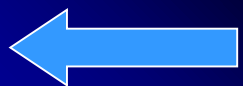
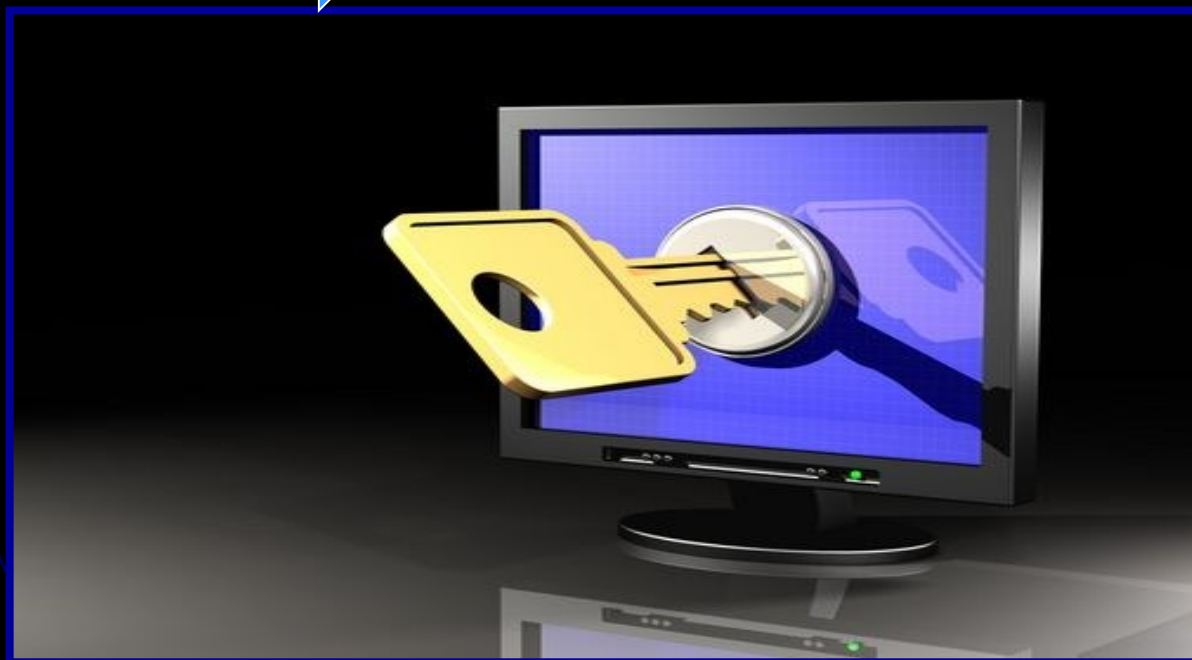
- L'accesso alla navigazione in Internet deve essere effettuato esclusivamente a mezzo della rete di istituto e solo per fini lavorativi o di studio. Gli utenti sono tenuti a utilizzare l'accesso ad internet in modo conforme e quindi devono:



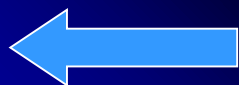
- navigare in Internet in siti attinenti allo svolgimento delle mansioni assegnate;
- registrarsi solo a siti con contenuti legati all'attività lavorativa;
- partecipare a forum o utilizzare chat solo per motivi strettamente attinenti l'attività lavorativa.



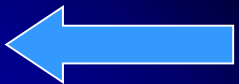
- Agli utenti è fatto espresso divieto di qualsiasi uso di internet che possa in qualche modo recare danno all'Istituto o a terzi e quindi di: 



- fare conoscere ad altri le proprie password di accesso, inclusi gli amministratori di sistema\*;
- usare Internet per motivi personali;
- servirsi dell'accesso Internet per attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente;
- scaricare il software gratuiti dalla rete, salvo casi di comprovata utilità e previa autorizzazione in tal senso da parte del responsabile;



- Tentare di guardare e/o scaricare immagini o video pornografici o pedo-pornografici;
- Effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati;
- Inviare fotografie, dati personali o di amici dalle postazioni Internet.



- Tentare di attaccare un altro utente o accedere abusivamente ad un altro sistema;
- Tentare di scaricare software pirata.
- Utilizzare in modo improprio, inconsapevole o non autorizzato i SOCIAL MEDIA

