

Segurança e Informação
Ativo de ouro dessa nova era
Aula 01

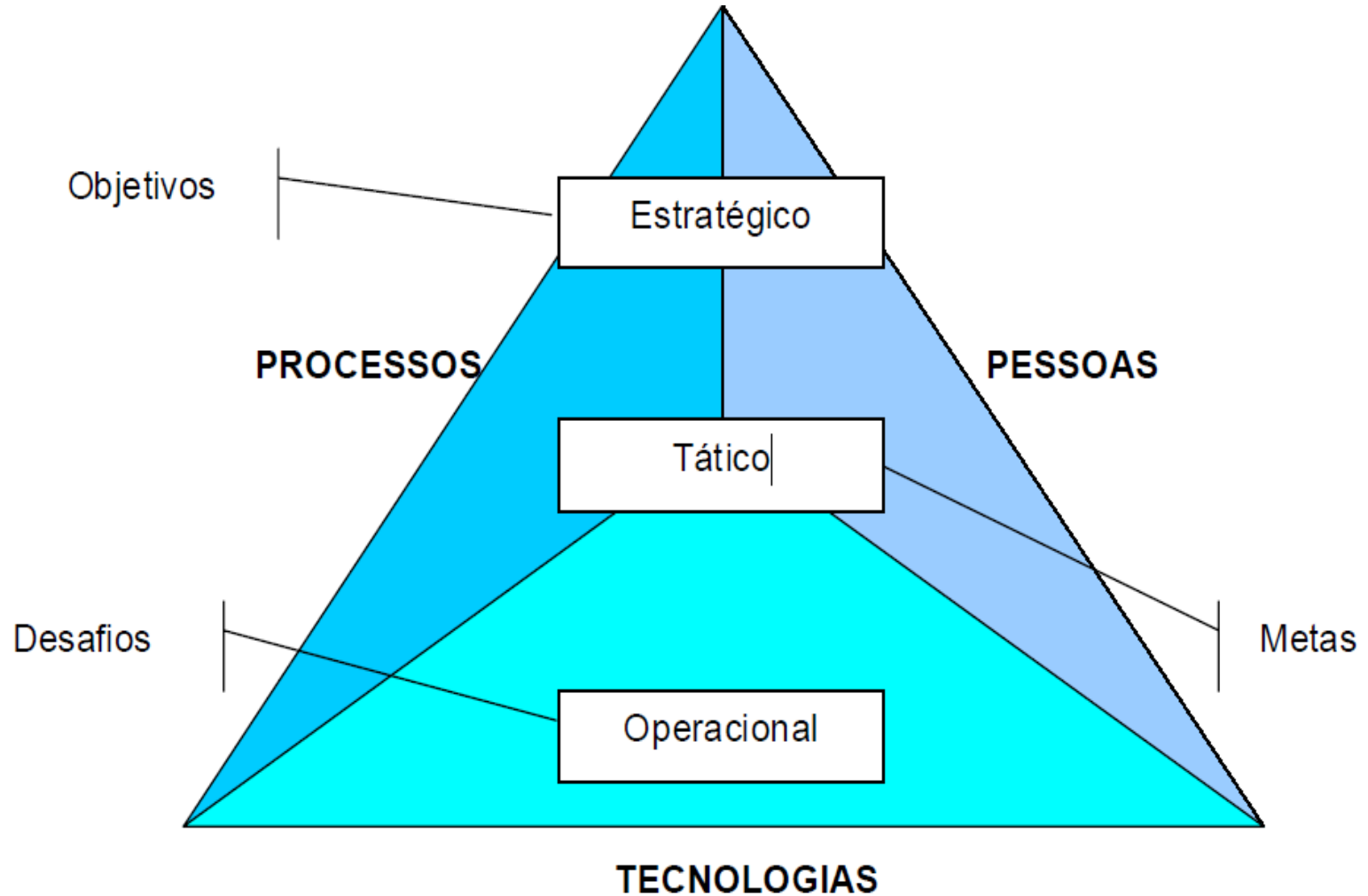


Soraya Christiane / Tadeu Ferreira

Informação

- ▶ É o ativo que tem um valor para a organização e necessita ser adequadamente protegida (NBR 17999, 2003).
- ▶ É o principal patrimônio da empresa e está sob constante risco (Dias, 2000).
- ▶ Representa a inteligência competitiva dos negócios e ativo crítico para a continuidade operacional (Sêmola, 2003).
- ▶ A informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade (Rezende e Abreu, 2000).
- ▶ As empresas já perceberam que o domínio da tecnologia como aliado para o controle da informação é vital.

Requisitos da Informação



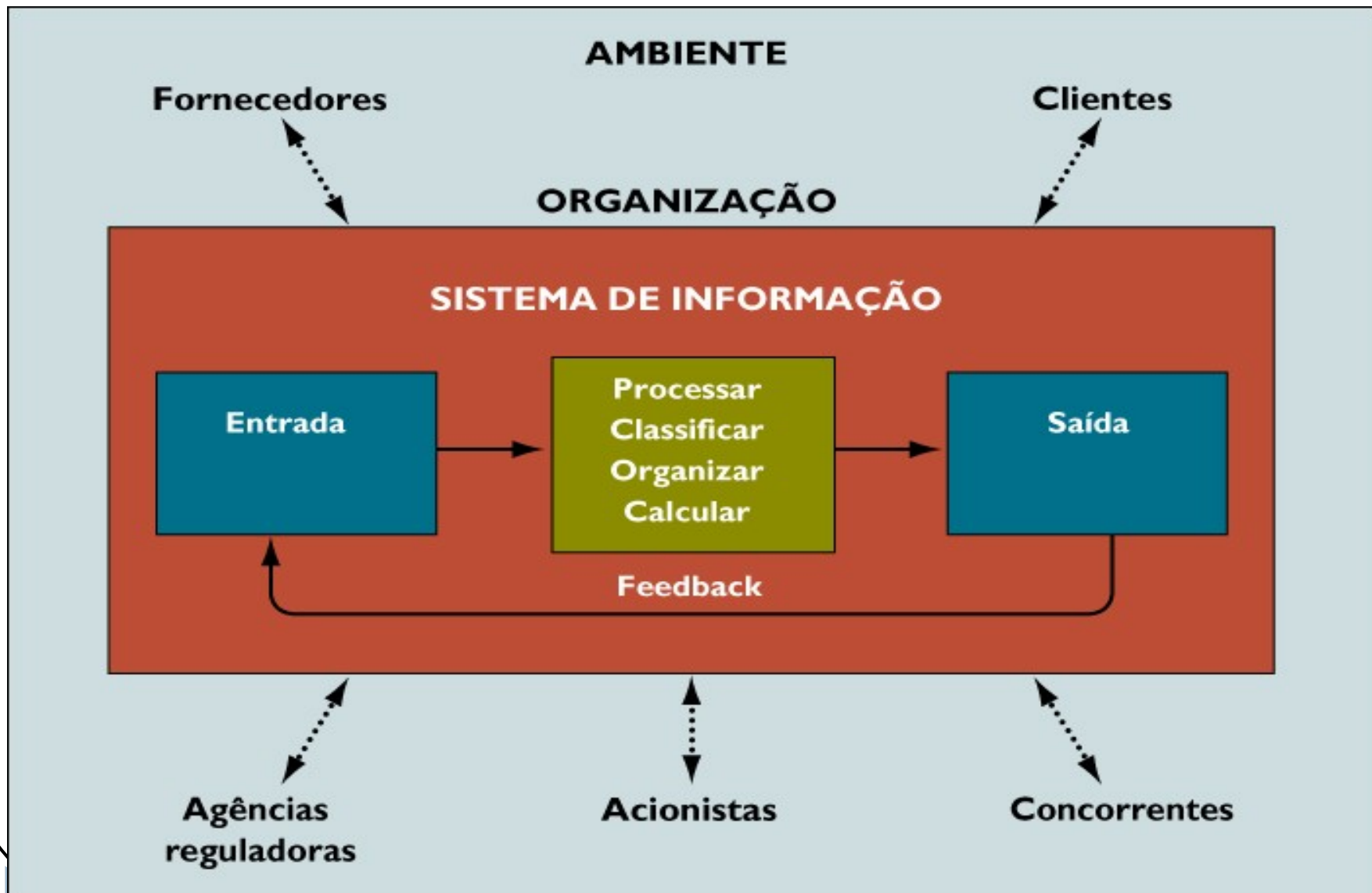
Informação

- ▶ Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente.
- ▶ A evolução dos dados e sistemas, a informação ganhou mobilidade, inteligência e real capacidade de gestão. A informação é substrato da inteligência competitiva;
- ▶ Deve ser administrada em seus particulares, diferenciada e salvaguardada.

Sistemas de informação

- ▶ Pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização.
- ▶ Auxiliam os gerentes e trabalhadores a analisar problemas, visualizar assuntos complexos e criar novos produtos.
- ▶ Contêm informações sobre pessoas, locais e coisas significativas para a organização ou para o ambiente que a cerca.
- ▶ Três atividades em um sistema de informação produzem as informações de que as organizações necessitam: a entrada, o processamento e a saída.

Sistemas de Informação



Produção da Informação

- ▶ A entrada captura ou coleta dados brutos de dentro da organização ou de seu ambiente externo.
- ▶ O processamento converte esses dados brutos em uma forma mais significativa.
- ▶ A saída transfere as informações processadas às pessoas que as utilizarão ou às atividades em que serão empregadas.
- ▶ Feedback é a entrada que volta a determinados membros da organização para ajudá-los a avaliar ou corrigir o estágio de entrada.

Oportunidades e Ameaças das Informações e sistemas.

- ▶ A informação auxilia os executivos a identificar ameaças, oportunidades e respostas eficazes para a empresa.
- ▶ Recurso essencial para a definição de estratégias alternativas, exige um constante aprendizado.
- ▶ A eficácia pode ser definida pela relação entre resultados obtidos e resultados pretendidos.
- ▶ Adotar políticas estratégicas eficazes, é necessário que estas sejam baseadas em informação.

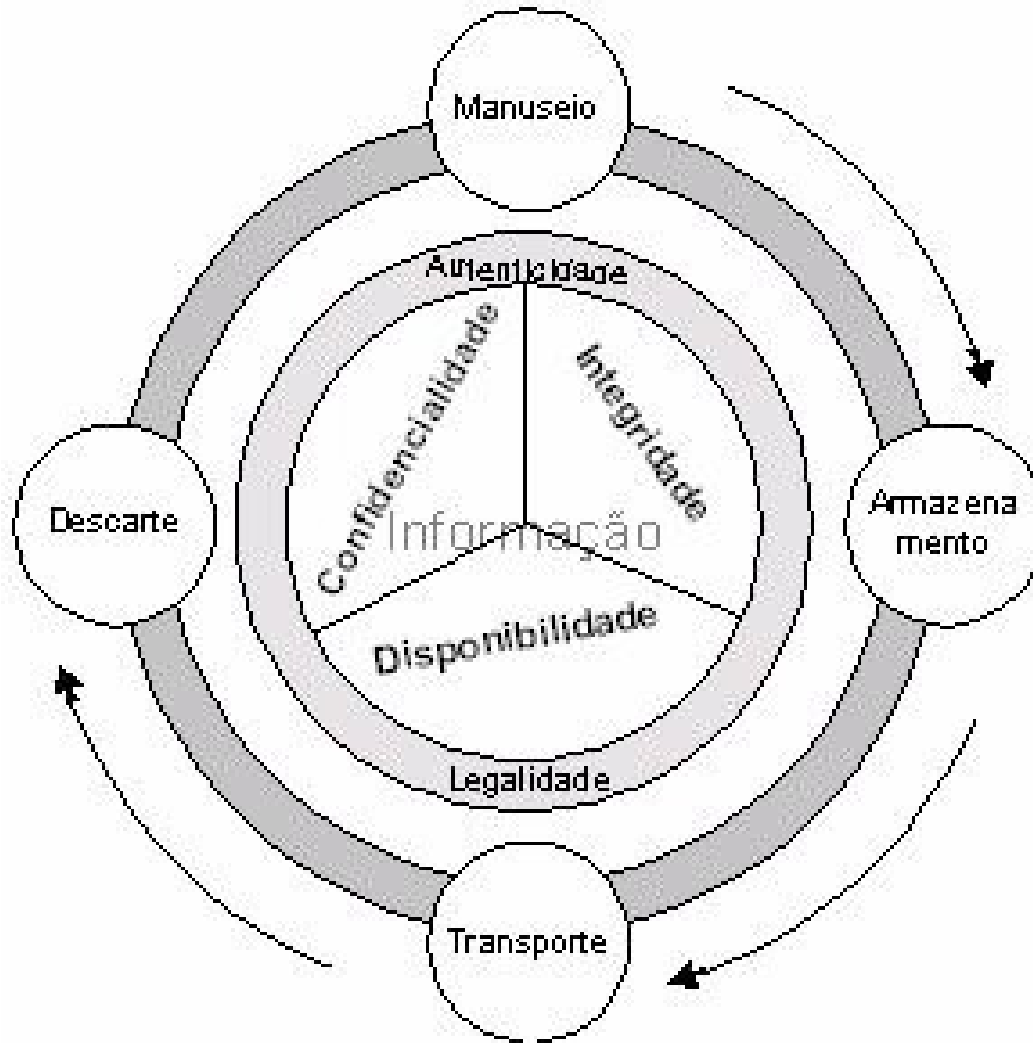
O valor da Informação

- ▶ A informação certa comunicada a pessoa certa é de importância vital para a empresa.
- ▶ Cuidado com a integridade, precisão, atualidade, interpretabilidade e valor da informação.
- ▶ Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais.
- ▶ No entanto, o custo de integridade da informação vital será menor que o custo de não dispor dela adequadamente

Tipos e prioridades da informação

- ▶ **Pública** - informação que pode vir a público sem maiores conseqüências ao funcionamento normal da empresa.
- ▶ **Interna** - o acesso a esse tipo de informação deve ser evitado, embora as conseqüências do uso não autorizado não sejam por demais sérias.
- ▶ **Confidencial** - informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;
- ▶ **Secreta** - informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas

Ciclo de vida da informação



Ciclo da Informação

- ▶ **Manuseio** - Momento em que a informação é criada e manipulada.
- ▶ **Armazenamento** - Momento em que a informação é armazenada.
- ▶ **Transporte** - Momento em que a informação é transportada.
- ▶ **Descarte** - Momento em que a informação é descartada.

Segurança e seus critérios

- ▶ Dependência do negócio aos sistemas de informação;
- ▶ Surgimento de novas tecnologias e formas de trabalho;
- ▶ Comércio eletrônico, as redes virtuais privadas e os funcionários móveis;
- ▶ As empresas despertaram para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.

Segurança e seus critérios

- ▶ As redes de computadores e a Internet mudaram as formas como se usam sistemas de informação.
- ▶ As oportunidades, os riscos à privacidade e integridade da informação tornaram-se amplos.
- ▶ A segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito.

Segurança e seus princípios

- ▶ É a base para dar às empresas a liberdade necessária para a criação de novas oportunidades de negócio.
- ▶ Os negócios estão cada vez mais dependentes das tecnologias e estas precisam estar de tal forma a proporcionar confidencialidade, integridade e disponibilidade (NBR 17999, 2003) -os princípios básicos para garantir a segurança da informação.

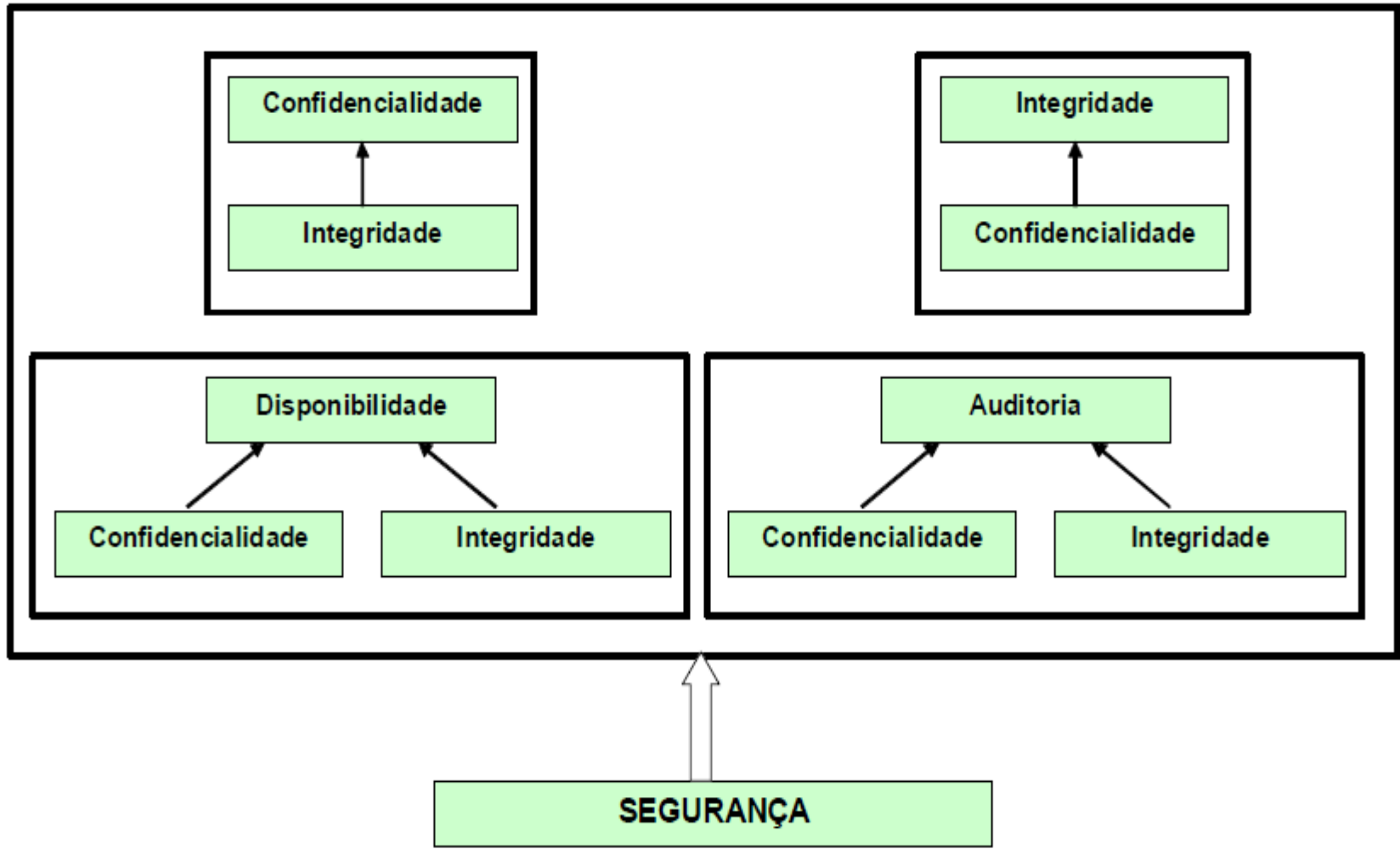
Princípios da Segurança da Informação

- ▶ **Confidencialidade** - A informação somente pode ser acessada por pessoas explicitamente autorizadas; Garantir a identificação e autenticação das partes envolvidas.
- ▶ **Disponibilidade** - A informação ou sistema de computador deve estar disponível no momento em que a mesma for necessária;
- ▶ **Integridade** - A informação deve ser retornada em sua forma original no momento em que foi armazenada; É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

Respeitar também

- ▶ **Autenticidade - Garante que a informação ou o usuário da mesma é autêntico;** Atesta com exatidão, a origem do dado ou informação;
- ▶ • **Não repúdio - Não é possível negar (no sentido de dizer que não foi feito)** uma operação ou serviço que modificou ou criou uma informação; Não é possível negar o envio ou recepção de uma informação ou dado;
- ▶ • **Legalidade - Garante a legalidade (jurídica) da informação; Aderência de** um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.
- ▶ • **Privacidade** -privada deve ser vista / lida / alterada somente pelo seu dono.
- ▶ • **Auditoria - Rastreabilidade dos diversos passos que um negócio ou** processo realizou ou que uma informação foi submetida, identificando os participantes, os locais e horários de cada etapa.

Outros aspectos importantes



Essenciais

- ▶ A confidencialidade é dependente da integridade, pois se a integridade de um sistema for perdida, os mecanismos que controlam a confidencialidade não são mais confiáveis.
- ▶ A integridade é dependente da confidencialidade, pois se alguma informação confidencial for perdida (senha de administrador do sistema, por exemplo) os mecanismos de integridade podem ser desativados.
- ▶ Auditoria e disponibilidade são dependentes da integridade e confidencialidade, pois estes mecanismos garantem a auditoria do sistema (registros históricos) e a disponibilidade do sistema (nenhum serviço ou informação vital é alterado).

Morais da segurança

- ▶ As portas dos fundos são tão boas quanto às portas da frente.



- ▶ Uma corrente é tão forte quanto o seu elo mais fraco.



Morais da segurança

- ▶ Um invasor não tenta transpor as barreiras encontradas, ele vai ao redor delas buscando o ponto mais vulnerável.



Ameaça

- ▶ **Qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e conseqüentemente gerando um determinado impacto.**

Quanto a intencionalidade

- ▶ **Naturais - Ameaças decorrentes de fenômenos da natureza, como** incêndios naturais, enchentes, terremotos, tempestades, poluição, etc.
- ▶ **Involuntárias - Ameaças inconscientes, quase sempre causadas pelo** desconhecimento. Podem ser causados por acidentes, erros, falta de energia, etc.
- ▶ **Voluntárias - Ameaças propositais causadas por agentes humanos como** *hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus* de computador, incendiários.

Ameaças em sistemas

- ▶ Falha de hardware ou software
- ▶ Ações pessoais
- ▶ Invasão pelo terminal de acesso
- ▶ Roubo de dados, serviços, equipamentos
- ▶ Incêndio
- ▶ Problemas elétricos
- ▶ Erros de usuários
- ▶ Mudanças no programa
- ▶ Problemas de telecomunicação
- ▶ Elas podem se originar de fatores técnicos, organizacionais e ambientais, agravados por más decisões administrativas (Laudon e Laudon, 2004).

Ataques

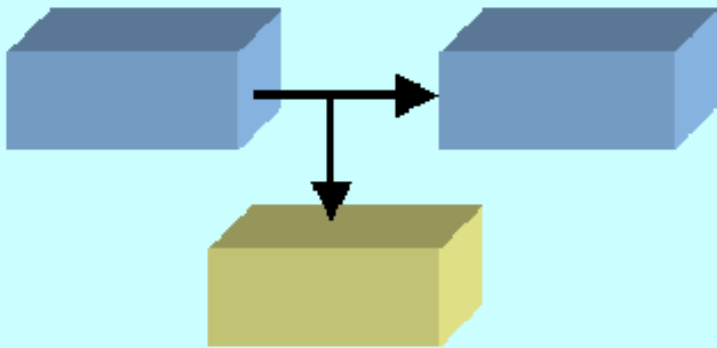
- ▶ O ataque é ato de tentar desviar dos controles de segurança de um sistema de forma a quebrar os princípios da segurança.
- ▶ O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contramedidas existentes.

Possíveis ataques

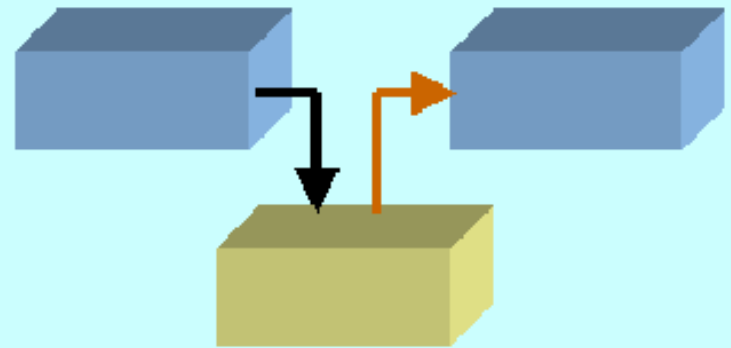
- ▶ **Interceptação:** considera-se interceptação o acesso a informações por entidades não autorizadas (violação da privacidade e confidencialidade das informações).
- ▶ **Interrupção:** pode ser definida como a interrupção do fluxo normal das mensagens ao destino.
- ▶ **Modificação:** consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.
- ▶ **Personificação:** considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidad

Possíveis ataques

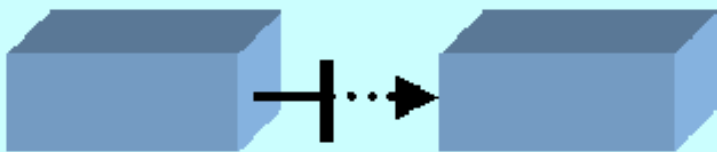
Interceptação



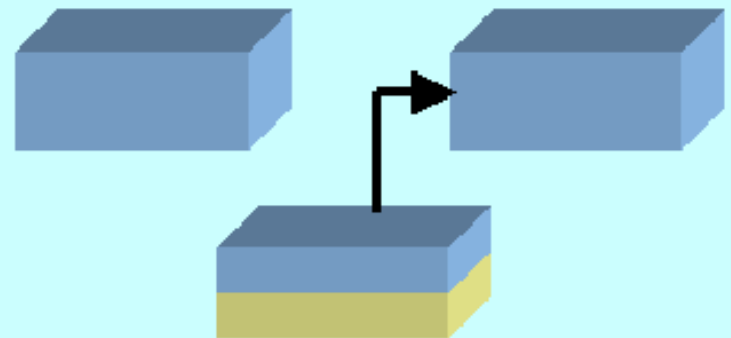
Modificação



Interrupção



Personificação

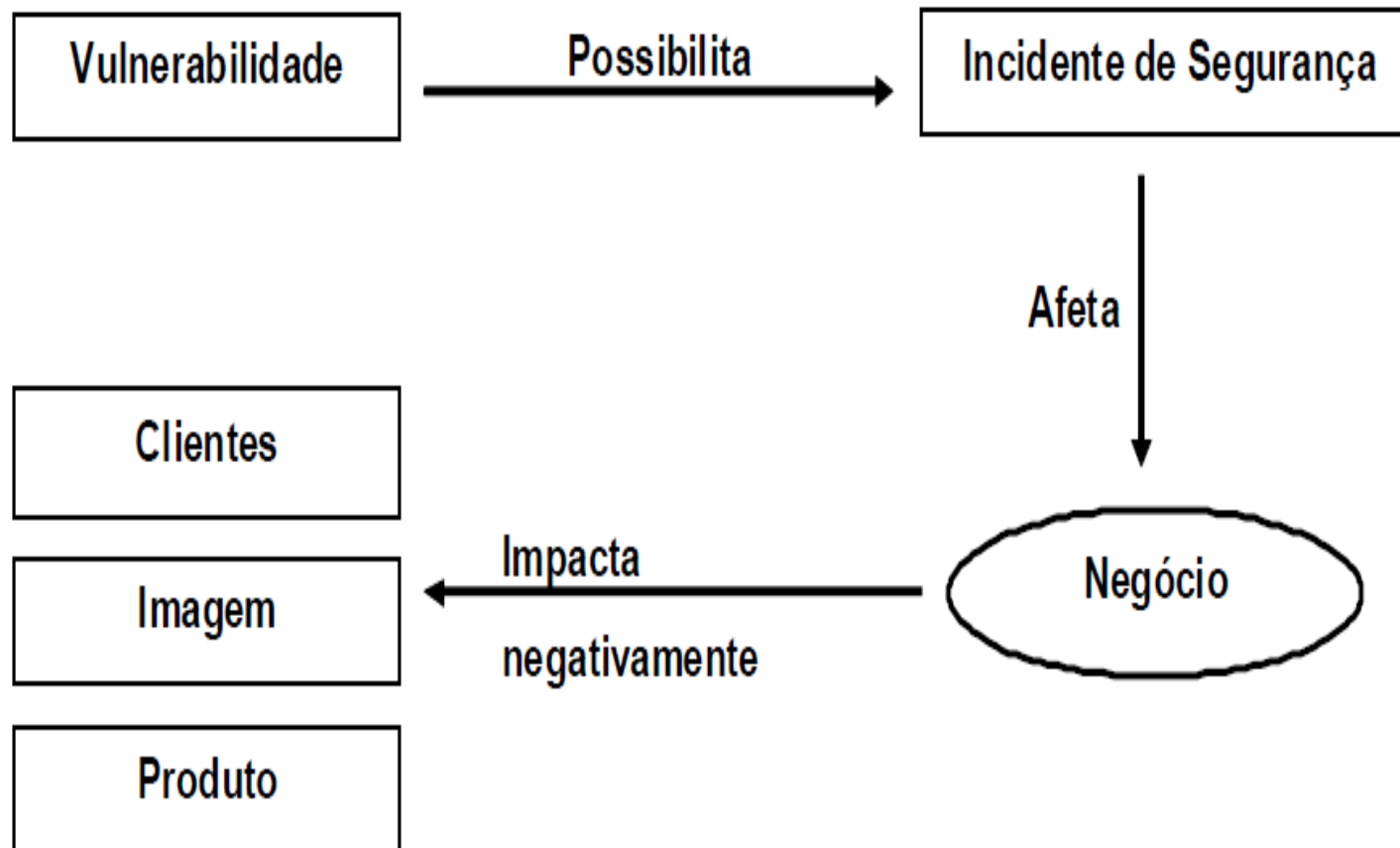


Vulnerabilidade

▶ A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque.

- ▶ Todos os ambientes são vulneráveis, partindo do princípio de que não existem ambientes totalmente seguros.
- ▶ Cada vulnerabilidade existente pode permitir a ocorrência de determinados incidentes de segurança.

Vulnerabilidade



Porque os sistemas podem estar vulneráveis?




- ▶ Nível de complexidade versus nível de proteção.
- ▶ Arranjos complexos de hardware, software, pessoas e organizacionais criam novas áreas e oportunidades para invasão e manipulação.
- ▶ Redes sem fio que utilizam tecnologias baseadas em rádio são ainda mais vulneráveis à invasão, porque é fácil fazer a varredura das faixas de radiofrequência.

Mecanismos de controle

▶ **Autenticação e autorização**

- ▶ A autorização é o processo de conceder ou negar direitos a usuários ou sistemas, por meio das chamadas listas de controle de acessos (*Access Control Lists - ACL*);
- ▶ A autenticação é o meio para obter a certeza de que o usuário ou o objeto remoto é realmente quem está afirmando ser. Determina quem está autorizado a ter acesso à informação, permite trilhas de auditoria e assegura a legitimidade do acesso.

Mecanismos de identificação

- ▶ **Identificação positiva (O que você sabe) - Na qual o requerente:** demonstra conhecimento de alguma informação utilizada no processo de autenticação, por exemplo um  **User Login** form with fields for Username and Password, and a Login button.
- ▶ **Identificação proprietária (O que você tem) - Na qual o requerente:** demonstrar possuir algo a ser utilizado no de autenticação, como um cartão magnético. 
- ▶ **Identificação Biométrica (O que você é) - Na qual o requerente exibe** alguma característica própria, tal como a sua impressão digital. 



Combate a ataques e invasões

- ▶ Dispositivos de software e hardware de proteção, controle de acesso e combate a ataques e invasões, mecanismos importante no modelo de gestão de segurança, à medida que as conexões eletrônicas e tentativas de acesso indevido crescem exponencialmente.
- ▶ Existem dispositivos destinados ao monitoramento, filtragem e registro de acessos lógicos, bem como dispositivos voltados pra a segmentação de perímetros, identificação e tratamento de tentativas de ataque.

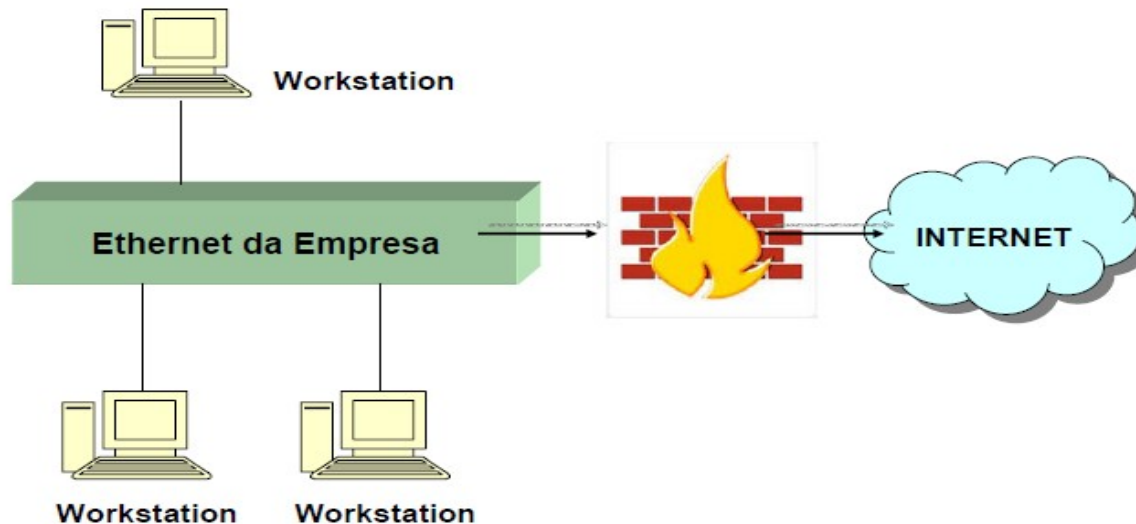
Firewall

- ▶ É um sistema (ou grupo de sistemas) que reforçam a norma de segurança entre uma rede interna segura e uma rede não-confiável como a Internet.
- ▶ Pode ser um PC, um roteador, um computador de tamanho intermediário ou a combinação destes que determine qual informação ou serviços podem ser acessados de fora e a quem é permitido usar a informação e os serviços de fora.
- ▶ É instalado no ponto onde a rede interna segura e a rede externa não-confiável se encontram, ponto que também é conhecido como ponto de estrangulamento.
- ▶ Semelhante a um edifício de acesso controlado.
- ▶ Projetado para permitir que dados confiáveis passem, negar serviços vulneráveis e proteger a rede interna contra ataques externos.
- ▶ O administrador da rede deve examinar regularmente os registros de eventos e alarmes gerados pelo firewall.

Filtro de Pacotes

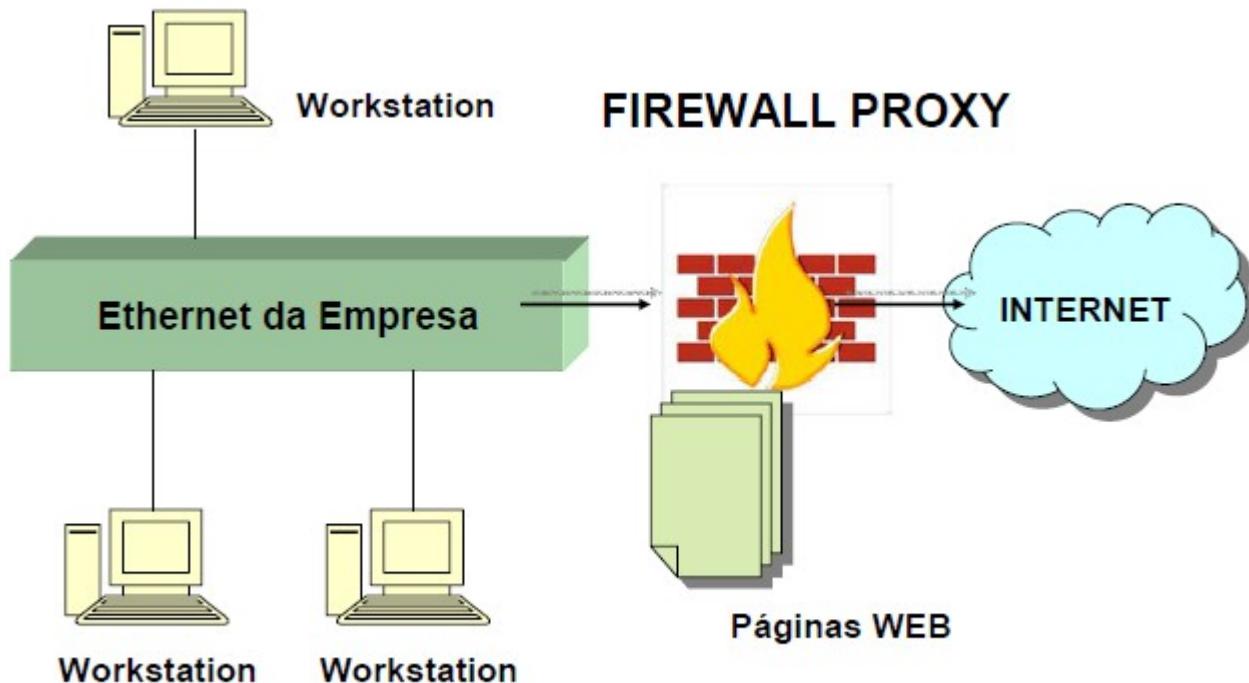
- ▶ Mecanismos que, mediante regras definidas pelo administrador em um firewall, permite ou não a passagem de datagramas IP em uma rede.
- ▶ Filtrar pacotes para impedir o acesso a um serviço de Telnet, um chat ou mesmo um site na Internet.

FIREWALL DUAL HOMED HOST



Servidores Proxy

- ▶ Permite executar a conexão ou não a serviços em uma rede modo indireto.



Detectores de intrusão - IDS

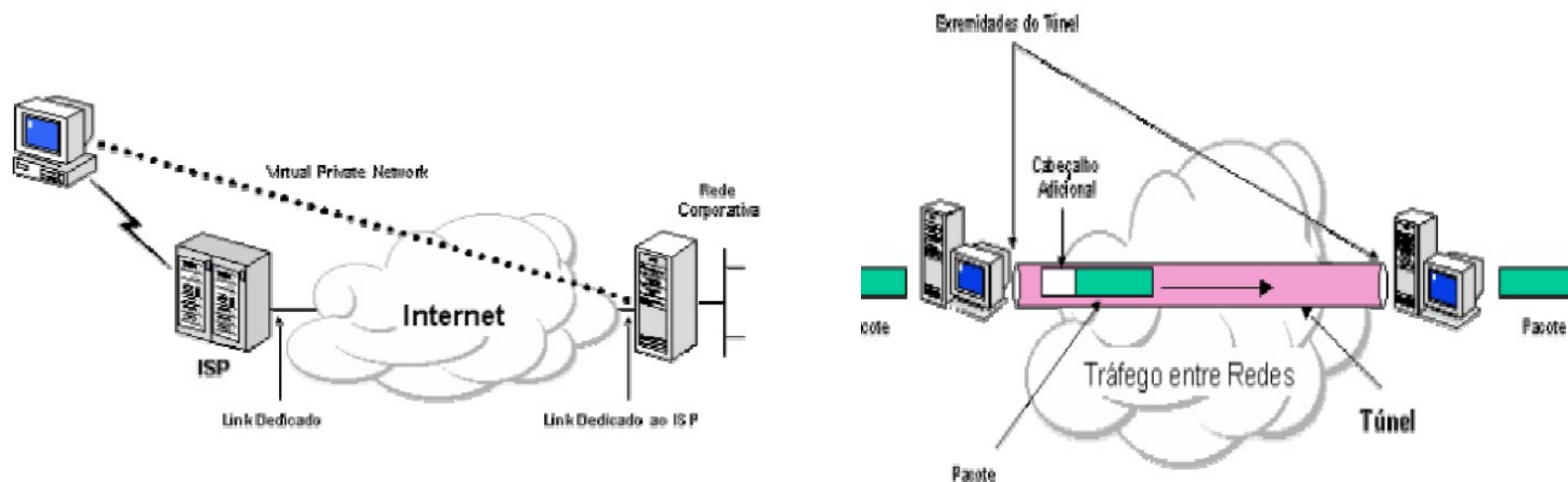
- ▶ Ferramenta com o objetivo detectar se alguém está tentando entrar em um sistema ou se algum usuário legítimo está fazendo mau uso do mesmo.
- ▶ É executada constantemente em *background* (somente gera uma notificação quando detecta alguma ocorrência que seja suspeita ou ilegal).
- ▶ Classificados com relação a sua forma de monitoração (origem dos dados) e aos mecanismos (algoritmos) de detecção utilizados.
- ▶ **Ex: Detecção por assinatura - os dados coletados são comparados com uma** base de registros de ataques conhecidos (assinaturas). Os sistemas antivírus também adotam a detecção por assinatura.

Privacidade das comunicações

- ▶ Criptografia é a ciência de escrever ocultamente;
- ▶ É a maneira mais segura de se enviar informações através de um canal de comunicação inseguro como, por exemplo, a Internet.
- ▶ Um conjunto de técnicas que são usadas para manter a informação segura.
- ▶ Estas técnicas consistem na utilização de chaves e algoritmos de criptografia. Tendo conhecimento da chave e do algoritmo usado é possível desembaralhar a mensagem recebida.

Virtual private network - VPN

- ▶ Túneis de criptografia entre pontos autorizados, através da Internet ou outras redes públicas e/ou privadas ou usuários remotos para transferência de informações, de modo seguro.
- ▶ Não permite que não sejam modificados ou interceptados.
- ▶ Vantagens: redução de custos (elimina a necessidade de links dedicados de longa distância que podem ser substituídos pela Internet).



Exercício de Apoio

1. Qual a importância da informação para as empresas no atual cenário?
2. O que é um sistema de informação e qual a sua utilidade na organização?
3. Quais as quatro fases do ciclo de vida da informação?
4. Qual a diferença entre ameaça, vulnerabilidade e incidente de segurança?
5. Cite e conceitue os princípios da segurança da informação?
6. Qual a norma que determina os requisitos de segurança da informação?
7. Quais os principais mecanismos de combate a ataques e invasões?
8. Qual a função do firewall e da VPN?