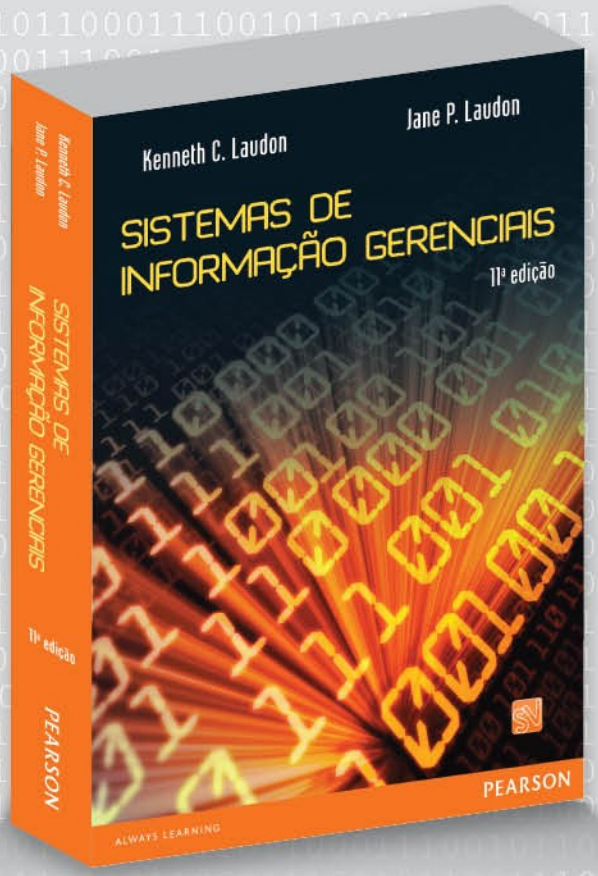
Capítulo 8

Segurança em sistemas de informação



Segurança em sistemas de informação

Kenneth C. Laudon Jane P. Laudon

SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

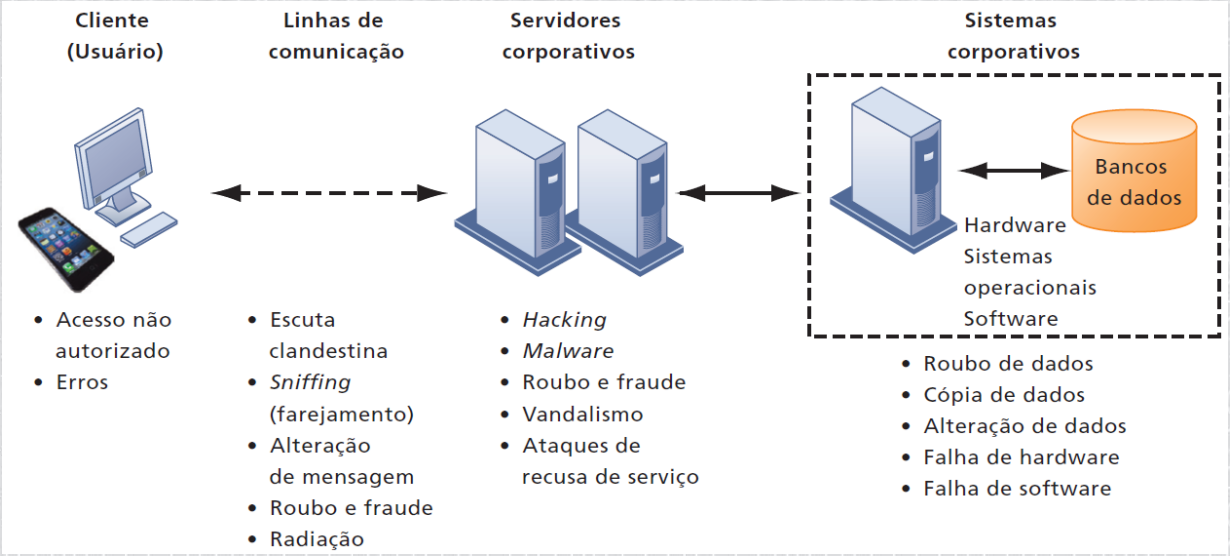
1. Por que os sistemas de informação estão vulneráveis a destruição, erros e uso indevido?
2. Qual o valor empresarial da segurança e do controle?
3. Quais os componentes de uma estrutura organizacional para segurança e controle?
4. Quais são as mais importantes tecnologias e ferramentas disponíveis para salvaguardar recursos de informação?

Vulnerabilidade dos sistemas e uso indevido

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- Quando grandes quantidades de dados são armazenadas no formato eletrônico, ficam vulneráveis a muito mais tipos de ameaças do que quando estão em formato manual.

- Vulnerabilidades e desafios de segurança contemporâneos:



Vulnerabilidade dos sistemas e uso indevido

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- A Internet é tão imensa que, quando usos indevidos ocorrem, eles podem causar um impacto de enormes proporções.
- A vulnerabilidade também aumentou com o uso disseminado de e-mail, mensagens instantâneas e programas de compartilhamento de arquivos ***peer-to-peer*** (**P2P**).
- É seguro se conectar a redes sem fio em aeroportos, bibliotecas ou outros locais públicos?
- Depende do quão alerta você está. Mesmo a rede sem fio de sua casa está vulnerável.

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

- **Vírus** de computador é um programa de software espúrio que se anexa a outros programas de software ou arquivos de dados a fim de ser executado, sem conhecimento nem permissão do usuário.
- ***Worms*** são programas de computador independentes que copiam a si mesmos de um computador para outro por meio de uma rede.
- O **cavalo de Troia** é uma porta para que vírus ou outros códigos mal-intencionados entrem no sistema do computador.
- ***Spyware*** são pequenos programas que se instalam nos computadores para monitorar a atividade do internauta e usar as informações para fins de marketing.

Hackers e crimes de informática

- **Hacker** é um indivíduo que pretende obter acesso não autorizado a um sistema de computador.
- O termo ***cracker*** normalmente é usado para designar o hacker com intenções criminosas.
- O ***spoofing*** (disfarce) também pode envolver o redirecionamento de um link para um endereço diferente do desejado.
- ***Sniffer*** (farejador) é um tipo de programa espião que monitora as informações transmitidas por uma rede.
- A maioria das atividades realizadas pelos hackers é composta por atos criminosos.

Hackers e crimes de informática

- **Roubo de identidade** é um crime em que um impostor obtém informações pessoais importantes, como número de identificação da Previdência Social, número da carteira de motorista ou número do cartão de crédito para se passar por outra pessoa.
- O ***phishing*** envolve 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.
- O ***pharming***, por sua vez, redireciona os usuários a uma página Web falsa, mesmo quando a pessoa digita o endereço correto da página Web no seu navegador.

Hackers e crimes de informática

- A **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.
- A **guerra cibernética** é uma séria ameaça à infraestrutura das sociedades modernas, uma vez que as suas principais instituições industriais, governamentais, médicas e financeiras dependem da Internet para as operações diárias.
- A guerra cibernética também envolve a defesa contra esses tipos de ataques.

Ameaças internas: funcionários

- Os funcionários, tanto usuários finais quanto especialistas em sistemas de informação, também são uma grande fonte de erros introduzidos nos sistemas de informação.
- Os usuários finais podem inserir dados incorretos ou deixar de seguir as regras para o processamento de dados e o uso do equipamento.
- Especialistas em sistemas de informação também geram erros de software ao projetar e desenvolver novos softwares, ou ao fazer a manutenção dos programas existentes.

Vulnerabilidade de software

- Um problema sério com o software é a presença de *bugs* escondidos ou defeitos do código do programa.
- Estudos demonstram que é praticamente impossível eliminar todos os *bugs* dos grandes programas.
- A principal fonte de erros é a complexidade do código de tomada de decisões.
- Para corrigir as falhas de software, uma vez que são identificadas, os fornecedores criam softwares denominados *patches* (remendos) para consertar as falhas sem prejudicar o bom funcionamento do software.

Valor empresarial da segurança e do controle

- Sistemas muitas vezes abrigam informações confidenciais sobre impostos, ativos financeiros, registros médicos e desempenho profissional das pessoas.
- Controle e segurança inadequados também podem criar sérios riscos legais.
- As empresas precisam proteger não apenas seus próprios ativos de informação, mas também os de clientes, funcionários e parceiros de negócios.
- Caso não consigam fazê-lo, podem ter de gastar muito em um litígio por exposição ou roubo de dados.

Prova eletrônica e perícia forense computacional

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- Em uma ação legal, uma empresa pode receber um pedido de produção de provas, sendo obrigada a fornecer acesso às informações que podem ser usadas como prova.
- A **perícia forense computacional** é o 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. Ela lida com os seguintes problemas:
- _____recuperar dados sem prejudicar seu valor probatório;
- _____armazenar e administrar dados eletrônicos recuperados;
- _____encontrar informações em um grande volume de dados;
- _____apresentar as informações em juízo.

Como estabelecer uma estrutura para segurança e controle

- **Controles gerais** controlam projeto, segurança e uso de programas de computadores, além da segurança de arquivos de dados.
- **Controles de aplicação** são controles específicos exclusivos a cada aplicação computadorizada, como processamento de pedidos.
- Uma **avaliação de risco** determina o nível de risco para a empresa caso uma atividade ou um processo específico não sejam controlados adequadamente.
- **Política de segurança** é uma declaração que estabelece hierarquia aos riscos de informação e identifica metas de segurança aceitáveis, assim como os mecanismos para atingi-las.

Plano de recuperação de desastres e plano de continuidade dos negócios

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- O **plano de recuperação de de**sastres inclui estratégias para restaurar os serviços de computação e comunicação após eles terem sofrido uma interrupção.
- O **plano de continuidade dos negócios** concentra-se em como a empresa pode restaurar suas operações após um desastre.
- Como a administração sabe que os controles e a segurança de seus sistemas de informação são eficientes?
- Uma **auditoria de sistemas de informação** avalia o sistema geral de segurança da empresa e identifica todos os controles que governam sistemas individuais de informação.

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

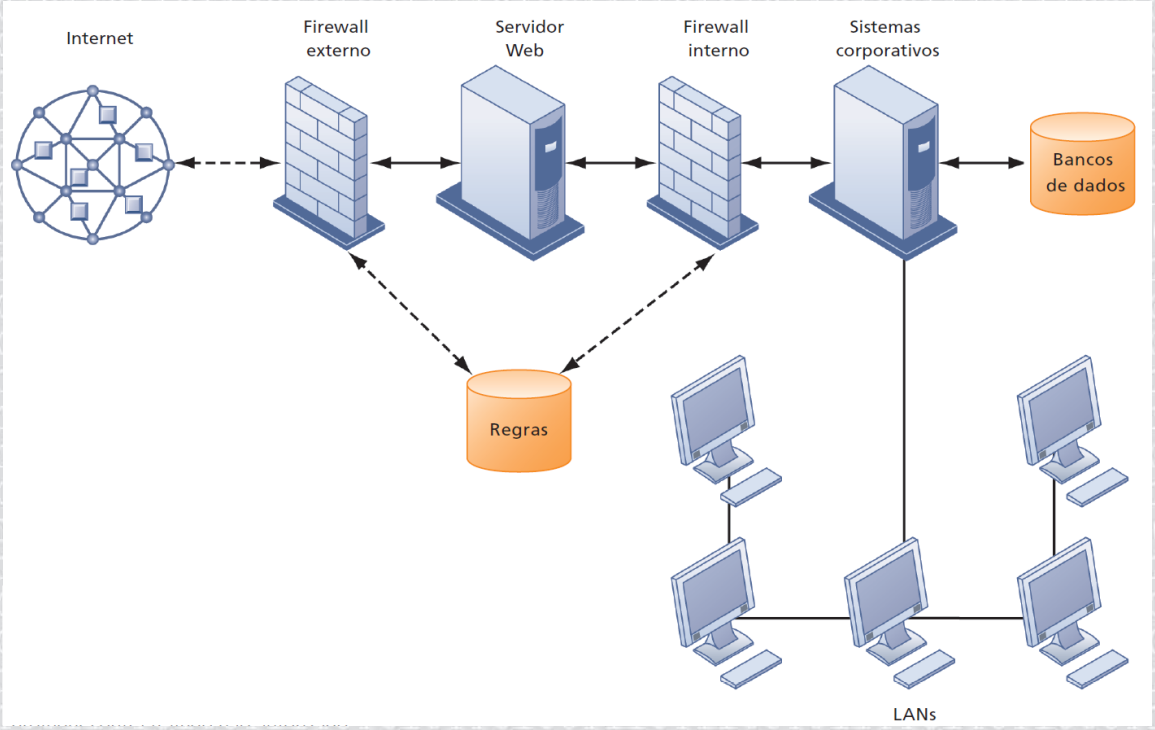
Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- O software de **gestão de identidade** automatiza o processo de manter o controle de todos esses usuários e seus privilégios de sistema, atribuindo a cada usuário uma única identidade digital para acessar cada sistema.
- **Autenticação** refere-se à capacidade de saber que uma pessoa é quem declara ser.
- A **autenticação biométrica** usa sistemas que leem e interpretam traços humanos individuais, como impressões digitais, íris e vozes, para conceder ou negar acesso.

Firewalls, sistemas de detecção de intrusão e softwares antivírus

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- **Firewall** é uma combinação de hardware e software que controla o fluxo de tráfego que entra na rede ou sai dela.



Firewalls, sistemas de detecção de intrusão e softwares antivírus

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- **Sistemas de detecção de intrusão** são ferramentas de monitoração contínua instaladas nos pontos mais vulneráveis (“mais quentes”) de redes corporativas, a fim de detectar e inibir invasores.
- O **software antivírus** previne, detecta e remove *malware*, incluindo vírus, *worms*, cavalos de Troia, *spyware* e *adware*.
- Esses abrangentes produtos para gestão da segurança são chamados de **sistemas unificados de gestão de ameaças** (UTM).

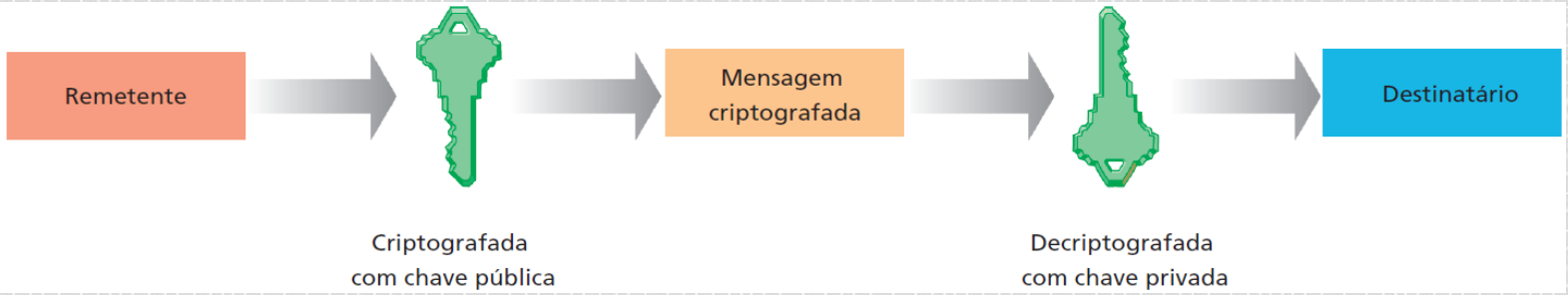
Segurança em redes sem fio

- O padrão de segurança inicial desenvolvido para Wi-Fi, chamado *Wired Equivalent Privacy* (WEP), não é muito eficaz, pois suas chaves de criptografia são relativamente fáceis de decifrar.
- WEP fornece alguma margem de segurança, no entanto, se os usuários se lembrarem de ativá-lo.
- As empresas podem aumentar a segurança Wi-Fi utilizando-o em conjunto com a tecnologia de rede privada virtual (VPN) ao acessar dados corporativos internos.

Criptografia e infraestrutura de chave pública

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

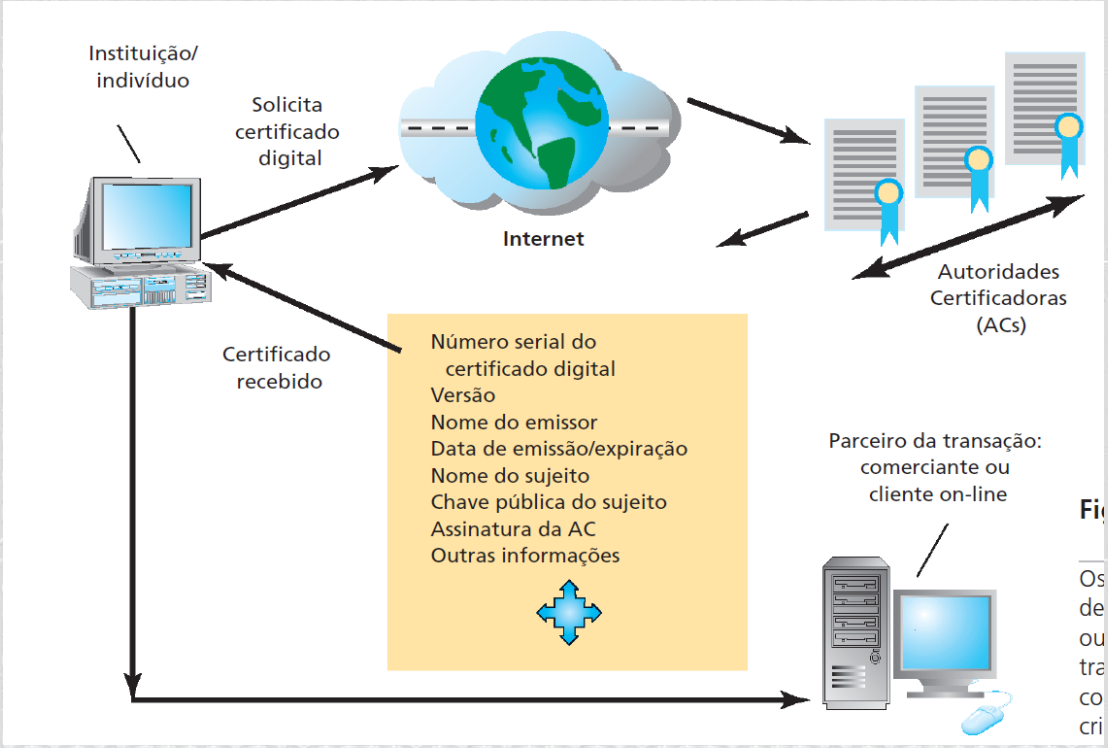
- **Criptografia** é o processo de transformar textos comuns ou dados em um texto cifrado, que não possa ser lido por ninguém a não ser o remetente e o destinatário desejado.
- Podemos citar dois métodos para criptografar o tráfego de rede: o SSL e o S-HTTP.
- Criptografia de chave pública:



Criptografia e infraestrutura de chave pública

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- Os **certificados digitais** protegem transações on-line ao oferecer comunicação on-line segura e criptografada:



Questões de segurança na computação em nuvem e na plataforma digital móvel

Kenneth C. Laudon Jane P. Laudon
SISTEMAS DE INFORMAÇÃO GERENCIAIS
11ª edição

- A natureza dispersa da computação em nuvem torna difícil rastrear atividades não autorizadas.
- Usuários da nuvem precisam confirmar que, independentemente do local onde seus dados estejam armazenados, eles estão protegidos em um nível que atende a seus requisitos corporativos.
- As empresas devem criptografar a comunicação sempre que possível.
- Todos os usuários de dispositivos móveis devem ser obrigados a usar o recurso de senha encontrado em todos os smartphones.

Garantia da qualidade de software

- Além de implantar segurança e controle eficientes, as empresas podem melhorar a qualidade e a confiabilidade dos sistemas por meio de métricas e testes rigorosos de software.
- Métricas de software são premissas objetivas do sistema na forma de medidas quantificadas.
- O teste inicial regular e completo também contribuirá significativamente para a qualidade do sistema.
- Muitos consideram esse teste uma maneira de provar a exatidão do trabalho realizado.

Resumo

1. Por que os sistemas de informação são vulneráveis a destruição, erros e uso indevido?
2. Qual o valor empresarial da segurança e do controle?
3. Quais são os componentes de uma estrutura organizacional para segurança e controle?
4. Quais as mais importantes tecnologias e ferramentas disponíveis para salvaguardar recursos de informação?