Segurança da Informação

Gerenciamento das Operações e Comunicações

Prof. Anderson Oliveira da Silva
D. Sc. Ciências em Informática
Engenheiro de Computação
anderson@inf.puc-rio.br

Departamento de Informática
Coordenação Central de Cooperação Internacional
PUC-Rio

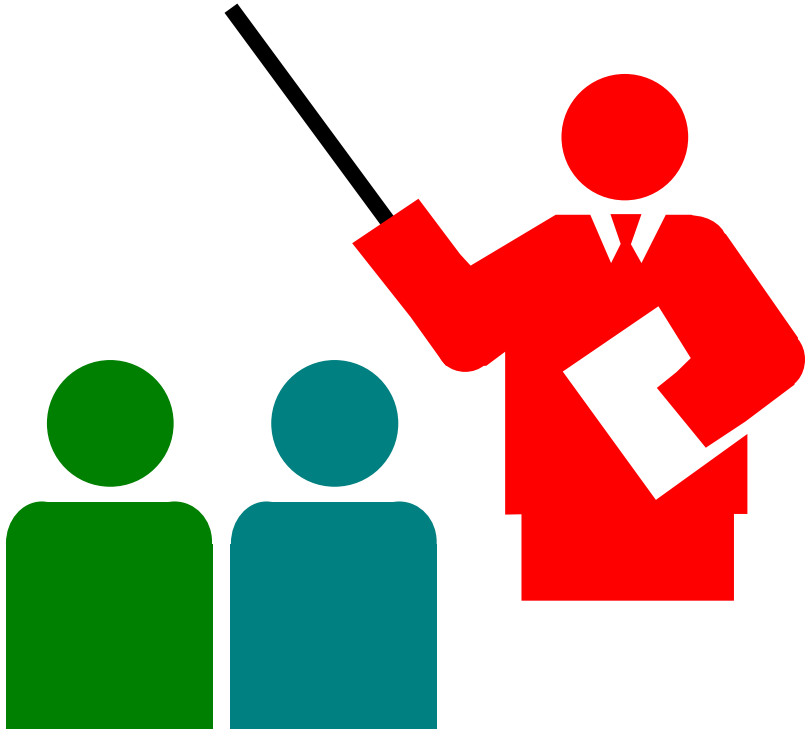
DEPARTAMENTO DE INFORMÁTICA PUC·RIO

Coordenação Central de Cooperação Internacional
International Cooperation Central Coordination Office

PUC RIO

Visão Geral de Segurança da Informação

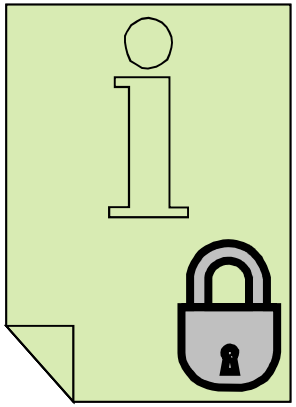
- Segurança da Informação
  Prof. Anderson O. da Silva



Proteção da Informação

- Segurança da Informação
  Prof. Anderson O. da Silva

Proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou sua missão.



- Proteger recursos de informação
  - Mídias, hardware e software.
- Selecionar e aplicar salvaguardas
  - Políticas, padrões e procedimentos.
- Ajudar a atingir o objetivo do negócio ou missão
  - Através da proteção dos ativos.

Proteção da Informação

- Segurança da Informação
  Prof. Anderson O. da Silva

Considerações importantes:

- No negócio, um programa de proteção de informação efetivo é secundário com relação à necessidade de se ter resultado.
- No setor público, o mesmo ocorre com relação aos serviços que a agência deve prover.
- O custo dos controles não deve exceder os benefícios esperados.
- Os controles devem ser apropriados e proporcionais.

Proteção da Informação

Mais que apenas segurança de computadores.

- Um programa de segurança da informação efetivo vai além da área de tecnologia da informação (TI) .
- Grande parte da informação disponível ainda se encontra impressa.
- Cada estágio do ciclo de vida do ativo informação, da criação à sua eventual destruição, deve ser acompanhado.
- A Política de Segurança da Informação deve fazer parte das políticas da empresa e não deve ser originada na área de TI.

Ameaças Comuns

De acordo com o survey "Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare", mais que 80% dos pesquisados apontaram empregados como ameaças ou potenciais ameaças para segurança da informação.

- **O típico criminoso de computadores é um usuário autorizado e não-técnico do sistema que teve oportunidade e tempo suficiente para determinar que ações podem prejudicar o sistema ou causar uma auditoria.**

Ameaças Comuns

A principal ameaça para a proteção da informação ainda está associada a erros e omissões, sendo responsável por 65% dos problemas.

- **Usuários, digitadores de dados, operadores de sistemas, programadores e equivalentes, freqüentemente cometem erros que contribuem diretamente ou indiretamente para este problema.**

Ameaças Comuns

Empregados desonestos são responsáveis por 13% dos problemas associados a proteção da informação.

- **Os empregados estão mais familiarizados com os ativos de informação e sistemas de processamento da organização, sabendo quais ações podem causar o maior dano, prejuízo ou sabotagem.**
  - **Destruição de hardware ou facilidades;**
  - **Instalação de códigos maliciosos (vírus, cavalos de tróia, etc);**
  - **Entrada de dados incorretos, remoção e alteração de dados.**

Ameaças Comuns

A perda de facilidades físicas ou da infra-estrutura de suporte levam a sérios problemas e provocam 8% dos problemas relacionados à proteção da informação.

- **Causas típicas:**
  - **Falha de energia, perda de comunicação;**
  - **Vazamento de água, problemas com dutos de esgoto;**
  - **Incêndio, inundação;**
  - **Agitação civil, greves;**
  - **Etc.**

Ameaças Comuns

Ataques de hackers e crakers maliciosos recebem a maior parte da atenção da imprensa, mas são responsáveis por 5% a 8% dos problemas.

- **Embora esses ataques sejam reais e possam causar grandes danos, se os recursos de proteção da informação forem limitados, é melhor concentrar os esforços nos outros problemas.**

- **Para determinar o risco, é importante conduzir uma análise de riscos.**

Gerenciamento de Risco

- Segurança da Informação
  Prof. Anderson O. da Silva

Risco é a possibilidade de alguma coisa adversa acontecer. O processo de gerenciamento de risco se resume em três etapas:

- **Identificação dos riscos, ameaças e vulnerabilidades para cada ativo;**
- **Avaliação da probabilidade desses riscos acontecerem e o impacto que isso terá no ativo ou na organização;**
- **Determinação dos controles e salvaguardas apropriados para minimizar os riscos a um nível aceitável.**

Gerenciamento de Risco

O custo inicial da implementação dos controles é apenas a ponta do iceberg. Várias outras questões devem ser identificadas.

- **O custo de longo prazo associado a manutenção e monitoramento;**
- **Recursos técnicos necessários para implementação dos controles;**
- **Barreiras culturais.**
  - **Medidas de controle que funcionam e são aceitas em uma localização, podem não ser aceitas em outras.**

Classificação da Informação

As empresas classificam as informações para estabelecer os níveis de proteção apropriados para cada categoria. Devido à limitação de recursos, é necessário priorizar e identificar o que realmente requer proteção.

- **O processo de classificação da informação é um processo de decisão de negócios e requer o papel ativo do setor gerencial da empresa.**
- **Os profissionais de segurança e os técnicos de computadores exercem papéis limitados nesse processo.**

Classificação da Informação

A informação que requer proteção tipicamente se enquadra em um ou mais dos seguintes quesitos:

- **Tem algum valor para a empresa e seus competidores, caracterizando uma vantagem competitiva;**
- **É resultado de algum tipo de gasto ou investimento feito pela empresa;**
- **É, de alguma forma, única e não é de conhecimento geral da indústria ou do público, ou não deve ser apurada ou averiguada.**

Classificação da Informação

Tipicamente, três categorias são utilizadas para classificar a informação:

1. **Confidencial (Sensível, Pessoal, Privilegiada)**
   - Se for exposta, viola a privacidade de indivíduos, reduz a vantagem competitiva da empresa ou causa danos a mesma.
     - Registros pessoais e informações de clientes;
     - Informações sobre custo, lucro e resultado financeiro;
     - Planos operacionais e estratégias de marketing e negócios;
     - Requisitos de mercado, tecnologias, planos de produtos.

Classificação da Informação

Tipicamente, três categorias são utilizadas para classificar a informação (continuação):

2. Restrita (Uso Interno)

- Informação destinada ao uso de funcionários na condução dos negócios da empresa.
  - Relatórios e informações sobre a operação do negócio;
  - Informações que pertencem a parceiros de negócios e que são protegidas por acordos de restrição de exposição;
  - Lista telefônica da empresa;
  - Políticas, padrões e procedimentos corporativos.

Classificação da Informação

Tipicamente, três categorias são utilizadas para classificar a informação (continuação):

3. Pública (Não Classificada)

- Informação que foi disponibilizada para distribuição pública através de canais da empresa devidamente autorizados, não requerendo proteção.
  - Relatório anual da empresa;
  - Boletins de serviço público;
  - Apresentações de marketing;
  - Propaganda.

Políticas e Procedimentos

Toda organização precisa de uma política de proteção da informação. O início de um programa é determinado pela implementação de uma política.

- **A política do programa cria uma atitude da organização em relação à informação e anuncia internamente e externamente que a informação é um ativo e propriedade da organização que deve ser protegido contra acesso, modificação, revelação e destruição não autorizados.**

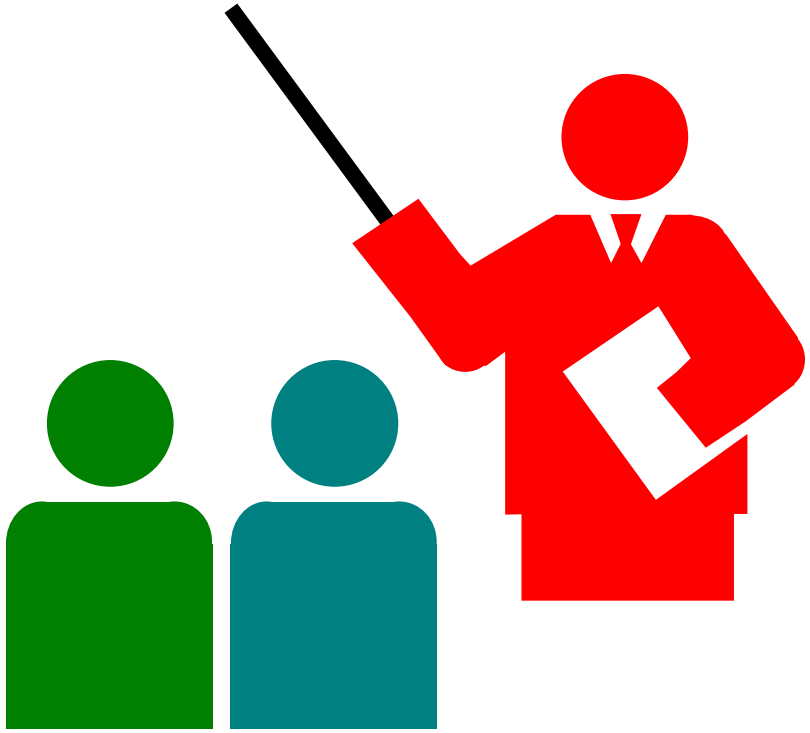
Políticas e Procedimentos

Políticas não são suficientes. Outras ações são necessárias para garantir a prática das políticas.

- Desenvolvimento de normas que definam os códigos de práticas para padronizar os requisitos para certificações.
- Definição de procedimentos e diretrizes capazes de implantar a prática da proteção da informação.
- Instauração de auditorias periódicas para validar a conformidade da empresa com os padrões adotados.

Normas e Padronização

- Segurança da Informação
  Prof. Anderson O. da Silva



Normas e Padronização

Norma é aquilo que se estabelece como base ou medida para a realização de alguma coisa. A padronização é uma referência de qualidade.

- **A atividade de normalização estabelece, em relação a problemas existentes ou potenciais, prescrições destinadas à utilização comum e repetitiva com vistas à obtenção do grau ótimo de ordem em um dado contexto.**

Principais Normas de Segurança

BS 7799 – início em 1995.

- Em 1995, o BSI publica a BS 7799-1:1995 (Information Technology - Code of Practice for Information Security Management).
- Proposta à ISO, em 1996, para homologação, mas foi rejeitada.
- Em 1998, a segunda parte desse documento foi publicado como BS 7799-2:1998 (Information Security Management Systems).
- Em abril de 1999, as duas normas foram publicadas após uma revisão, com o nome de BS 7799-1999.

BS 7799

BSI

Principais Normas de Segurança

ISO/IEC 17799:2000 – ano 2000.

- **Homologação da BS 7799-1 em padrão ISO, sendo *composta por 10 macro controles*, cada qual subdividido em controles específicos.**
- **Primeira norma homologada a apresentar soluções para o tratamento da informação de uma maneira mais ampla.**
- **Segundo essa norma, *todo tipo de informação deve ser protegido, independentemente da sua forma de armazenamento, seja analógica ou digital, e de seu valor para a organização*.**

ISO/IEC 17799

Principais Normas de Segurança

NBR ISO/IEC 17799:2001 – ano 2001.

- Em abril de 2001, a versão brasileira da norma ISO/IEC 17799:2000 foi disponibilizada para consulta pública.
- Em 01/08/2001 a ABNT homologou a versão brasileira.
- Essa norma *estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização*.
- Os objetivos definidos provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação.

NBR ISO/IEC 17799

Principais Normas de Segurança

BS 7799-2:2002 – ano 2002.

- Publicada em julho de 2002.
- Foi resultado de uma revisão que visava ajustá-la com normas internacionais, tais como a ISO 9001 e a ISO 14001, e remover aspectos próprios da lei britânica.
- Os controles da ISO/IEC 17799 foram adicionados a um anexo dessa versão, permitindo uma correspondência entre a numeração em ambas as normas.

BS 7799

BSI

Principais Normas de Segurança

Certificação de Segurança da Informação

- Até então, o padrão ISO apenas fornecia uma *diretriz para a implementação de melhores práticas de segurança das informações* e ainda não dispusera uma norma para a certificação destas práticas.

- As empresas, para se certificarem, implementavam os controles previstos na ISO 17799 e se submetiam a um processo de certificação de segurança da informação baseado na norma britânica BS 7799-2.

Principais Normas de Segurança

ISO/IEC 27001:2005 – ano 2005.

- **Publicada pela ISO como a primeira norma da série 27000, que é uma nova família de normas voltadas exclusivamente para segurança da informação.**
- **Substitui a BS 7799-2, tornando-se a *norma para certificação da segurança da informação*.**
- **Nela são organizados os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar o SGSI (Sistema de Gestão da Segurança da Informação).**

ISO/IEC 27001

Principais Normas de Segurança

NBR ISO/IEC 27001:2006 – ano 2006.

- Norma brasileira correspondente à ISO/IEC 27001:2005.
- Agora, para uma empresa estar certificada em um padrão internacional, basta submeter-se a um processo de auditoria baseada na norma ISO 27001.
- *A certificação agrega valor de mercado pois mostra que a empresa está apta a tratar as informações com os padrões mais exigentes e atuais de gestão da segurança das informações.*

NBR ISO/IEC 27001

Principais Normas de Segurança

ISO/IEC 27000 Standards: IT - Security Techniques

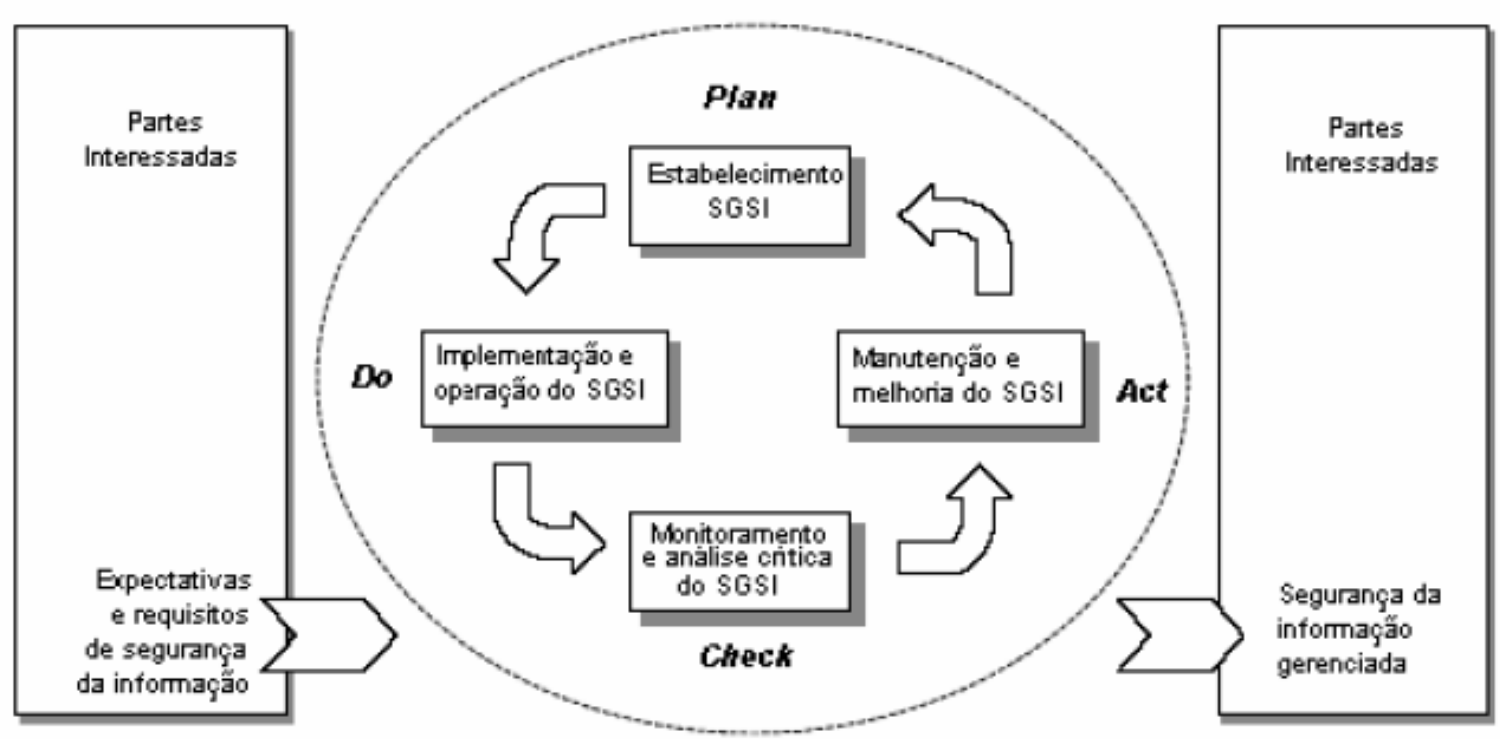
- 27001: Information security management systems – Requirements
- 27002: Code of practice for information security controls
- 27003: Information security management system implementation guidance
- 27004: Information security management – Measurement
- 27005: Information security risk management
- 27006: Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27001

NBR ISO/IEC 27001:2006

- Segurança da Informação
  Prof. Anderson O. da Silva

Processo de Implantação: Ciclo Plan-Do-Check-Act (PDCA)



NBR ISO/IEC 27001:2006

Controles da Norma (derivados da NBR ISO/IEC 17799:2005)

- Política de Segurança
- Organização da Segurança da Informação
- Gestão de Ativos
- Segurança em Recursos Humanos
- Segurança Física e do Ambiente
- Gerenciamento das Operações e Comunicações
- Controle de Acessos
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
- Gestão de Incidentes de Segurança da Informação
- Gestão da Continuidade do Negócio
- Conformidade

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Procedimentos e Responsabilidades Operacionais**
  - Garantir a operação segura e correta dos recursos de processamento da informação.
  - Consiste dos seguintes controles:
    - Documentação dos procedimentos de operações;
      - Disponibilidade da documentação atualizada para os usuários.
    - Gestão de mudanças;
      - Controle de modificações nos recursos de processamento e sistemas.
    - Segregação de funções;
      - Evitar uso indevido não autorizado ou não intencional.
    - Separação dos ambientes de desenvolvimento, teste e produção.
      - Reduzir o risco de acessos ou modificações nos sistemas operacionais.

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Gerenciamento de Serviços Terceirizados**
  - **Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em linha com acordos de entrega de serviços terceirizados.**
  - **Consiste dos seguintes controles:**
    - **Entrega de serviços;**
      - **Garantir os níveis de entrega de serviços acordados com terceiros.**
    - **Monitoramento e análise crítica de serviços terceirizados;**
      - **Monitoramento e análise dos serviços, relatórios e registros providos pelo terceiro.**
    - **Gerenciamento de mudanças para serviços terceirizados.**
      - **Gerenciamento das mudanças do provisionamento dos serviços do terceiro.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Planejamento e Aceitação dos Sistemas**
  - **Minimizar o risco de falhas nos sistemas.**
  - **Consiste dos seguintes controles:**
    - **Gestão de capacidade;**
      - **Utilização dos recursos deve ser monitorada e sincronizada.**
    - **Aceitação de sistemas.**
      - **Estabelecimento de critérios para aceitação de novos sistemas, atualizações e novas versões.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Proteção Contra Códigos Maliciosos e Códigos Móveis**
  - **Proteger a integridade do software e da informação.**
  - **Consiste dos seguintes controles:**
    - **Controle contra códigos maliciosos;**
      - **Controles de detecção, prevenção e recuperação;**
      - **Conscientização de usuários.**
    - **Controle contra códigos móveis.**
      - **Código móvel autorizado deve operar de acordo com uma política de segurança claramente definida;**
      - **Código móvel não autorizado deve ter sua execução impedida.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Cópias de Segurança**
  - **Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.**
  - **Consiste do seguinte controle:**
    - **Cópia de segurança das informações**
      - **Execução e testes regulares das cópias de segurança das informações.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Gerenciamento da Segurança em Redes**
  - **Garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte.**
  - **Consiste dos seguintes controles:**
    - **Controles de Redes**
      - **Proteger contra ameaças e manter a segurança de sistemas e aplicações.**
    - **Segurança dos serviços de rede**
      - **Garantir as características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede internos ou terceirizados.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Manuseio de Mídias**
  - **Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio.**
  - **Consiste dos seguintes controles:**
    - **Gerenciamento de mídias removíveis**
      - **Definir procedimentos para manipulação dessas mídias.**
    - **Descarte de mídias**
      - **Definir procedimentos para o descarte dessas mídias.**
    - **Procedimentos para tratamento de informação**
      - **Definir procedimentos para o tratamento e o armazenamento de informações.**
    - **Segurança da documentação dos sistemas**
      - **Proteger a documentação dos sistemas contra acessos não autorizados.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Troca de Informações**
  - **Manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.**
  - **Consiste dos seguintes controles:**
    - **Políticas e procedimentos para troca de informações**
      - **Estabelecer e formalizar controles para troca de informações.**
    - **Acordos para a troca de informações**
      - **Estabelecer acordos para trocas de informações.**
    - **Mídias em trânsito**
      - **Proteger contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Troca de Informações (continuação)**
  - **Manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.**
  - **Consiste dos seguintes controles:**
    - **Correio eletrônico**
      - **Proteger as mensagens de correio eletrônico.**
    - **Sistemas de informações do negócio**
      - **Proteger as informações associadas a interconexão de sistemas de informação do negócio.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Serviços de Comércio Eletrônico**
  - **Garantir a segurança de serviços de comércio eletrônico e sua utilização segura.**
  - **Consiste dos seguintes controles:**
    - **Comércio eletrônico**
      - **Proteger de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.**
    - **Transações on-line**
      - **Proteger para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.**
    - **Informações publicamente disponíveis**
      - **Proteger contra modificações não autorizadas.**

NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Monitoramento**
  - **Detectar atividades não autorizadas de processamento da informação.**
  - **Consiste dos seguintes controles:**
    - **Registros de auditoria**
      - **Produzir e manter registros (log) de auditoria para auxiliar em futuras investigações.**
    - **Monitoramento do uso do sistema**
      - **Estabelecer procedimentos para o monitoramento do uso dos recursos.**
    - **Proteção das informações dos registros (logs)**
      - **Proteger contra falsificação e acesso não autorizado.**

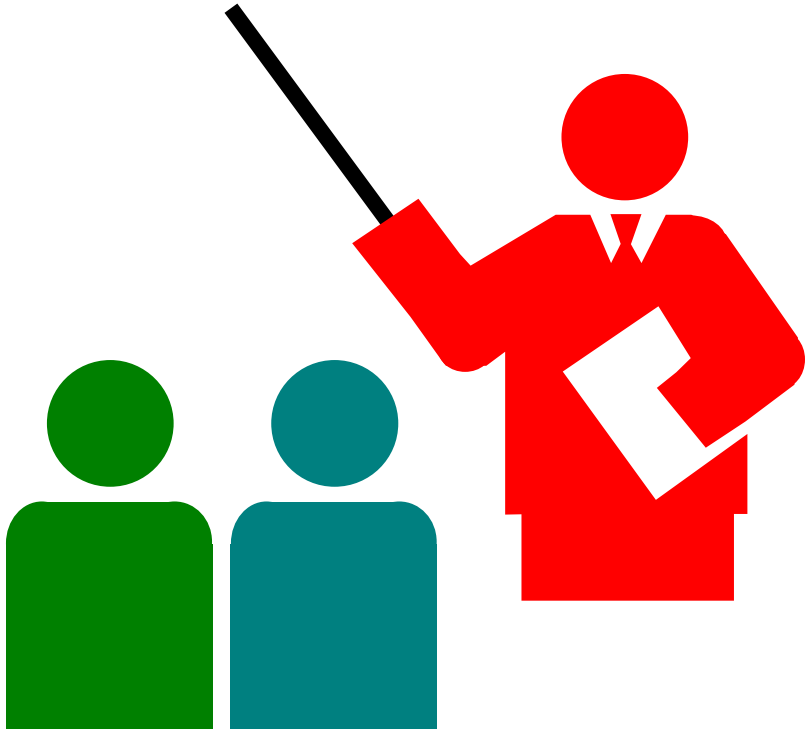
NBR ISO/IEC 27001:2006

Controles da Norma: Gerenciamento das Operações e Comunicações

- **Monitoramento (continuação)**
  - **Detectar atividades não autorizadas de processamento da informação.**
  - **Consiste dos seguintes controles:**
    - **Registros (log) de Administrador e Operador**
      - **Registrar as atividades dos administradores e operadores do sistema.**
    - **Registros (logs) de falhas**
      - **Registrar e analisar as falhas ocorridas.**
    - **Sincronização dos relógios**
      - **Sincronizar os relógios de todos os sistemas de processamento.**

Comunicação Segura

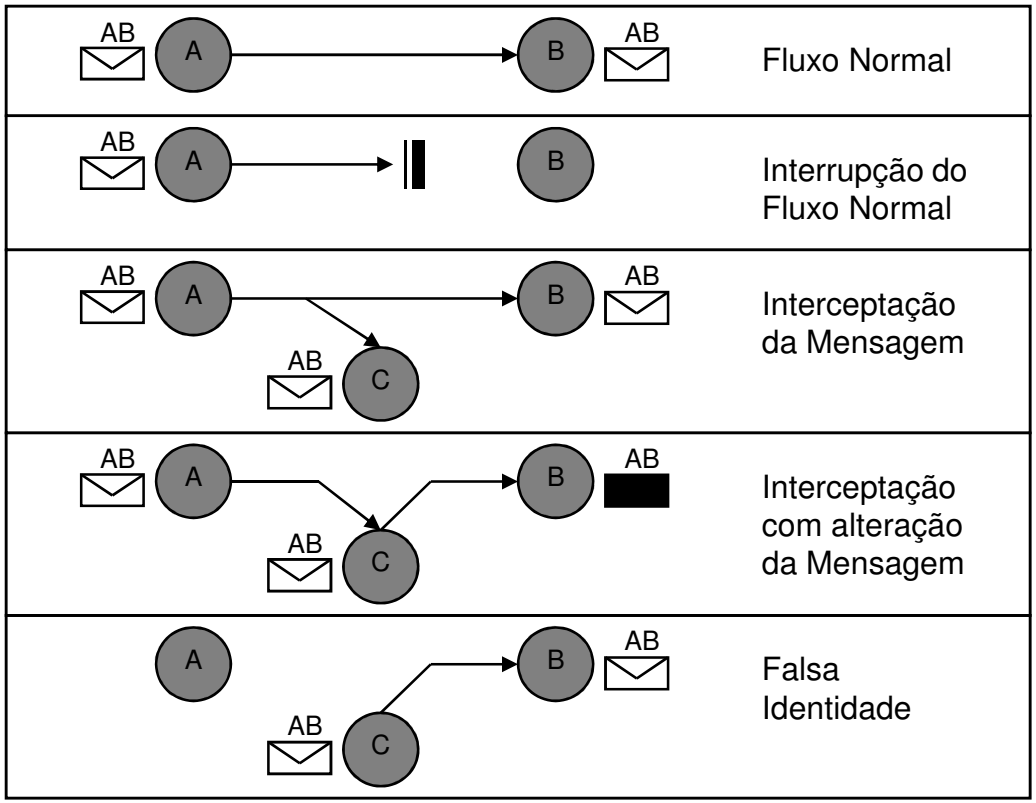
- Segurança da Informação
  Prof. Anderson O. da Silva



Comunicação Segura

- Segurança da Informação
  Prof. Anderson O. da Silva

Ameaças Comuns:



Comunicação Segura

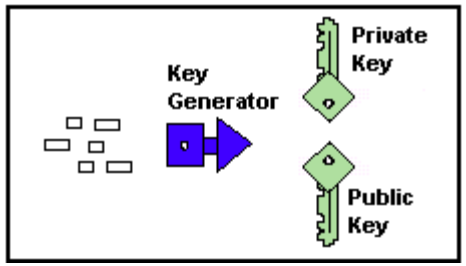
Objetivos:

- Controle de Temporalidade
  - Detectar a recepção de mensagens retransmitidas ou com o conteúdo antigo.
- Controle de Integridade
  - Detectar se mensagens não foram modificadas durante a transmissão.
- Controle de Autenticidade
  - Verificar a identidade do usuário que alega ter sido o gerador da mensagem.
- Controle de Confidencialidade
  - Proteger o conteúdo de mensagens de exposição a terceiros.

Comunicação Segura

Processo de Comunicação Segura:

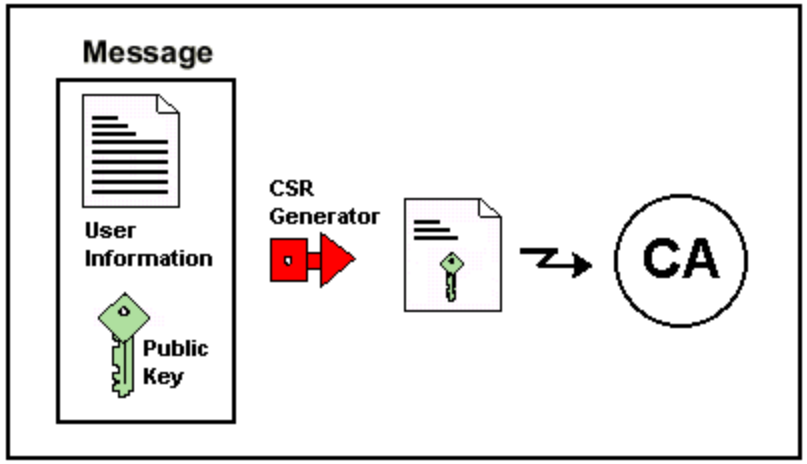
- **Gerar Par de Chaves Assimétricas**



Comunicação Segura

Processo de Comunicação Segura:

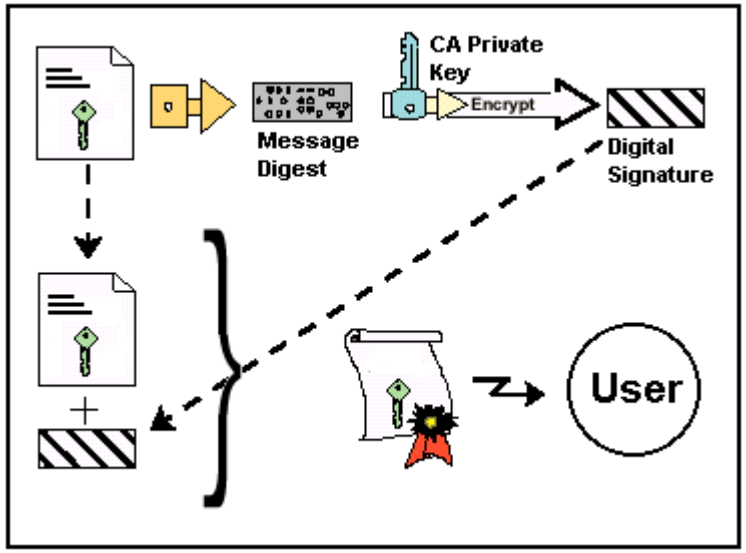
- **Enviar Mensagem de Solicitação de Certificado**



Comunicação Segura

Processo de Comunicação Segura:

- **Gerar Certificado e Enviar para Usuário**

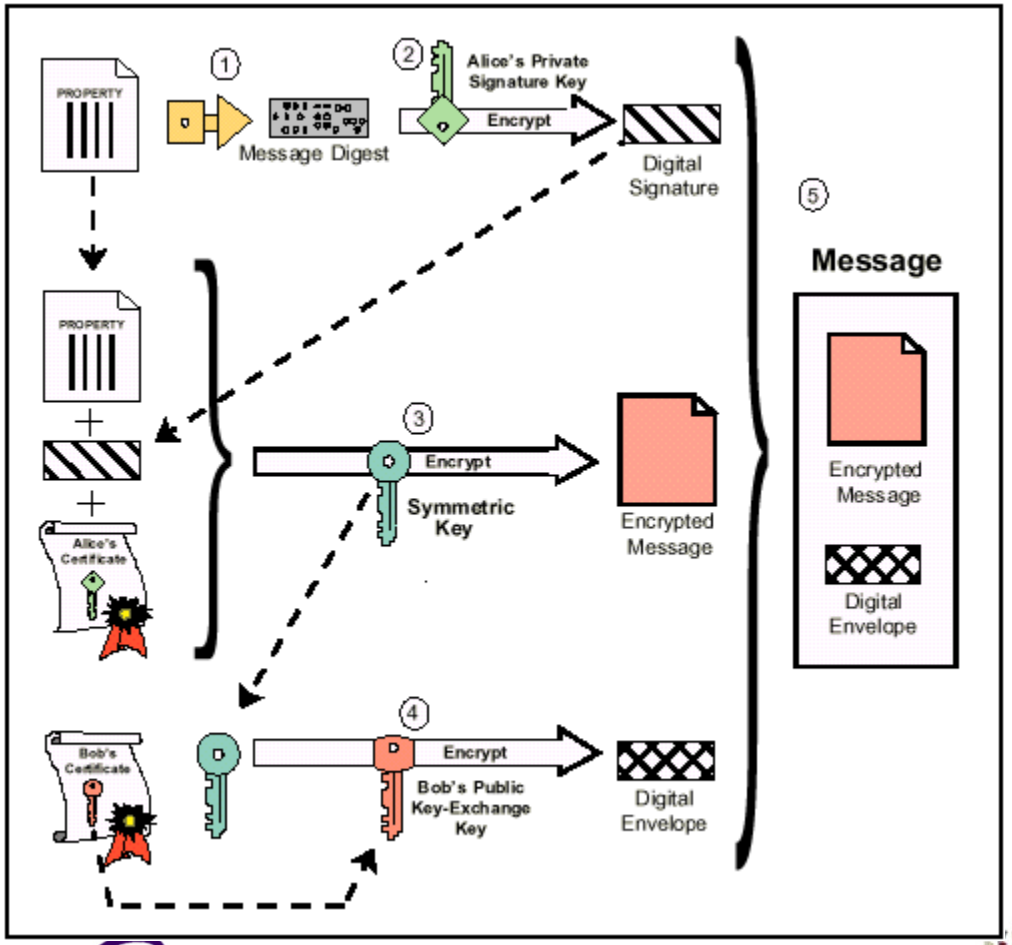


Comunicação Segura

- Segurança da Informação
  Prof. Anderson O. da Silva

Processo de Comunicação Segura:

- **Processo de Envio de Mensagem**

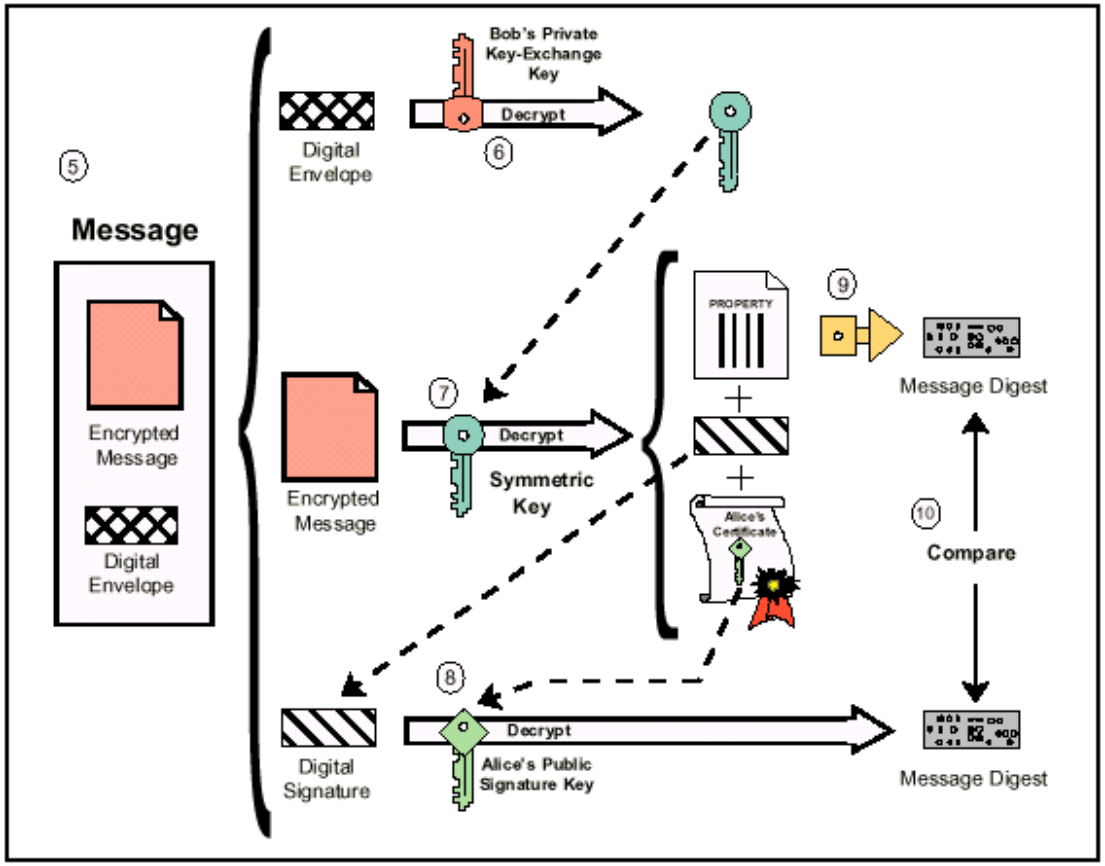


Comunicação Segura

- Segurança da Informação
  Prof. Anderson O. da Silva

Processo de Comunicação Segura:

- **Processo de Recepção de Mensagem**



Comunicação Segura

Secure Socket Layer (SSL):

- Desenvolvido pela Netscape, 1994.
- Amplamente aceito, distribuído e suportado em todos os navegadores e servidores mais importantes.
- Atualmente apresentado em três versões:
  - SSLv2, SSLv3 (versão predominante) e TLSv1 (padrão IETF, primeira versão, 1999).
- Características do SSLv3/TLSv1:
  - Autenticação do servidor obrigatória e autenticação do cliente pode ser opcional.
  - Permite que ambas as partes (cliente e servidor) renegociem as chaves e as cifragens a qualquer momento.
  - Permite compactação dos dados.

Comunicação Segura

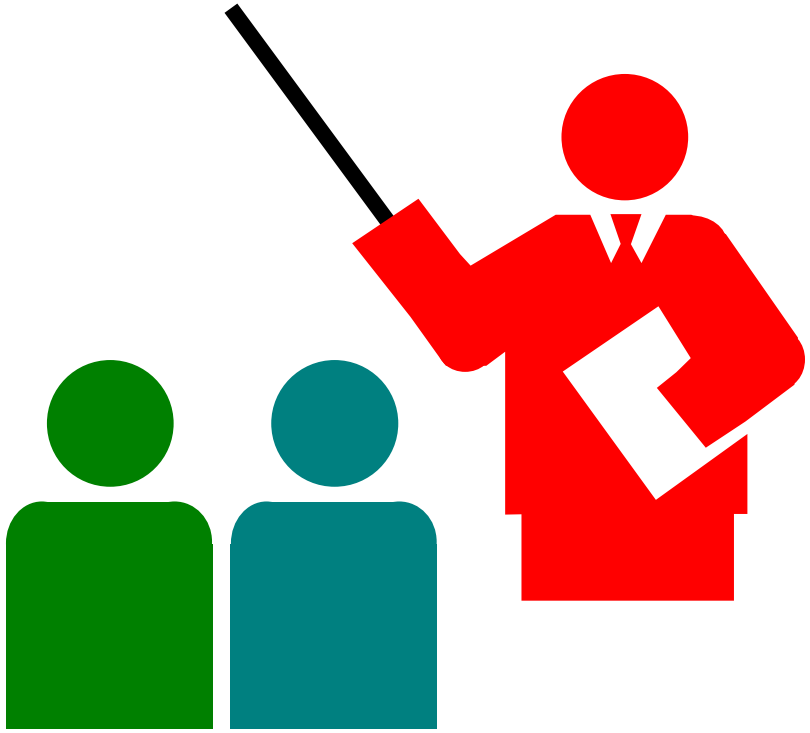
Secure Socket Layer (SSL):

- **Algoritmos de cifragem mais usados:**
  - **RSA (durante o processo de handshaking)**
  - **RC2, RC4, IDEA, DES, triple-DES, AES (após a troca de chaves)**
  - **MD5, SHA1 para message-digest**
  - **Diffie-Hellman (especificação fortemente desencoraja sua utilização)**

- **Certificado mais comum:**
  - **Certificados de chave pública X.509**

Técnicas de Ataque a Redes

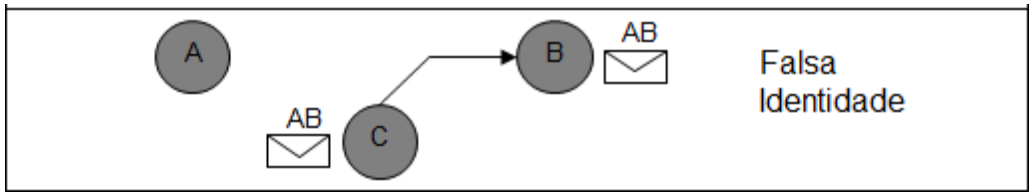
- Segurança da Informação
  Prof. Anderson O. da Silva



Técnicas de Ataque a Redes

Técnicas:

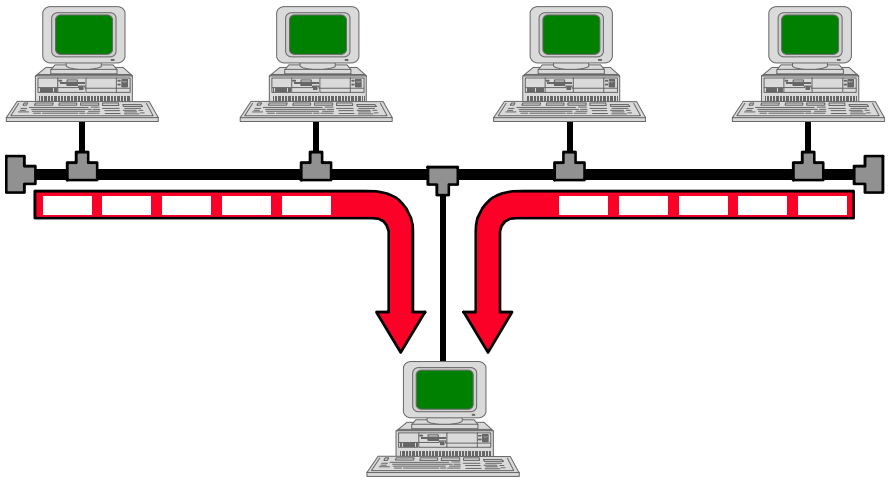
- **IP Spoofing (Forjando IP)**
  - Consiste em enviar ao alvo pacotes com endereço de origem falsificados.
  - Objetivo é ser identificado como um host confiável, de origem confiável, pelo alvo.
  - Utilizado para atravessar barreiras com regras baseadas em endereços IP.
  - Utilizado para ganhar acesso a serviços autenticados por endereço IP.



Técnicas de Ataque a Redes

Técnicas:

- **Network Sniffing (Farejando a Rede)**
  - **O objetivo é efetuar a escuta da rede em busca de informações úteis para um futuro ataque, tais como:**
    - **Informação sobre serviços, sistemas e usuários.**



Técnicas de Ataque a Redes

Técnicas:

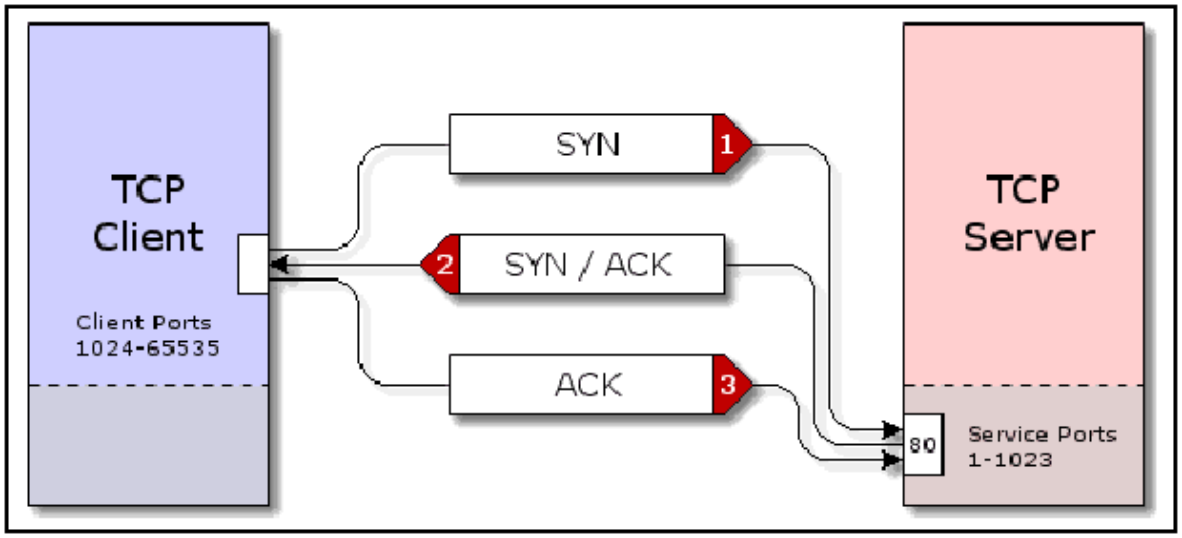
- **Denial of Service (DoS)**
  - **Sobrecarga das atividades do alvo ao ponto de torná-lo inoperante (ataque por negação de serviço).**
  - **Com a neutralização do alvo, centenas de usuários podem ser afetados.**
  - **Ataques são formados por uma grande armada (ex: botnet) que utiliza a técnica de inundação (flooding).**
  - **Considerado um dos ataques mais eficazes, mesmo contra grandes provedores de serviço.**

Técnicas de Ataque a Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

Técnicas:

- **Denial of Service (DoS)**
  - **TCP 3way-Handshake (operação normal)**

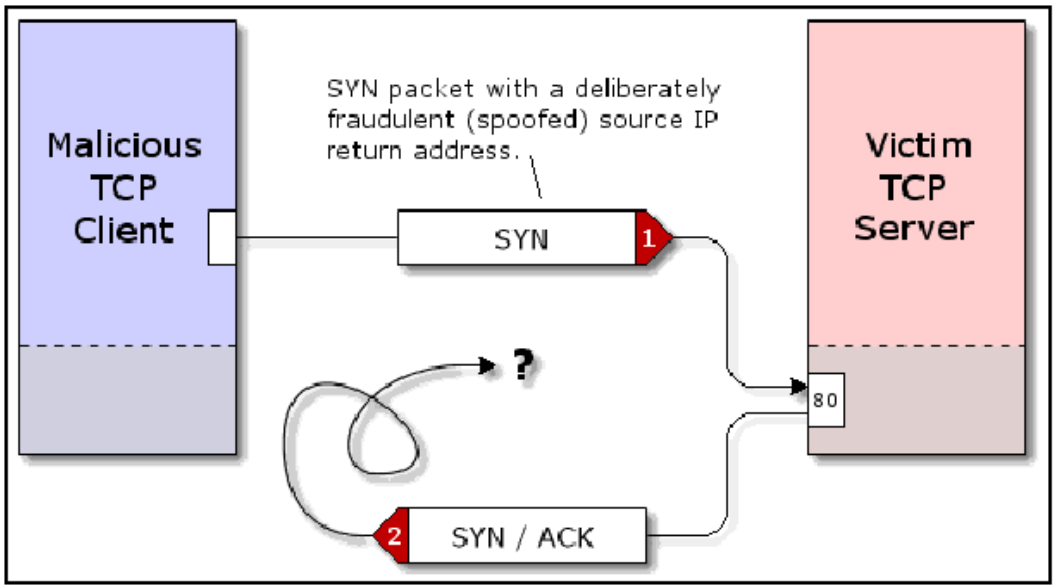


Técnicas de Ataque a Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

Técnicas:

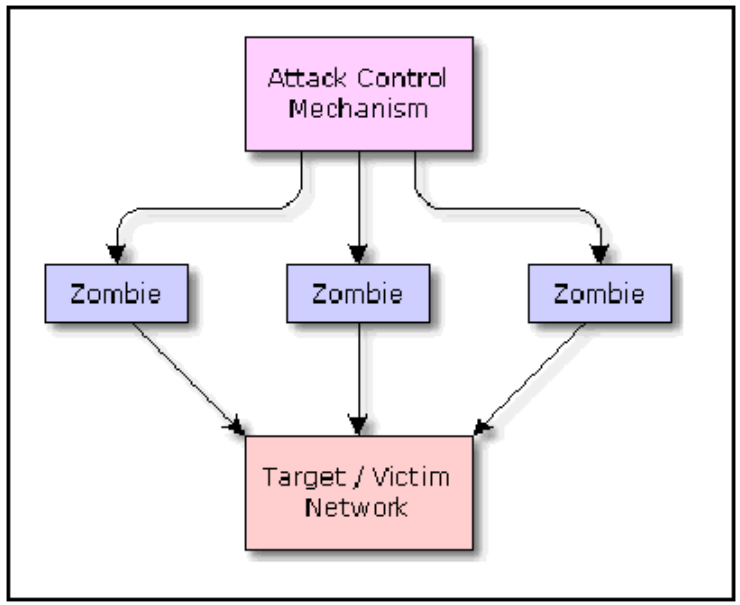
- **Denial of Service (DoS)**
  - **TCP SYN Flood**



Técnicas de Ataque a Redes

Técnicas:

- **Denial of Service (DoS)**
  - **Distributed Denial of Service (DDOS)**

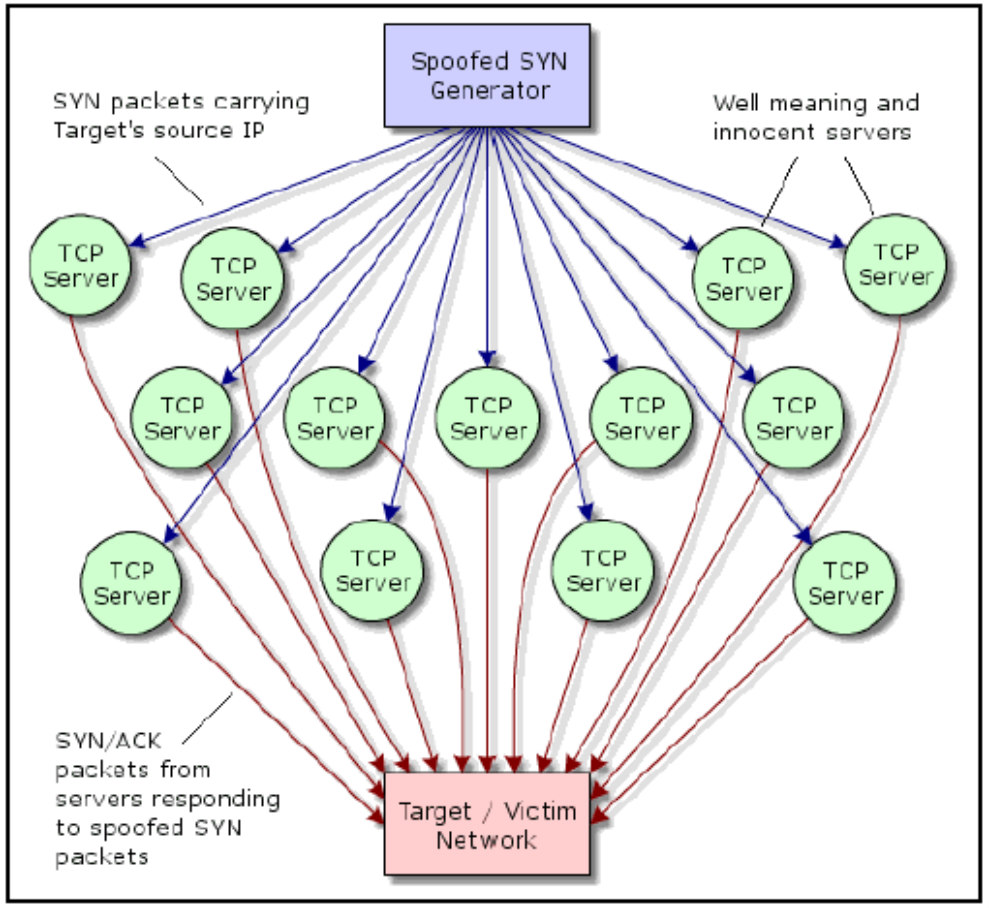


Técnicas de Ataque a Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

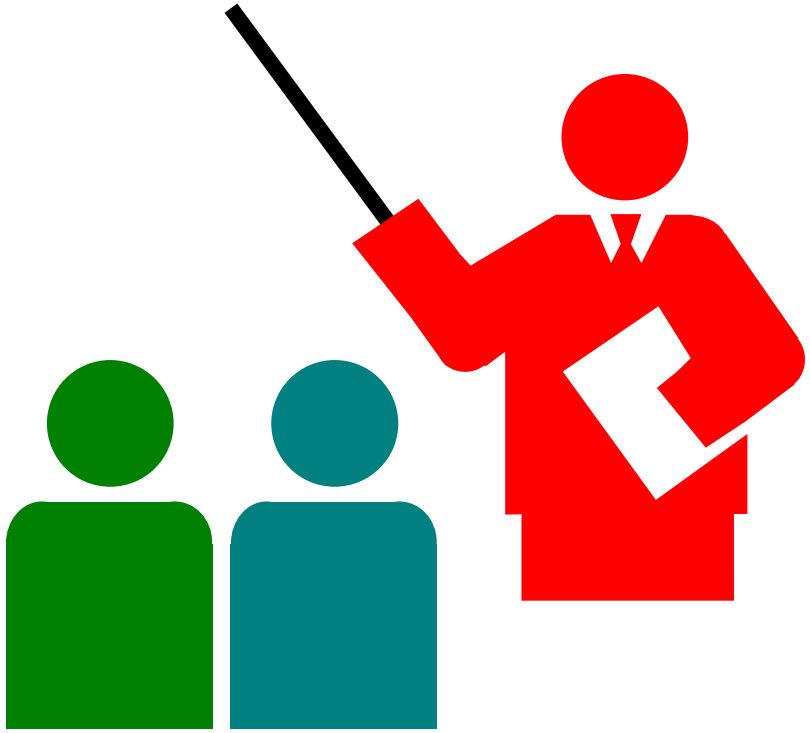
Técnicas:

- **Denial of Service (DoS)**
  - **Distributed Reflection Denial of Service (DRDOS)**



Técnica de Defesa de Redes

- Segurança da Informação
  Prof. Anderson O. da Silva



Técnica de Defesa de Redes

Defesa em Profundidade:

- Técnica de defesa baseada em camadas de segurança.
- Protege recursos de rede mesmo que uma das camadas de segurança seja comprometida.
- Envolve três fatores principais:
  - Perímetro
  - Rede interna
  - Humano
- Cada um dos fatores é formado por diversos componentes que funcionam de forma integrada para proteger a rede.

Técnica de Defesa de Redes

Perímetro:

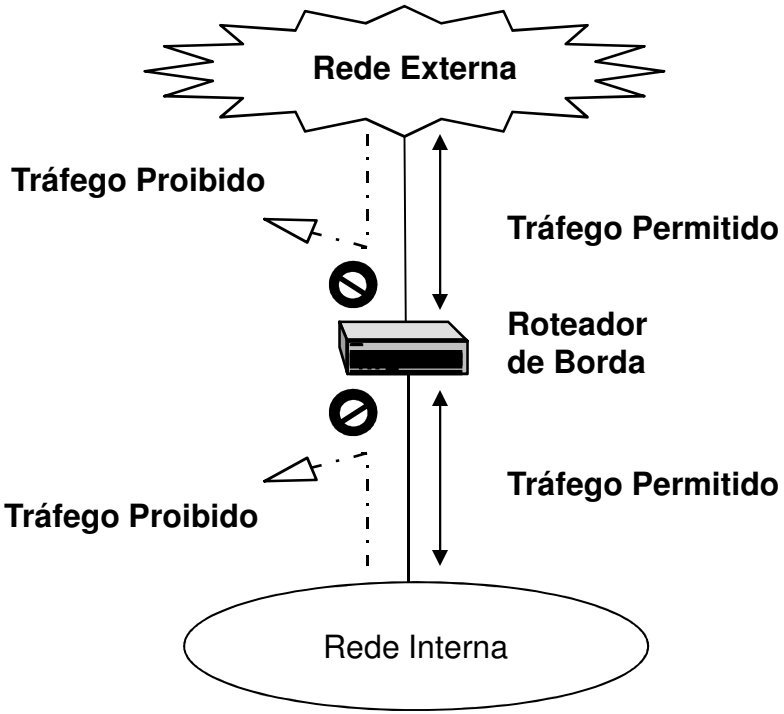
- Borda fortificada de uma rede.
- Composto por elementos que visam proteger a rede interna.
- Os mais importantes são:
  - Roteador de borda com filtro de pacote
  - Firewall com estado
  - Firewall proxy (procurador)
  - Redes com triagem (screened subnets)
  - Sistema de detecção de intrusão (IDS – Intruder Detection System)
  - DMZ (Des-Militarized Zone)
  - VPN (Virtual Private Network)

Técnica de Defesa de Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

Perímetro: Roteador de borda com filtro de pacotes

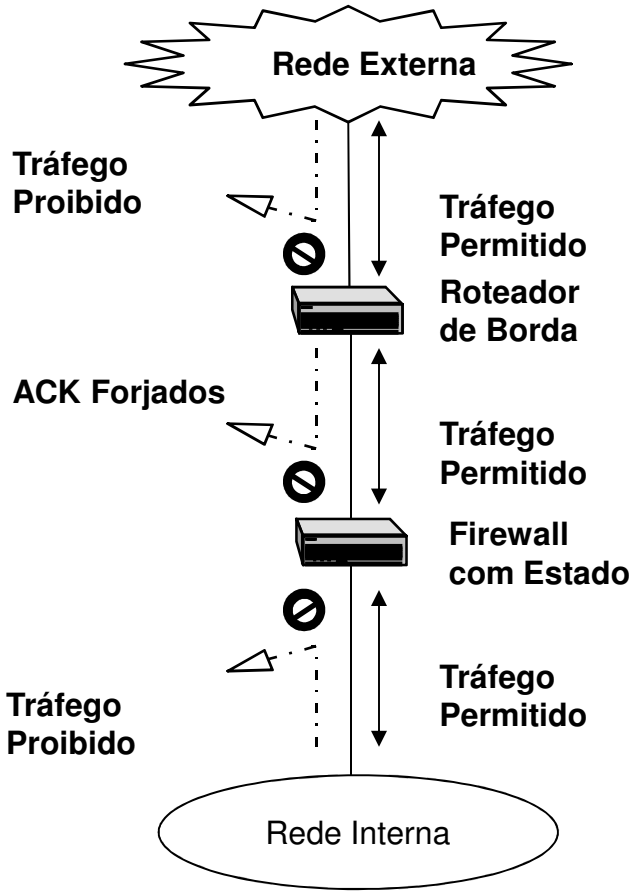
- **Esquema**



Técnica de Defesa de Redes

Perímetro: Firewall com estado

- **Esquema**

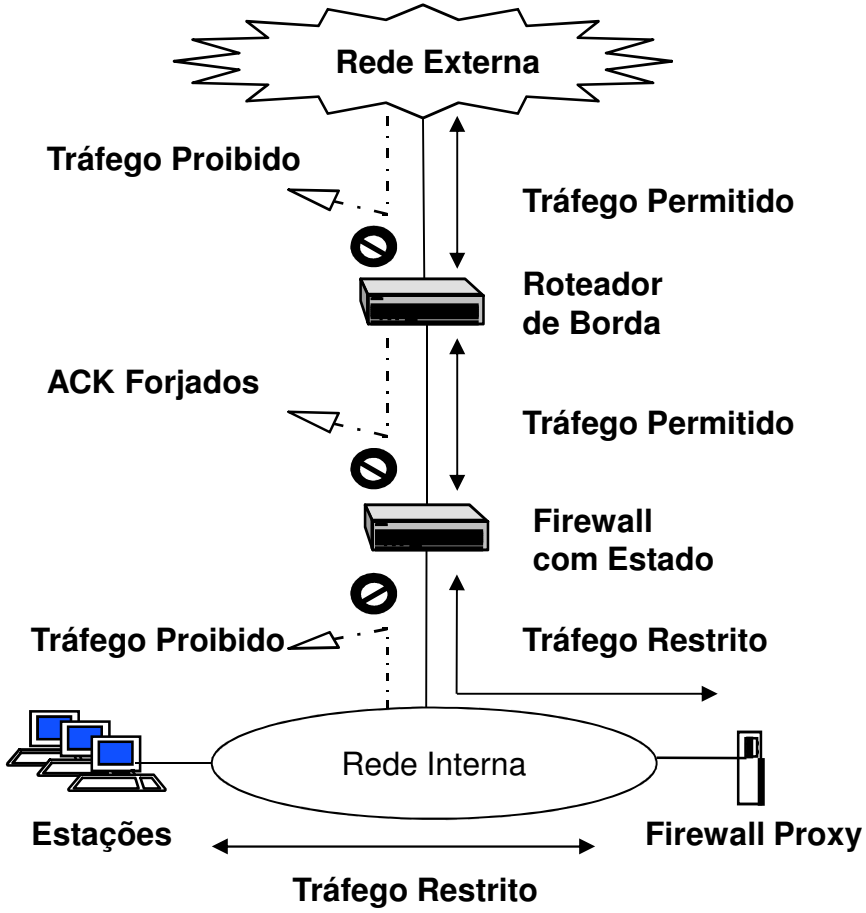


Técnica de Defesa de Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

Perímetro: Firewall Proxy

- **Esquema**

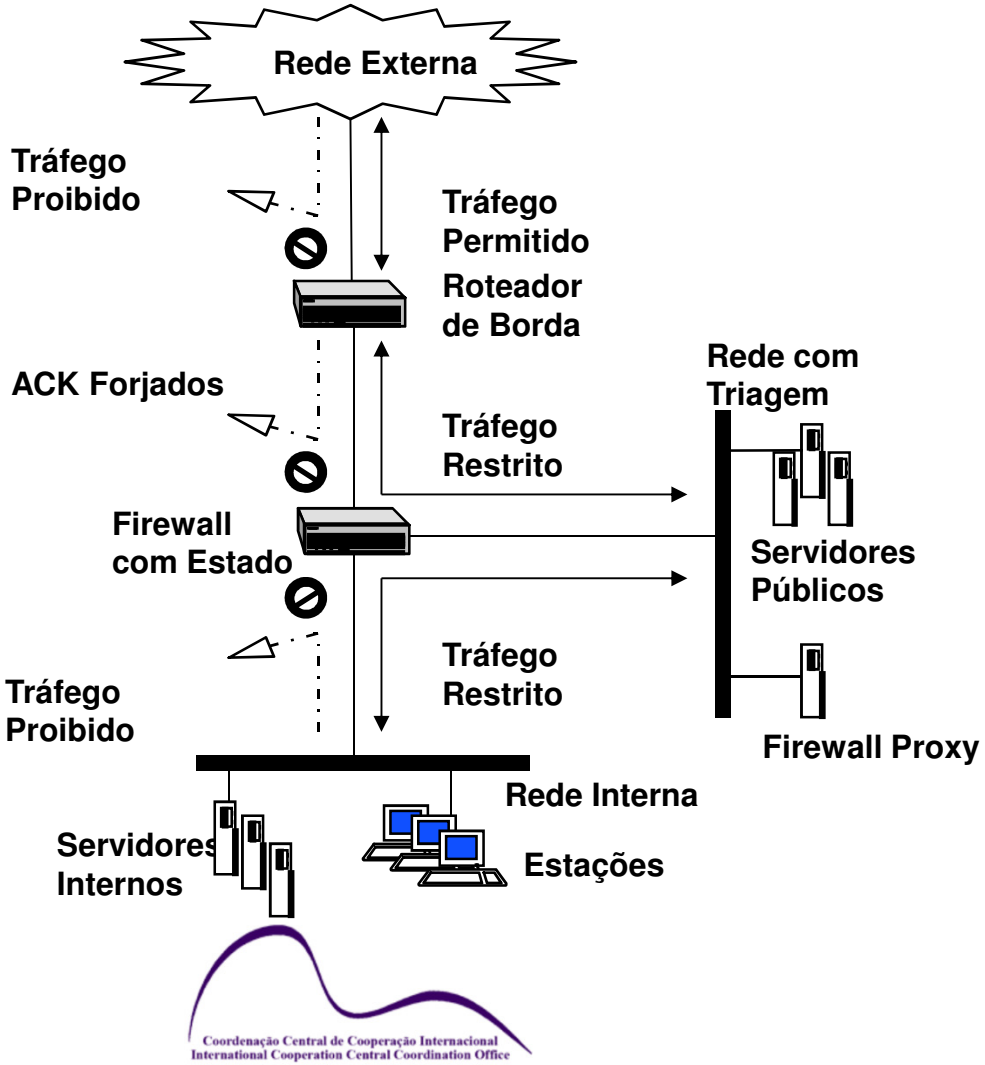


Técnica de Defesa de Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

Perímetro: Firewall Proxy

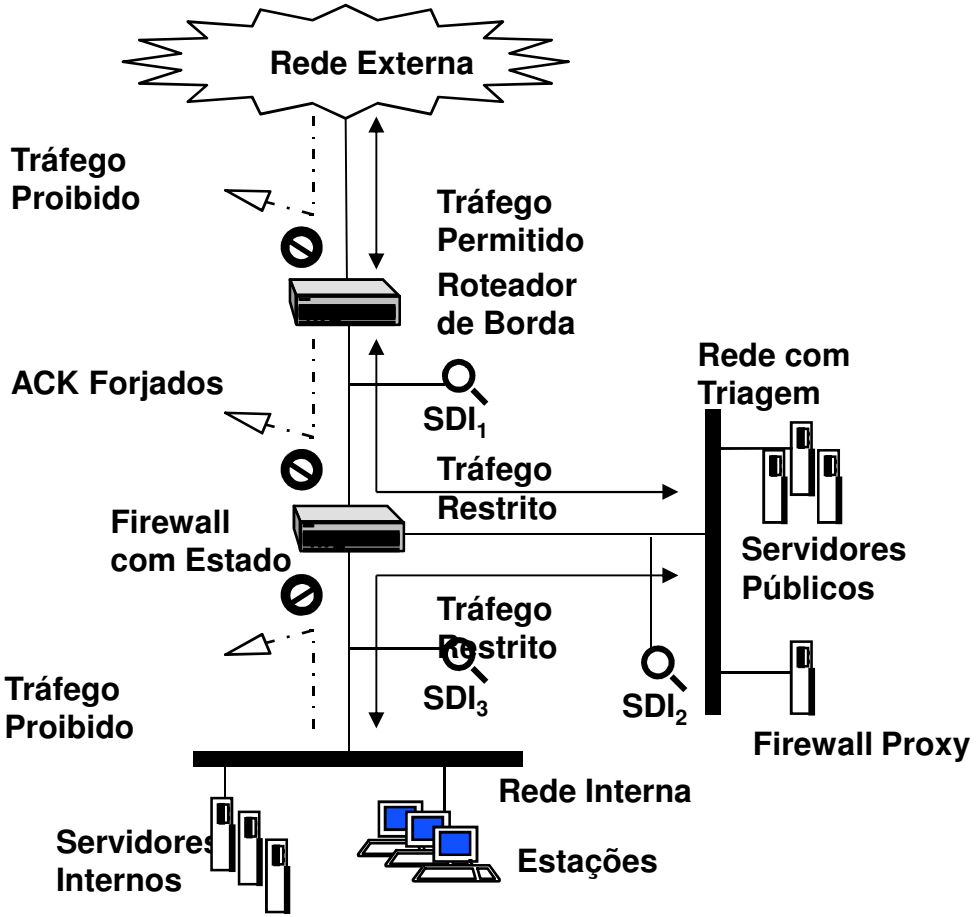
- **Esquema**



Técnica de Defesa de Redes

Perímetro: SDI

- **Esquema**

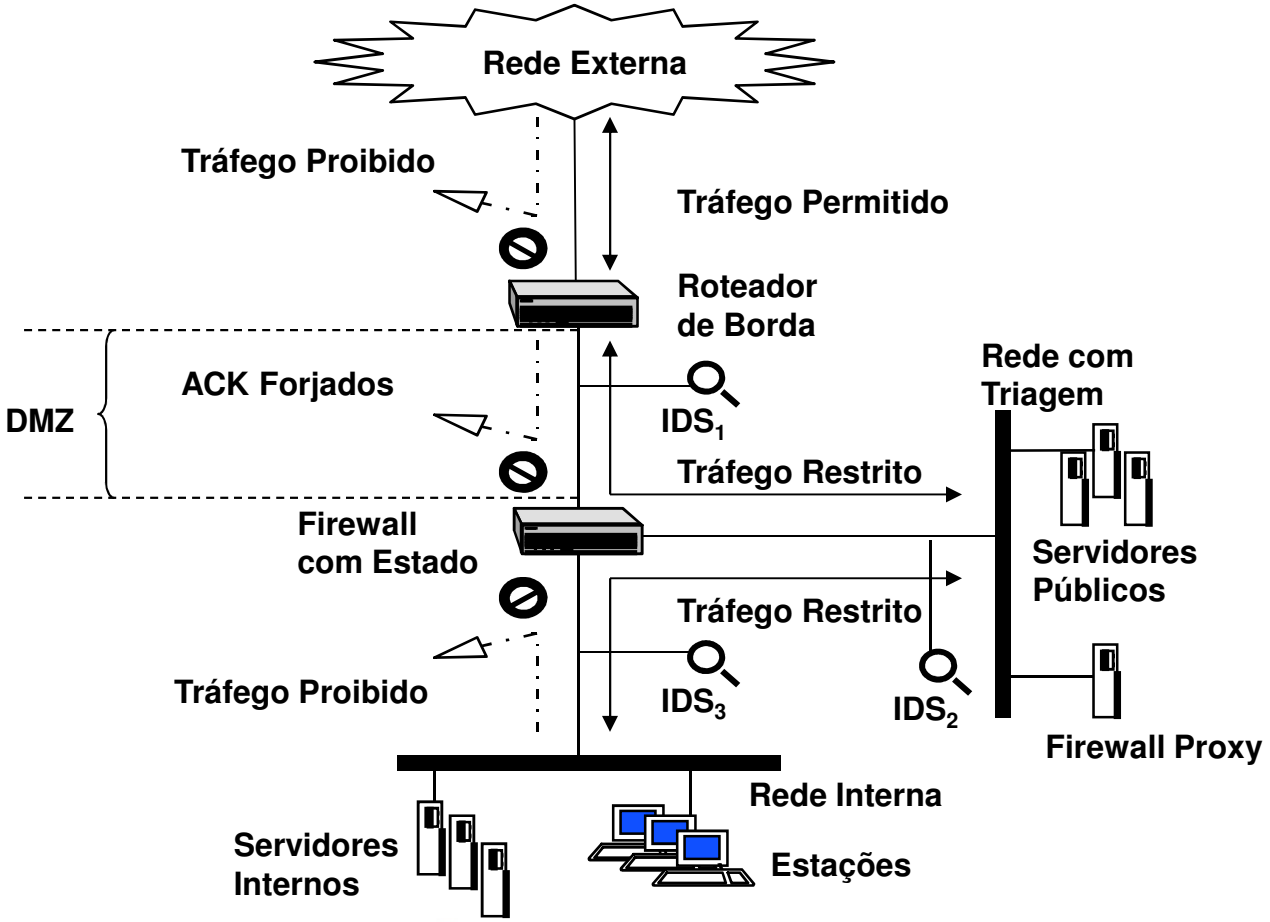


Técnica de Defesa de Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

Perímetro: DMZ

- **Esquema**

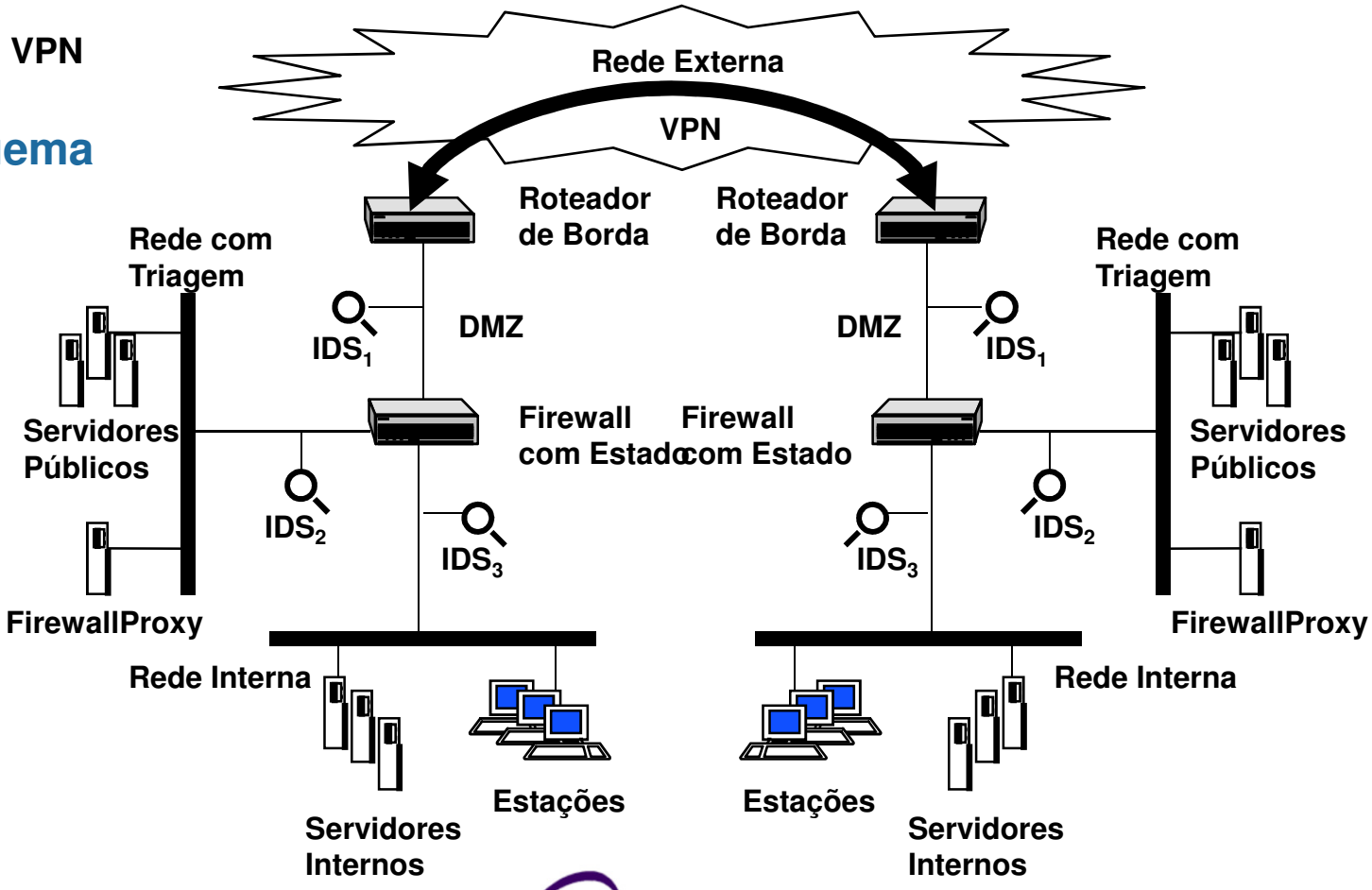


Técnica de Defesa de Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

Perímetro: VPN

- **Esquema**



Técnica de Defesa de Redes

Rede Interna

- Rede protegida pelo perímetro.
- Toda infra-estrutura interna deve ser mantida nela.
- Para garantir a sua real segurança, é necessário implementar uma rígida *política de segurança*, determinando um tráfego restrito de entrada e saída.
- Mesmo que todos os usuários sejam confiáveis, os mesmos usuários podem ser descuidados e, com isso, permitir a proliferação de um novo verme ou vírus.

Técnica de Defesa de Redes

- Segurança da Informação
  Prof. Anderson O. da Silva

Rede Interna

- **Procedimentos básicos de segurança**
  - ***Instalação de antivírus***. Permite detectar código malicioso no sistema. Implica na constante atualização da base de vírus conhecida.
  - ***Instalação de firewall pessoal***. Permite filtrar o tráfego que entra e sai do sistema. Alerta o usuário sobre qualquer aplicação que tente utilizar a rede como um cliente ou servidor em seu sistema.
  - ***Gerência de configuração***. Permite manter uma configuração padrão e segura em todas as estações, controlando a instalação de software não autorizado.
  - ***Auditoria***. Permite validar a implementação da política de segurança em todo sistema.

Técnica de Defesa de Redes

Fator Humano

- Fundamental para uma implementação de segurança de rede com sucesso.
- Implica na conscientização e no envolvimento de todos aqueles que possuem acesso a rede.
- Evita potenciais ataques de *engenharia social* com o objetivo de obter informações pessoais como contas e senhas.

Obrigado!

Prof. Anderson Oliveira da Silva
D. Sc. Ciências em Informática
Engenheiro de Computação
anderson@inf.puc-rio.br

Departamento de Informática
Coordenação Central de Cooperação Internacional
PUC-Rio

DEPARTAMENTO DE INFORMÁTICA PUC·RIO

Coordenação Central de Cooperação Internacional
International Cooperation Central Coordination Office

PUC RIO