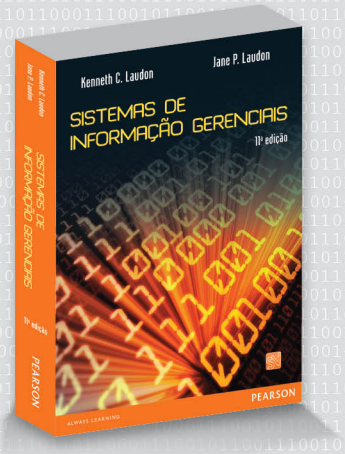
Capítulo 8

Segurança em sistemas de informação



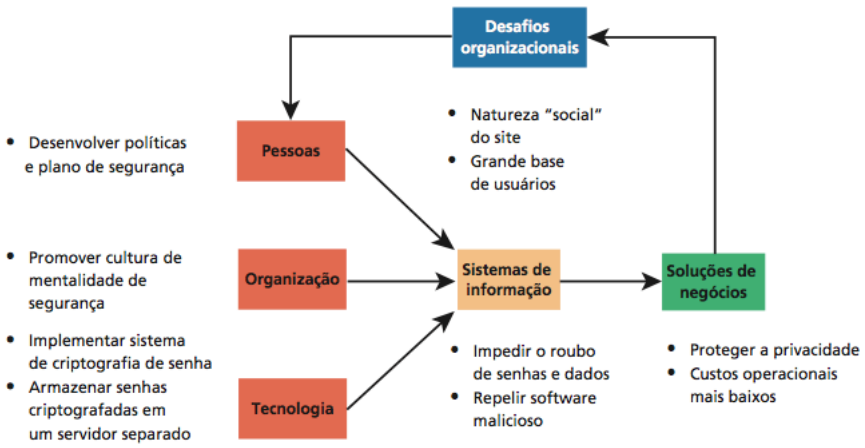
Segurança em sistemas de informação

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?

Caso de abertura:
Você está no LinkedIn? Cuidado!

- Contexto: LinkedIn tem mais de 225 milhões de usuários.
- A empresa é avaliada atualmente em mais de US$ 21 bilhões.
- Em junho de 2012, a empresa sofreu uma violação de dados que expôs as senhas de milhões de usuários. Os hackers violaram a segurança do site e roubaram 6,5 milhões de senhas de usuários; em seguida, publicaram abertamente as senhas em um fórum de hacking da Rússia.
- Não empregou várias técnicas de criptografia padrão usadas para proteger senhas. A maioria das empresas utiliza uma técnica conhecida como salting, que acrescenta uma série de dígitos aleatórios no final dos códigos hash das senhas para torná-las mais difíceis de decifrar. O salting pode ser realizado com pouco ou nenhum custo, com apenas algumas linhas adicionais de código.
- O custo total para uma empresa como o LinkedIn implantar uma senha robusta, um servidor Web e segurança de aplicação seria de, no mínimo, algumas centenas de milhares de dólares, mas uma violação média de dados custa às empresas 5,5M.
- Alguns especialistas em segurança acreditam que a falta da obrigação de indenizar das empresas como LinkedIn é uma das principais razões para suas fracas políticas de segurança.
- LinkedIn foi atingido com um processo de ação coletiva no valor de US$ 5 milhões.
- LinkedIn atualizou sua segurança mas é preciso um esforço contínuo.

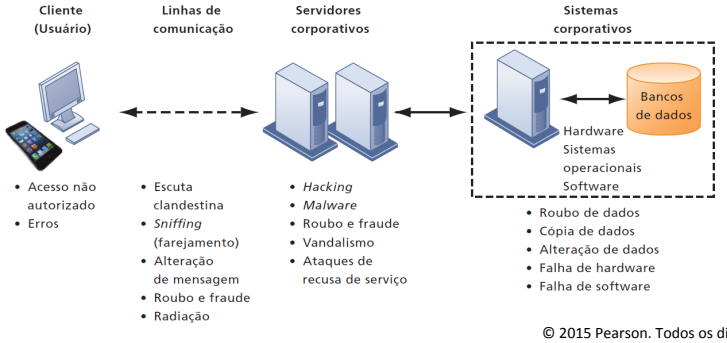
Caso de abertura:
Você está no LinkedIn? Cuidado!



Vulnerabilidade dos sistemas e uso indevido

- 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

- 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.

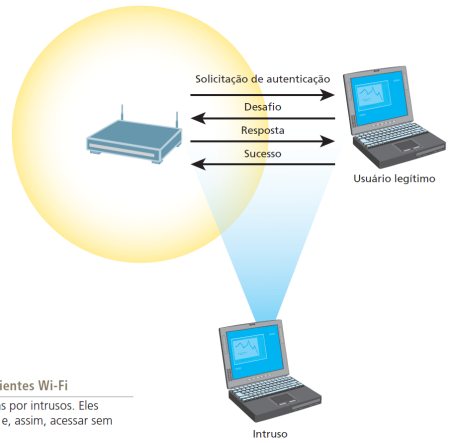


Figura 8.2 Desafios de segurança em ambientes Wi-Fi
Muitas redes Wi-Fi podem ser facilmente invadidas por intrusos. Eles usam programas *sniffers* para obter um endereço e, assim, acessar sem autorização os recursos da rede.

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.

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

Tabela 8.1

Exemplos de códigos mal-intencionados.

Nome	Tipo	Descrição
Conficker (também conhecido como Downadup, Downup)	Worm	Detectado pela primeira vez em novembro de 2008, esse código ainda prevalece. Usa falhas do Windows para controlar máquinas e conectá-las a um computador virtual que pode ser comandado remotamente. Possuía mais de 5 milhões de computadores em todo o mundo sob seu controle. Difícil de erradicar.
Storm	Worm/Cavalo de Troia	Identificado pela primeira vez em janeiro de 2007. Espalha-se por spam via e-mail com um falso anexo. Infectou mais de 10 milhões de computadores, levando-os a se juntar à sua rede zumbi de computadores ligados à atividade criminal.
Sasser.ftp	Worm	Apareceu pela primeira vez em maio de 2004. Espalhou-se pela Internet por meio do ataque a endereços IP aleatórios. Faz os computadores travarem e reiniciarem continuamente, e os leva a procurar mais vítimas. Infectou milhões de computadores ao redor do mundo, afetando as operações de *check-in* da British Airways, das estações da guarda costeira britânica, de hospitais em Hong Kong, das agências de correio de Taiwan e do Westpac Bank da Austrália. Sasser e suas variações causaram um dano estimado entre US$ 14,8 bilhões e US$ 18,6 bilhões ao redor do mundo.

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

MyDoom.A	Worm	Apareceu pela primeira vez em 26 de janeiro de 2004. Espalha-se como anexo de e-mail. Envia mensagens para endereços coletados de máquinas infectadas, falsificando o endereço do remetente. No seu auge, este worm reduziu o desempenho da Internet global em 10% e os tempos de download de página Web em até 50%. Foi programado para parar de espalhar depois de 12 de fevereiro de 2004.
Sobig.F	Worm	Detectado pela primeira vez em 19 de agosto de 2003. Espalha-se por meio de anexos de e-mail e envia montantes massivos de mensagens com informações falsas sobre o remetente. Foi desativado em 10 de setembro de 2003, depois de infectar mais de 1 milhão de PCs e causar um dano estimado entre US$ 5 bilhões e US$ 10 bilhões.
ILOVEYOU	Vírus	Detectado pela primeira vez em 3 de maio de 2000. Vírus de script escrito em Visual Basic Script e transmitido como um anexo em e-mails com o assunto ILOVEYOU. Sobrescreve música, imagens e outros arquivos com uma cópia de si mesmo e causou um dano estimado entre US$ 10 bilhões e US$ 15 bilhões.
Melissa	Macrovírus/Worm	Apareceu pela primeira vez em março de 1999. Script de macro do Word enviado para infectar arquivos do Word para as 50 primeiras entradas do livro de endereços do Microsoft Outlook do usuário. Infectou de 15% a 29% de todos os PCs corporativos, causando um prejuízo entre US$ 300 milhões e US$ 600 milhões.

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.

Hackers e crimes de informática

Tabela 8.2
Exemplos de crime de informática.

Computadores como alvos de crime
Violar a confidencialidade de dados computadorizados protegidos
Acessar um sistema de computador sem autorização
Acessar intencionalmente um computador protegido para cometer fraude
Acessar intencionalmente e infligir danos a um computador protegido, de maneira negligente ou deliberada
Transmitir intencionalmente um programa, código de programa ou comando que deliberadamente danifique um computador protegido
Ameaçar causar danos a um computador protegido
Computadores como instrumentos de crime
Roubo de segredos comerciais
Cópia não autorizada de software ou de material com propriedade intelectual registrada, como artigos, livros, músicas e vídeos
Esquemas para defraudação
Usar e-mail para ameaças ou assédio
Tentar interceptar comunicações eletrônicas intencionalmente
Acessar ilegalmente comunicações eletrônicas armazenadas, inclusive e-mail e caixa postal de voz
Possuir material de pedofilia armazenado em um computador ou transmiti-lo eletronicamente

Hackers e crimes de informática

Tabela 8.3
Principais incidentes de violação de dados.

Violação de dados	Descrição
Departamento de Assuntos Relacionados aos Veteranos dos Estados Unidos (*U.S. Veterans Affairs Department*)	Em 2006, os nomes, as datas de nascimento e os números de identificação da Previdência Social de 17,5 milhões de veteranos militares foram roubados de um laptop que um funcionário do Departamento de Assuntos Relacionados aos Veteranos tinha levado para casa. O departamento gastou pelo menos US$ 25 milhões para executar os serviços de atendimentos, enviar mensagens de e-mails e pagar por um ano de serviço de monitoramento de crédito para as vítimas.
Heartland Payment Systems	Em 2008, criminosos liderados pelo hacker Albert Gonzales, de Miami, instalaram softwares de espionagem na rede de computadores da Heartland Payment Systems, uma empresa que processa pagamentos, com sede em Princeton, Nova Jersey, e roubaram os números de até 100 milhões de cartões de crédito e de débito. Gonzales foi condenado em 2010 a 20 anos de prisão federal, e a Heartland pagou cerca de US$ 140 milhões em multas e acordos.
TJX	Um incidente de violação de dados ocorrido em 2007 na TJX, empresa varejista que possui cadeias nacionais, incluindo a TJ Maxx e a Marshalls, custou pelo menos US$ 250 milhões. Os criminosos cibernéticos roubaram mais de 45 milhões de números de cartões de crédito e de débito, alguns dos quais foram usados posteriormente para comprar produtos eletrônicos do Walmart e de outros lugares, no valor de milhões de dólares. Albert Gonzales, que desempenhou um papel importante no ataque à Heartland, também estava ligado a esse ataque cibernético.
Epsilon	Em março de 2011, hackers roubaram milhões de nomes e endereços de e-mail da Epsilon, empresa de marketing por e-mail, que lida com listas de e-mail para grandes varejistas e bancos como Best Buy, JPMorgan, TiVo e Walgreens. Os custos podem variar de US$ 100 milhões a US$ 4 bilhões, dependendo do que aconteceu com os dados roubados, sendo que a maior parte dos custos se deve à perda de clientes decorrente de danos à reputação lesada.
Sony	Em abril de 2011, hackers obtiveram informações pessoais, incluindo número de cartões de crédito, de débito e de conta bancária, de mais de 100 milhões de usuários da rede PlayStation e de usuários da Sony Online Entertainment. A violação pode custar à Sony e aos emissores de cartões de crédito um total de até US$ 2 bilhões.

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

- 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.

Controles gerais

Tabela 8.4
Controles gerais.

Tipos de controle geral	Descrição
Controles de software	Monitoram o uso de sistemas de software e previnem o acesso não autorizado a programas de software, sistemas de software e programas de computador.
Controles de hardware	Garantem que o hardware do computador esteja fisicamente seguro e verificam o mau funcionamento do equipamento. Organizações criticamente dependentes de seus computadores precisam prever a criação de cópias de segurança dos dados ou operações contínuas de manutenção de serviços constantes.
Controles de operações de computador	Supervisionam o trabalho do departamento de informática para garantir que os procedimentos programados sejam consistentes e corretamente aplicados ao armazenamento e processamento de dados. Incluem controles sobre as tarefas de processamento e dos procedimentos de recuperação do computador para processamentos que terminam de maneira anormal.
Controles de segurança de dados	Garantem que os valiosos arquivos de dados do sistema, gravados em disco ou fita, não estejam sujeitos a acesso não autorizado, a modificações ou a destruição enquanto estão em uso ou armazenados.
Controles de implementação	Auditam o processo de desenvolvimento de sistemas em diversos pontos para garantir que ele seja devidamente controlado e gerenciado.
Controles administrativos	Formalizam padrões, regras, procedimentos e controlam disciplinas de modo a garantir que os controles gerais e de aplicação da empresa sejam propriamente executados e cumpridos.

slide 21

Avaliação de risco

Tabela 8.5
Avaliação do risco no processamento de pedidos on-line.

Exposição	Probabilidade de ocorrência (%)	Faixa de prejuízo/média (US$)	Prejuízo anual esperado (US$)
Falta de energia	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

slide 22

Hackers e crimes de informática

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

Figura 8.3 Regras de acesso para um sistema de pessoal

Esses 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.

Plano de recuperação de desastres e plano de continuidade dos negócios

- 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.

Auditoria de sistemas de informação

Função: Empréstimos pessoais Localização: Peoria, IL	Preparado por: J. Ericson Data: 16 de junho de 2014		Recebido por: T. Benson Data de revisão: 28 de junho de 2014	
Natureza e impacto das deficiências	Chance de erro/uso indevido		Notificação à administração	
	Sim/Não	Justificativa	Data do relatório	Resposta da administração
Contas de usuários sem senhas	Sim	Deixa o sistema aberto para pessoas externas não autorizadas ou hackers	10/05/14	Eliminar contas sem senhas
Rede configurada para permitir apenas compartilhamento de arquivos do sistema	Sim	Expõe arquivos de sistemas críticos para partes hostis conectadas à rede	10/05/14	Garantir que apenas diretórios necessários sejam compartilhados e que sejam protegidos por senhas fortes
Patches de software podem atualizar programas de produção sem aprovação final do grupo de Padrões e Controles	Não	Todos os programas de produção exigem autorização da administração; o grupo de Padrões e Controles determina, para tais casos, um status de produção temporária		

Figura 8.4 Exemplo de listagem feita por um auditor para deficiências de controle

Esse 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.

slide 25

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

- 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. (PS: Senhas, Tokens)
- A **autenticação biométrica** usa sistemas que leem e interpretam traços humanos individuais, como impressões digitais, íris e vozes, para conceder ou negar acesso.

slide 26

Firewalls, sistemas de detecção de intrusão e softwares antivírus

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

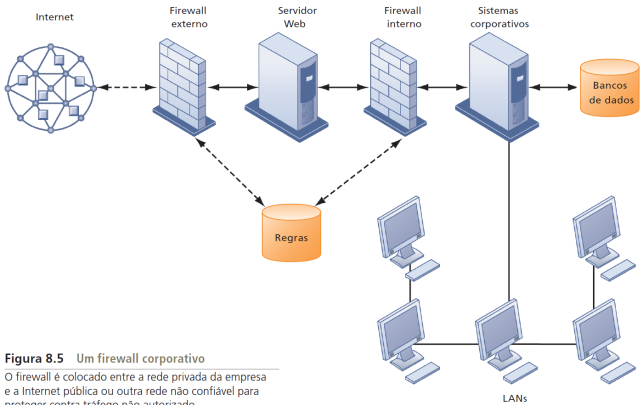


Figura 8.5 Um firewall corporativo
O firewall é colocado entre a rede privada da empresa e a Internet pública ou outra rede não confiável para

Firewalls, sistemas de detecção de intrusão e softwares antivírus

- **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

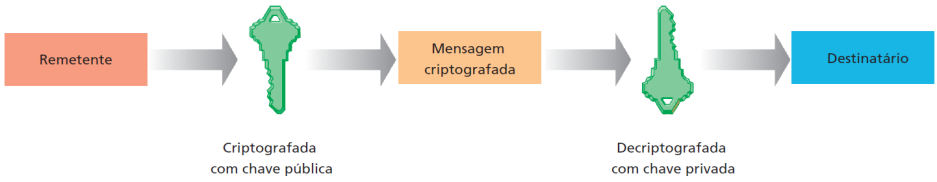
- O padrão de segurança inicial desenvolvido para Wi-Fi, chamado *Wired Equivalent Privacy* (WEP), não é muito eficaz, pois suas chaves de criptografia são relativamente fáceis de decifrar.
- WEP fornece alguma margem de segurança, no entanto, se os usuários se lembrarem de ativá-lo.
- As empresas podem aumentar a segurança Wi-Fi utilizando-o em conjunto com a tecnologia de rede privada virtual (VPN) ao acessar dados corporativos internos.
- Wi-Fi Protected Access 2 ou WPA2 substitui o WEP por padrões de segurança mais sólidos. Em vez das chaves de criptografia estáticas utilizadas no WEP, o novo padrão utiliza chaves bem mais longas que se modificam continuamente e, assim, dificultam sua descoberta. Também emprega um sistema de autenticação criptografado com um servidor de autenticação para garantir que somente usuários autorizados acessem a rede.

Criptografia e infraestrutura de chave pública

- **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:
  - SSL e o TLS são projetados para estabelecer uma conexão segura entre dois computadores;
  - S-HTTP só consegue lidar com mensagens individuais.

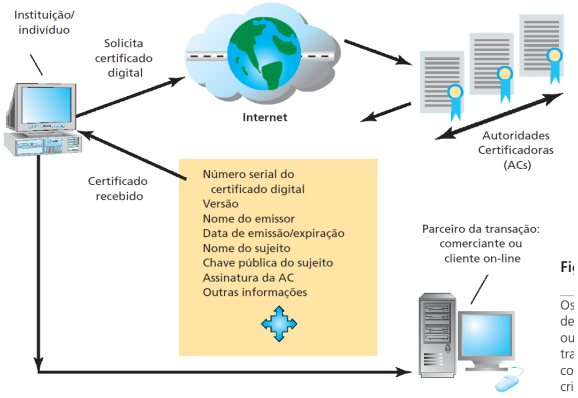
Criptografia e infraestrutura de chave pública

- Criptografia de chave simétrica:
  - remetente e o destinatário estabelecem uma sessão de Internet segura, criando uma única chave criptográfica, que é enviada ao destinatário, de forma que o remetente e o destinatário compartilham a mesma chave. A força da chave criptográfica é medida pelo seu comprimento em bits. Chave típica tem 128 bits.
- Criptografia de chave pública:
  - usa duas chaves: uma compartilhada (ou pública) e outra totalmente privada. As chaves são matematicamente relacionadas, de modo que os dados criptografados com uma chave somente podem ser decriptografados pela outra. Para enviar e receber mensagens, as duas partes envolvidas na comunicação primeiramente criam pares separados de chaves públicas e privadas. A chave pública é mantida em um diretório, e a privada deve ser mantida em segredo. O remetente criptografa uma mensagem com a chave pública do destinatário. Ao receber a mensagem, o destinatário usa sua chave privada para decriptografá-la.



Criptografia e infraestrutura de chave pública

- 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

- 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?