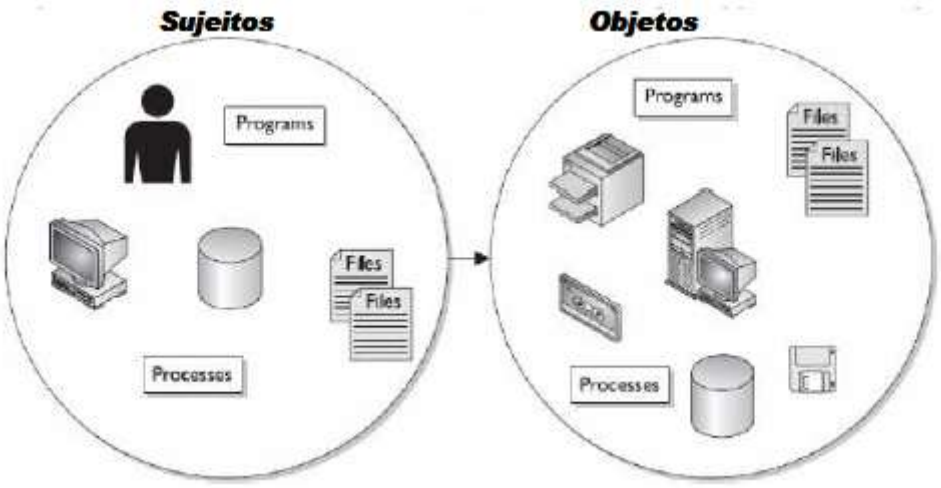
Controle de acesso Lógico

O controle de acesso lógico têm como objetivo proteger os recursos computacionais contra perda, danos, modificação ou divulgação não autorizada.

Os sistemas computacionais não podem ser somente protegidos por dispositivos físicos (cadeados, alarmes, etc...), ainda mais se os computadores estiverem conectados a redes locais ou de longa distância.



Os dados, programas e sistemas deve ser protegidos contra tentativas de acessos não autorizados, feitas por usuários ou outros programas. É preciso controlar também o acesso lógico. Este acesso é feito por um usuário ou um processo, através do acesso a um arquivo ou um outro recurso como uma impressora, por exemplo.

A segurança lógica é um processo em que um sujeito ativo deseja acessar um objeto passivo. O sujeito é um usuário ou um processo da rede e o objeto pode ser um arquivo ou outro recurso de rede (estação de trabalho, impressora, etc). Compreende um conjunto de medida e procedimentos, adotados pela empresa ou intrínsecos aos sistemas utilizados.

Recursos e informações a serem protegidos:

- Aplicativos (Programas Fonte e Objeto)
- Arquivos de Dados
- Utilitários e Sistema Operacional
- Arquivos de Senha
- Arquivos de LOG

Os controles de acesso lógico (CALs) tem com objetivo garantir que:

- Apenas usuários autorizados tenham acesso aos recursos realmente necessários para suas tarefas.

- O acesso a recursos críticos seja bem monitorado e restrito.
- Usuários sejam impedidos de executar transações incompatíveis com sua função ou além de suas responsabilidades.

Exemplos de utilização de controle de acesso lógico:

· Certificados Digitais
· Login e Senha
· Assinatura Digital
· CAPTCHA (Completely Automated Public Turing test to tell Computers and
· Humans Apart") – Teste de Turing público completamente automatizado para diferenciação de acesso entre computadores e humanos.

Controle de acesso Físico

A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Cuida da proteção de todos os ativos valiosos da organização e engloba todas as instalações físicas, internas e externas, em todas as localidades em que a organização se faz presente. Cuida também da proteção de ativos importante que estejam sendo transportados, como valores ou fitas de backup.

Itens para controle de acesso:

- Perímetro de Segurança
- Ativos de informação (Estações de Trabalho, Equipamentos Eletrônicos Portáteis)
- Instalações Físicas (DataCenter ou Centro de Dados)
- Usuários

Exemplos:

Barreiras de Contenção

- **Cercas** Uma das maiores vantagens do uso de cercas é o nível de visão que é mantido e o ruído produzido por alguém que tenta ultrapassá-las. As cercas podem ser eletrificadas,

possuir arame farpado e/ou alarmes de intrusão no topo, garantindo um maior nível de segurança. Um dos maiores problemas das cercas é a facilidade com que podem ser cortadas.

- Portões – Portões são mecanismos de controle de acesso físico que se aplicam a pessoas e, com maior freqüência, aos veículos.

Alarmes de intrusão

Tem a finalidade de alertar para a existência de um possível intruso no perímetro de segurança

Iluminação

Item muito importante na segurança física, pois além de iluminar e ampliar o campo de visão durante o período noturno, é também um mecanismo preventivo e desencorajador.

Sensores de presença

Detectan a presença de pessoas dentro de um ambiente controlado. Tencologias mais utilizadas:

· Quebra de circuito elétrico

· Interrupção de feixe de luz

· Infravermelho passivo

· Detector ultra-sônico

· Dispositivo de microondas

Alarmes – dispositivos de detecção de abertura e fechamento de portas ou janelas. Podem disparar alarmes ou ser monitorados remotamente por sistemas de vigilância mais complexos.