Vulnerabilidade dos sistemas e uso indevido

- Um computador desprotegido conectado à Internet pode ser desativado em segundos
- **Segurança:**
    - Políticas, procedimentos e medidas técnicas usadas para prevenir acesso não autorizado, roubo ou danos físicos aos sistemas de informação.
- **Controles:**
    - Métodos, políticas e procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e a confiabilidade de seus registros contábeis e a adesão operacional aos padrões administrativos.

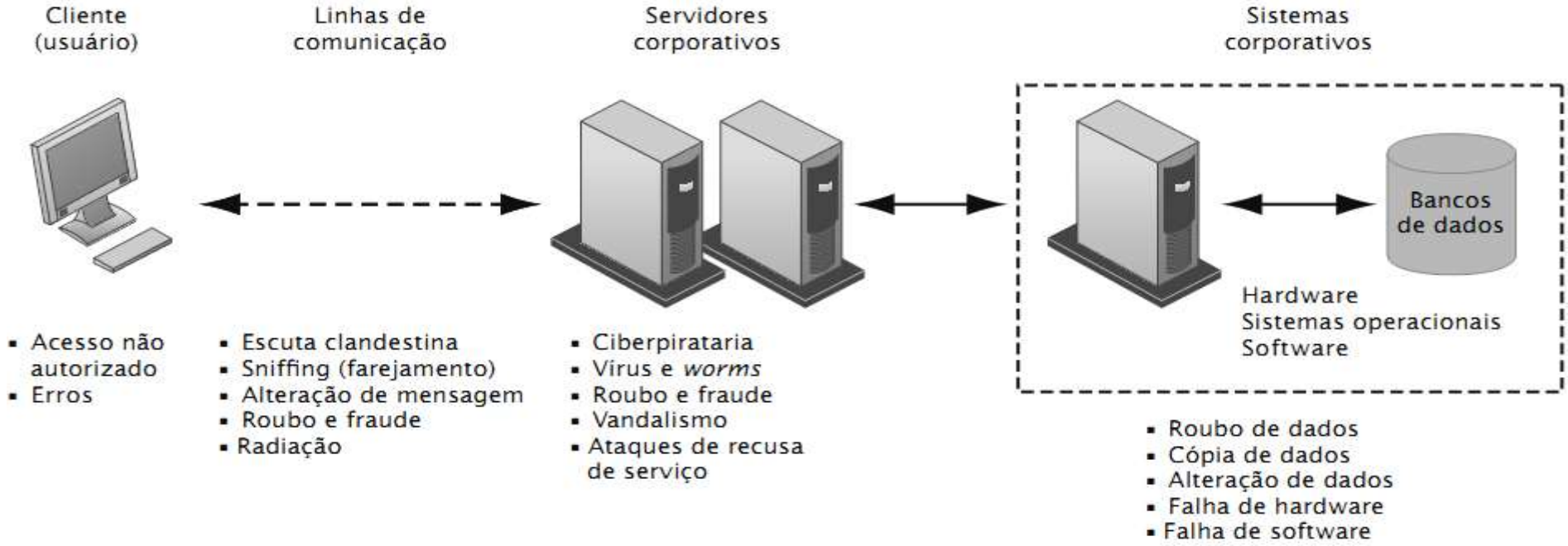
Vulnerabilidade dos sistemas e uso indevido

Por que os sistemas são vulneráveis

- **Problemas de hardware**
  - Avarias, erros de configuração, danos causados pelo uso impróprio ou por crimes.
- **Problemas de software**
  - Erros de programação, erros de instalação, mudanças não autorizadas.
- **Desastres**
  - Quedas de energia, enchentes, incêndios etc.
- **Uso de redes e computadores fora dos limites e do controle da empresa**
  - **Exemplo:** uso por fornecedores nacionais ou estrangeiros.

Vulnerabilidade dos sistemas e uso indevido

Vulnerabilidades e desafios de segurança contemporâneos



Normalmente, a arquitetura de uma aplicação baseada na Web inclui um cliente, um servidor e sistemas de informação corporativos conectados a bancos de dados. Cada um desses componentes apresenta vulnerabilidades e desafios de segurança. Enchentes, incêndios, quedas de energia e outros problemas técnicos podem causar interrupções em qualquer ponto da rede.

Vulnerabilidade dos sistemas e uso indevido

- Vulnerabilidades da Internet
  - Rede aberta a qualquer usuário
  - O tamanho da Internet propicia que os abusos tenham um alto impacto
  - Uso de endereços de Internet fixos com conexões permanentes à rede mundial facilita a identificação por *hackers*
  - Anexos de e-mail
  - E-mails usados para transmissão de segredos de negócios
  - Mensagens instantâneas não são seguras e podem ser facilmente interceptadas

Vulnerabilidade dos sistemas e uso indevido

- Desafios da segurança sem fio
  - Bandas de rádiofrequência são fáceis de serem escaneadas
  - Identificadores de conjunto de serviços (SSIDs)
    - Identificar pontos de acesso
    - Transmitidos várias vezes
  - *War driving*
    - Espião dirige um carro entre edifícios ou estaciona do lado de fora e tenta interceptar o tráfego por redes sem fio
    - Quando os *hackers* obtêm acesso ao SSID, conseguem acessar os recursos da rede
  - WEP (Wired Equivalent Privacy)
    - Padrão de segurança para 802.11
    - Especificações básicas compartilham a mesma senha tanto para usuários quanto para os pontos de acesso
    - Usuários não fazem uso de recursos de segurança

Vulnerabilidade dos sistemas e uso indevido

Desafios de segurança em ambientes Wi-Fi

Muitas redes Wi-Fi podem ser facilmente invadidas por intrusos. Eles usam programas *sniffers* para obter um endereço e, assim, acessar sem autorização os recursos da rede.

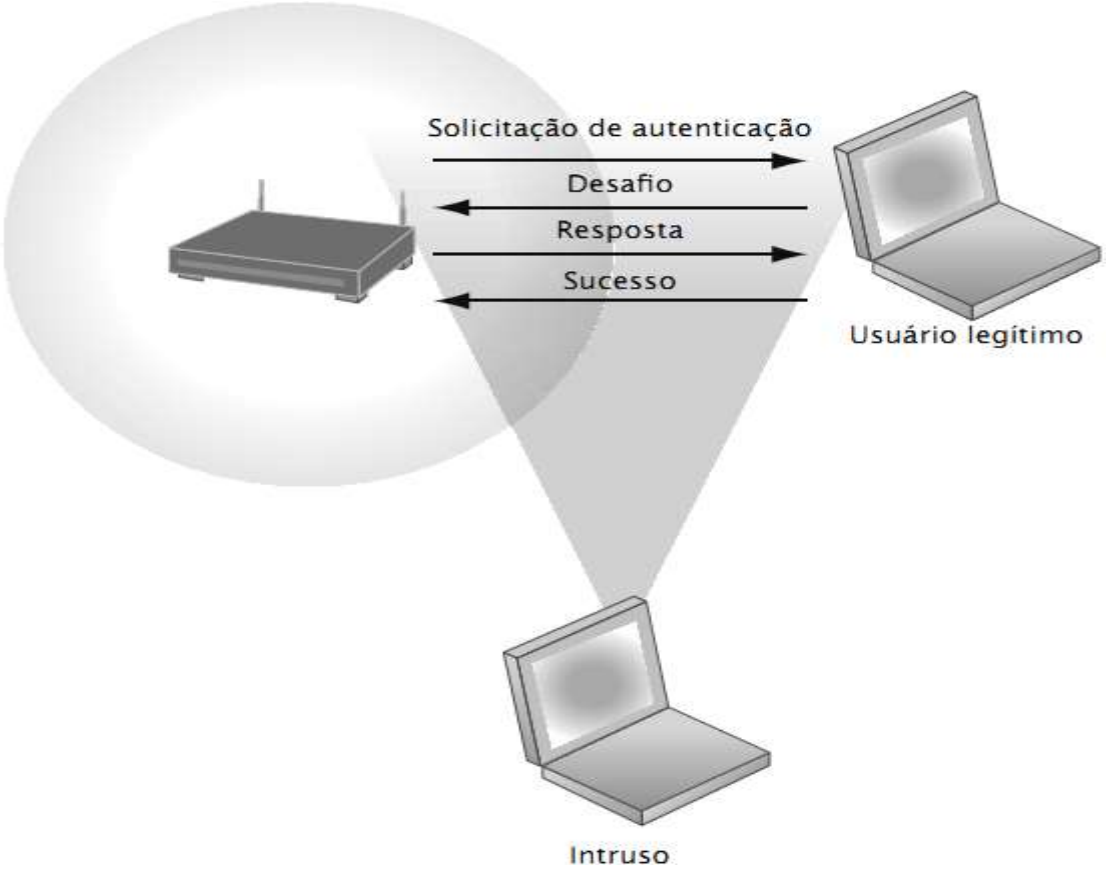


Figura 7.2

Vulnerabilidade dos sistemas e uso indevido

Software mal-intencionado: vírus, *worms*, cavalos de Troia e *spywares*

- *Malware*
  - Vírus
    - Programa de software espúrio que se anexa a outros programas de software ou arquivos de dados a fim de ser executado
  - *Worms*
    - Programas de computador independentes que copiam a si mesmos de um computador para outro por meio de uma rede
  - Cavalos de Troia
    - Software que parece benigno, mas depois faz algo diferente do esperado

Vulnerabilidade dos sistemas e uso indevido

Software mal-intencionado: vírus, *worms*, cavalos de Troia e *spywares*

- *Malware* (continuação)
  - *Spyware*
    - Pequenos programas que se instalam sorrateiramente nos computadores para monitorar a atividade do internauta e usar as informações para fins de marketing.
  - *Key loggers*
    - Registram cada tecla pressionada em um computador para roubar números seriais de softwares, senhas, deflagrar ataques na Internet.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- *Hackers versus crackers*
- Atividades incluídas:
  - invasão de sistemas;
  - danos a sistemas; e
  - cibervandalismo.
    - Interrupção, a alteração da aparência ou até mesmo a destruição intencional de um site ou sistema de informação corporativo.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- ***Spoofing***
  - Apresentar-se de maneira disfarçada, usando endereços de e-mail falsos ou fingindo ser outra pessoa.
  - Redirecionamento de um link para um endereço diferente do desejado, estando o site espúrio “disfarçado” como o destino pretendido.
- ***Sniffer***
  - Programa espião que monitora as informações transmitidas por uma rede.
  - Permitem que os *hackers* roubem informações de qualquer parte da rede, inclusive mensagens de e-mail, arquivos da empresa e relatórios confidenciais.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- **Ataque de recusa de serviço (DoS)**
  - Sobrecarregar o servidor com centenas de requisições falsas, a fim de inutilizar a rede
- **Ataque distribuído de recusa de serviço (DDoS)**
  - Uso de inúmeros computadores para iniciar um DoS
  - *Botnets*
    - Redes de PCs “zumbis” infiltradas por um *malware* robô

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- **Crimes de informática**
  - Definidos como “quaisquer violações da legislação criminal que envolvam conhecimento de tecnologia da informática em sua perpetração, investigação ou instauração de processo”
  - **Computadores podem ser alvo de crimes:**
    - Violar a confidencialidade de dados computadorizados protegidos
    - Acessar um sistema de computador sem autorização
  - **Computadores podem ser instrumentos de crimes:**
    - Roubo de segredos comerciais
    - Usar e-mail para ameaças ou assédio

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- **Roubo de identidade**
  - Roubo de informações pessoais (número de identificação da Previdência Social, número da carteira de motorista ou número do cartão de crédito) para se fazer passar por outra pessoa.
- ***Phishing***
  - Montar sites falsos ou enviar mensagens de e-mail parecidas com as enviadas por empresas legítimas, a fim de pedir aos usuários dados pessoais confidenciais.
- ***Evil twins***
  - Redes sem fio que fingem oferecer conexões Wi-Fi confiáveis à Internet.

Vulnerabilidade dos sistemas e uso indevido

Hackers e cibervandalismo

- ***Pharming***
  - Redireciona os usuários a uma página da Web falsa, mesmo quando a pessoa digita o endereço correto da página da Web no seu navegador.
- **Fraude do clique**
  - Ocorre quando um indivíduo ou programa de computador clica fraudulentamente em um anúncio on-line sem qualquer intenção de descobrir mais sobre o anunciante ou realizar uma compra.

Vulnerabilidade dos sistemas e uso indevido

Ameaças internas: funcionários

- Ameaças à segurança costumam ter origem na empresa
  - Conhecimento interno
  - Procedimentos de segurança frouxos
    - Falta de conhecimento do usuário
  - Engenharia social:
    - Intrusos mal-intencionados em busca de acesso ao sistema podem enganar os funcionários fingindo ser membros legítimos da empresa; assim, conseguem fazer com que revelem sua senha

Vulnerabilidade dos sistemas e uso indevido

Vulnerabilidade do software

- **Softwares comerciais contém falhas que criam vulnerabilidades na segurança**
  - *Bugs* escondidos (defeitos no código do programa).
    - A taxa zero de defeitos não pode ser alcançada porque teste completo simplesmente não é possível nos grandes programas.
  - As falhas podem tornar a rede vulnerável aos invasores.
- ***Patches***
  - Os fornecedores distribuem pequenos programas que corrigem as falhas.
  - Entretanto, a infinidade de softwares em uso pode fazer com que os *malwares* sejam criados mais rapidamente do que os *patches.*

Valor empresarial da segurança e do controle

- Sistemas computacionais com problemas podem levar a uma perda substancial, senão total, das funções empresariais.
- Atualmente, as empresas estão mais vulneráveis do que nunca.
- Uma falha de segurança pode diminuir o valor de mercado da empresa quase que imediatamente.
- Controle e segurança inadequados também podem criar sérios riscos legais.

Valor empresarial da segurança e do controle

Requisitos legais e regulatórios para a gestão de registros eletrônicos

- **As empresas enfrentam novas obrigações legais no que diz respeito à retenção de documentos e à gestão de registros eletrônicos, bem como à proteção da privacidade**
  - **HIPAA:** regras e procedimentos quanto à privacidade e à segurança médicas
  - **Lei Gramm-Leach-Bliley:** exige que as instituições financeiras assegurem a segurança e a confidencialidade dos dados do cliente
  - **Lei Sarbanes-Oxley:** cabe às empresas e a seus administradores salvaguardar a precisão e a integridade das informações financeiras utilizadas internamente e publicadas externamente

Valor empresarial da segurança e do controle

Prova eletrônica e perícia forense computacional

- As evidências para os crimes de colarinho branco costumam ser encontradas em formato digital.
  - Dados armazenados em dispositivos computacionais, e-mails, mensagens instantâneas, transações de *e-commerce .*
- O controle apropriado dos dados pode economizar tempo e dinheiro no atendimento às solicitações de produção de provas.
- Perícia forense computacional:
  - Procedimento científico de coleta, exame, autenticação, preservação e análise de dados mantidos em meios de armazenamento digital, de tal maneira que as informações possam ser usadas como prova em juízo.
  - Inclui a recuperação de dados ambientes ou ocultos.

Como estabelecer uma estrutura para segurança e controle

- **Controles de sistemas de informação**
  - **Controles gerais**
    - Controlam projeto, segurança e uso de programas de computadores e a segurança de arquivos de dados em geral em toda a infraestrutura de TI da empresa.
    - Aplicam-se a todas as aplicações computadorizadas.
    - Combinação de hardware, software e procedimentos manuais que criam um ambiente global de controle.

Como estabelecer uma estrutura para segurança e controle

- **Tipos de controles gerais**
  - Controles de software
  - Controles de hardware
  - Controles de operações de computador
  - Controles de segurança de dados
  - Controles de implementação
  - Controles administrativos

Como estabelecer uma estrutura para segurança e controle

- **Controles de aplicação**
  - Controles específicos exclusivos a cada aplicação computadorizada, como processamento de folha de pagamento ou pedidos.
  - Incluem tanto procedimentos manuais quanto automatizados.
  - Garantem que somente dados autorizados sejam completa e precisamente processados pelas aplicações.
  - Incluem **controles de entrada**, **controles de processamento** e **controles de saída**.

Como estabelecer uma estrutura para segurança e controle

- **Avaliação de risco**
  - Determina o nível de risco para a empresa caso uma atividade ou um processo específico não sejam controlados adequadamente
    - Tipos de ameaças
    - Probabilidade de sua ocorrência ao longo do ano
    - Perdas potenciais, valor da ameaça
    - Prejuízo anual esperado

Exposição	Probabilidade de ocorrência (%)	Faixa de prejuízo/média ($)	Prejuízo anual esperado ($)
Falta de energia elétrica	30	5.000-200.000 (102.500)	30.750
Apropriação indébita	5	1.000-50.000 (25.500)	1.275
Erro de usuário	98	200-40.000 (20.100)	19.698

Como estabelecer uma estrutura para segurança e controle

- **Política de segurança**
  - Estabelece hierarquia aos riscos de informação e identifica metas de segurança aceitáveis, assim como os mecanismos para atingi-las.
  - Dá origem a outras políticas:
    - **Política de uso aceitável (*acceptable use policy* — AUP)**
      - Define os usos aceitáveis dos recursos de informação e do equipamento de informática da empresa.
    - **Políticas de autorização**
      - Determinam diferentes níveis de acesso aos ativos de informação para diferentes níveis de usuários.

Como estabelecer uma estrutura para segurança e controle

- **Sistemas de gestão de autorização**
  - Estabelecem onde e quando um usuário terá permissão para acessar determinadas partes de um site ou de um banco de dados corporativo.
  - Permitem que cada usuário acesse somente as partes do sistema nas quais tem permissão de entrar, com base nas informações estabelecidas por um conjunto de regras de acesso.

Vulnerabilidade dos sistemas e uso indevido

Perfis de segurança para um sistema de pessoal

Estes dois exemplos representam dois perfis de segurança ou modelos de segurança de dados que podem ser encontrados em um sistema de pessoal. Dependendo do perfil de segurança, um usuário teria certas restrições de acesso a vários sistemas, localizações ou dados da organização.

PERFIL DE SEGURANÇA 1

Usuário: funcionário do departamento pessoal
Localização: Divisão 1
Códigos de identificação de funcionários com esse perfil: 00753, 27834, 37665, 44116

Restrições ao campo de dados	Tipo de acesso
Todos os dados de funcionários para a Divisão 1 somente	Leitura e atualização
▪ Dados de histórico médico	Nenhum
▪ Salário	Nenhum
▪ Proventos (para cálculo de aposentadoria)	Nenhum

PERFIL DE SEGURANÇA 2

Usuário: gerente da divisão de pessoal
Localização: Divisão 1
Códigos de identificação de funcionários com esse perfil: 27321

Restrições ao campo de dados	Tipo de acesso
Todos os dados de funcionários para a Divisão 1 somente	Somente leitura

Como estabelecer uma estrutura para segurança e controle

Plano de recuperação de desastres e plano de continuidade dos negócios

- **Plano de recuperação de desastres:** organiza planos para restauração de serviços que tenham sofrido interrupção
- **Plano de continuidade dos negócios:** concentra-se na restauração das operações de negócios após um desastre
  - Ambos os planos devem:
    - Identificar os sistemas mais importantes da empresa.
    - Realizar uma análise de impacto nos negócios, a fim de identificar o impacto de uma suspensão em seu funcionamento.
  - A administração precisa determinar quais sistemas serão restaurados primeiro.

Como estabelecer uma estrutura para segurança e controle

O papel da auditoria

- **Auditoria de sistemas**
  - Avalia o sistema geral de segurança da empresa e identifica todos os controles que governam sistemas individuais de informação.
  - Revê tecnologias, procedimentos, documentação, treinamento e recursos humanos .
  - Pode até mesmo simular um ataque ou desastre para verificar como os recursos tecnológicos, a equipe de sistemas de informação e os funcionários da empresa reagem.
  - Lista e classifica todos os pontos fracos do controle e estima a probabilidade de ocorrerem erros nesses pontos.
  - Avalia o impacto financeiro e organizacional de cada ameaça.

Vulnerabilidade dos sistemas e uso indevido

Exemplo de listagem feita por um auditor para deficiências de controle

Este diagrama representa uma página da lista de deficiências de controle que um auditor poderia encontrar em um sistema de empréstimos de um banco comercial. Além de ajudar o auditor a registrar e avaliar as deficiências de controle, o formulário mostra os resultados das discussões dessas deficiências com a administração, bem como quaisquer medidas corretivas tomadas por ela.

Função: Empréstimos pessoais Localização: Peoria, Il.	Preparado por: J. Ericson Data de preparação: 16 de junho de 2006		Recebido por: T. Barrow Data da revisão: 28 de junho de 2006	
	Chance de erro substancial		Notificação à administração	
Natureza e impacto das deficiências	Sim/ Não	Justificativa	Data do relatório	Resposta da administração
Os registros do pagamento das prestações de empréstimos não são conciliados com os registros do tomador do empréstimo durante o processamento.	Sim	Sem um controle de detecção, os erros nos balanços de um cliente individual podem continuar passando despercebidos.	10/5/06	O relatório de comparação de taxas de juros provê esse controle.
Não são feitas auditorias periódicas nos dados gerados por computador (débitos de juros).	Sim	A falta de uma auditoria periódica ou verificação de racionalidade pode resultar na ampla propagação de cálculos errados antes de os erros serem detectados.	10/5/06	Serão instituídas auditorias periódicas sobre os empréstimos.
Programas podem ser incluídos nas bibliotecas de produção para cumprir metas de prazo, sem aprovação final pelo grupo de Padrões e Controles.	Não	Todos os programas exigem autorização da administração. O grupo de Padrões e Controles controla o acesso a todos os sistemas de produção e determina, para tais casos, um *status* de produção temporária.		

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Controle de acesso

- Políticas e procedimentos que uma empresa usa para evitar acesso indevido a seus sistemas por pessoas não autorizadas dentro e fora da organização
    - Autorização
    - Autenticação
        - Senhas de sistemas
        - *Tokens*
        - *Smart cards*
        - Autenticação biométrica

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

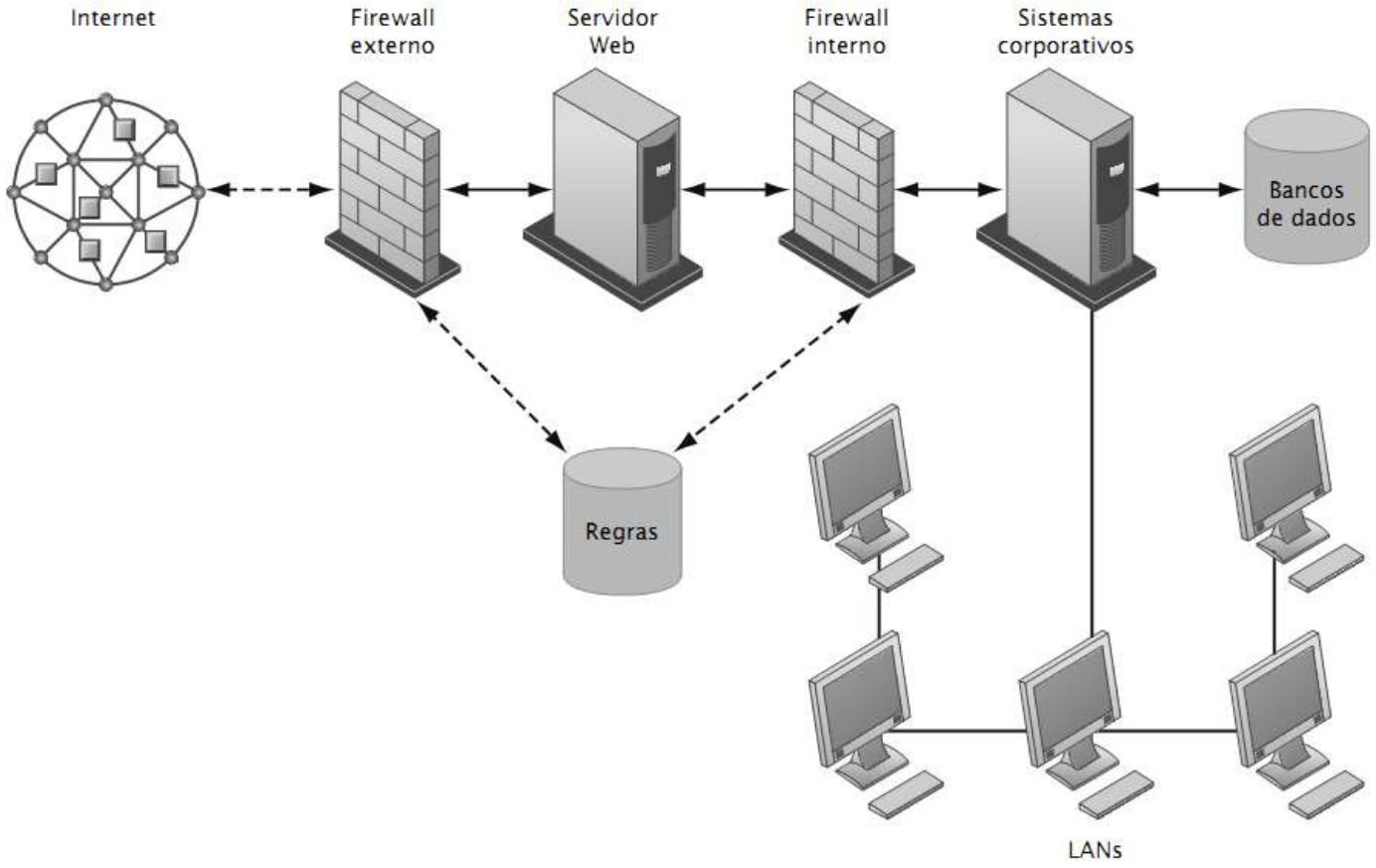
Firewalls, sistemas de detecção de invasão e softwares antivírus

- ***Firewall***:
  - Combinação de hardware e software que impede que usuários não autorizados acessem redes privadas
  - As tecnologias incluem:
    - Filtragem de pacotes estáticos
    - *Network address translation* (Tradução de Endereços IP)
    - Filtragem de aplicação *proxy*

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Um *firewall* corporativo

O *firewall* é colocado entre a Internet pública ou outra rede pouco confiável e a rede privada da empresa, com a intenção de proteger esta contra tráfego não autorizado.



Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Firewalls, sistemas de detecção de invasão e softwares antivírus

- **Sistemas de detecção de invasão:**
  - Monitoram os pontos mais vulneráveis de redes corporativas, a fim de detectar e inibir invasores.
  - Examinam os eventos em tempo real, em busca de ataques à segurança em curso.
- **Softwares antivírus e *anti-spyware*:**
  - Verificam os computadores a fim de detectar a presença de vírus e, muitas vezes, eliminá-los da área infectada.
  - Requerem atualização contínua.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Segurança em redes sem fio

- **O protocolo WEP oferece alguma margem de segurança se os usuários:**
  - Lembrarem-se de ativá-lo.
  - Atribuírem um nome único ao SSID de sua rede.
  - Utilizarem a tecnologia de rede privada virtual (VPN).
- **A Wi-Fi Alliance finalizou a especificação 802.11i, que substitui o WEP por padrões de segurança mais sólidos**
  - Mudança contínua de chaves.
  - Sistema de autenticação criptografado com um servidor.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Criptografia e infraestrutura de chave pública

- **Criptografia:**
  - Transforma textos comuns ou dados em um texto cifrado, que não possa ser lido por ninguém a não ser o remetente e o destinatário desejados.
  - Dois métodos para criptografar o tráfego de rede:
    - Secure Sockets Layer (SSL) e o seu sucessor, Transport Layer Security (TLS).
    - Secure Hypertext Transfer Protocol (S-HTTP).

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Criptografia e infraestrutura de chave pública

- **Dois outros métodos de criptografia:**
  - **Criptografia de chave simétrica**
    - Remetente e destinatário usam e compartilham uma única chave.
  - **Criptografia de chave pública**
    - Usa duas chaves matematicamente relacionadas: uma pública e outra privada.
    - O remetente criptografa a mensagem com a chave pública do destinatário.
    - O destinatário descriptografa utilizando a chave privada.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Criptografia de chave pública

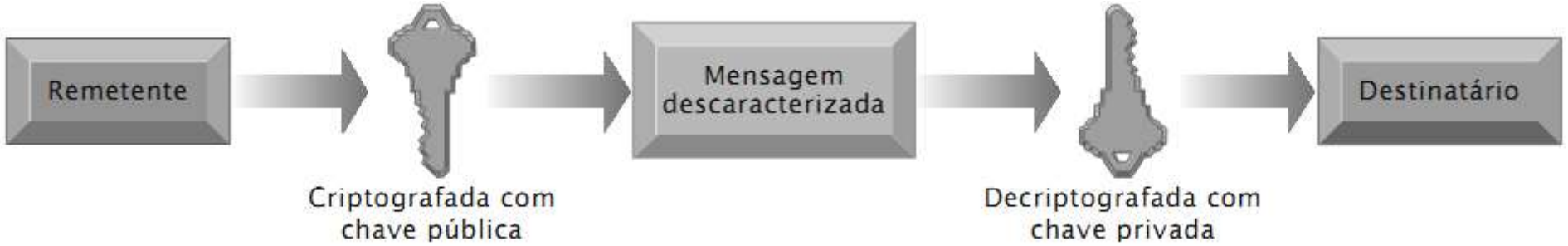


Figura 7.6

Um sistema de criptografia de chave pública pode ser visto como uma série de chaves públicas e privadas que “trancam” os dados quando são transmitidos e os “destrancam” quando são recebidos. O remetente localiza a chave pública do destinatário em um diretório e a utiliza para criptografar uma mensagem. A mensagem é enviada sob forma criptografada pela Internet ou por uma rede privada. Quando ela chega, o destinatário usa sua chave privada para descriptografar os dados e ler o conteúdo.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

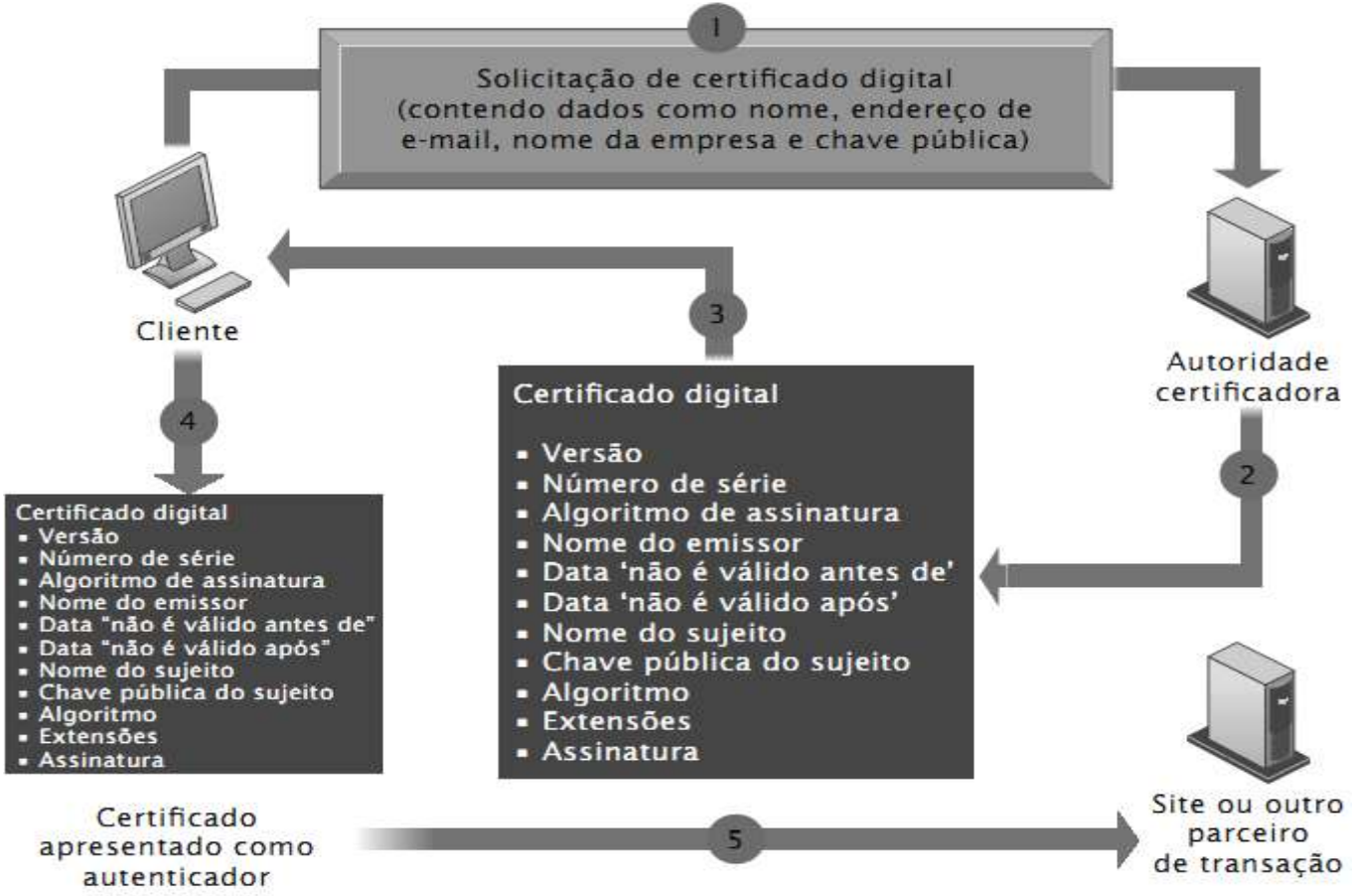
Criptografia e infraestrutura de chave pública

- **Certificado digital:**
  - Arquivos de dados usados para determinar a identidade de pessoas e ativos eletrônicos, a fim de proteger transações on-line
  - Usa uma terceira parte fidedigna, conhecida como autoridade certificadora (*Certificate Authority* — CA), para validar a identidade de um usuário
  - A CA verifica off-line a identidade do usuário e, em seguida, passa a informação para um servidor da CA, que gera um certificado digital criptografado contendo a identificação do proprietário e uma cópia de sua chave pública
- **Infraestrutura de chave pública (PKI)**
  - Uso da criptografia de chave pública em conjunto com uma CA
  - Amplamente utilizada no comércio eletrônico

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Certificados digitais

Os certificados digitais podem ser usados para determinar a identidade de pessoas ou ativos eletrônicos. Protegem transações on-line ao oferecer comunicação on-line segura e criptografada.



Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Como assegurar a disponibilidade do sistema

- O processamento on-line de transações requer 100% de disponibilidade e total tolerância a falhas.
- Sistemas de computação tolerantes a falhas:
  - Oferecem serviço contínuo. Exemplo: Bolsa de Valores.
  - Incluem componentes redundantes de hardware, software e fornecimento de energia elétrica, criando um ambiente que oferece serviço contínuo, ininterrupto.
- Computação de alta disponibilidade:
  - Ajuda na recuperação rápida de uma parada de sistema.
  - Minimiza, mas não elimina, o *downtime.*

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Como assegurar a disponibilidade do sistema

- **Computação orientada à recuperação**
  - Projeto de sistemas que se restabeleçam de forma rápida, com a implantação de recursos que ajudem os operadores a descobrir as fontes de falhas em sistemas compostos por múltiplos componentes
- **Controle do tráfego de rede**
  - Inspeção profunda de pacotes (*deep packet inspection* — DPI) (bloqueio de vídeo e música)
- ***Outsourcing* da segurança**
  - Provedores de serviços de segurança gerenciada (MSSPs)

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Garantia da qualidade de software

- **Métricas de software:** premissas objetivas do sistema na forma de medidas quantificadas
    - número de transações;
    - tempo de resposta on-line;
    - número de contracheques impressos por hora; e
    - erros conhecidos por cento de linhas de código.
- **Teste inicial regular e completo**
- **Acompanhamento:** revisão de uma especificação, ou documento de projeto, realizada por pequeno grupo de pessoas
- **Depuração:** processo através do qual os erros são eliminados

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Seção interativa: Tecnologia
Quão segura é a nuvem?

- Leia a Seção interativa e responda às seguintes perguntas:

  - Que problemas de segurança e controle são descritos nesse caso? Que fatores pessoais, organizacionais e tecnológicos contribuem para esse problema?
  - Quão segura é a computação em nuvem? Explique.
  - Se você fosse responsável pelo departamento de sistemas de informação de uma empresa, quais pontos gostaria de esclarecer com os possíveis fornecedores?