Segurança da Informação

Parte I

Prof. Wanderson Senra Michel

wanderson.senra@udf.edu.br

- **Ativos**
  - Qualquer elemento que tenha valor para a organização [ISO 27002];
  - Os ativos fornecem suporte aos processos de negócios, portanto devem ser protegidos. Todo elemento utilizado para armazenar, processar, transportar, armazenar , manusear e descartar a informação, inclusive a própria.
  - **Categorias de Ativos**
    - Os ativos podem ser classificados / agrupados de diversas formas:
      - Informações; Hardware; Software; Ambiente Físico; Pessoas;
      - Lógico; Físico Humano;
      - Equipamentos; aplicações, usuários, ambientes, informações e processos;

Dados - Conceituação

“conjunto de fatos distintos e objetivos, relativos a eventos”

Davenport & Prussak (1998)

- Estímulos captados pelos sentidos humanos - símbolos gráficos ou sonoros.
- É o registro estruturado de transações.
- É a matéria-prima essencial para a informação, é a descrição exata de algo ou de algum evento.
- Indica uma situação.
- Define o conteúdo de um campo.
- Não transmite conhecimento algum.
- Qualquer registro que pode ser armazenado em meio magnético (discos, fitas etc.) - palavras, letras ou símbolos organizados sobre um determinado assunto.

Informação - Conceituação

“são dados interpretados, dotados de relevância e propósito”

Drucker (1998)

- “A informação é um produto capaz de gerar conhecimento e a informação que um sinal transmite é o que podemos aprender com ela ...” (NONAKA e TAKEUCHI, 1997).
- Dados processados, com significado para o receptor
  - Transmite conhecimento e tem valor real ou percebido
  - É um recurso da organização - como seu patrimônio, investimentos e equipamentos
  - Possui **valor agregado** ao cliente/usuário - medido pelo grau de satisfação
  - Pode ser apresentada em forma de gráficos, textos, imagens e voz isoladamente ou juntos = multimídia

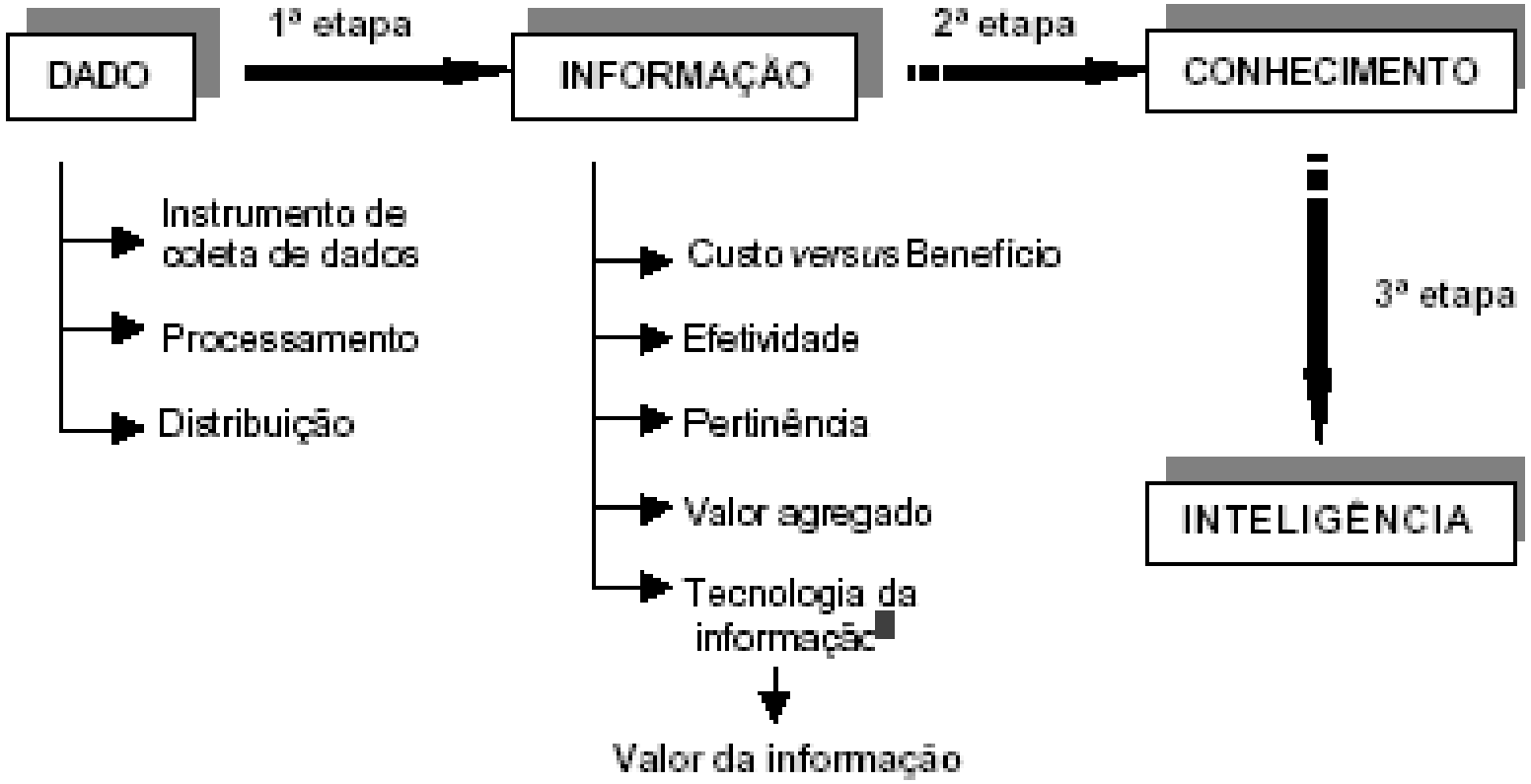
Conhecimento - Conceituação

... é a informação que muda algo ou alguém, seja provocando uma ação, seja tornando um indivíduo ou uma instituição capaz de uma ação diferente ou mais eficiente"

Drucker (1998)

- É uma mistura fluida de experiência condensada, valores, informação contextual e *insight* experimentado, a qual proporciona uma estrutura para a avaliação e incorporação de novas experiências e informações. (DAVENPORT & PRUSSAK, 1998).
- O conhecimento, também denominado intelecto, é a única vantagem duradoura que resulta da habilidade em gerar novas vantagens em oposição a fontes tradicionais de domínio, tal como, custos e qualidade, tempo e *know how*, criação de fortificações competitivas e dinheiro (QUINN et al, 2001).

Geração do Conhecimento



(Fonte: baseado em Tjaden, 1996)

Dado → Informação → Conhecimento

DADOS **INFORMAÇÃO** **CONHECIMENTO**

capacidade de entendimento

percepção **coleta** **organização** **processamento** **distribuição** **utilização**

- Identificação de eventos e indicadores
- Formas de reunir a informação relevante
- Estruturação da informação colhida em meios e formatos corretos
- Análise da informação através de métodos e técnicas
- Acumula e simplifica o acesso para os usuários
- Aplicação da informação em ações e decisões relevantes

âmbito do Plano de Informação

- Requisitos **estruturais**:
  - **conteúdo** - núcleo de valor da informação; o que ela transmite
  - **formato** - alfabético, numérico ou alfanumérico
  - **quantidade** - fornecida na medida certa de sua necessidade. Refere-se ao volume e periodicidade
  - **qualidade - definida pelos requisitos intrínsecos:**
    - adequabilidade
    - confiabilidade
    - integridade
    - acessibilidade
    - oportunidade
    - clareza

- Requisitos **intrínsecos** (qualidade):
  - **adequabilidade** - conteúdo e formato compatíveis com a natureza da decisão
  - **confiabilidade** - garantia de origem
  - **acessibilidade** - facilidade de obtenção
  - **oportunidade** - disponível no momento e no local da sua requisição (tempestividade)
  - **clareza** - de fácil entendimento

- Requisitos **de Segurança**
  - **Confidencialidade -** É a garantia de que a informação é acessível somente por pessoas autorizadas;
  - **Integridade -** É a salvaguarda da exatidão da informação;
  - **Disponibilidade -** É a garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário;

"Tenho uma crença simples, mas forte: a maneira mais significativa de diferenciar sua empresa da concorrência, o único modo de você se distanciar da multidão, é fazer um trabalho destacado com a informação. O modo como você reúne, administra e usa a informação determina se vencerá ou perderá. Há mais concorrentes. Há mais informação disponível sobre eles e sobre o mercado, que agora é global. Os vencedores serão aqueles que desenvolvem um sistema nervoso digital de categoria mundial de tal forma que a informação possa fluir com facilidade através de suas empresas para um máximo e constante aprendizado."

Bill Gates

- A informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário *(Rezende e Abreu, 2000)* .
- A informação tem um valor altamente significativo e pode representar grande poder para quem a possui.
- A informação contém valor, pois está integrada com os **processos**, **pessoas** e **tecnologias**.

- Vivemos em uma sociedade que se baseia em informações e que exibe uma crescente propensão para coletar e armazenar informações e o uso efetivo da informação permite que uma organização aumente a eficiência de suas operações. *(Katzam, 1977)*

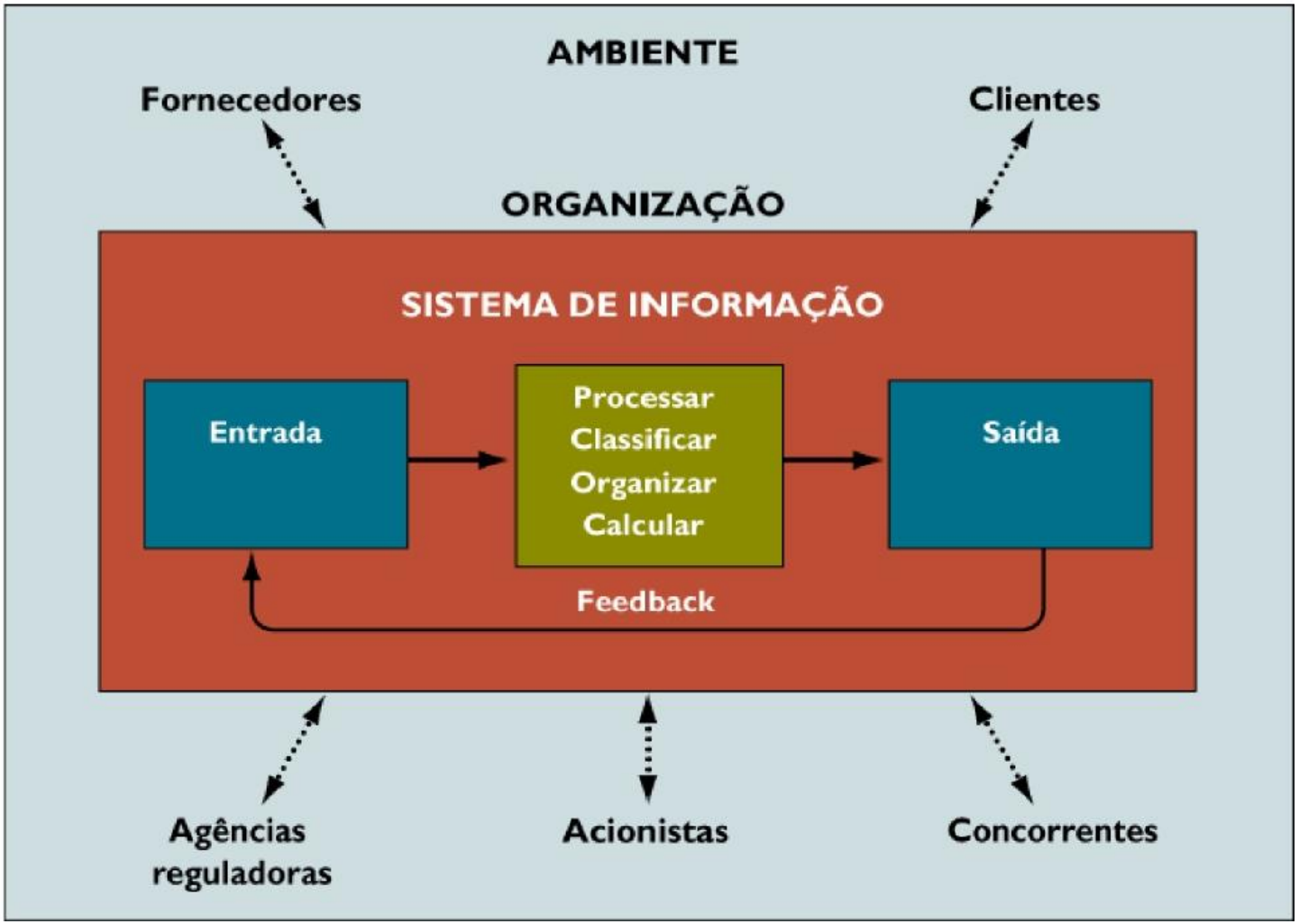
- A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida *(NBR 17799, 2003)*.

- Na sociedade da informação, a informação é o principal patrimônio da empresa e está sob constante risco *(Dias, 2000).*
- A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa *(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).*

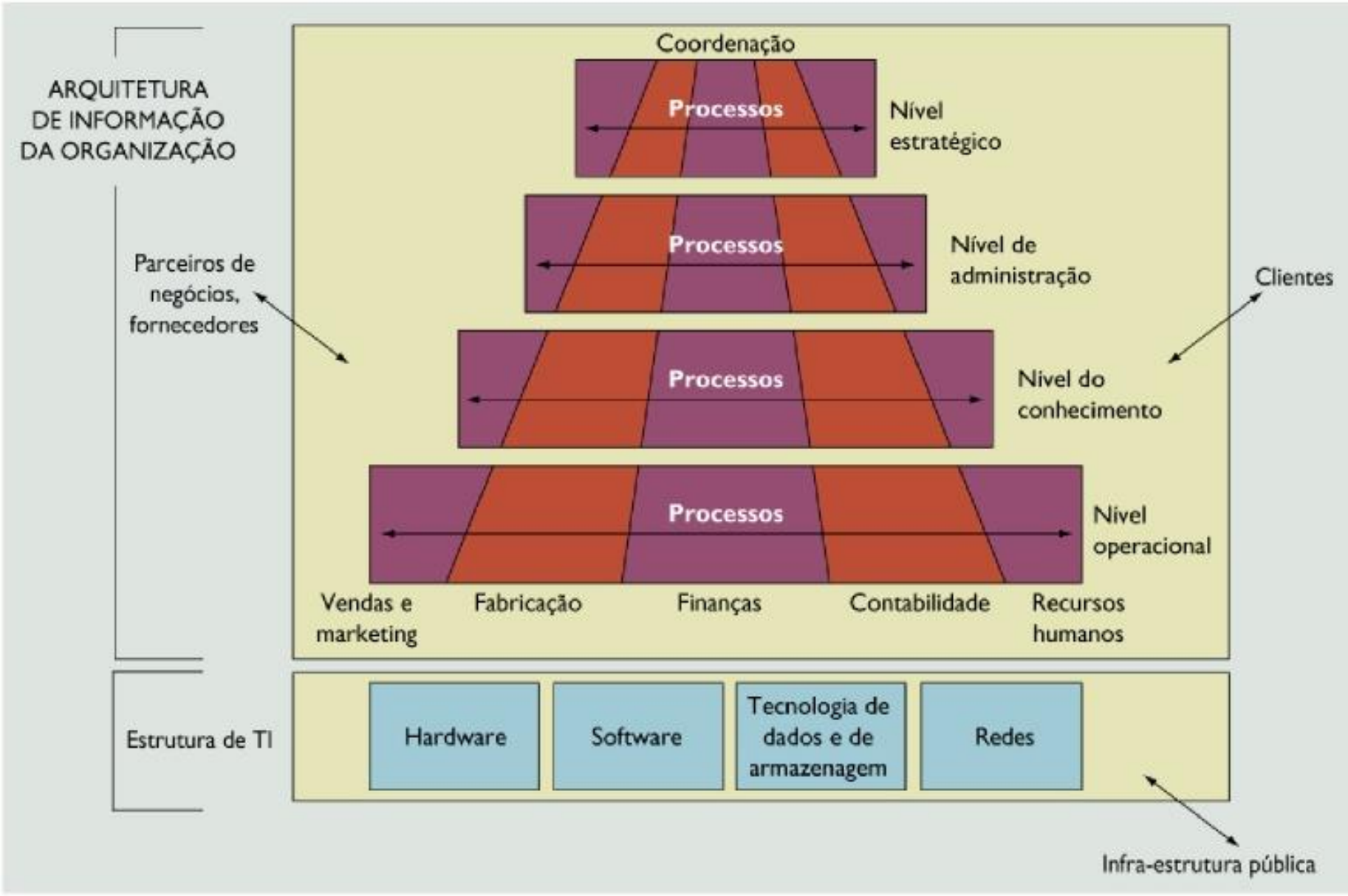
- As empresas já perceberam que o domínio da tecnologia como aliado para o controle da informação é vital. O controle da informação é um fator de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial *(Synnat, 1987; Feliciano Neto, Furlan e Higo, 1988).*

- Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente.
- Com 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.

Sistema de Informação



Arquitetura de Informação



- Da perspectiva de uma empresa, o sistema de informação é uma solução organizacional e administrativa baseada na tecnologia de informação para enfrentar um desafio proposto pelo ambiente *(Laundon e Laudon, 2004).*
- A informação certa comunicada a pessoas certas é de importância vital para a empresa. Para a tomada de decisões, é necessários um cuidado detalhado com a integridade, precisão, atualidade, interpretabilidade e valor geral da informação.

Classificação e ciclo de vida da Informação

- Nem toda informação é crucial ou essencial a ponto de merecer cuidados especiais.
- Por outro lado, determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente.
- Em *(Wadlow, 2000; Abreu, 2001; Boran, 1996)* é exposto, a necessidade de classificação da informação em níveis de prioridade, respeitando a necessidade de cada empresa assim como a importância da classe de informação para a manutenção das atividades da empresa.

- **Tangíveis**: ocupam espaço e o seu furto o fazem desaparecer. Exemplos: documentos impressos ou digitais, impressoras, móveis, computadores.
- **Intangíveis**: não ocupam espaço. Exemplos: Imagem da empresa, confiabilidade do órgão, marca, dados, informação, conhecimento (*know-how*).

Segundo a ISO 17799

- **Ativos de informação**: bancos de dados, documentações, materiais de treinamento, políticas de segurança, arquivos.
- **Ativos de software:** aplicações, sistemas operacionais, ferramentas de desenvolvimento, utilitários.
- **Ativos físicos:** computadores, equipamentos de rede, mídias digitais.
- **Serviços**: serviços de computação e redes, utilidades gerais.

- Para tanto, podemos classificar a informação dos seguintes modos:
  - **Pública**
    - Informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;
  - **Interna**
    - O acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;

- **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. A manipulação desse tipo de informação é vital para a companhia.

- Algumas informações são centrais para organização e a divulgação parcial ou total destas pode alavancar um número de repercussões cuja complexidade pode ser pouco ou nada administrável pela organização com consequências possivelmente nefastas.

- O conceito de engenharia da informação – que é um conjunto empresarial de disciplinas automatizadas, dirigindo ao fornecimento da informação correta para a pessoa certa no tempo exato *(Martin, 1991; Feliciano Neto, Furlan e Higo, 1988)* – já demonstrava a importância da segurança da informação para as instituições.

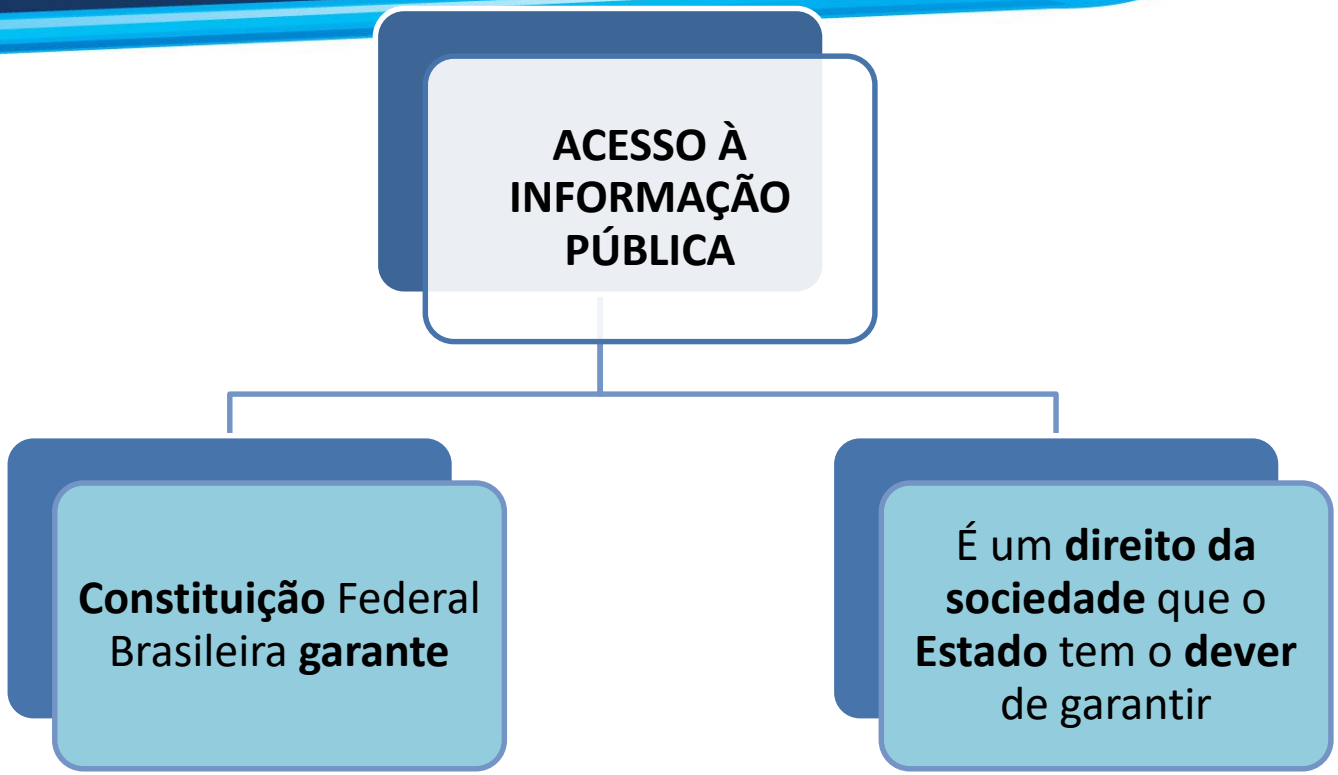
CGU

Acesso à Informação
Centro Universitário

LEI DE ACESSO À INFORMAÇÃO

LAI

Lei nº 12.527/2011



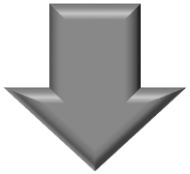
Art. 5º. - XXXIII

*XXXIII – todos têm direito a **receber dos órgãos públicos informações** de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas **no prazo da lei**, sob **pena de responsabilidade**, **ressalvadas aquelas** cujo **sigilo** seja **imprescindível à segurança** da sociedade e do Estado;*

NOVA LÓGICA NO SETOR PÚBLICO:

O **ACESSO** à informação pública é a **REGRA**, e o sigilo somente a exceção

As **EXCEÇÕES** devem ser definidas de forma **clara e** objetiva e serem **FUNDAMENTADAS**



CULTURA DE ACESSO

PEDIDO DE INFORMAÇÃO → **PRAZO**
- imediatamente ou
- 20 dias (pror. +10)

→ **RESPOSTA**

- **Quem pode solicitar informação? QUALQUER PESSOA física ou jurídica**
- **Pedido** não precisa ser motivado**, apenas conter a identificação do requerente e a especificação da informação**
- Decisão de **negativa de acesso** deve ser **motivada**
- Serviço de **busca e fornecimento** das informações **é gratuito, salvo** nas hipóteses de **reprodução** de documentos, situação em que poderá ser **cobrado exclusivamente o valor necessário ao ressarcimento do custo** dos serviços e dos materiais utilizados.
- **Para quem o pedido deve ser endereçado? Ao SIC do respectivo órgão ou entidade**

Informações Públicas – Classificação pela LAI

INFORMAÇÕES PESSOAIS

- Relativas à intimidade, à vida privada, à honra e à imagem das pessoas.
- O acesso é restrito, independentemente de classificação, pelo prazo de 100 anos.

Podem ter acesso a informações pessoais:

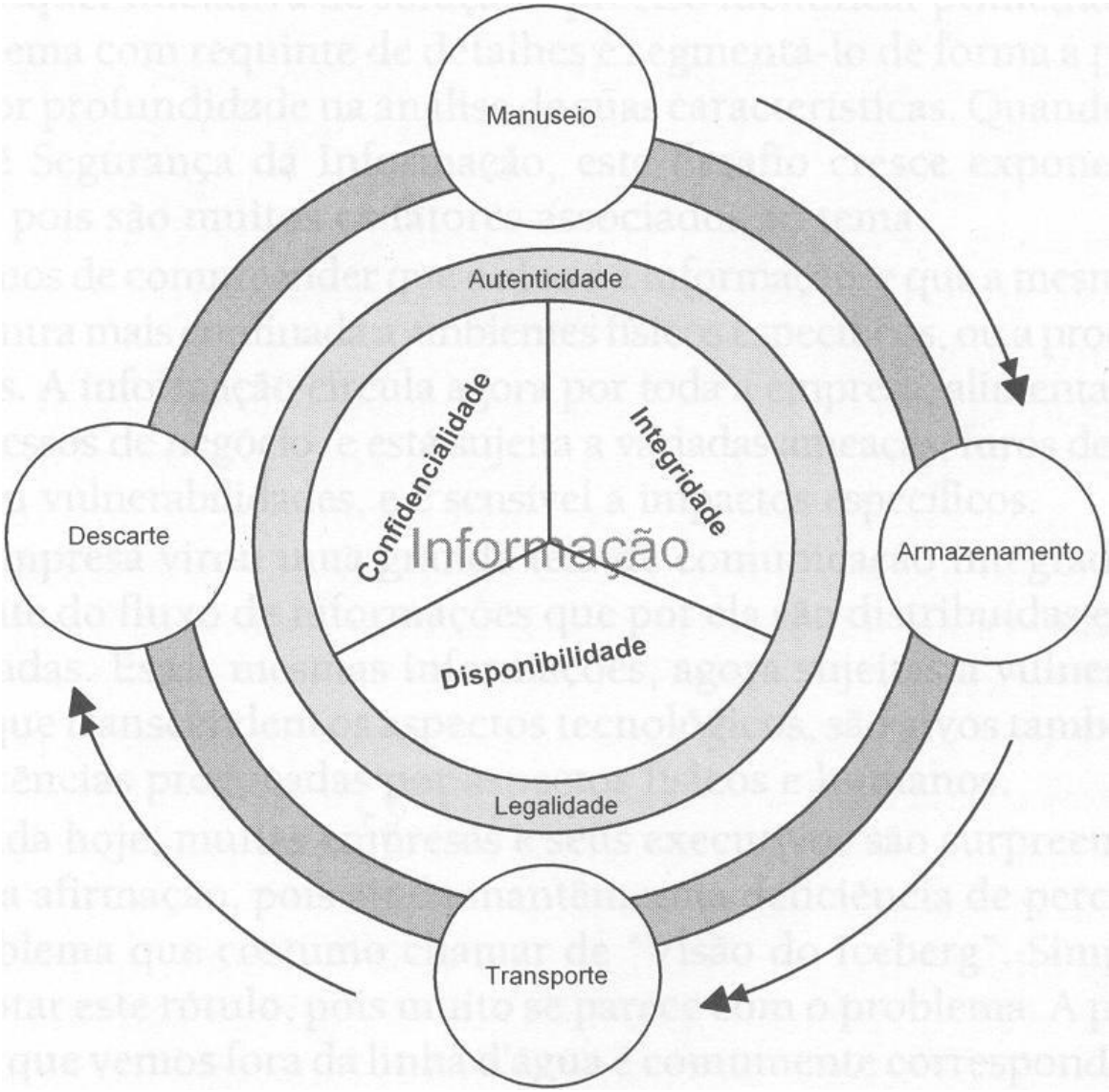
- Os **agentes públicos legalmente autorizados**;
- **Terceiros**, **mediante consentimento** expresso da pessoa à qual elas se referem; e
- Independentemente de consentimento**, para as finalidades** previstas no **art. 31**, § 3º da Lei nº 12.527/11.

- O Ciclo de Vida é composto e identificado pelos momentos vividos pela informação que a colocam em risco.

- Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa.

- Os órgãos (analogamente, ativos físicos, tecnológicos e humanos), se utilizam sangue (analogamente, informação), para pôr em funcionamento os sistemas digestivo, respiratório, etc. (analogamente, processos de negócio), para consequentemente, manter a consciência e a vida do indivíduo (analogamente, a continuidade do negócio).

Ciclo de Vida da Informação



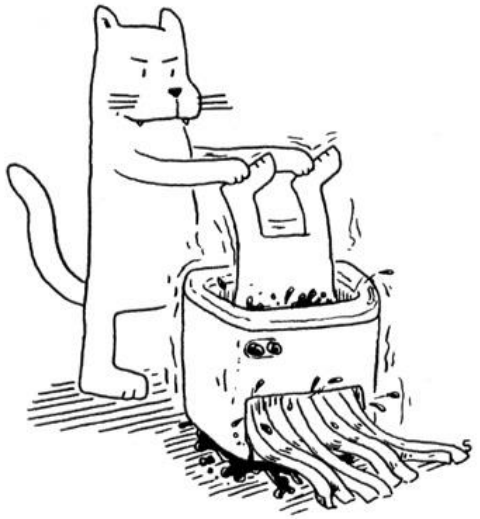
Ciclo de vida da informação
Fonte: Sêmola, 2003, pg. 11

- Correspondendo às situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, a última figura revela todos os 4 momentos do ciclo de vida que são merecedores de atenção.
  - **Manuseio**
    - Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou, ainda, ao utilizar sua senha de acesso para autenticação, por exemplo.

- **Armazenamento**
  - Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda em uma mídia de disquete depositada na gaveta da mesa de trabalho, por exemplo.
- **Transporte**
  - Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico, ao postar um documento via aparelho de fax, ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.
- **Descarte**
  - Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CD-ROM usado que apresentou falha na leitura.

Tratamento de Informações - Descarte

- Segundo os procedimentos de Tratamento de Informações:
- O descarte de documentos e informações de valor legal devem obedecer aos prazos estabelecidos em lei.
- Não poderão ser descartados documentos com valor histórico permanente.
- Documentos secretos, em princípio, são considerados documentos de valor histórico permanente.

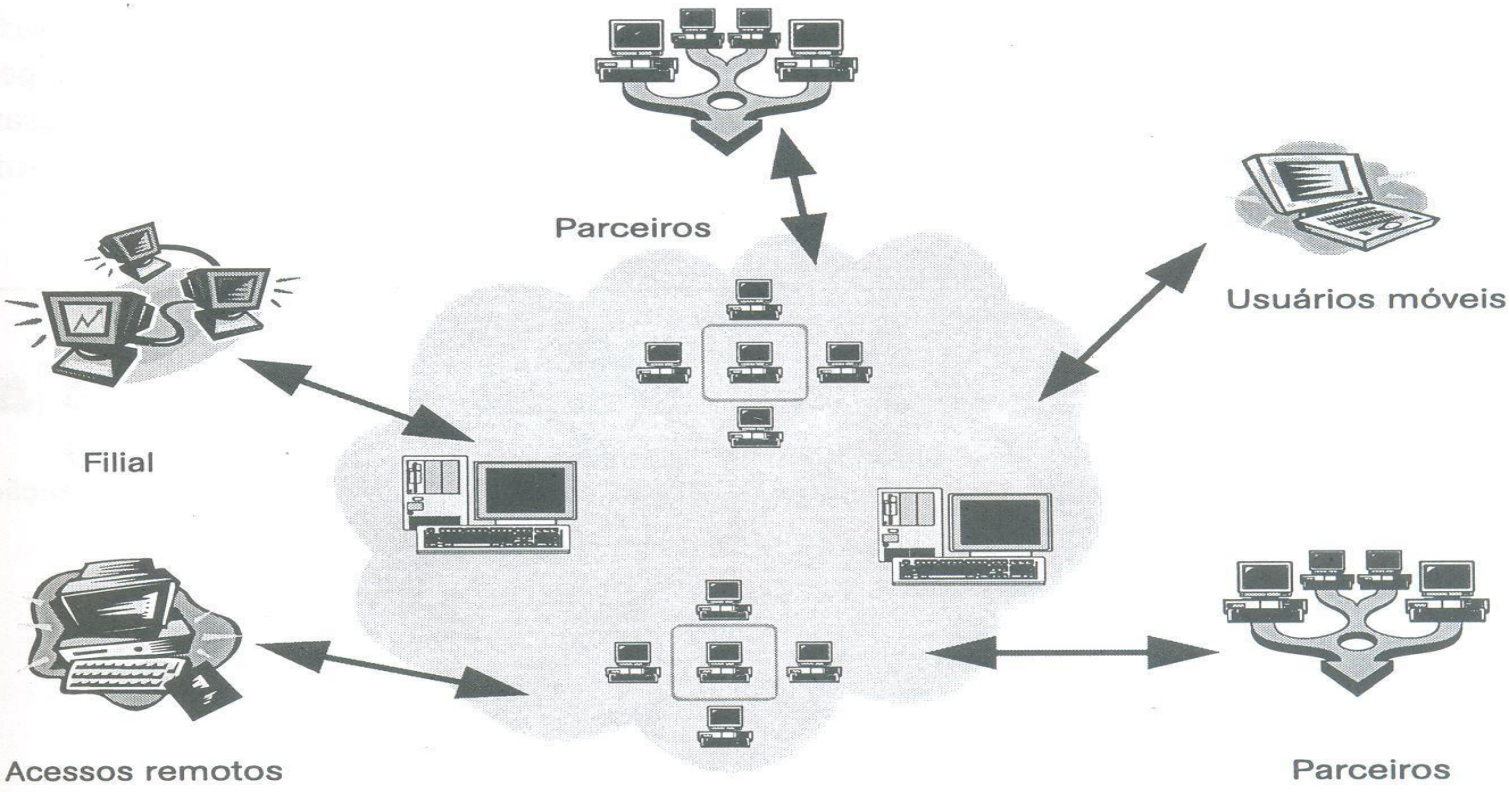


✓ ***Documentos confidenciais, reservados ou corporativos impressos ou armazenados em mídia transportável não reutilizável, deverão ser triturados em equipamento apropriado.***

Ciclo de Vida da Informação

O Ambiente Cooperativo e a Diversidade de Conexões

O ambiente cooperativo



O ambiente cooperativo — diversidade de conexões.

- Matrizes,
- Filiais,
- Clientes,
- Fornecedores,
- Parceiros Comerciais,
- Usuários Móveis

- Integração dos mais diversos sistemas de diferentes organizações.
- Partes envolvidas cooperam entre si, na busca de rapidez e eficiência nos processos e realizações dos negócios.
- Diferentes tipos de usuários
- Desafios a serem enfrentados no ambiente cooperativo
- Complexidade que envolve a segurança desses ambientes
- Modelo de segurança

- Existem vulnerabilidades, ameaças, ataques, riscos, e impactos.
- A complexidade da infraestrutura de rede atinge níveis consideráveis.
- Toda informação tem valor e precisa ser protegida.
- É preciso a segurança das informações que fazem parte dessa rede.

- Define restrições aos recursos da informação.
- Segurança da Informação é a gestão de tais restrições.
- Para gerir restrições, políticas de segurança precisam ser definidas.

- **Segurança da Informação**

  - “É a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidade de negócios” [ISO 27002].

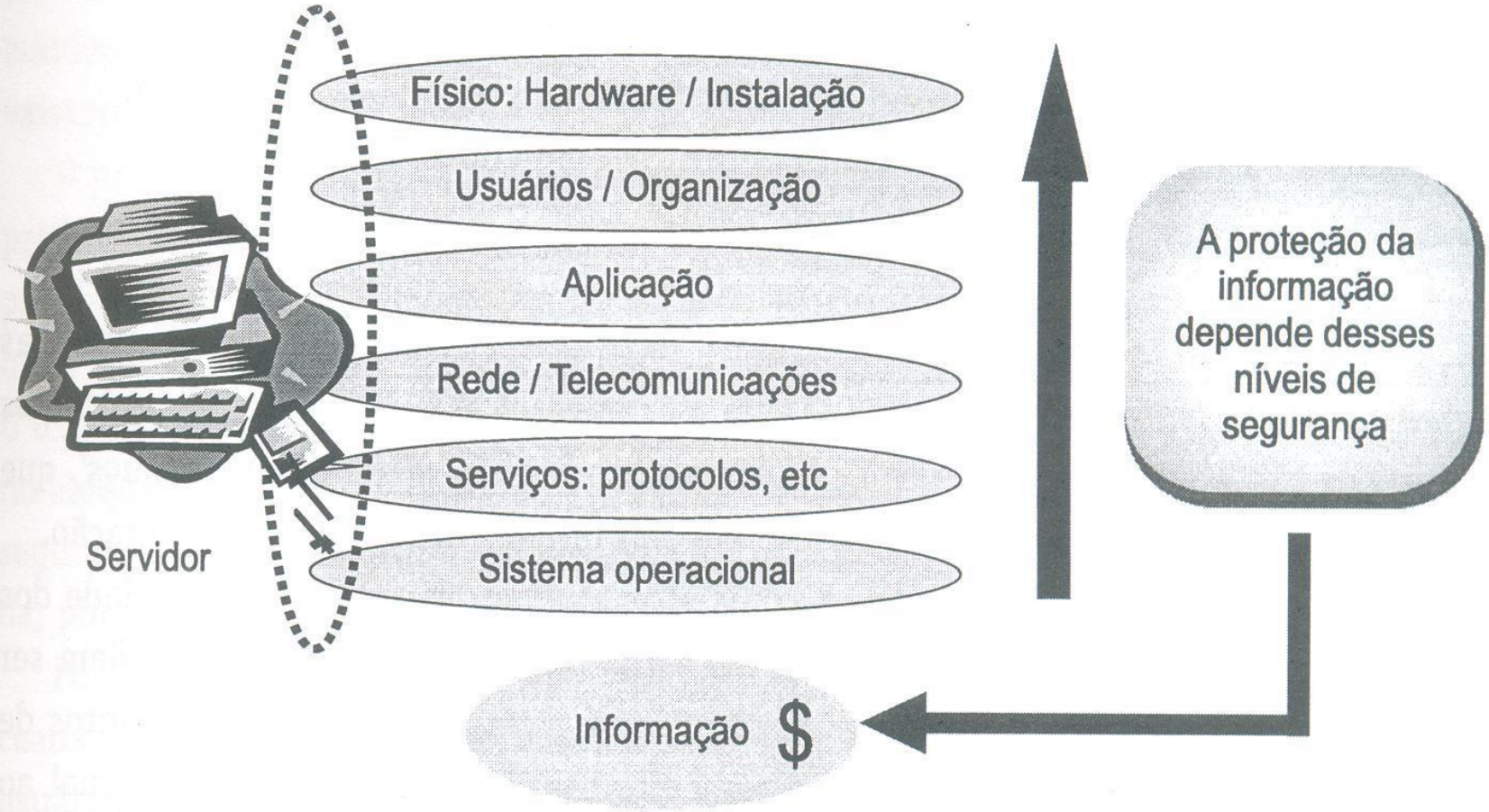
- É a **proteção** dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (NBR 17999, 2003)

- Garantir a continuidade do negócio
- Minimizar o risco ao negócio
- Maximizar o retorno sobre os investimentos.

- Fragilidade da tecnologia existente.
- Novas tecnologias trazem novas vulnerabilidades.
- Novas formas de ataques são criadas.
- Entender a natureza dos ataques é fundamental.
- Aumento da conectividade resulta em novas possibilidades de ataques.
- Existência de ataques direcionados e oportunísticos.
- Aumento dos crimes digitais.

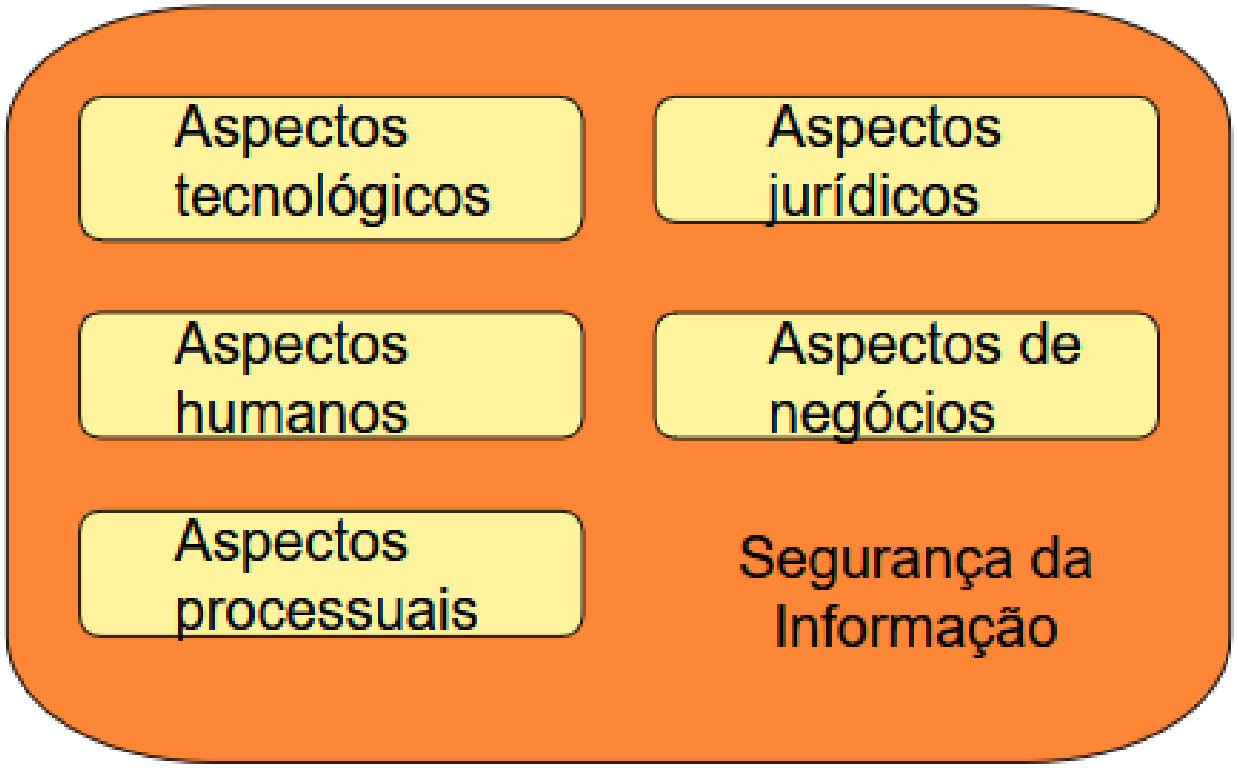
- A falta de uma classificação das informações quanto ao seu valor e a sua confiabilidade, para a definição de uma estratégia de segurança.
- Controle de acesso mal definido.
- A Internet é um ambiente hostil, e portanto, não confiável.
- A interação entre diferentes ambientes resulta na multiplicação dos pontos vulneráveis.
- Fazer a defesa (segurança) é mais complexa do que o ataque.

A Abrangência da Segurança



A abrangência da segurança e a complexidade da proteção da informação.

- Segurança é inversamente proporcional as funcionalidades (serviços, aplicativos, o aumento da complexidade das conexões, ...)



Aspectos envolvidos na segurança da informação

- A administração da segurança deve ser dimensionada, sem que a produtividade dos usuários seja afetada.

- Geralmente, a segurança é antagônica à produtividade dos usuários.

- A tentativa de estabelecer uma rede totalmente segura não é conveniente.

- As organizações devem definir o nível de segurança, de acordo com suas necessidades, já assumindo riscos.

- Construir um sistema altamente confiável, que seja capaz de dificultar ataques mais casuais.

Problemas de Segurança da Informação

- Garantir que pessoas mal intencionadas não leiam ou, pior ainda, modifiquem mensagens enviadas a outros destinatários.
- Pessoas que tentam ter acesso a serviços remotos, os quais elas não estão autorizadas.
- Distinção entre uma mensagem supostamente verdadeira e uma mensagem falsa.
- Mensagens legítimas podem ser capturadas e reproduzidas.
- Pessoas que negam ter enviado determinadas mensagens.

- Segurança da Informação,
- Segurança de Sistemas,
- Segurança de Aplicações,
- Segurança de Redes.

- Disponibilidade
- Confidencialidade
- Integridade
- Privacidade
- Autenticidade
- Controle de Acesso
- Não-Repúdio da Informação

- A informação deve ser entregue no momento que ela precisar.

- A informação estará disponível para acesso no momento desejado.

- A informação transmitida são acessíveis somente a partes autorizadas.

- As informações pessoais podem ser fornecidas, mas somente com a autorização do proprietário da informação ou medida judicial.

- Informações médicas ou financeira.

- Garante a proteção da informação contra modificações não autorizadas.
  - escrever,
  - mudar,
  - mudar status,
  - apagar,
  - Criar
  - Atrasar
  - responder mensagens.

Autenticidade

- Validar a identidade de um usuário, ou um dispositivo em um sistema.

- Assegura que a identidade e a informação não são falsas.

- Procedimentos operacionais para detectar e prevenir acessos não autorizados e permitir acessos autorizados num sistema.

- Nem o transmissor nem o receptor da informação, podem negar o envio/recepção da informação.

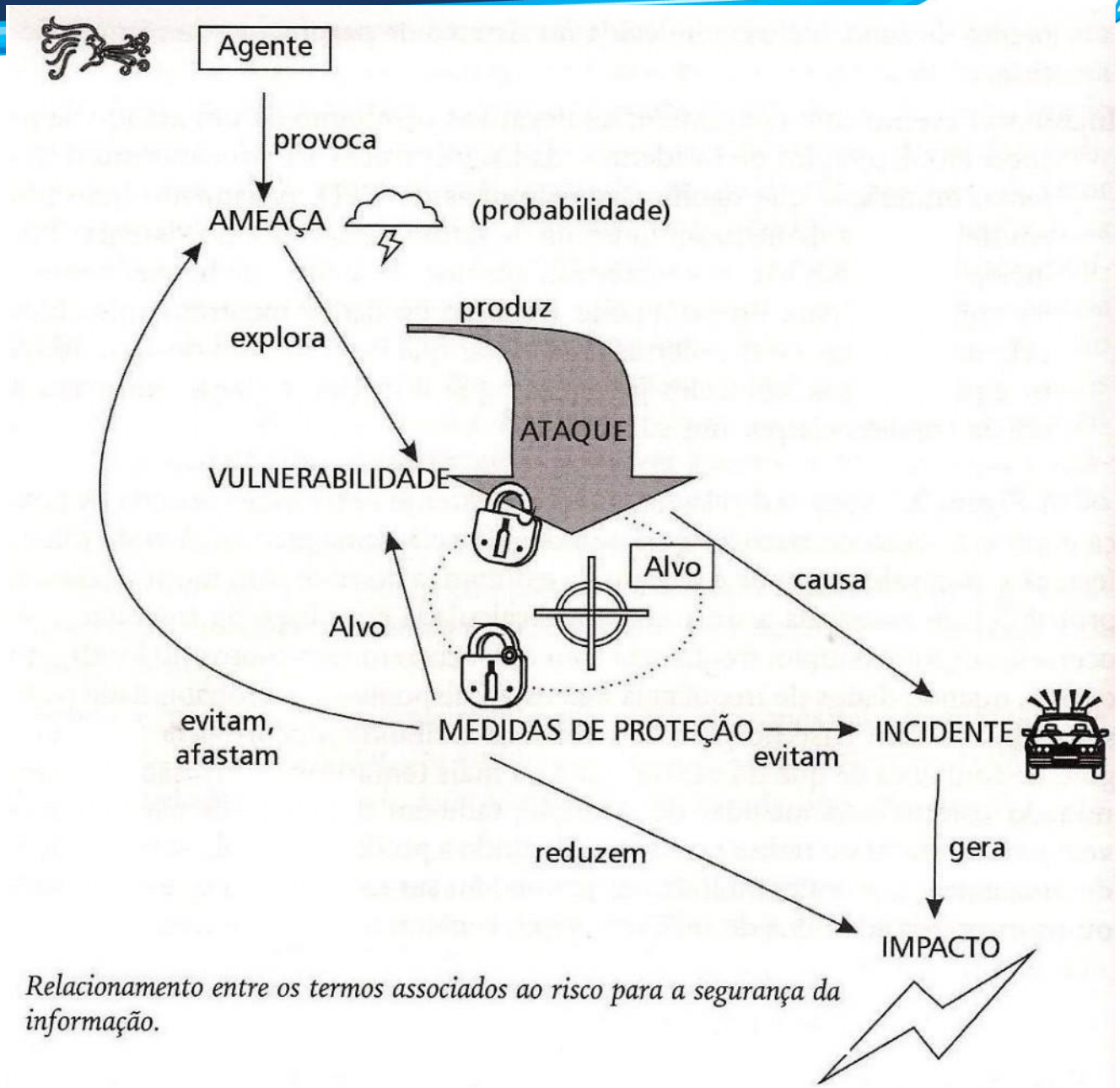
Resumo dos conceitos

- **Ativo:** tudo aquilo que tem valor e precisa ser protegido
- **Ameaça:** evento potencialmente prejudicial aos ativos
- **Medidas de proteção (controles):** controles que visam livrar os ativos de situações danosas, reduzindo o campo de ação das ameaças
- **Vulnerabilidades:** ausência ou falhas de mecanismos de proteção
- **Incidente:** a concretização da ação de uma ameaça (evento) devido a existência de vulnerabilidades
- **Agente:** agente que executa o ataque
- **Impacto:** tamanho do prejuízo causado após a concretização de uma ameaça (incidente)
- **Risco:** probabilidade de ocorrência da ameaça x impacto

Resumo dos conceitos

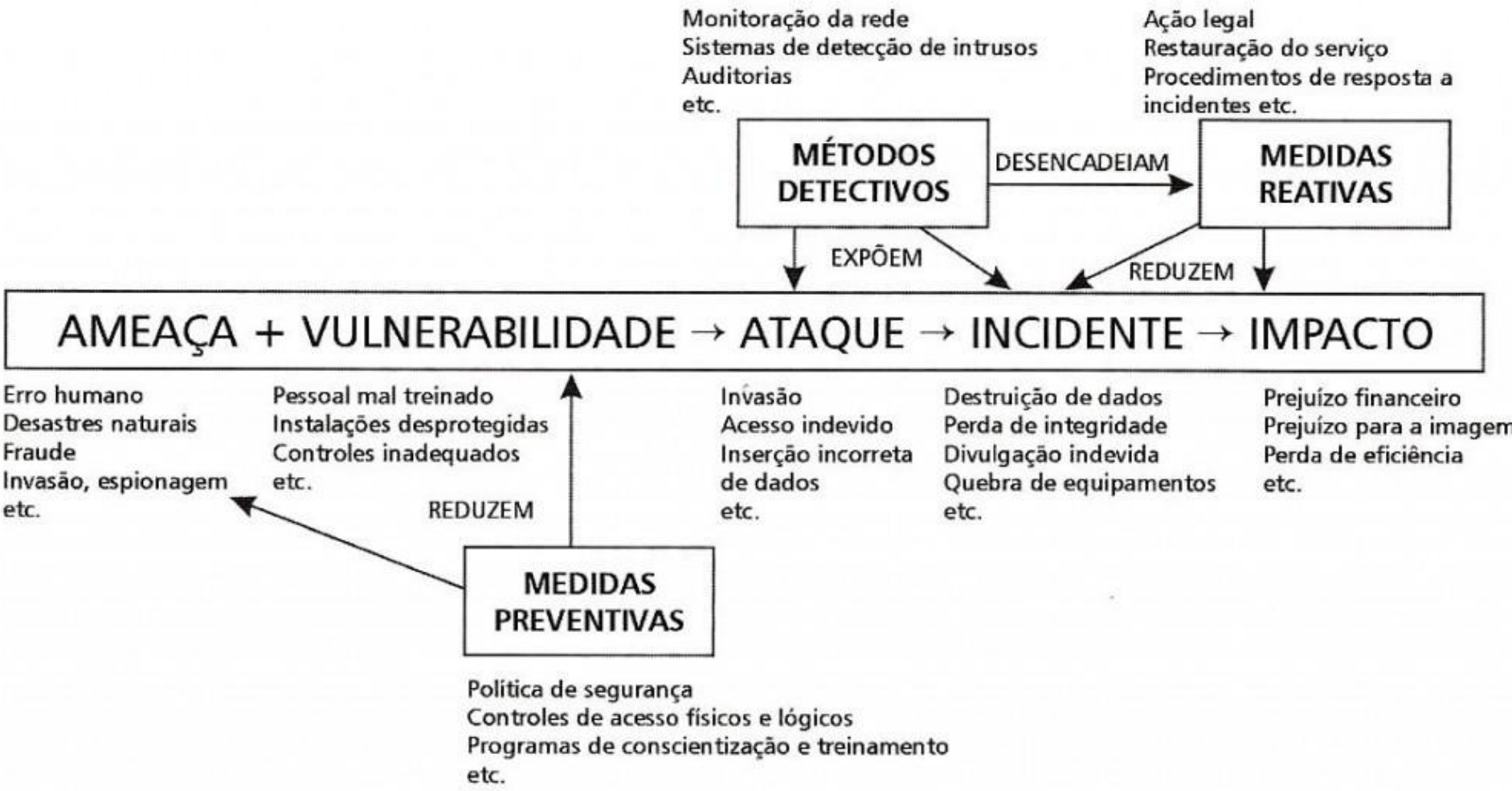
- **Autenticidade:** correta identificação das partes do sistema, sejam elas: recursos tecnológicos, transações, usuários ou outros sistemas. Garantia de que a parte é quem ela diz ser.
- **Não-repúdio:** impõe que nenhuma parte autorizada poderá negar a manipulação ou a transmissão uma informação na rede.
- **Autorização:** prevê que o acesso a um serviço da rede seja controlado.
- **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
- **Legalidade:** conformidade com um sistema de legislação.
- **Privacidade:** a informação privada deve ser acessada apenas pelo seu dono.
- **Confiabilidade:** o teor de uma informação ou sistema é verdadeiro.

Relação dos conceitos



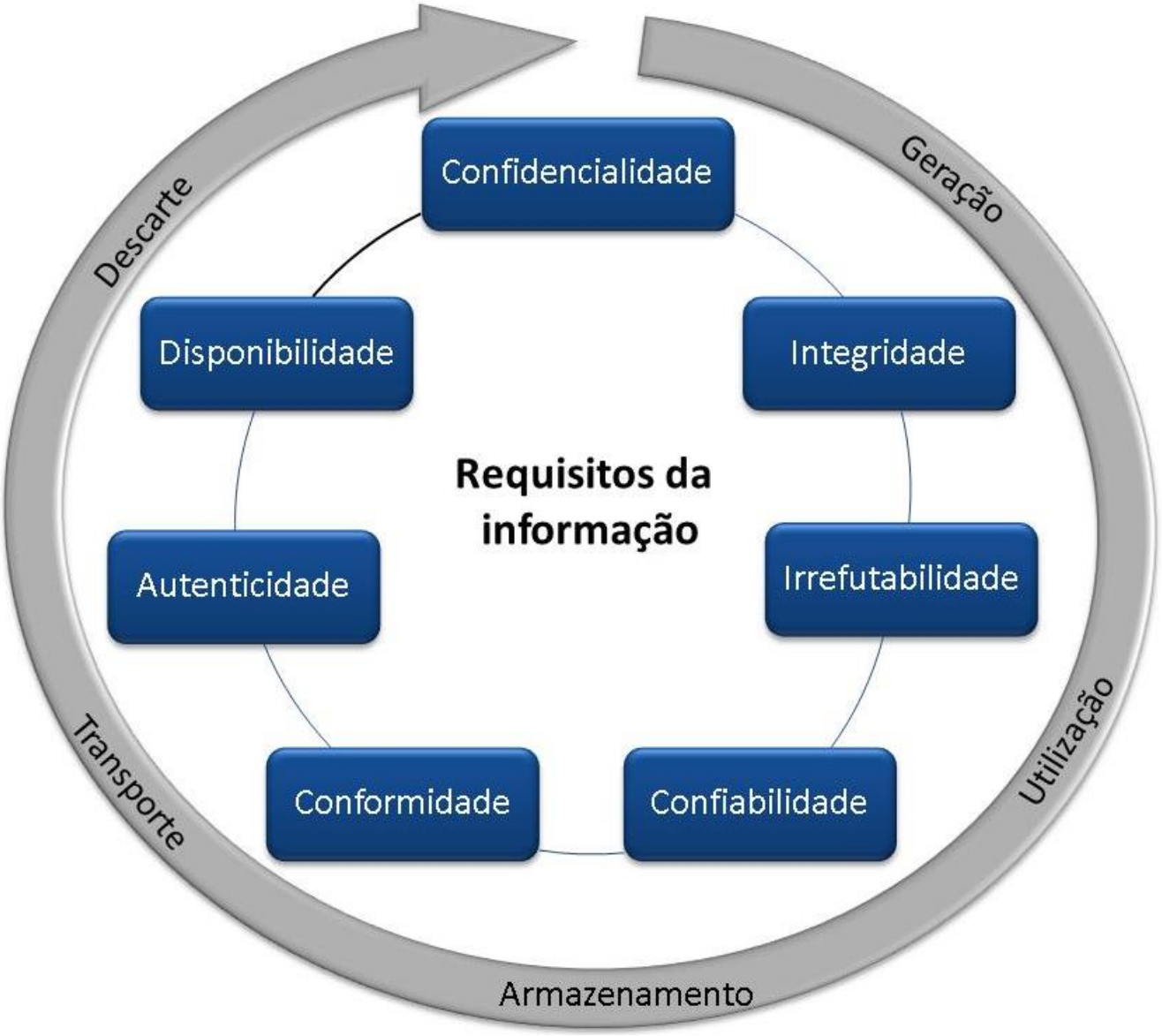
Relacionamento entre os termos associados ao risco para a segurança da informação.

Relação dos conceitos



Componentes do risco e medidas de proteção usadas para reduzi-lo.

Relação dos conceitos



- Política de Segurança é um conjunto de diretrizes e diretivas que definem formalmente as regras e os direitos dos funcionários e prestadores de serviços, visando à proteção adequada dos ativos da informação.
- Essa política está baseada em diretrizes de segurança e diretivas de privacidade.

- Proteger as informações
- Assegurar Recursos
- Garantir Continuidade
- Cumprir Normas
- Atender às Leis
- Selecionar Mecanismos
- Comunicar Descumprimento

- As informações são coletadas de forma legal e sob o conhecimento do usuário;
- As informações são enviadas à empresa de forma segura com métodos de criptografia e certificação digital.
- As informações enviadas à empresa serão armazenadas de forma íntegra, sem alteração de qualquer parte.

- As informações são armazenadas de forma segura e criptografada restringindo o acesso somente às pessoas autorizadas;
- As informações serão utilizadas apenas para as finalidades aprovadas pela Organização;
- As informações dos clientes nunca serão fornecidas a terceiros, exceto por determinação legal ou judicial.

- Da normatização ABNT NBR, ISO/IEC 27002:2005

- Mediante tal embasamento e considerando o disposto em seu Planejamento Estratégico, uma empresa pode resolver implantar um Sistema de Gestão de Segurança da Informação (SGSI), cuja estrutura e diretrizes são expressas num documento.

- O processo de segurança da informação pode ser visto, conforme o ciclo:

  - Análise de Segurança
  - Atualização de regras de segurança
  - Implementação e divulgação das regras
  - Administração de segurança
  - Auditorias

- Segurança de Sistemas Operacionais
- Segurança de Bancos de Dados

- Mecanismos de segurança inerentes à linguagem de programação usada.

- Segurança nos Navegadores, Aplicações na Web, Clientes de Email e aplicativos em geral.

- Segurança provida nos elementos de rede (roteadores, switches, pontos de acesso em redes sem fio, ...).
- Segurança provida nos segmentos de rede.
- Segurança nos protocolos de comunicação.

- Análise da Vulnerabilidade (descobrir o melhor caminho para chegar até a invasão).
- Preparação das Ferramentas (constrói ou escolhe as ferramentas para a invasão).
- Ameaça ou Tentativa de Ataque (quando o invasor pula o muro).
- Ataque (concretiza o arrombamento).
- Invasão ou Penetração (quando obtém sucesso).

- “Pontos Fracos” por onde se pode atacar.

- Uma falha de segurança em um sistema de software ou de hardware que pode ser explorada para permitir a efetivação de uma intrusão.

- “Pulando o Muro”
- Uma ação ou evento que pode prejudicar a segurança.
- É a tentativa de ataque a um sistema de informação, explorando suas vulnerabilidades, no sentido de causar dano à confidencialidade, integridade ou disponibilidade.

Ameaças x vulnerabilidades

- As ameaças aos sistemas de informação são definidas como as causas potenciais de um incidente não desejado e que podem resultar em danos a um sistema ou organização (ISO/IEC 27000:2012), estão presentes constantemente e evoluem em conjunto com a tecnologia, com a possiblidade de serem oriundas de softwares maliciosos, ou mesmo de *insiders*;
- A vulnerabilidade é a falha ou brecha da Segurança da Informação que pode ser explorada por ameaças;
- Quando a ameaça encontra uma vulnerabilidade ocorre a violação da segurança. O tamanho do dano causado pela violação pode variar conforme o tipo da ameaça e o grau de necessidade de proteção da informação (ABNT, 2005).

- Os *insiders* são pessoas de dentro de uma organização que têm privilégios de acesso e conhecimento dos processos organizacionais internos, permitindo-lhes explorar as vulnerabilidades proporcionadas por esses privilégios e conhecimentos (WILLISON e WARKENTIN, 2013);
- As violações de Segurança da Informação provocadas pelos *insiders* dentro da organização podem ser totalmente passivas e não intencionais, como por exemplo, a digitação de dados incorretos, que podem ameaçar a integridade das informações;

Ameaças à Informação - Erro humano como uma ameaça

- Os erros humanos são cometidos por diferentes motivos e vários deles são resultados de fatores que influenciam negativamente o comportamento responsável perante a Segurança da Informação, como por exemplo, a sobrecarga de trabalho, a urgência, a fadiga, ou a desmotivação;
- Não obstante, os erros humanos podem ser provocados por percepções limitadas, causadas pela falta de informações completas ou corretas em consideração às ameaças (LIGINLAL et al., 2009), que podem resultar em vulnerabilidades da Segurança da Informação (KRAEMER et al., 2009);
- Além disso, o erro humano também pode ser provocado por fatores organizacionais, como a comunicação, a cultura e a Política de Segurança da Informação (KRAEMER e CARAYON, 2007)

- Os softwares ditos maliciosos, ou mal-intencionados, são destinados a desempenhar um processo não autorizado que terá ter um impacto adverso sobre a confidencialidade, integridade e disponibilidade de um sistema de informação;
- São especialmente projetados para se transferir de forma autônoma de um software para outro, com o objetivo de extrair informações ou modificar intencionalmente os sistemas de um dispositivo de TI sem o consentimento do usuário, comprometendo a confidencialidade, integridade e disponibilidade dos sistemas de computação infectados (CHEN et al., 2012
- São exemplos de software maliciosos:
  - **Vírus**: software malicioso que se replica de forma autônoma, anexando-se a outro software do mesmo dispositivo de TIC ou de outros dispositivos, sem deixar vestígios óbvios da sua presença (WORKMAN, PHELPS e GATHEGI, 2013);

- ***Spyware*:** software malicioso que é instalado secretamente ou sub-repticiamente em um sistema de informação, com o objetivo de reunir informações sobre os usuários ou organizações sem o seu conhecimento (VACCA, 2009). Uma forma popular de spyware utilizado na atualidade é o denominado *tracking cookie* que permite rastrear a navegação de um usuário a partir de um site onde ele se identificou primariamente (WORKMAN, PHELPS e GATHEGI, 2013).

- ***Worm***: software malicioso que se replica e propaga de forma autônoma para outros dispositivos de TIC de forma independente e autossuficiente, utilizando mecanismos da rede de computadores. Ao contrário de um vírus, não precisa se anexar a um programa existente, sendo utilizados, por exemplo, para instalar *backdoors* ou enviar arquivos via e-mail de forma autônoma e sem deixar vestígios claramente perceptíveis (WORKMAN, PHELPS e GATHEGI, 2013).
- ***Trojan***: também conhecido como *horse Trojan* ou cavalo de Tróia, é um software malicioso que aparenta possuir uma função útil, mas possui funções ocultas potencialmente danosas (COLE, 2009). Age burlando os mecanismos de segurança dos dispositivos de TIC através de uma autorização legítima para a sua execução, muitas vezes fornecida pelo próprio usuário (WORKMAN, PHELPS e GATHEGI, 2013).

- Alguns tipos de malwares podem instalar um *backdoor*, também conhecido como *back door*, produzindo uma vulnerabilidade a Segurança da Informação, que poderá ser explorada por demais *hackers* (COLE, 2009);
- O *backdoor* é uma forma irregular de acessar um Sistema de Informação, ignorando os mecanismos normais de autenticação. Podem ser colocados no software pelo próprio programador do software (TRIPTON e KRAUSE, 2007) ou através de uma vulnerabilidade do sistema, tal como um vírus ou um *worm* (VACCA, 2009);
- Normalmente os *hackers* utilizam o *backdoor* para facilitar o acesso contínuo a um sistema após a segurança ter sido comprometida (VACCA, 2009).

- Muitos malwares são instalados através de *phishing*, que é uma forma de enganar os usuários na busca de suas informações pessoais, utilizando meios enganosos (WORKMAN, PHELPS e GATHEGI, 2013);
- Segundo os autores, o *phishing* começa com uma isca, normalmente uma mensagem de spam que parece ser de um banco legítimo ou comércio eletrônico. A mensagem instiga o leitor a visitar um site fraudulento, que finge ser legítimo. O site fraudulento tenta replicar ao máximo a aparência do site legítimo. Dessa forma, as vítimas são induzidas a fornecer informações pessoais valiosas (VACCA, 2009);

- “Arrombamento”

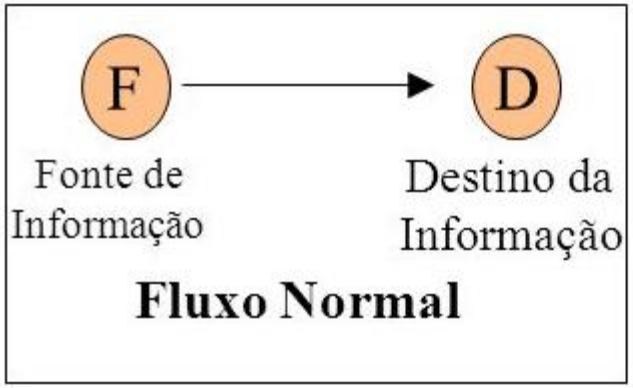
- O ato de tentar desviar dos controles de segurança de um sistema.

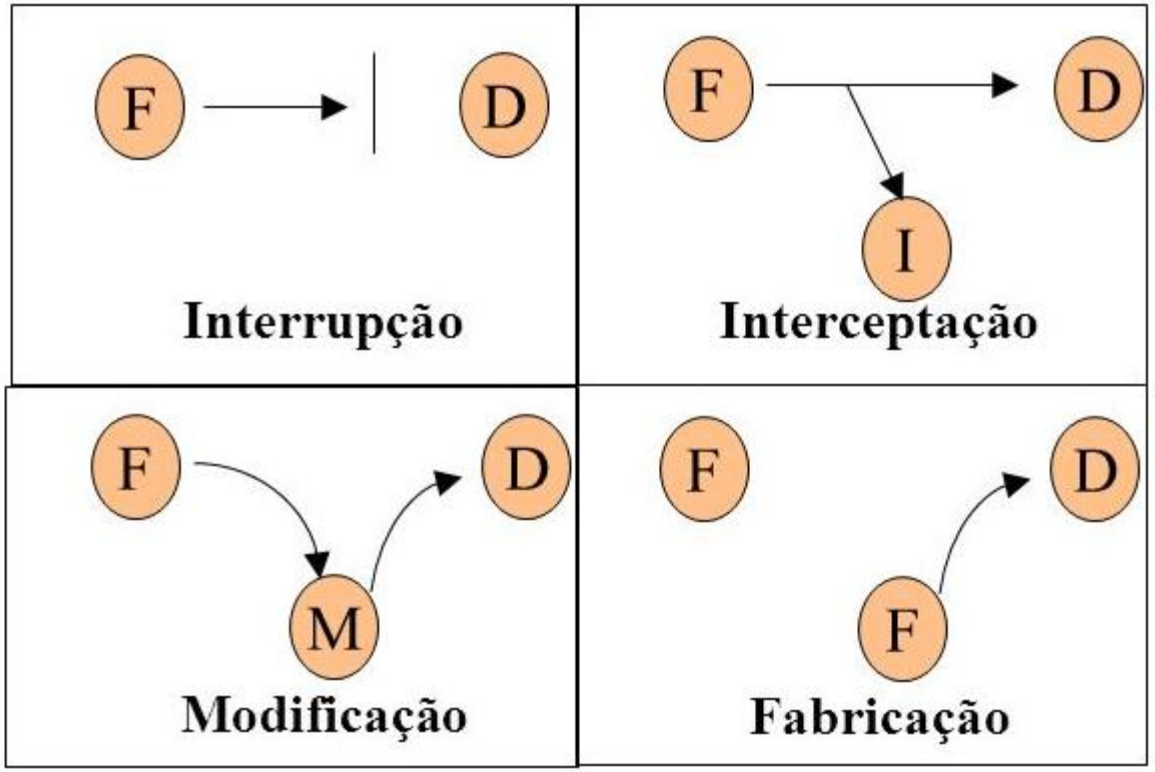
- Qualquer ação que comprometa a segurança da informação de propriedade de uma organização.

- Conceito
- Tipos de ataques
  - Passivo
    - Interceptação, monitoramento, análise de tráfego (origem, destino, tamanho, frequência)
  - Ativo
    - Adulteração, fraude, reprodução (imitação), bloqueio

- Ataques sobre o fluxo de informação
  - Interrupção: ataca a disponibilidade
  - Interceptação: ataca a confidencialidade
  - Modificação: ataca a integridade
  - Fabricação: ataca a autenticidade

Ataques


F
D
Fonte de Informação
Destino da Informação
Fluxo Normal


F
D
Interrupção
F
D
I
Interceptação
F
D
M
Modificação
F
D
F
Fabricação

- Pode ser externo, quando originado de fora da rede protegida.

- Pode ser interno, quando originado de dentro da rede protegida de uma instituição.

- 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 eficiência das contramedidas de segurança existentes

Conceito de Intrusão (Invasão)

- Acesso bem sucedido, porém não autorizado, em um sistema de informação.
- Sucesso no ataque.
- Obtenção da Informação.

- Risco é a probabilidade da ocorrência de uma ameaça particular.

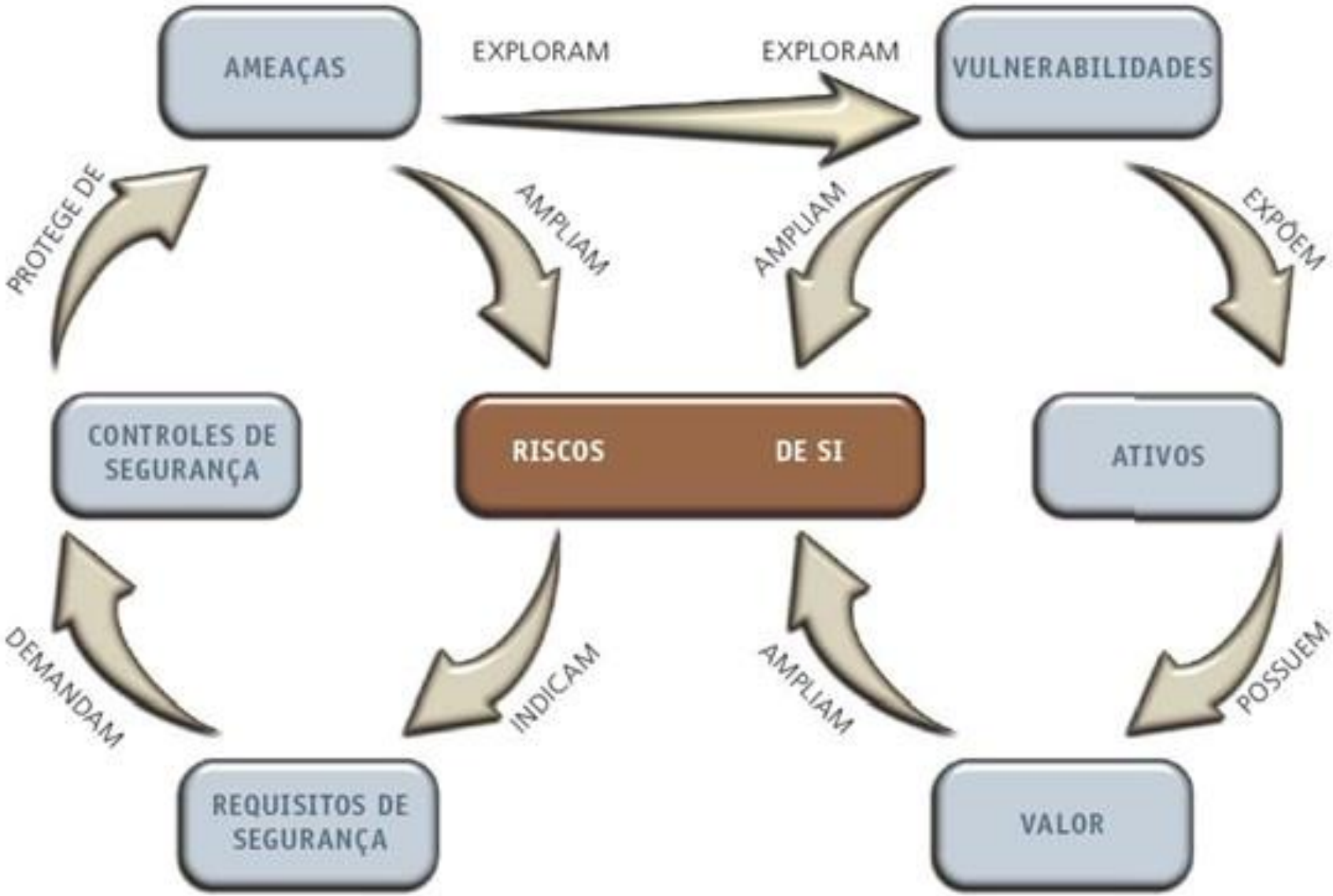
- Análise de Risco – Identificação e avaliação do riscos que os recursos da informação estão sujeitos.

- Gerenciamento de Riscos - Inclui a análise de risco, a análise de custo-benefício, a avaliação de segurança das proteções e a revisão total da segurança.

- Risco Residual: Riscos ainda existentes depois de terem sido aplicadas medidas de segurança.

- É a representação (normalmente em forma de avaliação) do grau de dano percebido associado aos bens de uma empresa.
- Grau de Dano = Severidade (qualitativo)
- A consequência para uma organização da perda de confidencialidade, disponibilidade e (ou) integridade de uma informação.

Resumo


AMEAÇAS
EXPLORAM
EXPLORAM
VULNERABILIDADES
PROTEGE DE
AMPLIAM
AMPLIAM
EXPÕEM
CONTROLES DE SEGURANÇA
RISCOS DE SI
ATIVOS
DEMANDAM
INDICAM
AMPLIAM
POSSUEM
REQUISITOS DE SEGURANÇA
VALOR

Proteção da informação - Abordagem técnica: Antivírus

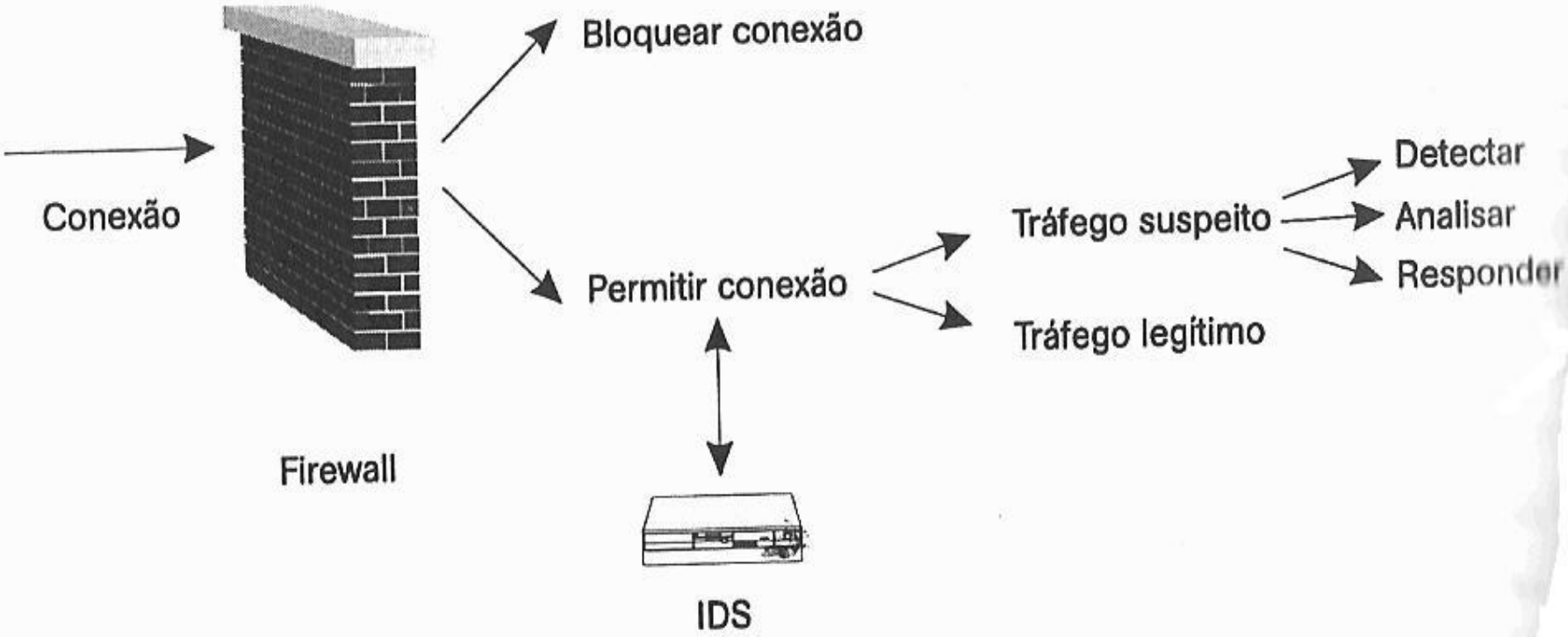
- Software que utiliza uma variedade de técnicas para prevenir, detectar e remover vírus. A técnica mais básica é a detecção baseada em assinaturas, que são trechos de programação únicos que identificam um vírus. Essa técnica envolve a busca por padrões conhecidos de dados em uma programação executável (VACCA, 2009);
- No entanto, é possível que o computador seja infectado com um novo vírus sem assinatura conhecida, para combater tais vírus podem ser utilizadas técnicas chamadas de heurísticas
- Muitos usuários deixam de atualizar o antivírus ou consideram que há perda de performance ao utilizá-lo e o desligam em determinadas circunstâncias (COLE, 2009).

- Dispositivos de hardware ou software que limitam o acesso entre redes e sistemas, de acordo com uma política de segurança específica (CNSSI-4009, 2010);
- Os **firewalls de rede** são limitados e protegem principalmente a rede interna de ameaças provindas de redes externas (WORKMAN, PHELPS e GATHEGI, 2013). Por outro lado, **firewalls de aplicação,** executados no próprio dispositivo, podem ser mais eficazes na segurança, pois possibilitam identificar softwares mal-intencionados pré-identificados ou questionar ao usuário o que deve ser feito em caso de softwares desconhecidos;

IDS – *Intrusion Detection Systems*

- IDS é um sistema de detecção de intrusão que adquire informações sobre um sistema de informação para realizar um diagnóstico sobre o estado da sua segurança;
- O objetivo é descobrir falhas de segurança, brechas ou vulnerabilidades que poderiam conduzir a possíveis violações. (WORKMAN, PHELPS e GATHEGI, 2013). Um sistema de detecção de intrusão pode ser descrito em um nível muito geral como um detector que processa as informações provenientes do sistema a ser protegido;

Firewall x **IDS**



Intrusion Detection System

Passivo

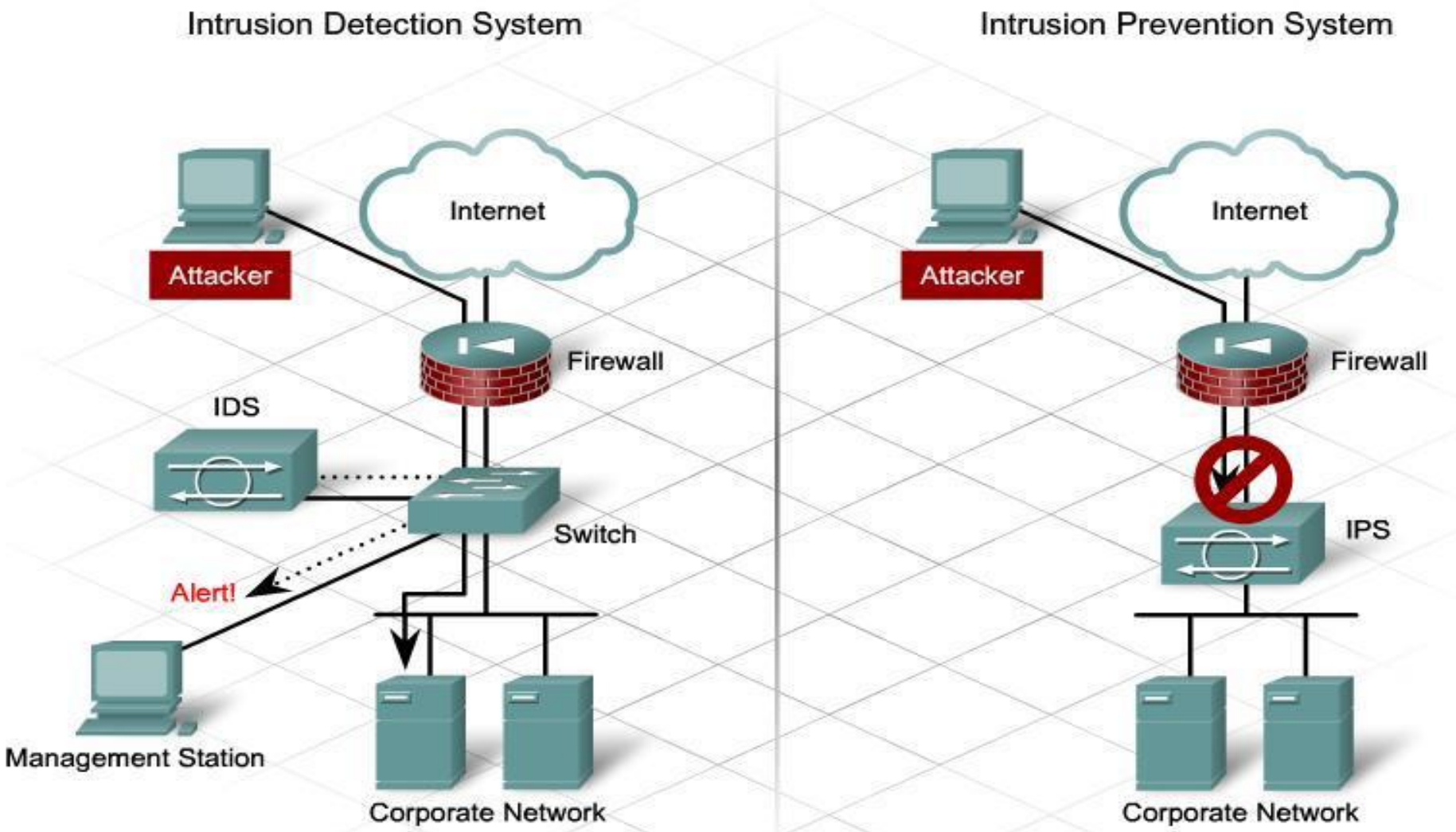
- Registra informação (log)
- Emite um alerta (trigger)

Ativo

- Encerra sessão do usuário
- Interage com o Firewall

Intrusion Prevention System

- Regras e políticas para o tráfego da rede
- Previne o ataque
- Bloqueia o ataque


Intrusion Detection System
Internet
Attacker
Firewall
IDS
Switch
Alert!
Management Station
Corporate Network
Intrusion Prevention System
Internet
Attacker
Firewall
IPS
Corporate Network

Proteção da informação - Abordagem técnica: **Criptografia**

- Técnica baseada na cifragem de informações que depende do sigilo de uma chave criptográfica, que pode ser uma chave única na criptografia simétrica ou a chave privada na criptografia assimétrica;
- A chave de criptografia é usada para embaralhar matematicamente as comunicações, tornando-a ilegível caso não se tenha a chave adequada para decifrá-la. A criptografia garante sigilo, em termos práticos, mas não garante uma segurança perfeita. As chaves de criptografia podem ser decifradas, mas o tempo para adivinhar a chave correta aumenta exponencialmente com o comprimento da chave;

Proteção da informação - Abordagem normativa

- A Norma **ISO/IEC 27001:2006** (ABNT, 2006), que abordam os requisitos para os sistemas de gestão da Segurança da Informação, e
- A Norma **ISO/IEC 27002:2005** (ABNT, 2005), que trata das práticas de sistemas de gestão da Segurança da Informação, substituindo a norma anterior ISO/IEC 17799:2005 e estabelecendo diretrizes e princípios gerais para iniciar, programar, manter e melhorar a gestão de Segurança da Informação em uma organização.
- A Norma ABNT NBR **ISO/IEC 27005:2008** – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação define as diretrizes para o processo de gestão de riscos de segurança da informação..