Segurança da informação:

Esta relacionada diretamente a proteção que um determinado conjunto de dados que possuem alguma forma de valor seja para uma organização ou pessoa. A segurança da informação se divide em três pilares básicos essenciais são eles:

* Confidencialidade
* Integridade
* Disponibilidade

Confidencialidade – propriedade que limita o acesso à informação somente por entidades legitimas ou autorizadas pelo proprietário de informação.

Integridade – propriedade que garante que a informação mantenha todas as características originais estabelecidas pelo proprietário da mesma, incluindo garantia do seu ciclo de vida (nascimento, manutenção e destruição).

Disponibilidade – propriedade que garante que a informação esteja sempre disponível para seu uso legitimo, ou seja por aqueles autorizados a pelo proprietário da informação.

## Mecanismos de segurança:

Controles físicos – são barreiras que limitam o contato ou acesso a informação ou a infraestrutura que há suporta, são exemplos: portas, trancas, paredes, blindagem, guarda, etc.

Controles lógicos – são barreiras que impedem ou limitam o acesso à informação que está em um ambiente eletrônico controlado, e que de outra maneira ficaria exposto a alteração não autorizada.

## Mecanismos que ajudam no controle logico:

Criptografia- permite a transformação reversível da informação em formato ininteligível a terceiros. Utilizando para isso algoritmos determinados e uma chave secreta, para a partir de um conjunto de dados não criptografados produzir um sequencia de dados criptografados. A operação inversa e a decifração.

Assinatura digital- conjunto de dados geralmente criptografados associados a um documento com a finalidade de garantir sua integridade.

Mecanismo de controle de acesso- palavras chaves, sistemas biométricos firewalls e cartões inteligentes.

Honeypot – e o nome dado a um software cuja a função e a de detectar ou impedir a ação de um cracker ou spammer, ou de qualquer agente externo estranho ao sistema.