Aspectos de Segurança da Informação - Ataques

OUTRAS AULAS EM:

www.projetoderedes.com.br

Prof. José Maurício S. Pinheiro – UBM 2016

“É fácil ter-se um sistema de computação seguro. Você meramente tem que desconectar o seu sistema de qualquer rede externa, e permitir somente terminais ligados diretamente a ele. Pôr a máquina e seus terminais em uma sala fechada e um guarda na porta.”

F.T. Grampp e R.H. Morris

Definindo Segurança da Informação

Área do conhecimento dedicada à proteção dos ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Informação

Conjunto de dados utilizados para a transferência de uma mensagem entre pessoas e / ou máquinas em processos de troca de mensagens (comunicativos) ou transacionais (transferência de arquivos).

Princípios Básicos

- Confidencialidade: proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação;
- Disponibilidade: garantir o funcionamento do serviço de informação e acesso aos usuários autorizados;
- Integridade: evitar que dados sejam apagados ou alterados sem a permissão do gestor da informação.

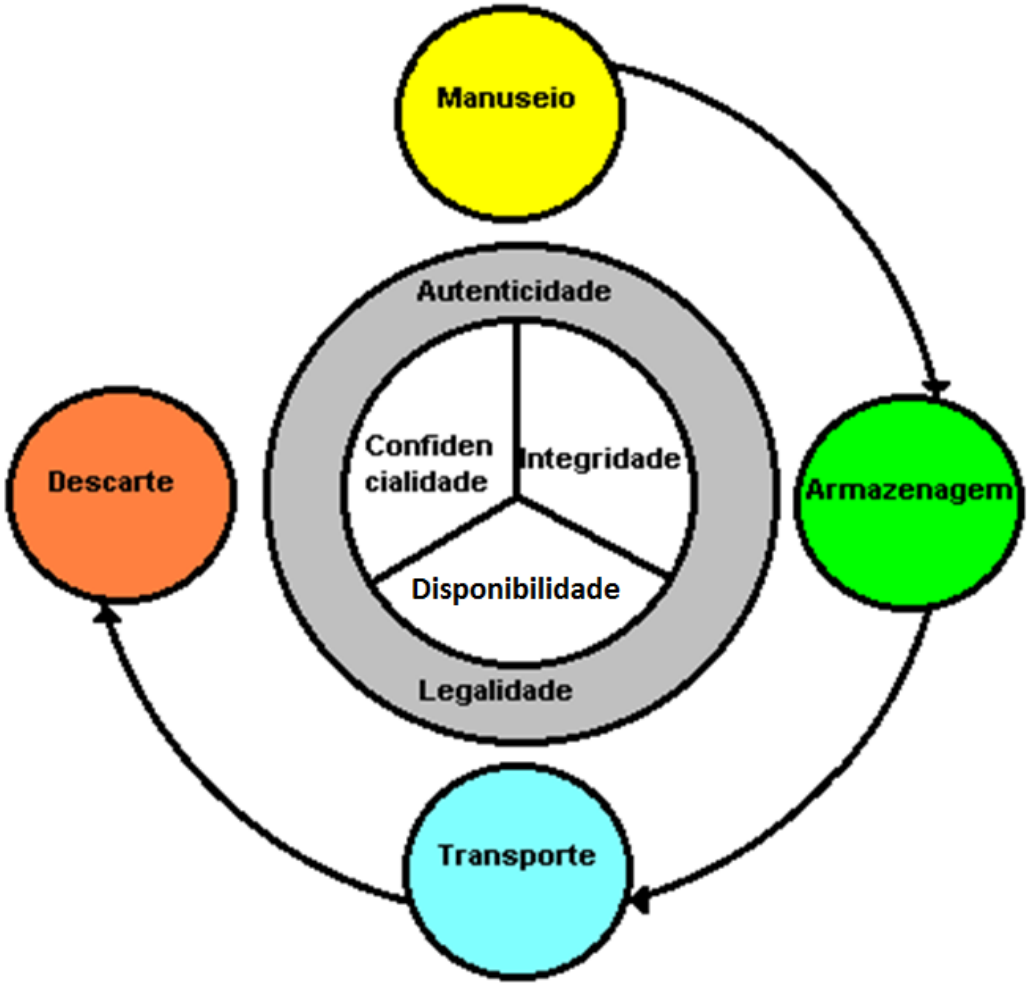
Aspectos Associados

- Autenticidade – garantia de que as entidades (máquinas, informação, usuários) identificadas no processo de comunicação sejam elas mesmas e a informação não foi alterada após o envio ou validação;

- Legalidade - a informação deve estar em conformidade com os preceitos da legislação em vigor.

Ciclo de Vida da Informação

- Manuseio – instante em que a informação é criada e manipulada;
- Armazenamento – instante em que a informação é armazenada de alguma forma (banco de dados, papel, etc);
- Transporte – instante em que a informação é transportada (e-mail, mídia, fax, telefone, etc);
- Descarte – instante em que a informação é descartada (lixo, eliminação e arquivo de computador, etc).


Manuseio
Autenticidade
Confiden
cialidade
Integridade
Disponibilidade
Legalidade
Descarte
Armazenagem
Transporte

Vulnerabilidade

Ponto pelo qual alguém pode ser atacado, molestado ou ter suas informações corrompidas.

Exemplos de Vulnerabilidades

- Físicas – Instalações prediais fora do padrão, salas de equipamentos mal planejadas; falta de sistemas de proteção ambiental;

- Naturais – Incêndios, enchentes, falta de energia, umidade excessiva;

Exemplos de Vulnerabilidades

- Hardware – Falha de recursos, danos em mídias, erros de instalação;
- Software – Erros na instalação e ou na configuração;

Exemplos de Vulnerabilidades

- Comunicação – Acessos não autorizados ou perda de comunicação;
- Humanos – Falta de treinamento, erros ou omissão, vandalismo.

Ameaça

Algo que possa provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade.

Ameaças quanto a sua Intencionalidade

- Naturais – fenômenos da natureza (incêndio, terremoto, tempestade, etc);
- Involuntárias – causadas quase sempre pelo desconhecimento (acidentes, erros, falta de energia, etc);
- Voluntárias – causadas propositalmente por agentes humanos (hackers, espiões, ladrões, invasores, etc)

Ameaças aos Sistemas Computacionais

- **Vazamento:** ocorre quando um usuário legítimo (autorizado) fornece informação para um ou mais receptores não autorizados. Isto pode ocorrer propositalmente, ou não.

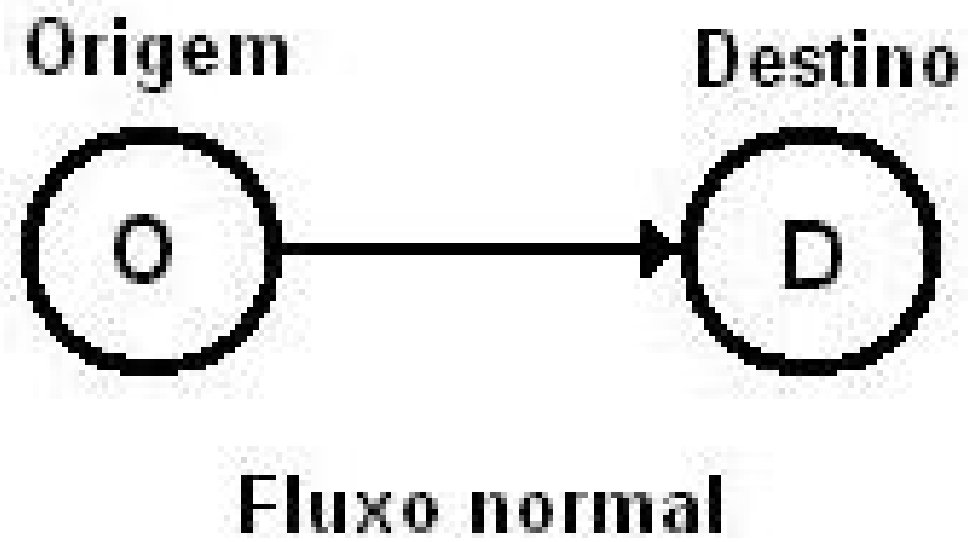
- **Violação** ocorre quando uma informação legítima sofre alteração não autorizada (incluindo programas).

Ameaças aos Sistemas Computacionais

- **Furto de recursos:** ocorre quando alguém não autorizado beneficia-se das facilidades dos sistemas computacionais.

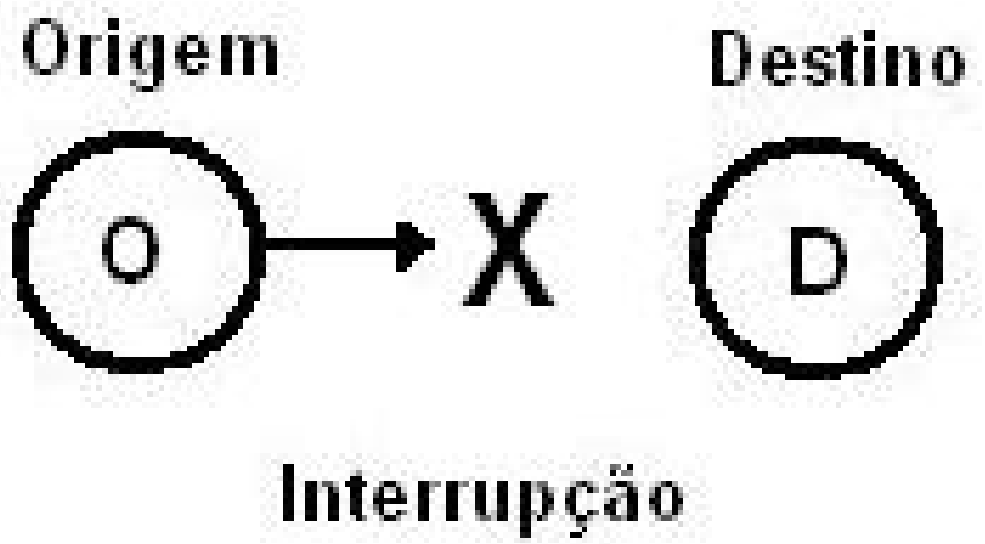
- **Vandalismo:** quando alguém não autorizado, interfere, causando prejuízo às operações dos sistemas, sem ganhos próprios.

Fluxo normal

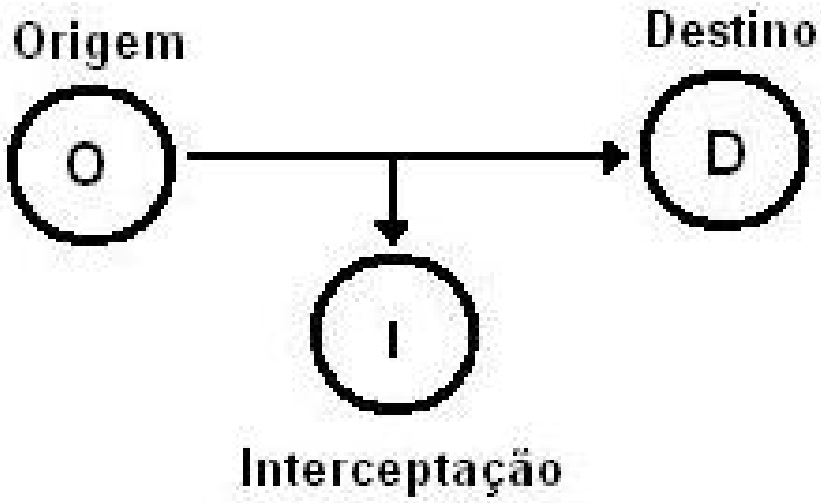


Fluxo normal

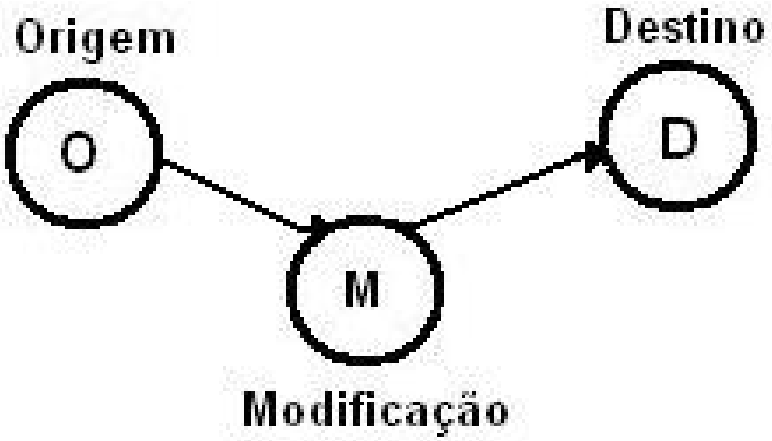
Ameaça de Interrupção



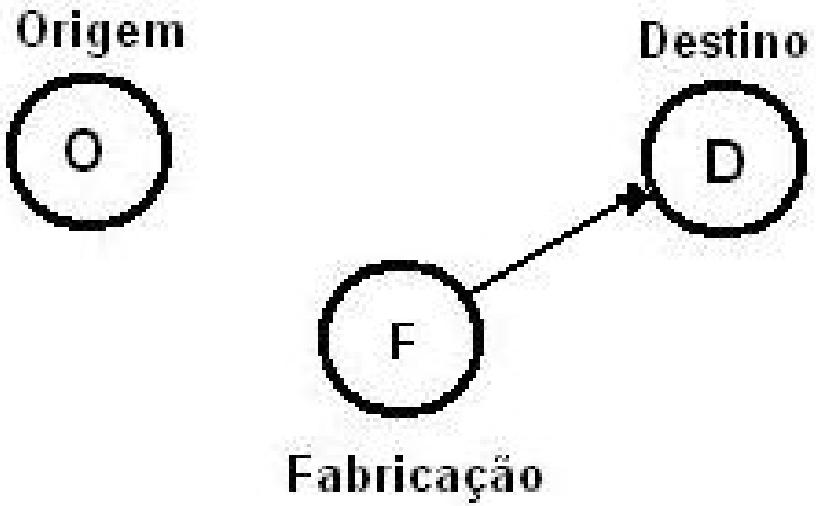
Ameaça de Interceptação



Ameaça de Modificação



Ameaça de Fabricação



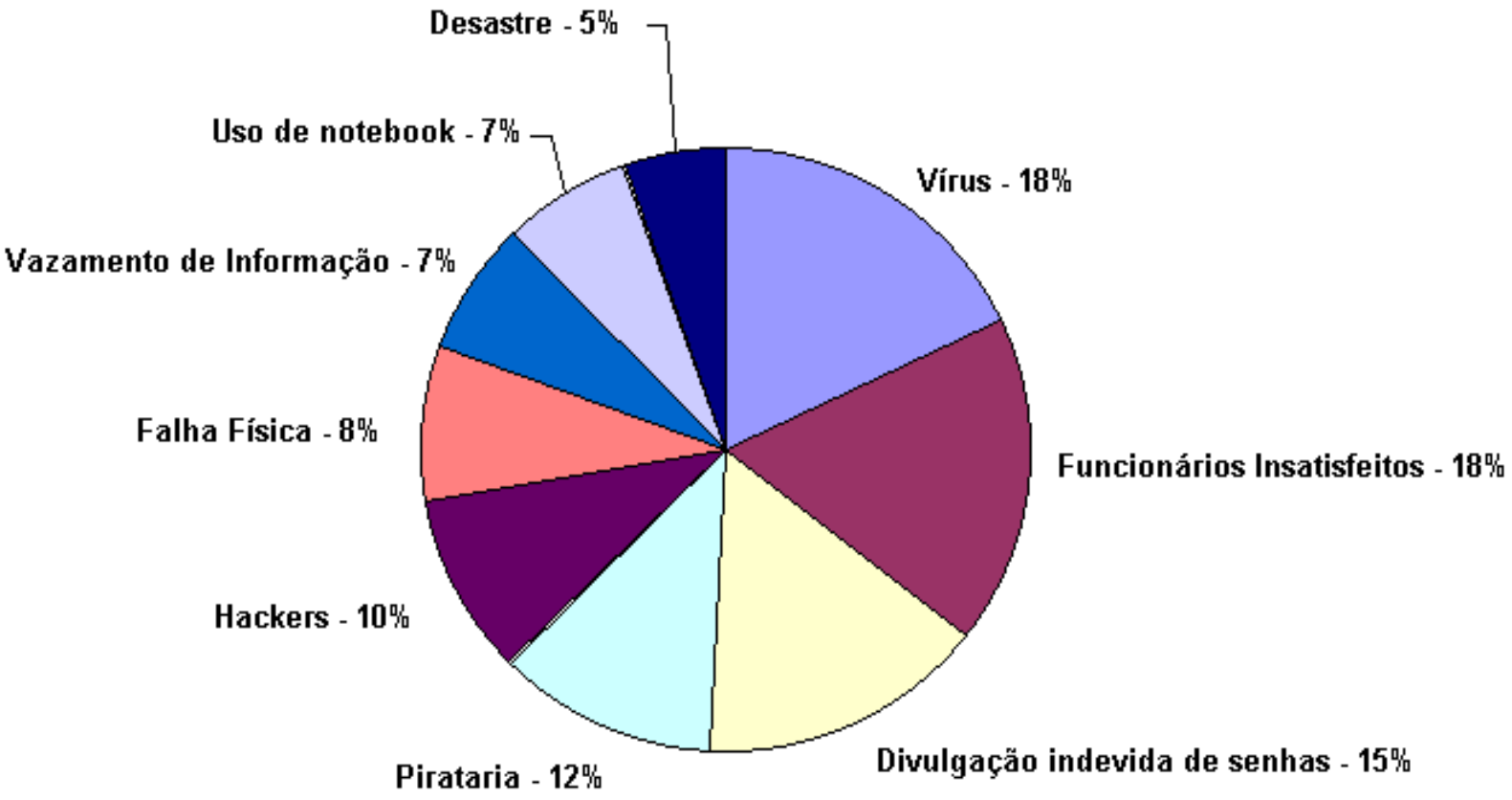
Ataques

- Um ataque ocorre quando uma ameaça intencional é realizada.
- Os ataques ocorrem por motivos diversos.

Risco

- É medido pela probabilidade de uma ameaça acontecer e o dano potencial à empresa.

- Existem algumas maneiras de se classificar o grau de risco no mercado de segurança, mas de uma forma simples, poderíamos tratar como alto, médio e baixo risco.


Desastre - 5%
Uso de notebook - 7%
Vírus - 18%
Vazamento de Informação - 7%
Falha Física - 8%
Funcionários Insatisfeitos - 18%
Hackers - 10%
Divulgação indevida de senhas - 15%
Pirataria - 12%

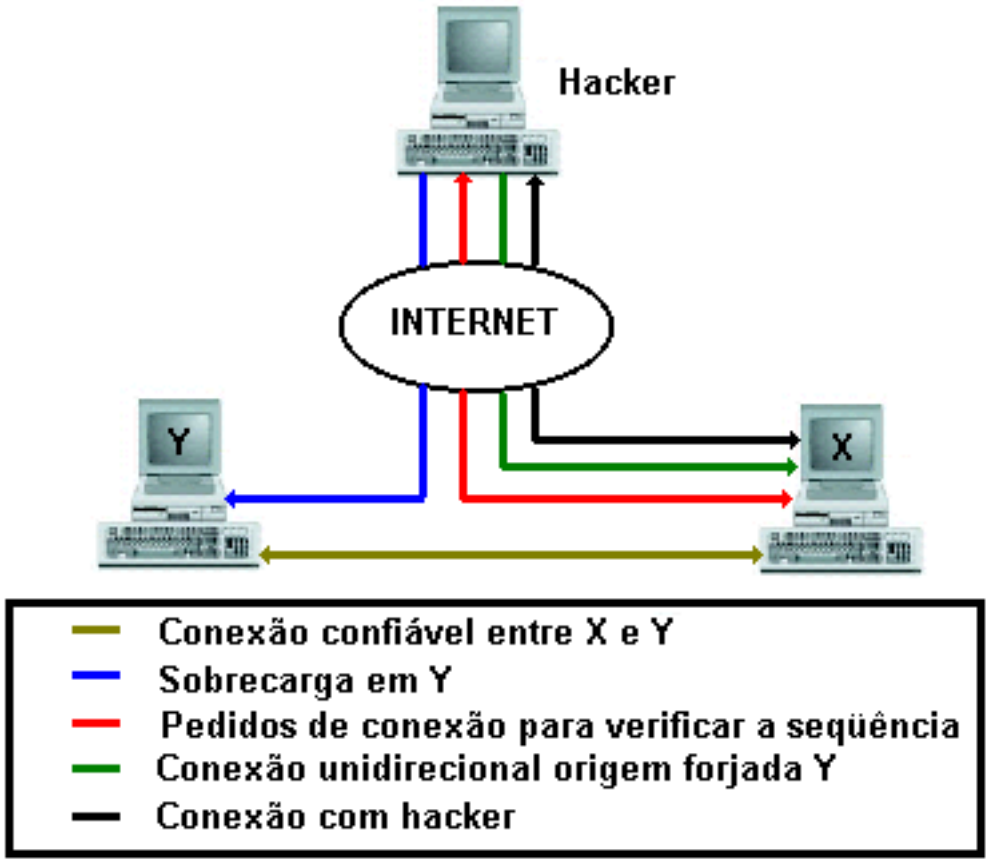
Ataque baseado em senhas

- Trata-se de um ataque que consiste na cifragem das palavras de um dicionário e posterior comparação com os arquivos de senhas de usuários.

IP Spoofing

- Falsificação de endereço IP
- Utilizada em conjunto com outros ataques para esconder a identidade do atacante.
- Consiste na manipulação direta dos campos do cabeçalho de um pacote para falsificar o número IP máquina que dispara a conexão.

- Quando um host X quer se conectar ao host Y, a identificação é feita através do número IP que vai no cabeçalho
- Se o IP do cabeçalho enviado pelo host X for falsificado (IP de um host hacker), o host Y acredita estar falando com o host X


Hacker
INTERNET
Y
X
Conexão confiável entre X e Y
Sobrecarga em Y
Pedidos de conexão para verificar a seqüência
Conexão unidirecional origem forjada Y
Conexão com hacker

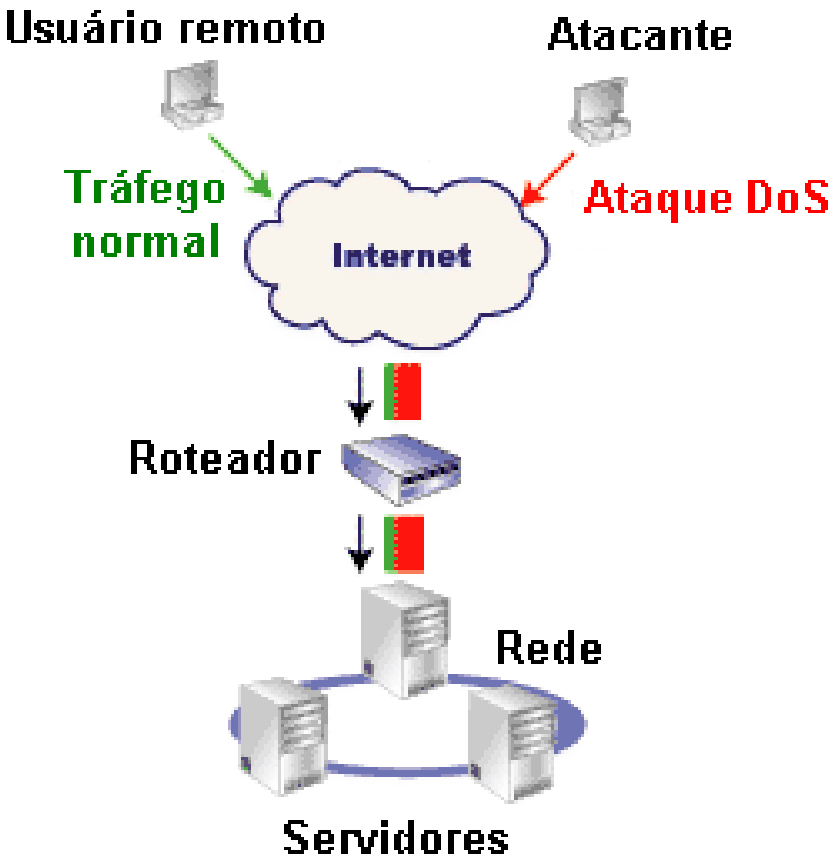
Ataque de Negação de Serviços

Os ataques de negação de serviço DoS (Denial of Service) têm como objetivos:

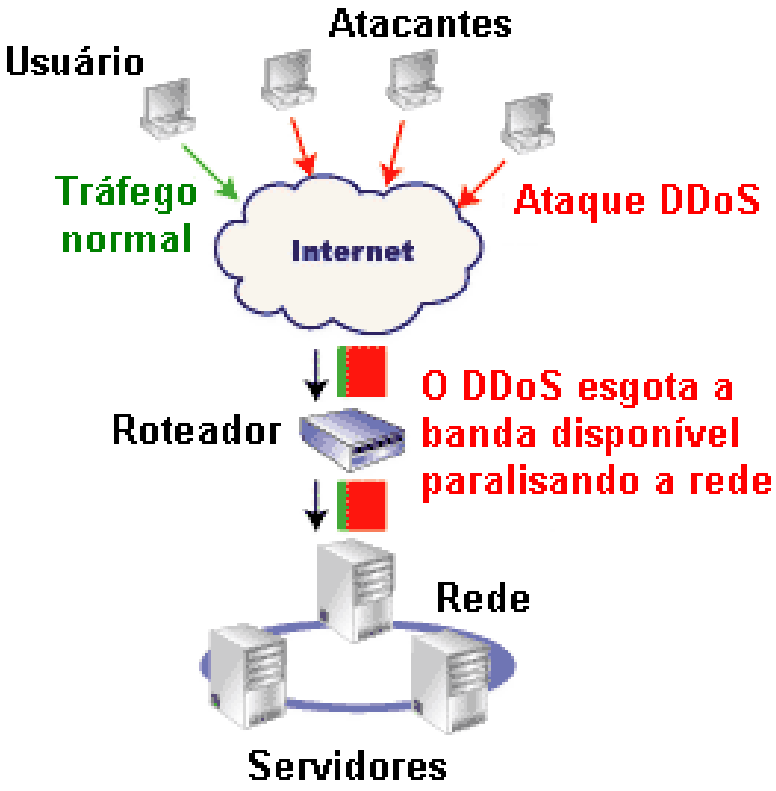
- Paralisar um serviço em um servidor;
- gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;
- Gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível.

Tipos de Ataques

- Denial of Service (Dos): Neste ataque, apenas uma máquina estranha a rede ataca a máquina alvo.


Usuário remoto
Atacante
Tráfego normal
Internet
Ataque DoS
Roteador
Rede
Servidores

- Distributed Denial of Service (DDos): Este ataque utiliza várias máquinas em conjunto para atacar uma máquina alvo. O objetivo do ataque é esgotar algum recurso da máquina alvo.


Atacantes
Usuário
Tráfego
normal
Internet
Ataque DDoS
O DDoS esgota a
banda disponível
paralisando a rede
Roteador
Rede
Servidores

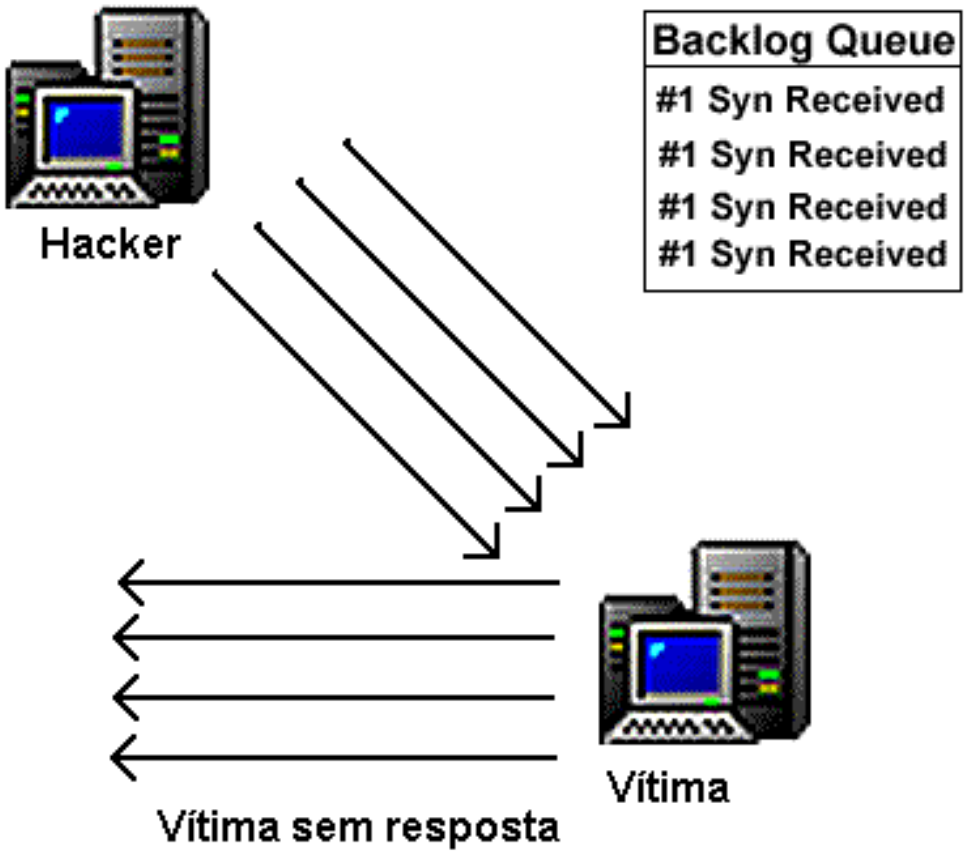
Vulnerabilidades Exploradas

- Falhas em softwares
- Falhas de Protocolo
- Esgotamento de recursos

SYN Flood

- Consiste no envio de um grande número de pacotes de abertura de conexão, com um endereço de origem forjado (IP Spoofing), para um determinado servidor.
- O servidor ao receber os pacotes, coloca uma entrada na fila de conexões em andamento, envia um pacote de resposta e fica aguardando uma confirmação da máquina cliente.

- Como o endereço de origem dos pacotes é falso, a confirmação nunca chega ao servidor.
- A fila de conexões no servidor fica lotada e, a partir daí, todos os pedidos de abertura de conexão são descartados e o serviço paralisado.
- A paralisação persiste até o tempo para o o servidor identificar a demora e remover a conexão em andamento da lista.


Backlog Queue
#1 Syn Received
#1 Syn Received
#1 Syn Received
#1 Syn Received
Hacker
Vítima
Vítima sem resposta

Ataque de LOOP

Consiste em mandar para um host um pacote IP com endereço de origem e destino iguais, ocasionando um loop na tabela de conexões de uma máquina atacada.

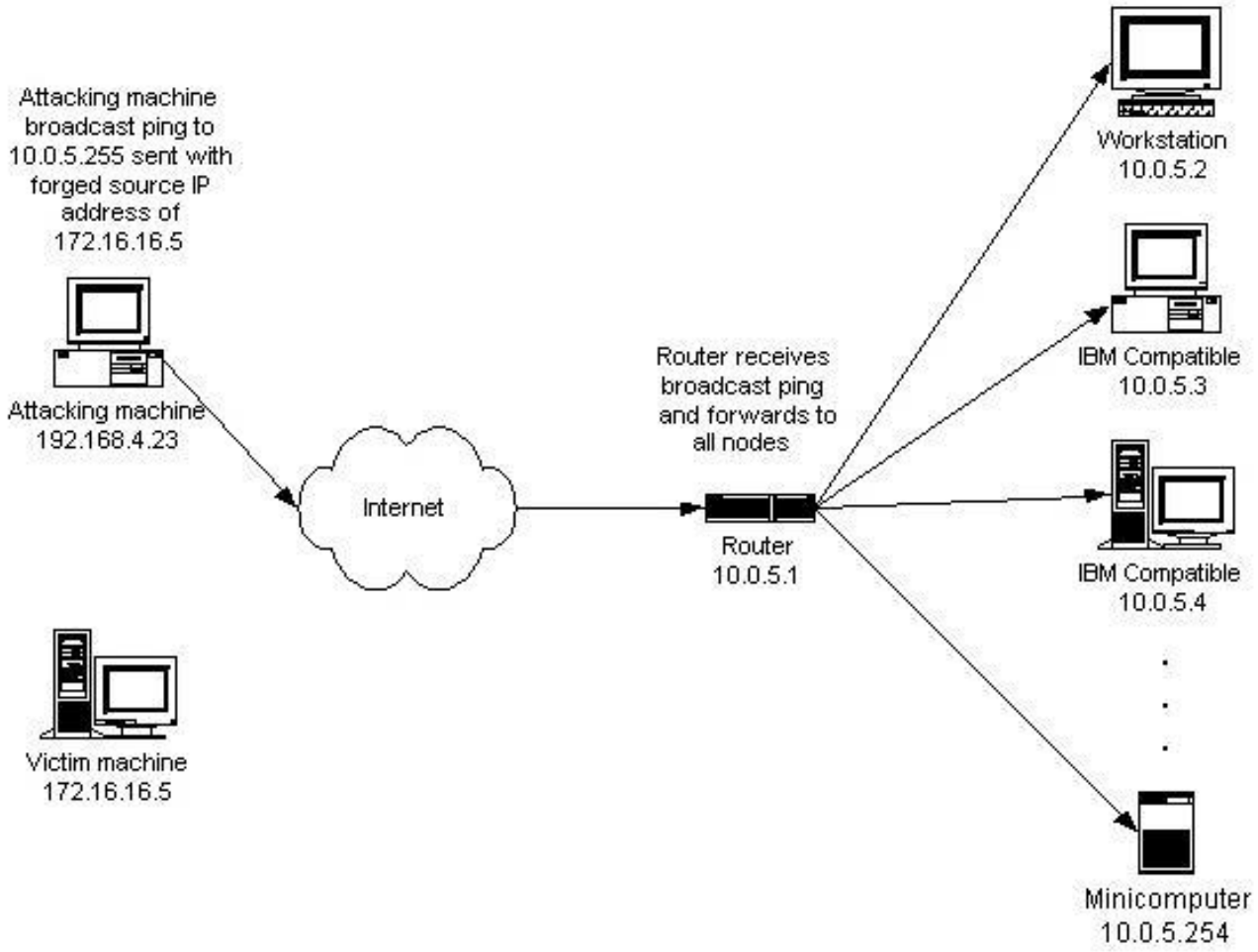
Ataques via ICMP

- O protocolo ICMP (Internet Control Message Protocol) é utilizado no transporte de mensagens de erro e de controle.

- O ICMP não tem garantias se a informação recebida é verdadeira, e por este motivo, um atacante pode utilizar as ICMP para interromper conexões já estabelecidas.

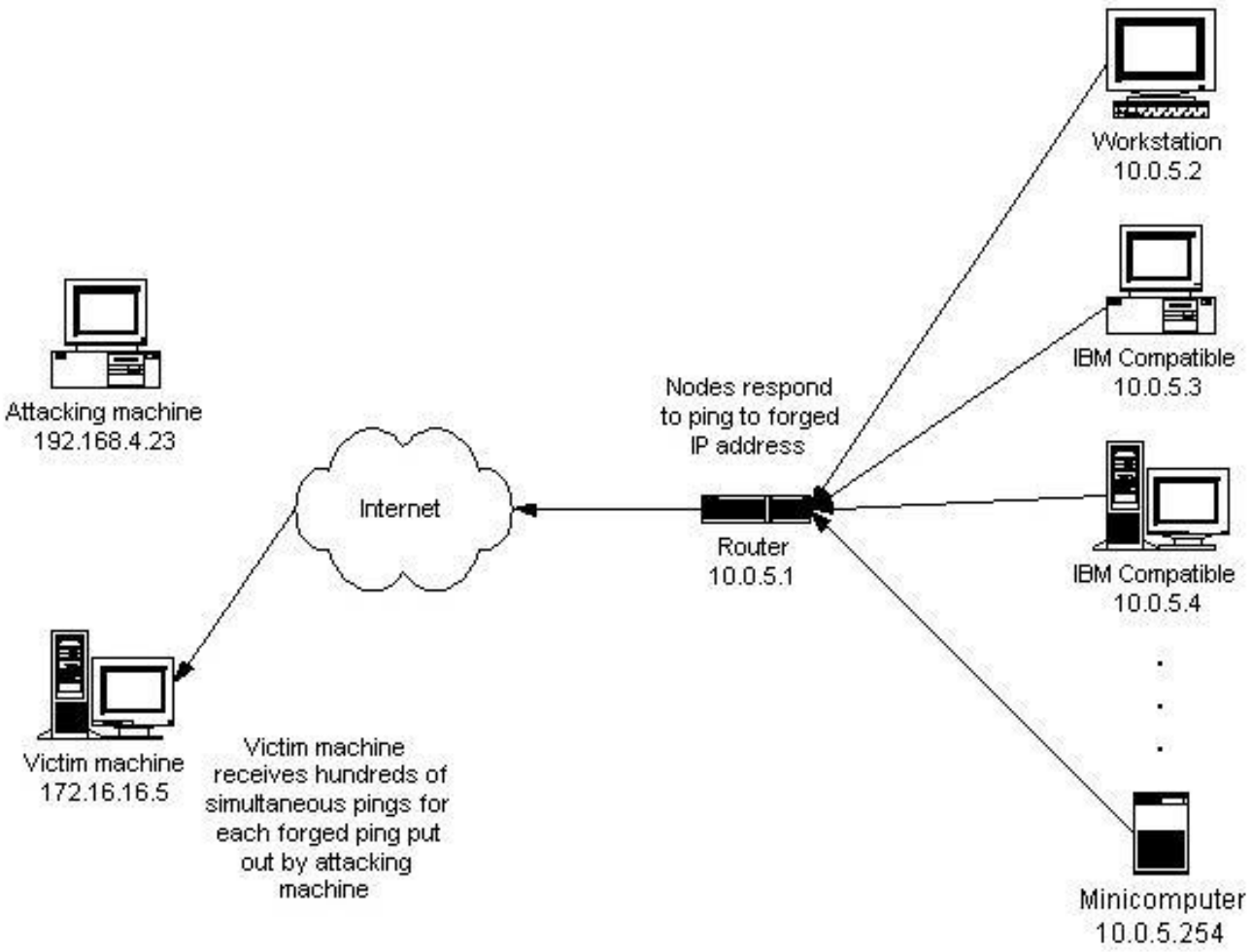
Ataque de Ping (Smurf Atack)

- Envia pacotes ICMP de echo request para um endereço de broadcast da rede


Attacking machine broadcast ping to 10.0.5.255 sent with forged source IP address of 172.16.16.5
Attacking machine
192.168.4.23
Internet
Router receives broadcast ping and forwards to all nodes
Router
10.0.5.1
Workstation
10.0.5.2
IBM Compatible
10.0.5.3
IBM Compatible
10.0.5.4
Minicomputer
10.0.5.254
Victim machine
172.16.16.5

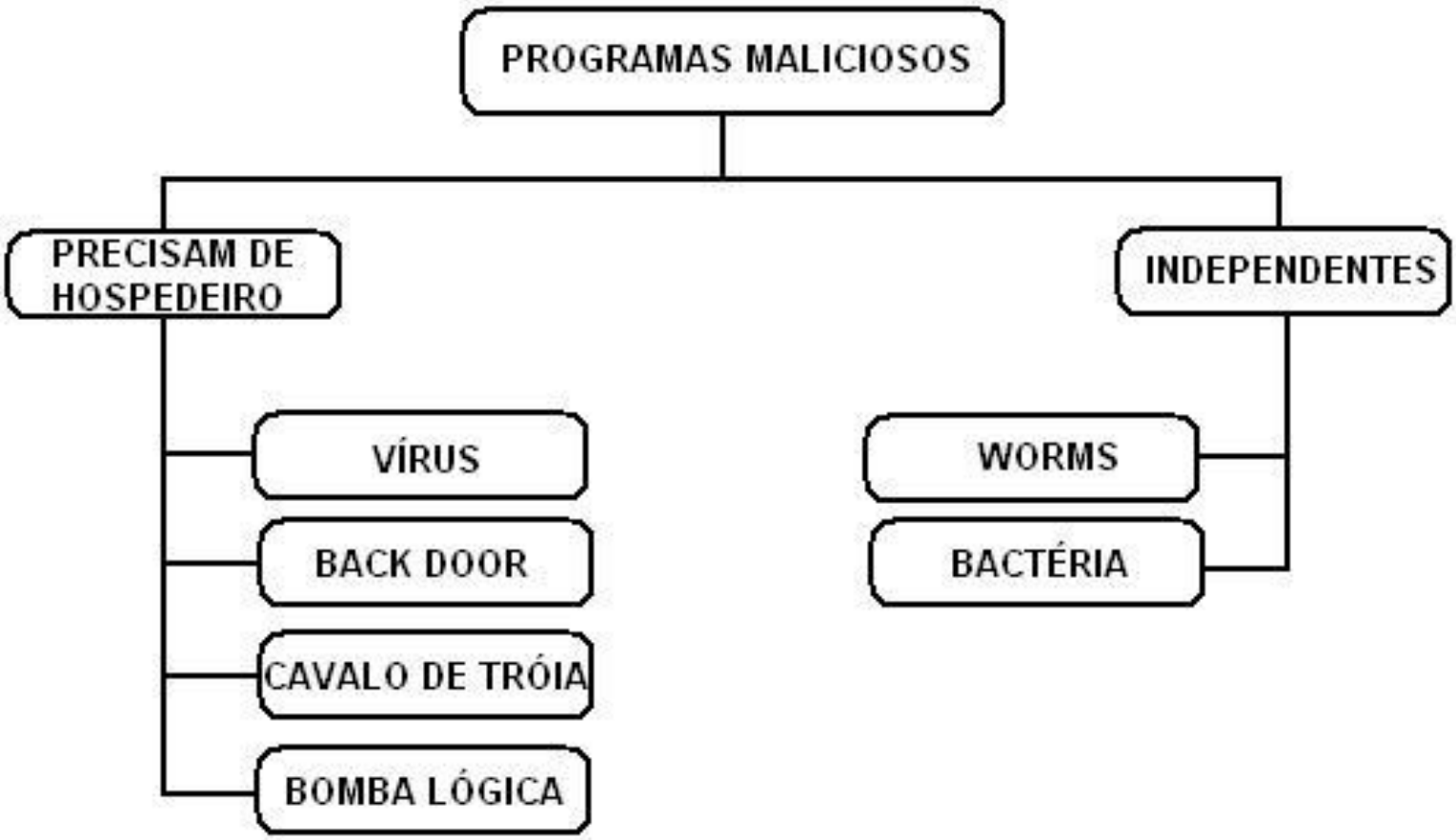
Ataque de Ping (Smurf Atack)

- Redireciona todas as respostas (através de IP Spoofing) para a máquina atacada, causando um volume grande de conexões de *echo reply* para a mesma.


Workstation
10.0.5.2
IBM Compatible
10.0.5.3
IBM Compatible
10.0.5.4
Minicomputer
10.0.5.254
Nodes respond
to ping to forged
IP address
Router
10.0.5.1
Internet
Attacking machine
192.168.4.23
Victim machine
172.16.16.5
Victim machine
receives hundreds of
simultaneous pings for
each forged ping put
out by attacking
machine

Ataque de Ping of Death

- Consiste em enviar um pacote IP com tamanho maior que o máximo permitido (65.535 bytes) para a máquina atacada. O pacote é enviado na forma de fragmentos (porque nenhuma rede permite o tráfego de pacotes deste tamanho).
- O dano é causado quando uma máquina destino tenta montar os fragmentos.


PROGRAMAS MALICIOSOS
PRECISAM DE HOSPEDEIRO
INDEPENDENTES
VÍRUS
BACK DOOR
CAVALO DE TRÓIA
BOMBA LÓGICA
WORMS
BACTÉRIA

Vírus

- A RFC 2828 define um vírus de computador como sendo um software com capacidade de se multiplicar, infectando outros programas, usualmente com alguma intenção maliciosa.
- Um vírus não pode executar-se sozinho, requerendo que o programa hospedeiro seja executado para ativar o vírus.

Backdoor

- Definido pela RFC 2828 como sendo um mecanismo que provê acesso a um sistema e seus recursos através de um procedimento diferente do usual.
- Normalmente é projetado pelos produtores de sistemas para ser utilizado na fase de testes do software ou hardware, normalmente não sendo de conhecimento público.

Cavalo de Tróia

- É definido pela RFC 2828 como sendo um programa que aparenta ter uma função útil, mas possui alguma função maliciosa que burla os mecanismos de segurança.

- Não possui a capacidade de se autorreplicar.

Bomba Lógica

- Ameaça programada, camuflada em programas, que é ativada quando certas condições são satisfeitas.
- As bombas lógicas permanecem inativas em softwares de uso comum por um longo período de tempo até que sejam ativadas.

Worm

- Definido pela RFC 2828 como sendo um programa de computador que pode se executar independentemente, propagar-se pelos computadores de uma rede sozinho, podendo consumir os recursos dos computadores destrutivamente

Bactéria

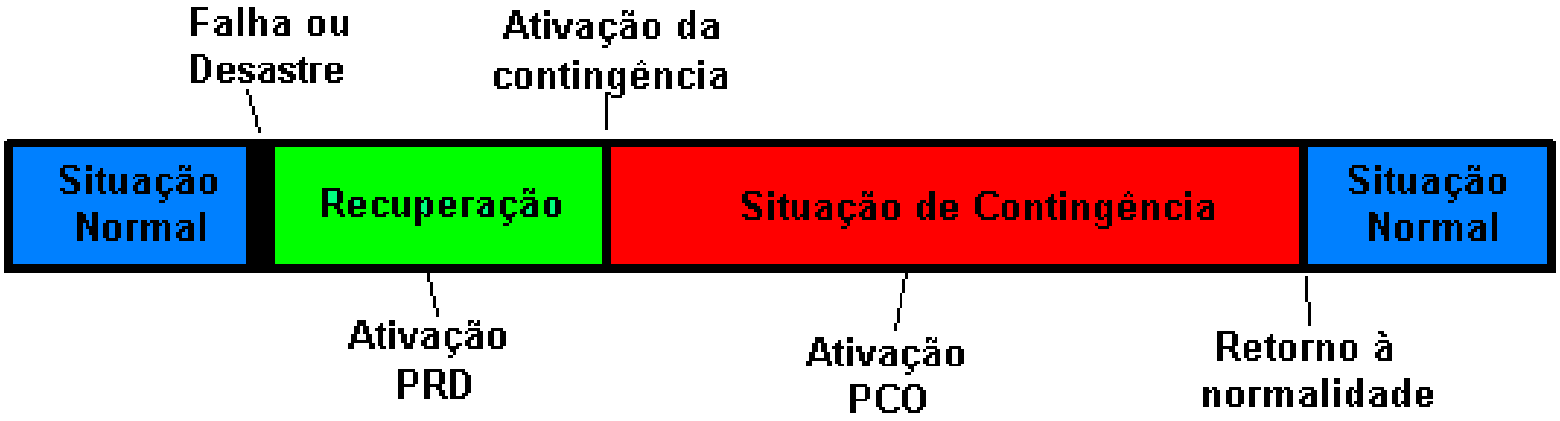
- Programa que gera cópias de si mesmo com intuito de sobrecarregar um sistema de computador.
- As bactérias são programas que não causam explicitamente danos aos arquivos.
- Seu único propósito é a sua replicação.

Plano de Recuperação de Desastres - PRD

- Objetiva definir quais recursos e ações serão tomadas em caso de desastre para que o negócio da empresa funcione, total ou parcialmente, até o retorno à situação normal.

Plano de Continuidade Operacional PCO

- Objetiva a manutenção dos processos de negócio na ocorrência de falhas nos sistemas de informação.


Falha ou
Desastre
Ativação da
contingência
Situação
Normal
Recuperação
Situação de Contingência
Situação
Normal
Ativação
PRD
Ativação
PCO
Retorno à
normalidade

Gerenciamento e Avaliação de Riscos

- **É o processo completo e contínuo de análise, avaliação, priorização e implementação das recomendações (meios de proteção) conforme o grau de criticidade do Risco.**

- **O que pode acontecer (evento de uma ameaça)?**
- **Se for acontecer, quão ruim poderia ser (impacto da ameaça)?**

- **Com que freqüência poderia acontecer (freqüência anual da ameaça)?**
- **Com que grau certeza estão as respostas das três primeiras perguntas (reconhecimento da incerteza)?**

Definições

Risco - Perigo ou possibilidade de perigo

É o potencial de que uma ameaça irá explorar as vulnerabilidades.

Definições

- **Severidade - é o grau do dano ao ativo.**
- **Ativo - é todo e qualquer recurso que manipule direta ou indiretamente informações.**
- **Impacto - é o impacto potencial para a organização.**

Analisar os Riscos

- É o processo de identificar os ativos e ameaças, priorizando as vulnerabilidades exploradas pelas ameaças e identificando as medidas de segurança apropriadas.

Avaliar os Riscos

- É o processo de conhecer os graus dos riscos aos ativos e decidir o que fazer sobre eles. Existem três formas de agir com os riscos

Aceitar os Riscos

- esta opção só deve ser utilizada, quando o custo para implementação de controles para proteção dos ativos for maior que o impacto causado pela ocorrência de um evento.

Reduzir o Risco

- tomar ações para reduzir os riscos para um nível aceitável.

Transferir o Risco

- Significa transferir a responsabilidade sobre o impacto causado ao ativo para as mãos de terceiros (colocar no seguro), isto só serve para criar compensação, pois não impede um acontecimento indesejado.

Valor do Ativo

- É o valor da importância do ativo para a organização.
- Devem ser levados em consideração:
  - valor da reposição da informação,
  - valor da reposição do equipamento,
  - valor da perda de credibilidade da empresa,
  - valor da perda de confiança do cliente.

Fator de Exposição (FE)

- É o fator que representa o quanto um ativo esta exposto à uma determinada ameaça.
- Expresso em percentagem (0% a 100%).

Expectativa de Perda Única(EPU)

- Fórmula que determina a perda (monetária ou não) do valor do ativo.
- A fórmula é representada pela seguinte expressão:

$$EPU = \text{Valor do ativo} * FE$$

Taxa de Ocorrência Anual(TOA)

- Fórmula que determina em base anual, a freqüência que uma ameaça pode ocorrer.
- Representada pela seguinte expressão:

TOA = nº de vezes que uma ameaça ocorre / quantidade de anos

Expectativa de Perda Anual(EPA)

- Fórmula que define o valor final do impacto aos ativos, representando a base para uma análise de custo/benefício de medidas de segurança.
- Representada pela seguinte expressão:

$$EPA = EPU * TOA$$

Fases do Gerenciamento

- Definir o escopo
- Identificar os ativos
- Mapeamentos de processo(com os ativos identificados, identificar os ativos críticos aos processos)
- Classificação dos ativos

Fases do Gerenciamento

- Identificação das ameaças e dos agentes causadores
- Identificação das vulnerabilidades
- Determinar a probabilidades
- Mensurar os impactos
- Seleção de controles e recomendações

Benefícios do Gerenciamento

- Justificar investimento
- Relacionar homem x hora
- Guia com planejamento anual de critérios para execução das atividades de segurança