

transação eletrônica para os prestadores de serviços de saúde na administração das informações dos pacientes, prevendo penalidades para violações da privacidade médica, *disclosure* (transparência) de registros de pacientes por e-mail ou acesso não autorizado à rede.

Se você trabalhar nos Estados Unidos, em uma empresa que presta serviços financeiros, ela deverá cumprir a **Lei Gramm-Leach-Bliley**. A Lei de Modernização dos Serviços Financeiros, de 1999 — mais conhecida como Lei Gramm-Leach-Bliley (GLBA), em homenagem aos congressistas que a propuseram —, exige que as instituições financeiras assegurem a segurança e a confidencialidade dos dados do cliente. As informações precisam ser armazenadas em um meio seguro. Medidas especiais de segurança precisam ser tomadas para proteger tais dados, tanto no meio de armazenagem quanto durante a transmissão.

Se trabalhar em uma empresa com ações negociadas na bolsa norte-americana, deverá obedecer à **Lei Sarbanes-Oxley**. A Lei de Proteção ao Investidor e de Reforma Contábil das Empresas de Capital Aberto, promulgada em 2002 nos Estados Unidos e mais conhecida como Sarbanes-Oxley — em homenagem a seus formuladores, o senador Paul Sarbanes, de Maryland, e o deputado federal Michael Oxley, de Ohio —, foi elaborada para proteger investidores após os escândalos financeiros envolvendo a Enron, a WorldCom e outras empresas de capital aberto. Segundo essa lei, cabe às empresas e a seus administradores salvaguardar a precisão e a integridade das informações financeiras utilizadas internamente e publicadas externamente.

A Lei Sarbanes-Oxley diz respeito, fundamentalmente, à garantia de que existam controles internos para governar a criação e a documentação de informações nos demonstrativos financeiros. Como são usados sistemas de informação para gerar, armazenar e transportar tais dados, a legislação exige que as empresas levem em conta a segurança dos sistemas de informação e outros controles necessários para garantir a integridade, a confidencialidade e a precisão dos dados. Cada aplicativo de sistema que lida com dados de relatórios financeiros críticos exige controles para garantir a exatidão desses dados. Da mesma maneira, são essenciais controles para proteger a rede corporativa, evitar acesso não autorizado aos sistemas e dados e garantir a disponibilidade e integridade das informações, na eventualidade de um desastre ou de uma interrupção qualquer nos serviços.

Prova eletrônica e perícia forense computacional

Segurança, controle e gestão de registros eletrônicos se tornaram essenciais para lidar com ações legais. Atualmente, grande parte das provas em casos envolvendo fraude acionária, desvio de dinheiro, roubo de segredos empresariais, crimes de informática e muitos casos civis encontra-se no formato digital. Além das informações impressas ou digitadas, as ações jurídicas atuais dependem cada vez mais de provas apresentadas na forma de dados armazenados em discos portáteis, CDs e discos rígidos, assim como em e-mails, mensagens instantâneas e transações de e-commerce pela Internet. Atualmente, o e-mail é o tipo mais comum de prova eletrônica.

Em uma ação legal, uma empresa pode receber um pedido de produção de provas, tendo de dar acesso a informações usadas como garantia. Como a empresa está obrigada por lei a apresentar esses dados, o custo pode ser enorme se tiver problemas para reuni-los, ou se forem corrompidos ou destruídos. Atualmente, os tribunais impõem severas penalidades financeiras e até mesmo criminais no caso de destruição indevida de documentos eletrônicos.

Uma política de retenção de documentos eletrônicos eficiente assegura que documentos eletrônicos, e-mails e outros registros estejam bem organizados e acessíveis, e que nunca sejam detidos por tempo demais nem descartados cedo demais. Tal política também reflete uma preocupação em preservar provas potenciais para a perícia forense computacional. A **perícia forense computacional** é o procedimento científico de coleta, exame, autenticação, preservação e análise de dados mantidos em — ou recuperados por — 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 de computadores sem prejudicar seu valor probatório;
- armazenar e administrar com segurança os dados eletrônicos recuperados;
- encontrar informações significativas em um grande volume de dados eletrônicos;
- apresentar as informações em juízo.

As provas eletrônicas podem estar em um meio de armazenamento digital, na forma de arquivos de computador ou como *dados ambientes*, não visíveis ao usuário comum. Exemplo disso é um arquivo que tenha sido apagado no disco rígido do PC. Os dados que um usuário tenha apagado no meio de armazenamento digital podem ser recuperados por meio de várias técnicas. Os peritos forenses computacionais tentam recuperar esses dados ocultos para que possam ser apresentados como prova.

A preocupação com as necessidades da perícia digital pode ser incorporada ao processo de planejamento de contingência da empresa. O CIO, os especialistas em segurança, a equipe de sistemas de informação e o conselho jurídico da empresa devem, todos juntos, trabalhar em prol de um plano que, caso surja uma necessidade legal, possa ser posto em marcha.

Como estabelecer uma estrutura para segurança e controle

Mesmo com as principais ferramentas de segurança, seus sistemas de informação somente serão confiáveis e seguros se souber como e onde utilizá-los. Será necessário saber onde sua empresa corre riscos e de quais controles precisa para proteger seus sistemas de informação. Também será preciso desenvolver uma política de segurança e planos para manter seu negócio em funcionamento se seus sistemas de informação não estiverem operando.

Controles de sistemas de informação

Controles de sistemas de informação podem ser manuais ou automatizados e são compostos tanto por controles gerais quanto por controles de aplicações. **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. De modo geral, os controles gerais se aplicam a todas as aplicações computadorizadas e consistem de uma combinação de hardware, software e procedimentos manuais que criam um ambiente global de controle.

Entre os controles gerais há controles de software, de hardware físico, de operações de computador e de segurança de dados, além de controles administrativos e sobre a implementação de processos do sistema. A Tabela 7.3 descreve as funções de cada um desses controles.

Controles de aplicação são controles específicos exclusivos a cada aplicação computadorizada, como processamento de folha de pagamento ou pedidos. Incluem tanto procedimentos manuais quanto automatizados que garantem que somente dados autorizados sejam completa e precisamente processados pelas aplicações. Os controles de aplicação podem ser classificados como (1) controles de entrada, (2) controles de processamento e (3) controles de saída.

Controles de entrada verificam a precisão e completude dos dados quando entram no sistema. Existem controles de entrada específicos para autorização de entrada, conversão de dados, edição de dados e tratamento de erros. *Controles de processamento* verificam se os dados estão completos e precisos durante a atualização. *Controles de saída* garantem que os resultados do processamento computacional sejam precisos, completos e distribuídos de maneira apropriada.

Avaliação de risco

Antes que a sua empresa comprometa recursos com segurança, ela precisa saber quais ativos exigem proteção e em que medida eles são vulneráveis. Uma avaliação de risco ajuda a responder a essas questões e determina o conjunto de controles com melhor custo-benefício para proteger os ativos.

Tabela 7.3 Controles gerais

Tipo 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	Controlam o processo de desenvolvimento de sistemas em diversos pontos para garantir que o processo 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.

Uma avaliação de risco determina o nível de risco para a empresa caso uma atividade ou um processo específico não sejam controlados adequadamente. Os administradores da empresa, em cooperação com os especialistas em sistemas de informação, podem determinar o valor dos ativos de informação, os pontos de vulnerabilidade, a frequência provável de um problema e seu prejuízo potencial. Por exemplo: se a probabilidade de um evento ocorrer não for maior que uma vez por ano, com um limite máximo de mil dólares de prejuízo para a organização, não seria viável gastar 20 mil dólares no projeto e manutenção de um controle para evitar esse evento. Entretanto, se aquele mesmo evento pudesse ocorrer, no mínimo, uma vez por dia, com um prejuízo potencial de mais de 300 mil dólares por ano, gastar 100 mil dólares em um controle seria totalmente apropriado.

A Tabela 7.4 traz amostras dos resultados de uma avaliação de risco para um sistema de processamento de pedidos on-line que processa 30 mil pedidos por dia. A probabilidade de ocorrer falta de energia elétrica no período de um ano está expressa na forma de porcentagem. A coluna seguinte mostra o maior e o menor prejuízos possíveis esperados a cada ocorrência e, entre parênteses, o prejuízo médio, calculado somando-se os números mais

Tabela 7.4 Avaliação do risco no processamento de pedidos on-line

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

alto e mais baixo e dividindo-os por dois. O prejuízo anual esperado para cada falta de energia elétrica pode ser determinado multiplicando-se o prejuízo médio por sua probabilidade de ocorrência.

A avaliação de risco mostra que a probabilidade de faltar energia elétrica no período de um ano é de 30 por cento. O prejuízo nas transações de pedidos durante o período em que a energia elétrica estiver desligada pode variar entre 5 mil e 200 mil dólares (média de 102.500 dólares) para cada ocorrência, dependendo de quanto tempo o processamento permanecer paralisado. A probabilidade de ocorrer apropriação indébita durante um período de um ano é de cerca de cinco por cento, com prejuízos potenciais na faixa de mil a 50 mil dólares (média de 25.500 dólares) para cada ocorrência. A probabilidade de ocorrerem erros de usuários durante o período de um ano é de 98 por cento, com prejuízos entre 200 dólares e 40 mil dólares (média de 20.100 dólares) a cada ocorrência.

Uma vez avaliados os riscos, os desenvolvedores de sistemas podem concentrar-se nos pontos de controle cuja vulnerabilidade e prejuízo potencial são maiores. No caso aqui descrito, os controles devem focar em maneiras de minimizar os riscos de falta de energia elétrica e erros de usuários, pois os prejuízos anuais esperados são maiores nessas áreas.

Política de segurança

Uma vez que identificou os principais riscos para seus sistemas, sua empresa precisará desenvolver uma política de segurança para proteger esses ativos. **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. Quais são os ativos de informação mais importantes da empresa? Quem produz e controla essa informação? Quais políticas de segurança já estão em curso para proteger essa informação? Qual nível de risco a administração está disposta a aceitar para cada um dos ativos? Está disposta, por exemplo, a perder dados de crédito dos clientes uma vez a cada dez anos? Ou desenvolverá um sistema de segurança para dados de cartão de crédito capaz de enfrentar um desastre que só ocorre a cada cem anos? A administração precisa estimar ainda quanto custará atingir esse nível de risco aceitável.

A política de segurança dá origem a outras políticas que determinam o uso aceitável dos recursos de informação da empresa e quais membros terão acesso a esses ativos. Uma **política de uso aceitável (acceptable use policy — AUP)** define os usos aceitáveis dos recursos de informação e do equipamento de informática da empresa, incluindo computadores de mesa e laptops, dispositivos sem fio, telefones e Internet. A política deve deixar clara a posição da empresa no que diz respeito à privacidade, à responsabilidade do usuário e ao uso pessoal do equipamento de informática e das redes. Uma boa política de uso aceitável define as ações aceitáveis e inaceitáveis para cada usuário, especificando as consequências do não cumprimento às normas. Por exemplo, a política de segurança na Unilever, a multinacional de bens de consumo, exige que cada empregado equipado com um laptop portátil utilize um dispositivo específico da empresa e use uma senha ou outro método de identificação quando se conectar à rede corporativa.

As **políticas de autorização**, por sua vez, determinam diferentes níveis de acesso aos ativos de informação para diferentes níveis de usuários. Os **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. Tais sistemas 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.

O sistema de gestão de autorização sabe exatamente quais informações cada usuário tem permissão para acessar. A Figura 7.3 ilustra o que a segurança permite a dois conjuntos de usuários de um banco de dados pessoais on-line, com informações sensíveis tais como salários, benefícios e históricos médicos dos funcionários. Um dos conjuntos consiste em todos os funcionários que executam funções burocráticas, tais como digitar os dados no sistema. Todos os indivíduos com esse perfil podem atualizar o sistema, mas não podem ler nem atualizar dados sensíveis como salários, históricos médicos ou dados de remuneração.

Figura 7.3

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

O outro perfil se aplica a um gerente de divisão, que não pode atualizar o sistema, mas pode ler todos os campos dos dados referentes aos funcionários de sua divisão, incluindo histórico médico e salário. Esses perfis seriam estabelecidos e mantidos por um sistema de segurança de dados, baseado em regras de acesso fornecidas por grupos especiais dentro da empresa. O exemplo da Figura 7.3 estabelece restrições de segurança específicas e detalhadas, tais como permitir que usuários autorizados da divisão de pessoal consultem todas as informações de funcionários, exceto as dos campos confidenciais, como salário ou histórico médico.

Plano de recuperação de desastres e plano de continuidade dos negócios

Se você gerencia uma empresa, precisa se planejar para eventos como blecautes, enchentes, terremotos ou ataques terroristas que irão impedir que seus sistemas de informação e sua empresa funcionem. O **plano de recuperação de desastres** inclui estratégias para restaurar os serviços de computação e comunicação após eles terem sofrido uma interrupção causada por eventos como terremotos, inundações ou ataques terroristas. Os planos de recuperação de desastres concentram-se primordialmente em questões técnicas relacionadas à preservação do funcionamento dos sistemas, tais como os arquivos que devem ter backup e a manutenção de sistemas de computador reservas ou de serviços de recuperação de desastres.

A MasterCard, por exemplo, possui um centro de informática duplicado em Kansas City, Missouri, que pode servir como reserva de emergência para seu centro de informática ‘oficial’, localizado em St. Louis. Em vez de construir sua própria infraestrutura de reserva, muitas empresas contratam companhias especializadas em recuperação de desastres, como a Comdisco Disaster Recovery Services, de Rosemont, Illinois, e a SunGard, sediada em Wayne, Pensilvânia. Essas empresas oferecem *hot sites*, centros que abrigam computadores sobressalentes em vários pontos do território norte-americano, onde as empresas assinantes do serviço podem rodar os seus principais aplicativos em caso de emergência. A Champion Technologies, por exemplo, que fornece produtos químicos utilizados em operações de petróleo e gás, consegue mudar seus negócios de Houston para um local seguro da SunGard em Scottsdale, no Arizona, em apenas duas horas.

O **plano de continuidade dos negócios** concentra-se em como a empresa pode restaurar suas operações após um desastre. O plano de continuidade dos negócios identifica os processos de negócio críticos e determina planos de ação para lidar com funções essenciais caso os sistemas saiam do ar. O Deutsche Bank, por exemplo, que oferece investimento bancário e serviços de gestão de ativos para 74 países diferentes, possui um sólido plano de

continuidade de negócios frequentemente atualizado e aprimorado. Ele mantém equipes em tempo integral em Cingapura, Hong Kong, Japão, Índia e Austrália para coordenar planos que lidem com perdas de instalações, pessoas ou sistemas críticos de modo que a empresa possa continuar a operar quando ocorre um evento catastrófico. O plano do Deutsche Bank faz distinção entre processos críticos para sobrevivência do negócio e aqueles críticos para que tolere a crise e está coordenado com o plano de recuperação de desastres para seus centros computacionais.

Os administradores do negócio e os especialistas em tecnologia de informação precisam trabalhar juntos nesses dois tipos de plano, para determinar quais sistemas e processos de negócio são mais importantes para a empresa. Eles precisam conduzir uma análise de impacto nos negócios, a fim de identificar os sistemas mais importantes da empresa e o impacto que uma suspensão em seu funcionamento teria nos negócios. A administração precisa determinar o período máximo que a empresa pode sobreviver sem seus sistemas e quais partes dela precisam ser restauradas primeiro.

O papel da auditoria

Como a administração sabe que os controles de seus sistemas de informação são eficientes? Para responder a essa pergunta, ela deve realizar auditorias abrangentes e sistemáticas. Uma **auditoria de sistemas** avalia o sistema geral de segurança da empresa e identifica todos os controles que governam sistemas individuais de informação. O auditor deve monitorar o fluxo de uma amostra de transações através do sistema e, caso necessário, realizar testes usando software de auditoria automatizada. A auditoria de sistemas também pode avaliar a qualidade dos dados.

As auditorias de segurança devem rever tecnologias, procedimentos, documentação, treinamento e recursos humanos. Uma auditoria completa 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.

A auditoria lista e classifica todos os pontos fracos do controle e estima a probabilidade de ocorrerem erros nesses pontos. Avalia então o impacto financeiro e organizacional de cada ameaça. A Figura 7.4, um exemplo da listagem feita por um auditor, mostra as deficiências verificadas no controle de um sistema de empréstimo. O documento inclui uma seção para notificar a administração de tais deficiências e para a sua devida resposta. Espera-se que a administração elabore um plano para combater os problemas mais significativos.

Figura 7.4

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	
Natureza e impacto das deficiências	Chance de erro substancial			Notificação à administração	
	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 razoabilidade 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 <i>status</i> de produção temporária.			

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Existe uma gama de ferramentas e tecnologias para ajudar as empresas a salvaguardar seus sistemas e dados. Entre elas estão ferramentas e tecnologias para segurança de dados e sistemas, garantia de disponibilidade de sistemas e garantia da qualidade de software.

Controle de acesso

Por **controle de acesso** entende-se todo o conjunto de políticas e procedimentos que uma empresa usa para evitar acesso indevido a seus sistemas por pessoas não autorizadas dentro e fora da organização. Para obter acesso, o usuário precisa ser autorizado e autenticado. **Autenticação** refere-se à capacidade de saber que uma pessoa é quem declara ser. Um software de controle de acesso é elaborado para garantir que, por meio de algum tipo de autenticação, somente usuários autorizados usem os sistemas ou acessem os dados.

A autenticação geralmente é estabelecida pelo uso de senhas conhecidas apenas por usuários autorizados. O usuário final usa uma senha para ‘logar-se’ ao sistema de computador e também pode usar senhas para acessar sistemas ou arquivos específicos. Muitas vezes, porém, os usuários esquecem senhas, revelam-nas para outras pessoas ou escolhem senhas inadequadas, fáceis de adivinhar; isso compromete a segurança. Sistemas de senha excessivamente rigorosos tolhem a produtividade do funcionário. Quando os funcionários precisam alterar senhas complexas com muita frequência, acabam utilizando atalhos, como escolher senhas fáceis de adivinhar ou escrever a senha em suas estações de trabalho, à vista de todos. Senhas também podem ser ‘sniffed’ (‘farejadas’) quando transmitidas por rede, ou roubadas por meio da engenharia social.

Novas tecnologias de autenticação, como tokens, smart cards e autenticação biométrica, resolvem alguns desses problemas. **Token** é um dispositivo físico, parecido com um cartão de identificação, projetado para provar a identidade do usuário. Os tokens são pequenos dispositivos com visor ou que se encaixam em uma porta USB e exibem senhas que mudam a toda hora. Já um **smart card** é um dispositivo com tamanho aproximado de um cartão de crédito; ele contém um chip formatado com a permissão de acesso e outros dados. (Smart cards também são utilizados em sistemas de pagamento eletrônico.) Após interpretar os dados do smart card, o dispositivo leitor permite ou nega acesso.

A **autenticação biométrica** usa sistemas que leem e interpretam traços humanos individuais, como impressões digitais, íris e vozes, para conceder ou negar acesso. A autenticação biométrica fundamenta-se na medição de um traço físico ou comportamental que torna cada indivíduo único. Ela compara as características exclusivas de uma pessoa, tais como as impressões digitais, o rosto ou a imagem da retina, com um conjunto de perfis armazenados, determinando se existe alguma diferença entre elas e o perfil armazenado. Se os dois perfis ‘baterem’, o acesso será concedido. As tecnologias de reconhecimento de impressões digitais e face estão apenas começando a ser usadas para aplicações de segurança. Os laptops estão começando a ser equipados com dispositivos de identificação de impressões digitais.

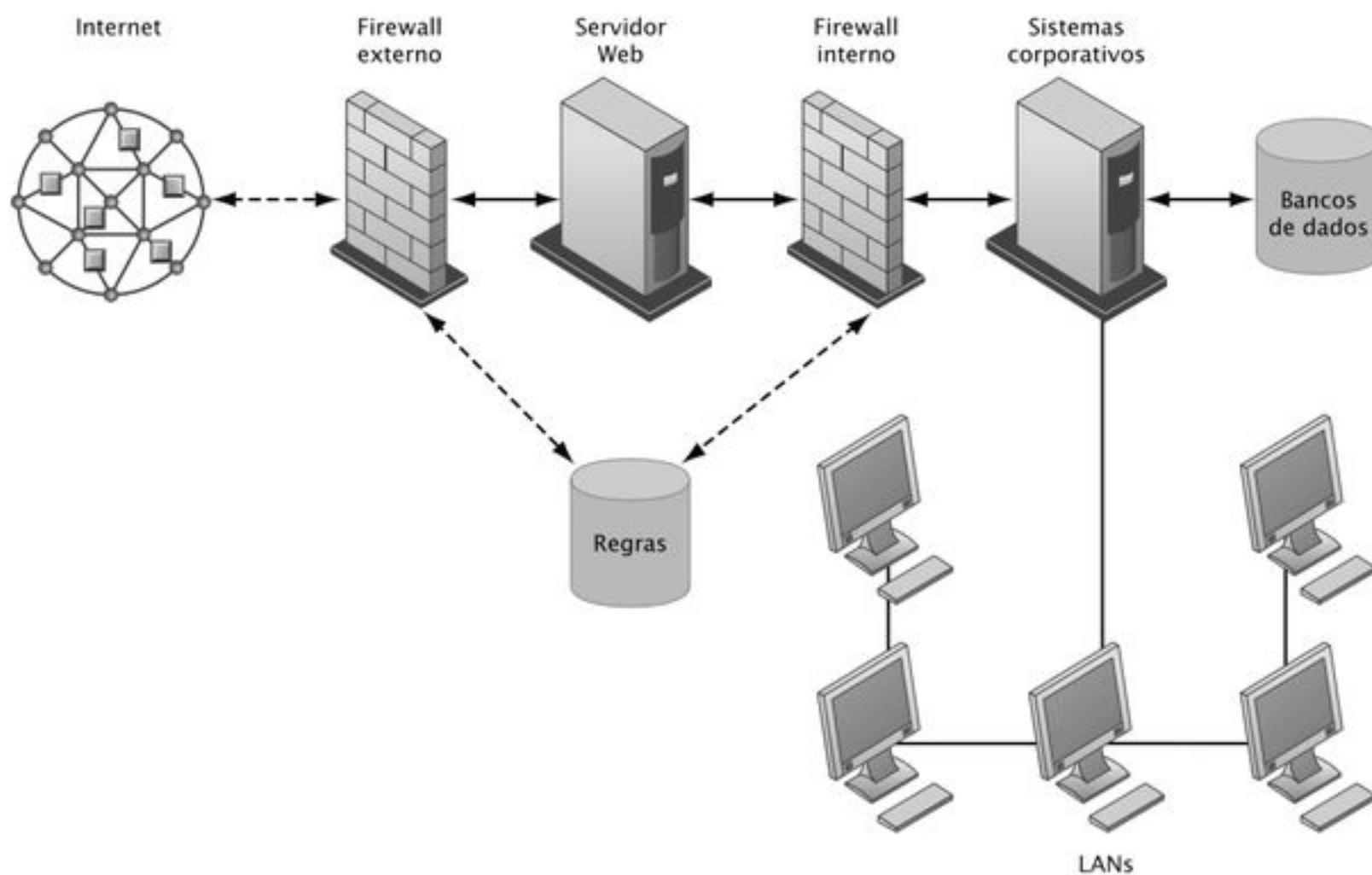
Firewalls, sistemas de detecção de invasão e softwares antivírus

Sem proteção contra *malware* e intrusos, a conexão com a Internet seria muito perigosa. Firewalls, sistemas de detecção de invasão e softwares antivírus se tornaram ferramentas empresariais essenciais.

Firewalls

Firewalls impedem que usuários não autorizados acessem redes privadas. Firewall é uma combinação de hardware e software que controla o fluxo de tráfego que entra na rede ou sai dela. Geralmente é instalado entre as redes internas da empresa e as redes externas, como a Internet, embora possa também ser usado para proteger parte de uma rede da empresa do resto da rede (veja a Figura 7.5).

O firewall age como um porteiro que examina as credenciais de cada usuário antes que ele possa acessar a rede. O firewall identifica nomes, endereços IP, aplicativos e outras



características do tráfego de entrada. Em seguida, compara essas informações com as regras de acesso que foram programadas no sistema pelo administrador da rede. Impede, então, que comunicações não autorizadas entrem na rede ou saiam dela.

Em grandes organizações, o firewall muitas vezes reside em um computador reservado especialmente para ele, separado do resto da rede, de maneira que nenhuma solicitação possa entrar e acessar diretamente os recursos da rede privada. Os firewalls usam diferentes tecnologias de inspeção, incluindo a filtragem de pacotes estáticos, a inspeção de pacotes SPI (*stateful packet inspection*), a Network Address Translation (Tradução de Endereços IP) e a filtragem de aplicação proxy. As técnicas a seguir são usadas em conjunto para fornecer a proteção de firewall.

A *filtragem de pacotes* examina campos selecionados nos cabeçalhos dos pacotes de dados que fluem de lá para cá entre a rede confiável e a Internet, examinando isoladamente pacotes individuais. No entanto, essa tecnologia de filtragem pode deixar passar muitos tipos de ataque. A *inspeção de pacotes SPI* oferece mais segurança, na medida em que determina se os pacotes fazem parte de um diálogo corrente entre um emissor e um receptor. Ela monta tabelas de *status* para monitorar as informações de múltiplos pacotes. Os pacotes serão aceitos caso façam parte de um diálogo aprovado ou estejam tentando estabelecer uma conexão legítima.

A *Network Address Translation (NAT)* pode oferecer uma camada extra de proteção quando a filtragem de pacotes estáticos e a inspeção de pacotes SPI estiverem sendo usadas. A NAT pode ocultar os endereços IP do(s) computador(es) hospedeiro(s) interno(s) da organização, evitando assim que programas *sniffer* fora do firewall os descubram e usem essa informação para penetrar nos sistemas internos.

A *filtragem de aplicação proxy* examina o conteúdo de aplicação dos pacotes. Um servidor proxy detém os pacotes de dados que se originam fora da organização, inspeciona tais pacotes e, em seguida, passa um proxy (que significa ‘procurador’, ‘representante’) para o outro lado do firewall. Quando um usuário externo quer comunicar-se com um usuário da empresa, primeiramente ‘conversa’ com a aplicação proxy, e esta se comunica com o computador interno. Da mesma maneira, um usuário de computador interno passa pelo proxy para ‘conversar’ com computadores fora da organização.

Figura 7.5

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.

A fim de criar um bom firewall, alguém tem de escrever e manter as regras internas para identificar pessoas, aplicações ou endereços permitidos ou rejeitados, com os mínimos detalhes. Como podem inibir — embora não impeçam completamente — a invasão da rede por estranhos, os firewalls devem ser vistos como um dos elementos do plano geral de segurança.

Sistemas de detecção de invasão

Além de firewalls, fornecedores de segurança comercial agora oferecem ferramentas e serviços de detecção de intrusos que protegem a empresa contra o tráfego de rede suspeito e tentativas de acesso a arquivos e bancos de dados. **Sistemas de detecção de invasão** são ferramentas de monitoração continua instaladas nos pontos mais vulneráveis ('mais quentes') de redes corporativas, a fim de detectar e inibir invasores. O sistema emite um alarme quando encontra um evento suspeito ou anômalo. Um software de varredura procura padrões indicativos de métodos conhecidos de ataque, como senhas erradas, verifica se foram removidos ou modificados arquivos importantes e envia alertas de vandalismo ou de erros de administração de sistema. O outro componente do sistema, um software de monitoração, examina os eventos em tempo real, em busca de ataques à segurança em curso. A ferramenta de detecção de invasão também pode ser customizada para isolar uma parte sensível de uma rede, caso receba tráfego não autorizado.

Software antivírus e antispyware

Planos de tecnologia defensiva, sejam residenciais ou empresariais, precisam incluir proteção antivírus para todos os computadores. O **software antivírus** é projetado para verificar sistemas de informação e drives, a fim de detectar a presença de vírus de computador. Muitas vezes o software pode eliminar o vírus da área infectada. Todavia, a maioria dos softwares antivírus somente é efetiva contra espécies que já eram conhecidas quando foram programados — por isso, para permanecer eficiente, o software antivírus deve ser continuamente atualizado. Softwares antivírus estão disponíveis para os mais diferentes tipos de dispositivos móveis e portáteis, além de servidores, estações de trabalho e PCs desktop.

Os principais fornecedores de software antivírus — como Avira, McAfee, Symantec e Trend Micro — aprimoraram seus produtos para incluir proteção contra *spyware*. Ferramentas de software antispyware como Ad-Aware, Spybot S&D, e Spyware Doctor também são muito úteis.

Sistemas unificados de gestão de ameaças

Para ajudar as empresas a reduzir os custos e melhorar sua administração, fornecedores de produtos de segurança combinaram diversas ferramentas de segurança em uma única aplicação que inclui firewalls, redes virtuais privadas, sistemas de detecção de invasão, filtragem de conteúdo da Web e software antispam. Esses abrangentes produtos para gestão da segurança são chamados de **sistemas unificados de gestão de ameaças** (*unified threat management – UTM*). Embora originalmente criados para as pequenas e médias empresas, os produtos UTM estão disponíveis para todos os tamanhos de rede. Entre os principais fornecedores de sistemas UTM estão Crossbeam, Fortinet e Check Point, e fornecedores de redes como a Cisco Systems e a Juniper Networks oferecem alguns recursos UTM em seus equipamentos.

Segurança em redes sem fio

Apesar de suas falhas, o protocolo WEP (*Wired Equivalent Privacy*) oferece alguma margem de segurança se os usuários de Wi-Fi se lembrarem de ativá-lo. Um primeiro passo simples na prevenção do ataque de hackers é atribuir um nome único ao SSID de sua rede e configurar o roteador para não transmiti-lo. As empresas podem aumentar a segurança do WEP utilizando-o em conjunto com a tecnologia de rede privada virtual (VPN), nos casos em que a rede sem fio tenha acesso aos dados corporativos internos.

Em junho de 2004, o grupo setorial denominado Wi-Fi Alliance finalizou a especificação 802.11i (também conhecida como *Wi-Fi Protected Access 2* ou WP2), que 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 autenti-

cação criptografado com um servidor de autenticação para garantir que somente usuários autorizados acessem a rede.

Criptografia e infraestrutura de chave pública

Muitas organizações usam a criptografia para proteger as informações digitais que elas armazenam, transferem fisicamente ou enviam pela Internet. **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. Os dados são criptografados por meio de um código numérico secreto, denominado chave criptográfica, que transforma dados comuns em texto cifrado. Para ser lida, a mensagem deve ser decriptografada pelo destinatário.

Podemos citar dois métodos para criptografar o tráfego de rede: o SSL e o S-HTTP. O **Secure Sockets Layer (SSL)** e o seu sucessor, o **Transport Layer Security (TLS)**, permitem que computadores clientes e servidores administrem as atividades de criptografia e decriptografia à medida que se comunicam entre si durante uma sessão da Web segura. O **Secure Hypertext Transfer Protocol (S-HTTP)** é outro protocolo usado para criptografar os dados que fluem pela Internet, mas ele só consegue lidar com mensagens individuais, enquanto o SSL e o TLS são projetados para estabelecer uma conexão segura entre dois computadores.

Embutida no software navegador do cliente da Internet e nos servidores, a função que gera sessões seguras é executada automaticamente, com pouca intervenção do usuário. O cliente e o servidor negociam qual chave e qual nível de segurança serão utilizados. Uma vez que se estabeleça uma sessão segura entre cliente e servidor, todas as mensagens dessa sessão serão criptografadas.

Existem ainda dois outros métodos de criptografia: a criptografia de chave simétrica e a criptografia de chave pública. Na **criptografia de chave simétrica**, para estabelecer uma sessão de Internet segura, o remetente e o destinatário criam uma única chave criptográfica, enviada ao destinatário; assim, este e o remetente compartilham a mesma chave. Quanto maior for o comprimento em bits dessa chave, mais segura ela será. Atualmente, uma chave típica tem 128 bits (um conjunto de 128 dígitos binários).

O problema comum a todos os esquemas de criptografia simétrica é que a chave precisa ser compartilhada de algum modo entre remetente e destinatário, deixando-a exposta a invasores que podem interceptá-la e decriptográfi-la. Uma forma mais segura de criptografia, denominada **criptografia de chave pública**, usa duas chaves: uma compartilhada (ou pública) e outra totalmente privada, como ilustrado na Figura 7.6. 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 decriptográfi-la.

Certificados digitais são arquivos de dados usados para determinar a identidade de pessoas e ativos eletrônicos, a fim de proteger transações on-line (veja a Figura 7.7). Um certificado digital usa uma terceira parte fidedigna, conhecida como autoridade certificadora (*Certificate Authority — CA*), para validar a identidade de um usuário. Existem muitas CAs nos Estados Unidos e no mundo todo, tais como VeriSign, IdenTrust e KeyPost, da Austrália.

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. O certificado autentica que a chave

Figura 7.6

Criptografia de chave pública

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 decriptografar os dados e ler o conteúdo.



Figura 7.7**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.



pública pertence ao proprietário designado. A CA disponibiliza publicamente a sua própria chave pública em meio impresso, ou às vezes na Internet. O destinatário da mensagem criptografada usa, então, a chave pública da CA para decodificar o certificado digital anexo à mensagem, verifica se ele foi emitido mesmo pela CA e por fim obtém a chave pública do remetente e a informação de identificação contida no certificado. Usando essa informação, o destinatário pode enviar uma resposta criptografada. O sistema de certificado digital capacita, por exemplo, um usuário de cartão de crédito e um comerciante a validar, antes de trocar seus dados, que seus certificados digitais foram emitidos por uma terceira parte autorizada e fidedigna. A **infraestrutura de chave pública (public key infrastructure — PKI)**, isto é, o uso da criptografia de chave pública em conjunto com uma autoridade certificadora, é amplamente utilizada no comércio eletrônico.

Como assegurar a disponibilidade do sistema

À medida que a receita e as operações dependem cada vez mais de redes digitais, as empresas precisam tomar medidas adicionais para assegurar que seus sistemas e aplicativos estejam sempre disponíveis. Instituições financeiras, companhias aéreas e outras empresas cujas aplicações críticas requerem processamento de transação on-line há muitos anos usam sistemas de informação tolerantes a falhas, para garantir cem por cento de disponibilidade. No **processamento de transação on-line**, as transações registradas on-line são imediatamente processadas pelo computador. A cada instante ocorrem alterações nos bancos de dados, relatórios ou requisições.

Os **sistemas de computação tolerantes a falhas** incluem componentes redundantes de hardware, software e fornecimento de energia elétrica, criando um ambiente que oferece serviço contínuo, ininterrupto. Computadores tolerantes a falhas contêm chips de memória, processadores e dispositivos de armazenagem de discos extras, que fazem o backup do sistema e o mantêm em funcionamento para evitar falhas. Além disso, as peças desses computadores podem ser removidas e consertadas sem causar dano ao sistema.

Não se deve confundir tolerância a falhas com **computação de alta disponibilidade**. Tanto a tolerância a falhas quanto a computação de alta disponibilidade tentam minimizar o *downtime*. **Downtime** é o termo usado para designar os períodos em que um sistema não está operante. Entretanto, a computação de alta disponibilidade ajuda as empresas a se

recuperar rapidamente de uma parada de sistema, enquanto a tolerância a falhas promete disponibilidade contínua e eliminar todo o tempo de recuperação.

Ambientes de computação de alta disponibilidade são requisito mínimo para empresas com alto volume de processamento em comércio eletrônico ou para as que dependem de redes digitais a suas operações internas. A computação de alta disponibilidade requer servidores de reserva, distribuição do processamento entre múltiplos servidores, alta capacidade de armazenamento e bons planos de recuperação de desastres e de continuidade dos negócios. A plataforma de computação da organização precisa ser extremamente robusta, com largura de banda, armazenamento e capacidade de processamento escaláveis.

Os pesquisadores estão explorando maneiras de fazer os sistemas de computação recuperar-se ainda mais rapidamente após incidentes — uma abordagem denominada **computação orientada a recuperação**. Esse trabalho inclui projeto de sistemas que se restabeleçam de forma rápida, assim como a implantação de recursos e ferramentas que ajudem os operadores a descobrir as fontes de falhas em sistemas compostos por múltiplos componentes, podendo corrigir os erros de modo mais fácil.

Controle do tráfego de rede: inspeção profunda de pacotes

Já tentou utilizar, em uma universidade, uma rede de campus e achou seu desempenho muito lento? Pode ser porque os alunos utilizam a rede para baixar músicas ou acessar o YouTube. Aplicações que consomem a largura de banda, como os programas de compartilhamento de arquivos, serviços de telefonia pela Internet e vídeo on-line, conseguem obstruir e desacelerar as redes corporativas, diminuindo o desempenho. A Ball State University, em Muncie, Indiana, por exemplo, descobriu que sua rede estava lenta porque uma pequena quantidade de alunos utilizava programas P2P de compartilhamento de arquivos para baixar músicas e vídeos.

Uma tecnologia denominada **inspeção profunda de pacotes (deep packet inspection – DPI)** ajuda a resolver esse problema. Essa inspeção examina os arquivos de dados e organiza o material on-line de baixa prioridade enquanto atribui alta prioridade aos arquivos de negócios críticos. Com base nas prioridades estabelecidas por um operador de rede, a inspeção decide se um pacote específico de dados pode continuar rumo a seu destino ou deve ser bloqueado ou atrasado enquanto o tráfego mais importante segue adiante. Utilizando sistema DPI da Allot Communications, a Ball State conseguiu identificar o volume de tráfego referente ao compartilhamento de arquivos e atribui-lhe uma prioridade bem baixa. O tráfego prioritário para a Ball State foi, assim, acelerado.

Outsourcing da segurança

Muitas empresas, especialmente as pequenas, não possuem os recursos e o conhecimento técnico necessários para criar, por conta própria, ambiente de computação seguro e de alta disponibilidade. Nesse caso, elas podem terceirizar muitas funções de segurança para **provedores de serviços de segurança gerenciada (MSSPs)**, que monitoram as atividades da rede e realizam testes de vulnerabilidade e detecção de invasões. VeriSign e Symantec são provedores líderes de serviços MSSP.

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

Embora a computação em nuvem e a plataforma digital móvel emergente possuam o potencial para distribuir benefícios poderosos, elas representam novos desafios para segurança dos sistemas e confiabilidade. Descrevemos agora alguns desses desafios e como devem ser tratados.

Segurança na nuvem

Quando o processamento acontece na nuvem, a responsabilidade pela proteção de dados sensíveis ainda pertence à empresa proprietária dos dados. É essencial que se compreenda como o provedor de computação em nuvem organiza seus serviços e gerencia os dados. A Seção Interativa sobre tecnologia detalha algumas questões de segurança da nuvem que devem ser consideradas.

SEÇÃO INTERATIVA: TECNOLOGIA

Quão segura é a nuvem?

A empresa de investimentos bancários e serviços financeiros Cowen and Co., com sede em Nova York, transferiu seus sistemas de vendas para a nuvem por meio da Salesforce.com. Até agora, Daniel Flax, CIO da empresa, está satisfeito. A utilização de serviços da nuvem ajudou a Cowen a diminuir os gastos iniciais com tecnologia, diminuir o downtime, e oferecer serviços adicionais. Contudo, ele está tentando lidar com as questões de segurança. A segurança na computação em nuvem é, de fato, turva, e essa falta de transparência é preocupante para muitos. Um dos maiores riscos da computação em nuvem é que ela é altamente distribuída. Aplicações da nuvem e combinações de aplicações residem em bibliotecas virtuais de grandes centros de dados remotos e em fazendas de servidores que oferecem serviços empresariais e gestão de dados para diversos clientes corporativos. Para economizar dinheiro e manter os custos baixos, os provedores de computação em nuvem costumam distribuir o trabalho por centros de dados ao redor do mundo onde o trabalho pode ser executado de modo mais eficiente. Quando você usa a nuvem, pode não saber ao certo onde seus dados estão hospedados, nem sequer saber o país onde eles estão armazenados.

A natureza dispersa da computação em nuvem dificulta o rastreamento de atividades não autorizadas. Quase todos os provedores de nuvem utilizam criptografia como SSL (secure sockets layer) para proteger os dados que gerenciam enquanto são transmitidos. Mas, se os dados estão armazenados em dispositivos que também guardam arquivos de outras empresas, é importante garantir que esses dados também são criptografados.

Indian Harvest Specialtfoods, uma empresa de Bemidji, Minnesota, que distribui arroz, grãos e legumes para restaurantes de todo o mundo, utiliza o provedor de software para nuvem NetSuite a fim de garantir que seus dados enviados à nuvem estejam totalmente protegidos. Mike Mullin, diretor de TI da empresa, diz que utilizar SSL para criptografar os dados lhe confere certo nível de certeza de que os dados estão seguros. Ele também observa que sua empresa e outros usuários dos serviços da nuvem precisam estar atentos a suas próprias práticas de segurança, em especial aos controles de acesso. "Seu lado da infraestrutura é tão vulnerável, senão mais, quanto o lado do provedor", comenta ele.

Uma maneira de lidar com esses problemas é usar um fornecedor de nuvem que seja uma empresa pública, obrigada por lei a informar como gerencia as informações. A Salesforce.com é uma empresa desse tipo, com processos e diretrizes estritos para a gestão de seus centros de dados. "Sabemos que nossos arquivos estão nos Estados Unidos e sabemos exatamente em qual centro de dados estão localizados", diz Flax.

Outra alternativa é utilizar um provedor de nuvem que ofereça aos assinantes a possibilidade de escolher onde será realizado o trabalho de computação em nuvem. Terremark Worldwide Inc., por exemplo,

oferece a um de seus assinantes, a Agora Games, a opção de escolher onde suas aplicações vão funcionar. A Terremark possui instalações em Miami, mas está abrindo outras unidades. No passado, a Agora não tinha como escolher onde a Terremark hospedaria suas aplicações e seus dados.

Mesmo que seus dados estejam totalmente seguros na nuvem, pode ser que você não consiga provar. Alguns provedores de nuvem não atendem aos atuais requisitos de conformidade relacionados à segurança, e alguns desses provedores, como a Amazon, já afirmaram que não pretendem seguir essas regras e não irão permitir auditorias locais.

Existem regras que restringem onde as empresas podem enviar e armazenar alguns tipos de informação — informações pessoalmente identificáveis na União Europeia, trabalho do governo nos Estados Unidos, ou aplicações que utilizem determinados algoritmos de criptografia. Seja nos Estados Unidos ou na União Europeia, as empresas das quais se exige o cumprimento dessas regras relacionadas à proteção de dados não poderão utilizar provedores públicos de nuvem.

Algumas dessas regras exigem provas de que os sistemas são gerenciados de modo seguro, o que pode demandar confirmação por parte de uma auditoria independente. É possível que os grandes provedores de nuvem não permitam que auditores de outra empresa inspecionem seus centros de dados. A Microsoft encontrou uma maneira interessante de lidar com esse problema. A empresa reduziu 26 tipos diferentes de auditoria a uma lista de 200 controles necessários para cumprimento dos padrões de conformidade aplicados aos ambientes e serviços de seus centros de dados. A Microsoft não permite o acesso de todos os clientes ou auditores aos centros de dados, mas sua estrutura de conformidade permite que auditores selecionem testes a partir de uma lista e recebam seus resultados.

As empresas esperam que seus sistemas funcionem em tempo integral, mas os provedores de nuvem nem sempre conseguem oferecer esse nível de serviço. Milhões de consumidores da Salesforce.com sofreram 38 minutos de pane no início de janeiro de 2009 e outras paradas alguns anos antes. A parada de janeiro de 2009 impediu que mais de 900 mil assinantes acessassem aplicações e dados cruciais para transações empresariais com seus clientes. Usuários dos serviços de nuvem da Amazon vivenciaram inúmeras quedas em 2008. (Em julho de 2008, o serviço ficou interrompido por oito horas.)

Acordos para serviços como o Amazon EC2 e o Microsoft Azure definem que essas empresas não podem ser responsabilizadas por perdas de dados, multas ou outras penalidades legais quando as empresas usam seus serviços. Ambos os fornecedores oferecem instruções sobre como usar suas plataformas de nuvem de modo seguro, e ainda podem proteger seus dados de maneira mais segura do que as instalações locais.

A Salesforce.com vem construindo e replanejando sua infraestrutura para garantir serviços melhores. A empresa investiu 50 milhões de dólares na tecnologia Mirrorforce, um sistema de espelhamento que cria um banco de dados duplicado em um local separado e sincroniza instantaneamente os dados. Se um banco de dados não estiver disponível, o outro assume seu lugar. A Salesforce.com abriu dois novos centros de dados nas Costas Leste e Oeste, além de suas instalações no Vale

do Silício. A empresa distribuiu por esses centros o processamento de seus grandes clientes de modo a balançar a carga de seu banco de dados.

Fontes: John Edwards, "Cutting Through the Fog of Cloud Security". *Computerworld*, 23 fev. 2009; Wayne Rash, "Is Cloud Computing Secure? Prove It". *eWeek*, 21 set. 2009; Robert Lemos, "Five Lessons from Microsoft on Cloud Security". *Computerworld*, 25 ago. 2009; Mike Fratto, "Cloud Control". *Information Week*, 26 jan. 2009.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. Que problemas de segurança e controle são descritos neste caso?
2. Que fatores pessoais, organizacionais e tecnológicos contribuem para esse problema?
3. Quão segura é a computação em nuvem? Explique.
4. Se fosse responsável pelo departamento de sistemas de informação de uma empresa, quais pontos gostaria de esclarecer com os possíveis fornecedores?
5. Você confiaria seus sistemas corporativos a um provedor de computação em nuvem? Justifique.

Usuários da nuvem precisam confirmar que, independentemente do local onde seus dados estejam armazenados ou para onde sejam transferidos, eles estão protegidos em um nível que atende a seus requisitos corporativos. É preciso exigir que o provedor da nuvem armazene e processe os dados em jurisdições específicas segundo as regras de privacidade da jurisdição em questão. Clientes da nuvem devem descobrir como o provedor separa os dados de sua empresa dos arquivos das outras e solicitar provas de que o mecanismo de criptografia é seguro. É importante também saber como o provedor da nuvem responde em caso de desastre: se consegue restaurar completamente os dados e quanto tempo essa operação leva. Usuários da nuvem devem questionar ainda se os provedores da nuvem são submetidos a auditorias externas e certificações de segurança. Esses tipos de controle podem ser escritos no acordo de nível de serviços (*service level agreement* — SLA) antes de contratar um provedor de nuvem.

Segurança em plataformas móveis

Malwares direcionados a dispositivos móveis não são tão comuns quanto aqueles direcionados a computadores, mas, ainda assim, estão se espalhando através de e-mail, mensagens de texto, Bluetooth e cópias de arquivos da Web por meio de redes sem fio ou celulares. Se os dispositivos móveis estão executando muitas das funções dos PCs, precisam, como os desktops e laptops, estar seguros contra *malware*, roubo, perda acidental, acesso não autorizado e tentativas de invasão. Dispositivos móveis que acessem sistemas e dados corporativos demandam proteção especial.

As empresas devem se certificar de que sua política de segurança corporativa inclui os dispositivos móveis, com detalhes adicionais sobre como esses dispositivos devem receber suporte e proteção e de que modo devem ser utilizados. As diretrizes devem estipular softwares e procedimentos necessários ao acesso remoto de sistemas corporativos. Por enquanto, a segurança dos *smartphones* não está tão bem desenvolvida quanto a dos dispositivos maiores. Esses dispositivos podem não conseguir proteger integralmente informações sensíveis, em especial os dados transmitidos via anexos de e-mail e aqueles armazenados localmente nos dispositivos.

Garantia da qualidade de software

Além de implantar segurança e controle eficientes, as empresas podem melhorar a qualidade e a confiabilidade dos sistemas através de métricas e testes rigorosos de software. Métricas de software são premissas objetivas do sistema na forma de medidas quantificadas. O uso contínuo de métricas permite que o departamento de sistemas de informação

e os usuários finais meçam conjuntamente o desempenho do sistema e identifiquem problemas à medida que eles ocorrem. Exemplos de métricas de software incluem números de transações que podem ser processadas em uma unidade específica de tempo, tempo de resposta on-line, número de cheques de pagamentos impressos por hora, e número de erros conhecidos por centenas de linhas de código. Para que as métricas sejam bem-sucedidas, precisam ser cuidadosamente definidas e devem ser formais, objetivas e usadas com consistência.

O teste inicial regular e completo também irá contribuir para a qualidade do sistema. Muitos consideram o teste uma maneira de provar a exatidão do trabalho realizado. Na verdade, sabemos que todo software, independentemente de seu tamanho, está recheado de erros que precisam de testes para serem descobertos.

O bom teste começa antes de o software sequer ser escrito através de um *acompanhamento* — uma revisão de uma especificação, ou documento de projeto, realizada por pequeno grupo de pessoas cuidadosamente selecionadas com base nas habilidades necessárias para os objetivos particulares que serão testados. Uma vez que os desenvolvedores começem a escrever os programas, podem ser utilizados acompanhamentos de codificação para que se revise o código. Entretanto, o código deve ser testado por meio de execuções do programa. Quando erros são descobertos, a fonte é identificada e eliminada através de um processo denominado *depuração*. No Capítulo 11, é possível saber mais sobre os vários estágios de testes realizados antes que um sistema de informação entre em funcionamento.

Projetos práticos em SIG

Os projetos nesta seção lhe oferecem experiência prática na análise de vulnerabilidades de segurança utilizando software de planilha eletrônica para análise de riscos e acessando ferramentas da Web para pesquisar sobre serviços de terceirização da segurança.

Problemas de decisões gerenciais

1. A K2 Network mantém sites de jogos on-line acessados por cerca de 16 milhões de pessoas em cem países. Os jogadores podem entrar gratuitamente nos jogos, mas devem comprar ‘ativos’ digitais da empresa, como espadas para lutar contra dragões, se quiserem se envolver com maior profundidade. Os jogos conseguem acomodar milhões de jogadores ao mesmo tempo e são jogados simultaneamente por pessoas em todas as partes do mundo. Prepare uma análise de segurança para esse negócio. Que tipos de ameaças devem ser antecipados? Qual seria o impacto desse negócio? Que medidas podem ser tomadas para prevenir que aconteçam danos aos sites ou às operações contínuas?
2. Uma pesquisa sobre a infraestrutura de TI de sua empresa produziu a seguinte estatística de análise de segurança:

Entre as fragilidades de alto risco estão o acesso às aplicações por usuários não autorizados, senhas previsíveis, nomes de usuários idênticos às senhas, contas ativas de usuários sem senha e existência de programas não autorizados nos sistemas aplicativos. Entre as fragilidades de médio risco, a possibilidade de os usuários desligarem o sistema sem se conectarem, configurações de senhas e protetores de tela que não foram definidas para PCs, além de versões desatualizadas de software que permanecem armazenadas no disco rígido. Entre as fragilidades de baixo risco, a impossibilidade de os usuários modificarem suas senhas, utilização de senhas que não são alteradas periodicamente e senhas menores do que o tamanho mínimo especificado pela empresa.

Vulnerabilidades de segurança por tipo de plataforma computacional

<u>Plataforma</u>	<u>Número de computadores</u>	<u>Alto risco</u>	<u>Risco médio</u>	<u>Baixo risco</u>	<u>Total de vulnerabilidades</u>
Windows Server (aplicações corporativas)	1	11	37	19	
Windows 7 Enterprise (administradores de alto nível)	3	56	242	87	
Linux (serviços de e-mail e impressão)	1	3	154	98	
Sun Solaris (UNIX) (servidores de e-commerce e Web)	2	12	299	78	
Windows 7 Enterprise, usuários de desktops e laptops com ferramentas de produtividade de escritório que também podem ser conectadas a redes corporativas rodando aplicações corporativas e provendo acesso à intranet	195	14	16	1.237	

- Calcule o número total de vulnerabilidades de cada plataforma. Qual o impacto potencial dos problemas de segurança de cada plataforma computacional?
- Se você conta somente com um especialista em sistemas de informação responsável pela segurança, quais plataformas deve considerar primeiro na tentativa de eliminar essas vulnerabilidades? Seguindo a ordem, quais seriam as plataformas seguintes?
- Identifique os tipos de problemas de controle ilustrados por essas vulnerabilidades e explique as medidas a serem tomadas para resolvê-los.
- Ao ignorar as vulnerabilidades de segurança identificadas, o que sua empresa arrisca?

Aperfeiçoando a tomada de decisão: usando software de planilha eletrônica para realizar uma avaliação de risco de segurança

Habilidades de software: fórmulas de planilhas e gráficos

Habilidades organizacionais: avaliação de risco

Este projeto utiliza software de planilha eletrônica para calcular as perdas anuais estimadas causadas por diversas ameaças à segurança identificadas para uma pequena empresa.

A Mercer Paints é uma pequena, porém renomada, fabricante de tintas do Alabama. A empresa possui rede que conecta várias de suas operações. Embora acredite que a segurança seja adequada, a recente implantação de um site tornou-se um convite a *hackers*. A administração solicitou, então, uma avaliação de risco, que identificou uma série de ameaças potenciais. Essas ameaças, as probabilidades associadas a elas e seus prejuízos médios são resumidos na tabela a seguir.

Avaliação de risco da Mercer Paints

Risco	Probabilidade de ocorrência (%)	Prejuízo médio (\$)
Ataque de malware	60	75.000
Perda de dados	12	70.000
Desvio de dinheiro	3	30.000
Erros de usuário	95	25.000
Ameaças de hackers	95	90.000
Uso indevido por parte de funcionários	5	5.000
Falta de energia	15	300.000

- Além dos riscos enumerados, você precisa identificar pelo menos três outras ameaças potenciais à Mercer Paints, atribuir-lhes probabilidades e estimar uma faixa de prejuízo.
- Usando software de planilha e os dados da avaliação de risco, calcule o prejuízo anual esperado para cada risco.
- Apresente suas conclusões na forma de gráfico. Quais pontos de controle estão mais vulneráveis? Quais recomendações você faria à Mercer Paints? Prepare um relatório por escrito que resuma suas conclusões e recomendações.

Aperfeiçoando a tomada de decisão: avaliando serviços de terceirização de segurança

Habilidades de software: navegador Web e software de apresentação

Habilidades empresariais: avaliação de serviços de terceirização

Atualmente, as empresas têm a opção de terceirizar suas funções de segurança ou manter sua própria equipe interna para esse fim. Este projeto lhe ajudará a desenvolver suas habilidades de Internet na utilização da rede para pesquisar e avaliar serviços de terceirização de segurança.

Como especialista em sistemas de informação de sua empresa, você foi encarregado de ajudar os gerentes a decidir sobre a terceirização da segurança ou a manutenção da função de segurança dentro da organização. Pesquise na Web para encontrar informações que lhe ajudem a decidir sobre a terceirização da segurança e a localizar serviços terceirizados de segurança.

- Apresente um breve resumo dos argumentos contra e a favor do *outsourcing* da segurança em informática.
- Selecione duas empresas que ofereçam esse tipo de serviço, comparando as empresas e seus serviços.
- Prepare uma recomendação por escrito à administração indicando por que acredita que deveriam optar (ou não) pelo *outsourcing* da segurança e qual das duas empresas acha que deveriam selecionar caso decidissem terceirizar.

Resumo

1. Por que os sistemas de informação precisam de proteção especial contra destruição, erros e uso indevido? Dados digitais estão vulneráveis a destruição, uso indevido,

erro, fraude e falhas de software e hardware. A Internet foi projetada para ser um sistema aberto, por isso deixa os sistemas corporativos internos mais vulneráveis a ações de inva-

sores. Hackers podem desencadear ataques de recusa de serviço (DoS) ou invadir redes corporativas, causando sérios prejuízos aos sistemas. As redes de Wi-Fi podem facilmente ser penetradas por invasores com programas sniffer, que obtêm um endereço e, assim, acessam os recursos da rede. Os vírus de computador e worms podem desabilitar sistemas e sites. A natureza dispersa da computação em nuvem dificulta o rastreamento de atividades não autorizadas ou a aplicação de controles a distância. Os softwares também apresentam problemas, pois as vulnerabilidades do software podem ser exploradas por hackers e softwares mal-intencionados. Por fim, os usuários finais também acabam introduzindo erros.

2. Qual o valor empresarial da segurança e do controle? Falta de segurança e controle sólidos pode fazer com que as empresas que dependem de sistemas computacionais para as suas funções empresariais vitais percam vendas e produtividade. Ativos de informação — registros confidenciais sobre funcionários, segredos comerciais ou planos de negócios, por exemplo — perdem muito de seu valor se forem revelados para pessoas de fora da organização. Além disso, sua revelação expõe a empresa a riscos legais. Novas leis, como a Lei HIPAA, a Lei Sarbanes-Oxley e a Lei Gramm-Leach-Bliley, exigem que as empresas pratiquem uma minuciosa gestão de registros eletrônicos e que adotem rígidos padrões de segurança, privacidade e controle. A possibilidade de ações legais que exijam perícia forense computacional e provas eletrônicas também obrigam as empresas a prestar mais atenção à segurança e à gestão dos registros eletrônicos.

3. Quais os componentes de uma estrutura organizacional para segurança e controle? As empresas devem estabelecer uma adequada estrutura gerencial e organizacional para segurança e controle. Uma avaliação de risco analisa os ativos de informação, identifica pontos de controle e vulnerabilidades de controle e determina o con-

junto de controles com a melhor relação custo-benefício. As empresas também precisam desenvolver uma política de segurança corporativa coerente e planos para dar continuidade às suas operações na hipótese de desastres ou panes. A política de segurança abrange políticas para autorização e uso aceitável. Uma auditoria de sistemas metódica e abrangente ajuda as organizações a determinar a eficiência da segurança e dos controles adotados em seus sistemas de informação.

4. Quais as mais importantes tecnologias e ferramentas disponíveis para salvaguardar recursos de informação? Quando conectados à Internet, firewalls evitam que usuários não autorizados accedam a rede privada. Sistemas de detecção de invasão monitoram as redes privadas em busca de tráfego de rede suspeito ou tentativas de acessar os sistemas corporativos. Senhas, tokens, smart cards e autenticação biométrica são usados para autenticar usuários de sistemas. Softwares antivírus verificam se há infecções causadas por vírus e worms no sistema de computador e, muitas vezes, eliminam o software mal-intencionado; softwares antispyware, por sua vez, combatem programas spyware danosos e invasivos. A criptografia — isto é, a codificação e o embaralhamento de mensagens — é uma tecnologia amplamente utilizada para salvaguardar as transmissões eletrônicas realizadas por redes desprotegidas. Os certificados digitais, combinados com a criptografia de chave pública, oferecem proteção adicional às transações eletrônicas, pois autenticam a identidade do usuário. As empresas podem utilizar sistemas computacionais tolerantes a falhas ou criar ambientes computacionais de alta disponibilidade para garantir que seus sistemas de informação estejam sempre disponíveis. O uso de métricas de software e testes rigorosos ajudam a melhorar a qualidade e a confiabilidade do software.

Palavras-chave

- | | | |
|--|--|---|
| Ataque de recusa de serviço, 221 | Controle de acesso, 234 | Lei Gramm-Leach-Bliley, 228 |
| Ataque distribuído de recusa de serviço, 221 | Controles, 215 | Lei Sarbanes-Oxley, 228 |
| Ataques por SQL injection, 219 | Controles de aplicação, 229 | Malware, 218 |
| Auditória de sistemas, 233 | Controles gerais, 229 | Patches, 226 |
| Autenticação, 234 | Crimes de informática, 222 | Perícia forense computacional, 228 |
| Autenticação biométrica, 234 | Criptografia, 237 | Pharming, 223 |
| Avaliação de risco, 230 | Criptografia de chave pública, 237 | Phishing, 223 |
| Botnet, 221 | Downtime, 238 | Plano de continuidade dos negócios, 232 |
| Bugs, 226 | Engenharia social, 226 | Plano de recuperação de desastres, 232 |
| Cavalo de Troia, 219 | Evil twins, 223 | Política de uso aceitável, 231 |
| Certificados digitais, 237 | Firewalls, 234 | Política de segurança, 231 |
| Cibervandalismo, 221 | Fraude do clique, 225 | Políticas de autorização, 231 |
| Computação de alta disponibilidade, 238 | Hacker, 221 | Processamento de transação on-line, 231 |
| Computação orientada a recuperação, 239 | HIPAA, 227 | Provedores de serviços de segurança gerenciada (MSSPs), 239 |
| | Infraestrutura de chave pública (PKI), 238 | |
| | Inspeção profunda de pacotes, 239 | |
| | Key loggers, 220 | |

Roubo de identidade, 223
Secure Hypertext Transfer Protocol (S-HTTP), 237
Secure Sockets Layer (SSL), 237
 Segurança, 215
 Sistemas de computação tolerantes a falhas, 238

Sistemas de detecção de invasão, 236
 Sistemas de gestão de autorização, 231
 Sistemas unificados de gestão de ameaças, 236
 Smart card, 234
 Sniffer, 221
 Spoofing, 221

Spyware, 219
 Software antivírus, 236
 Token, 234
 Vírus de computador, 218
 War driving, 217
 Worms, 218

Questões de revisão

1. Por que os sistemas de computador são tão vulneráveis a destruição, erros e uso indevido?

- Liste e descreva as ameaças mais comuns aos sistemas de informação contemporâneos.
- Defina *malware* e descreva as diferenças entre vírus, worm e cavalo de Troia.
- Defina o que é um *hacker* e explique como ele cria problemas de segurança e causa danos ao sistema.
- Defina crime de informática. Dê dois exemplos de crimes em que os computadores sejam alvo e dois exemplos em que os computadores sejam usados como instrumento.
- Defina roubo de identidade e *phishing* e explique por que o roubo de identidade é um problema contemporâneo tão grande.
- Descreva os problemas de segurança e confiabilidade de sistemas criados por empregados.
- Explique como os defeitos de software afetam a confiabilidade e a segurança.

2. Qual o valor empresarial da segurança e do controle?

- Explique como a segurança e o controle agregam valor ao negócio.
- Descreva a relação entre segurança e controle, as recentes exigências regulatórias do governo norte-americano e a perícia forense computacional.

3. Quais os componentes de uma estrutura organizacional para segurança e controle?

- Defina controles gerais e descreva cada tipo de controle dessa categoria.

- Defina controles de aplicação e descreva cada tipo de controle dessa categoria.
- Descreva a função da avaliação de risco e explique como ela é conduzida no caso dos sistemas de informação.
- Defina e descreva o seguinte: política de segurança, política de uso aceitável e política de autorização.
- Explique como a auditoria de sistemas promove a segurança e o controle.

4. Quais as ferramentas e tecnologias mais importantes para salvaguardar os recursos de informação?

- Nomeie e descreva três métodos de autenticação.
- Descreva a função de *firewalls*, sistemas de detecção de invasão e software antivírus na promoção da segurança.
- Explique como a criptografia protege as informações.
- Descreva a função da criptografia e da certificação digital na infraestrutura de chave pública.
- Faça a distinção entre computação de alta disponibilidade e computação tolerante a falhas, e entre plano de recuperação de desastres e plano de continuidade dos negócios.
- Identifique e descreva os problemas de segurança trazidos pela computação em nuvem.
- Descreva as medidas para melhoria da qualidade e da confiabilidade de software.

Para discutir

1. Segurança não é simplesmente uma questão tecnológica, é uma questão empresarial. Discuta essa afirmação.

2. Se você tivesse de desenvolver um plano de continuidade de negócios para sua empresa, por onde começaria? Quais aspectos da organização o plano deveria abordar?

Colaboração e trabalho em equipe

Avaliando ferramentas de software de segurança

Formem um grupo de três ou quatro colegas. Usem a Web para pesquisar e avaliar produtos de segurança oferecidos por dois vendedores concorrentes. Esses produtos podem ser softwares antivírus, firewalls ou softwares antispyware, por exemplo. Descrevam os recursos de

cada produto, para quais tipos de empresa eles são mais indicados, e quais os custos de compra e instalação. Qual é o melhor produto? Por quê? Se possível, usem software de apresentação eletrônica para apresentar suas conclusões à classe.

Resolvendo problemas organizacionais

Estamos prontos para uma guerra virtual?

Para a maioria de nós, a Internet é uma ferramenta utilizada para e-mail, notícias, entretenimento, socialização e compras. Entretanto, para os especialistas em segurança de computadores afiliados a agências governamentais e fornecedores particulares, bem como para seus hackers opositores espalhados pelo mundo, a Internet transformou-se em um campo de batalha — uma zona de combate na qual a guerra virtual está se tornando mais frequente e onde as técnicas de invasão ficam cada vez mais avançadas. A guerra virtual representa um conjunto único e desanimador para os especialistas em segurança não só na detecção e prevenção de invasões, mas também no rastreamento dos invasores e na ação judicial contra eles.

A guerra virtual pode assumir muitas formas. Frequentemente, os hackers usam botnets, grandes redes de computadores que controlam graças a spyware e outros tipos de malware, para desencadear ataques DDoS em larga escala nos servidores-alvo. Existem outros métodos que permitem que os invasores acessem remotamente computadores seguros e copiem ou deletem e-mails e arquivos da máquina, ou mesmo monitorem remotamente os usuários de uma máquina utilizando softwares mais sofisticados. Para os criminosos virtuais, o benefício da guerra virtual é que eles podem competir com supercomputadores tradicionais por uma fração do custo construindo, por exemplo, um arsenal nuclear. Como a infraestrutura tecnológica irá depender cada vez mais da Internet para funcionar, os guerreiros virtuais não sofrerão com falta de alvos para atacar.

A guerra virtual também aumenta a defesa contra esses tipos de ataques. Esse é o foco principal das agências de inteligência norte-americanas. Embora os Estados Unidos estejam na linha de frente das tecnologias de guerra virtual, é improvável que mantenham a dominação tecnológica por conta do custo relativamente baixo das tecnologias necessárias para montar esses tipos de ataque.

Na verdade, hackers em todo o mundo já começaram a levar isso a sério. Em julho de 2009, 27 agências governamentais dos Estados Unidos e da Coreia do Sul, além de outras organizações, foram vítimas de um ataque DDoS. Estima-se que 65 mil computadores pertencentes a botnets estrangeiras inundaram os sites com solicitações. Dentre os sites afetados estão os pertencentes à Casa Branca, Tesouro, Comissão Federal do Comércio, Departamento de Defesa, Serviço Secreto, Bolsa de Valores de Nova York, Washington Post, além dos sites de instituições como Ministério de Defesa Coreano, Assembleia Nacional, Casa Azul presidencial, dentre outros. Os ataques não foram sofisticados, mas foram dispersos e prolongados. Eles obtiveram êxito na diminuição da velocidade de muitos sites norte-americanos e forçaram diversos sites coreanos a interromper a operação. Grupos da Coreia do Norte ou a favor do país são suspeitos de estar por trás dos ataques, mas o governo de Pyongyang negou qualquer envolvimento.

O lado positivo dos ataques é que somente essas agências foram afetadas. Entretanto, outras invasões sugerem

que os hackers já dispõem do potencial para atos muito mais perigosos de guerra virtual. A Agência Federal de Aviação, que supervisiona a atividade aérea nos Estados Unidos, já foi alvo de ataques bem-sucedidos a seus sistemas, incluindo um em 2006 que interrompeu parcialmente os sistemas aéreos no Alasca.

Em 2007 e 2008, espiões computacionais invadiram o projeto Joint Strike Fighter, do Pentágono, avaliado em 300 bilhões de dólares. Os invasores conseguiram copiar e apagar muitos terabytes de dados relacionados ao projeto e a sistemas eletrônicos que facilitaram potencialmente a defesa contra o inimigo quando produzido. Os invasores entraram através de vulnerabilidades de dois ou três fornecedores que trabalhavam no projeto do avião de caça. Felizmente, computadores que continham os dados mais sensíveis não estavam conectados à Internet e, portanto, não podiam ser acessados pelos invasores. Ex-oficiais norte-americanos dizem que esse ataque teve origem na China, e que o país progride com estabilidade no desenvolvimento de técnicas de guerra virtual. A China rebate as afirmações dizendo que, ao culpá-los, a mídia norte-americana baseia-se em um pensamento desatualizado da época da Guerra Fria. Além disso, alega que os hackers chineses não eram hábeis o suficiente para realizar um ataque daquela magnitude.

Em abril de 2009, espiões virtuais se infiltraram na rede elétrica norte-americana utilizando pontos frágeis nos quais os computadores na rede estão conectados à Internet, e deixaram para trás programas de computador com finalidades pouco claras, mas que possivelmente poderiam ser utilizados para interromper o sistema. Relatórios indicaram que os espiões partiram de computadores na China e na Rússia. Mais uma vez, ambas as nações negaram envolvimento. Em resposta a essas e outras invasões, o Congresso norte-americano está considerando uma legislação que exigiria que todas as empresas com infraestrutura crítica se adequassem a padrões de segurança mais robustos. À época de redação deste livro, a maioria das agências federais era aprovada por atender aos requisitos da Lei de Gestão de Segurança da Informação Federal, o mais recente conjunto de padrões aprovado. Entretanto, à medida que as tecnologias de guerra virtual se desenvolvem e se tornam mais avançadas, os padrões impostos pela legislação poderão se tornar insuficientes na defesa contra os ataques.

Em cada incidente da guerra virtual, os governos dos países considerados responsáveis negaram veementemente o envolvimento sem qualquer repercussão. Como isso é possível? A principal razão é que o rastreamento da identidade de invasores específicos através do cibercírculo é quase impossível, viabilizando a negação da culpa.

Embora a tarefa seja difícil o suficiente para que as agências do governo com recursos e conhecimento ataquem esses problemas, dois grupos — Information Warfare Monitor (IWM) e Citizen Lab — compartilham o objetivo

de fortalecer os grupos não governamentais com ferramentas de investigação que tradicionalmente estiveram disponíveis somente para a polícia. Esses grupos fizeram progressos surpreendentes na identificação de cibercriminosos e identificação de suas técnicas.

Nart Villeneuve, que trabalha para os dois grupos, descobriu que um software chinês semelhante ao Skype era utilizado para vigilância de um operador de rede sem fio, e que um sistema espião que ele e outros investigadores chamaram de 'Ghostnet' espionava os computadores espalhados pelos governos do sul da Ásia. Uma auditoria na rede do escritório do dalai-lama, em Dharamsala, na Índia, que sofreu inúmeros ataques de hackers, foi o que desencadeou a descoberta. Diz-se que a operação foi patrocinada pelo governo chinês, tradicionalmente contra o dalai-lama e seu governo no exílio.

A IWM usou um programa gratuito denominado Wireshark para identificar o tráfego de entrada e saída nos computadores do antigo governo tibetano. O programa detectou que o sistema Ghostnet havia instalado remotamente software secreto de vigilância nos computadores e conseguia acessar arquivos e e-mails.

A preocupação real para os especialistas em segurança e para os oficiais do governo é a possibilidade de um ato de guerra virtual contra um recurso crítico, como a rede elétrica, o sistema financeiro ou o sistema de comunicações. Em primeiro lugar, os Estados Unidos não possuem uma política clara sobre como o país responderia a esse nível de ataque virtual. Embora a rede elétrica tenha sido acessada por hackers, ela ainda não foi atacada. Um estudo de três anos da cibersegurança norte-americana recomendou que se criasse tal política e que ela se tornasse pública. Sugeriu também que os Estados Unidos tentassem se unir às outras nações contra esses ataques.

Em segundo lugar, os efeitos de um ataque desse tipo provavelmente seriam devastadores. Mike McConnell, antigo diretor da inteligência nacional norte-americana, declarou que mesmo que um grande banco norte-americano sofresse um ataque bem-sucedido, "ele teria um impacto ainda maior sobre a economia global" do que os ataques às Torres Gêmeas, e que "a habilidade de ameaçar a oferta de dinheiro norte-americana é hoje o equivalente a uma guerra nuclear". Tal ataque teria um efeito catastrófico sobre o sistema financeiro norte-americano e, por extensão, sobre a economia mundial.

Por fim, muitos analistas do setor estão preocupados com a desorganização da segurança virtual, sem líder definido entre as agências de inteligência. Diversas agências, entre elas o Pentágono e a Agência Nacional de Segurança (ANS), têm suas próprias visões sobre ser a principal agência nos esforços contínuos para combater a guerra virtual. Em junho de 2009, Robert Gates, secretário de Defesa norte-americana, ordenou a criação da primeira matriz com finalidade de coordenar os esforços de cibersegurança do governo, temporariamente denominado Cybercom. O propósito da instituição será coordenar a operação e proteção das redes de computadores militares e do Pentágono na esperança de que se desfaça esse nó organizacional.

O presidente Barack Obama já havia anunciado sua intenção de expandir o programa de 17 bilhões de dóla-

res aprovado em 2008. É provável que a maior parte dessa quantia vá para a Cybercom, já que ela coordena os esforços de restringir o acesso aos computadores do governo, além de proteger os sistemas que processam as operações da bolsa de valores, limpar as transações bancárias globais e gerenciar o sistema de controle de tráfego aéreo. Seu objetivo final será prevenir ataques virtuais catastróficos contra os Estados Unidos. Alguns participantes sugerem, entretanto, que talvez não seja possível organizar de maneira eficiente as agências governamentais sem acesso direto ao presidente; o que atualmente não existe. Ainda assim, a primeira tarefa da instituição seria organizar os vários componentes e recursos dispersados pelas quatro forças armadas.

Na solução desse problema, surge uma questão crítica: que nível de controle deve ser dado às agências de espionagem norte-americana na imposição da cibersegurança, já que estão proibidas de atuar em território norte-americano? Os ataques virtuais não têm fronteiras e, portanto, distinguir entre territórios norte-americano e estrangeiro significa que as agências nacionais serão desnecessariamente inibidas em sua possibilidade de lutar contra o crime virtual. Se a ANS, por exemplo, estivesse investigando a fonte de um ciberataque aos sites do governo e descobrisse que o ataque partiu de servidores norte-americanos, de acordo com a lei vigente, não poderia investigar mais.

Alguns especialistas acreditam que não existe uma maneira eficiente de uma agência nacional conduzir operações computacionais sem entrar em redes proibidas dentro dos Estados Unidos, ou mesmo conduzir investigações em países aliados dos norte-americanos. A ANS já esteve sob fogo cruzado intenso por suas ações de vigilância depois do 11 de setembro, e essa situação tem o potencial de levantar preocupações semelhantes. A prevenção de ataques terroristas ou virtuais pode demandar a análise de algumas mensagens de e-mail de outros países ou a concessão para as agências de inteligência de mais acesso às redes ou aos provedores de serviços de Internet. Existe a necessidade de um debate franco sobre o que constitui uma violação de privacidade e o que é aceitável durante os 'tempos de guerra virtual', que, em essência, ocorrem o tempo inteiro. A lei pode precisar de alterações para acomodar técnicas eficientes de cibersegurança, mas não está claro se isso pode ser feito sem que se violem alguns direitos de privacidade considerados essenciais.

Uma maneira de lidar com isso seria confiar parte do trabalho aos fornecedores privados de defesa. Muitos deles estão torcendo para receber valiosos contratos com o governo, tanto para desenvolver sistemas de defesa para as redes quanto para criar medidas ofensivas para desmontar as redes dos inimigos. Nas principais forças, equipes de qualificados engenheiros de computação já atuam e podem conseguir driblar as restrições que impedem que as agências governamentais investiguem dentro do país.

Com relação às medidas ofensivas, não está claro o quão fortes são os recursos ofensivos dos Estados Unidos contra a guerra virtual. O governo vigia de perto essa informação, quase sempre secreta. Entretanto, ex-militares e ex-oficiais de inteligência dizem que

os recursos norte-americanos contra a guerra virtual aumentaram drasticamente em termos de sofisticação nos últimos dois anos. E, como rastrear os cibercriminosos tornou-se muito difícil, um ataque ofensivo pode ser a melhor defesa.

Fontes: J., Nicholas Hoover, "Cybersecurity Balancing Act". *Information Week*, 27 abr. 2009; David E. Sanger, John Markoff, e Thom Shanker, "U.S. Steps Up Effort on Digital Defenses". *The New York Times*, 28 abr. 2009; John Markoff e Thom Shanker, "Panel Advises Clarifying U.S. Plans on Cyberwar". *The New York Times*, 30 abr. 2009; Siobhan Gorman e Evan Ramstad, "Cyber Blitz Hits U.S., Korea". *The Wall Street Journal*, 9 jul. 2009; Lolita C. Baldor, "White House Among Targets of Sweeping Cyber Attack". *Associated Press*, 8 jul. 2009; Choe Sang-Hun, "Cyberattacks Hit U.S. and South Korean Web Sites". *The New York Times*, 9 jul. 2009; Siobhan Gorman, "FAA's Air-Traffic Networks Breached by Hackers". *The Wall*

Street Journal, 7 maio 2009; Thom Shanker, "New Military Command for Cyberspace". *The New York Times*, 24 jun. 2009; David E. Sanger e Thom Shanker, "Pentagon Plans New Arm to Wage Wars in Cyberspace". *The New York Times*, 29 maio 2009; Lolita C. Baldor, "Obama Setting Up Better Security for Computers". *Associated Press*, 29 maio 2009; Christopher Drew e John Markoff, "Contractors Vie for Plum Work, Hacking for U.S.". *The New York Times*, 31 maio 2009; Thom Shanker e David E. Sanger, "Privacy May Be a Victim in Cyberdefense Plan". *The New York Times*, 13 jun. 2009; Siobhan Gorman, August Cole e Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project". *The Wall Street Journal*, 21 abr. 2009; Carlos Tejada e Juliet Ye, "Computer Spying: China Responds". *The Wall Street Journal*, 22 abr. 2008; Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies". *The Wall Street Journal*, 8 abr. 2009; "Has Power Grid Been Hacked? U.S. Won't Say". *Reuters*, 8 abr. 2009; John, Markoff, "Vast Spy System Loots Computers in 103 Countries". *The New York Times*, 29 mar. 2009; John, Markoff, "Tracking Cyberspies Through the Web Wilderness". *The New York Times*, 12 maio 2009.

Questões

1. A guerra virtual é um problema sério? Justifique.
2. Avalie os fatores humanos, organizacionais e tecnológicos que criaram esse problema.
3. Que soluções foram propostas? Você acha que elas serão eficientes? Justifique.
4. Existem outras soluções para esse problema que devem ser consideradas? Quais são elas?

Referências bibliográficas

- ACOHIDO, B. "Cybercrooks Descend on Twitter with Spam Attacks". *USA Today*, 6 jul. 2009.
- AUSTIN, R. D.; DARBY, C. A. R. "The Myth of Secure Computing". *Harvard Business Review*, jun. 2003.
- BALDOR, L. C. "White House Among Targets of Sweeping Cyber Attack". *Associated Press*, 8 jul. 2009.
- BANHAM, R. "The Strategic Advantages of Managing Risk". *The Wall Street Journal*, 5 jun. 2007.
- BERNSTEIN, C. "The Cost of Data Breaches". *Baseline*, abr. 2009.
- BOWLEY, G. "Ex-Worker Said to Steal Goldman Code". *The New York Times*, 7 jul. 2009.
- BRENNER, S. W. "U.S. Cybercrime Law: Defining Offenses". *Information Systems Frontiers*, 6, n. 2, jun. 2004.
- CARVAJAL, D. "High-Tech Crime is an Online Bubble that Hasn't Burst". *The New York Times*, 7 abr. 2008.
- CAVUSOGLU, H.; MISHRA, B.; RAGHUNATHAN, S. "A Model for Evaluating IT Security Investments". *Communications of the ACM*, 47, n. 7, jul. 2004.
- CHECKLER, J. "Programmer Suspended Following His Arrest". *The Wall Street Journal*, 8 jul. 2009.
- CHICKOWSKI, E. "Is Your Information Really Safe?". *Baseline*, abr. 2009.
- CHOE Sang-Hun. "Cyberattacks Hit U.S. and South Korean Web Sites". *The New York Times*, 9 jul. 2009.
- CONSUMER Reports. "State of the Net 2009". jun. 2009.
- D'ARCY, John; HOVAV, A. "Deterring Internal Information Systems Use". *Communications of the ACM*, 50, n. 10, out. 2007.
- DREGER, R.; MOERSCHEL, G. "Inside Smartphone Security". *Information Week*, 6 out. 2008.
- EPSTEIN, K. "Defenseless on the Net". *Business Week*, 16 abr. 2008.
- ERICKSON, J. "Dr. Dobb's Report: Information Security". *Information Week*, 22 jun. 2009.
- FERETIC, E. "Is Security a Myth?". *Baseline*, abr. 2009.
- FERNANDEZ, M. "Computer Error Caused Rent Troubles for Public Housing Tenants". *The New York Times*, 5 ago. 2009.
- FOLEY, J. "P2P Peril". *Information Week*, 17 mar. 2008.
- FRATTO, M. "What's Your Appetite for Risk?". *Information Week*, 22 jun. 2009.
- FRATTO, M. "Cloud Control". *Information Week*, 26 jan. 2009.
- _____. "Precision Security". *Information Week*, 30 jun./7 jul. 2008.
- GAUR, N.; KIEP, B. "Managing Mobile Menaces". *Optimize Magazine*, maio 2007.
- GIORDANO, S. M. "Electronic Evidence and the Law". *Information Systems Frontiers*, 6, n. 2, jun. 2004.
- GORMAN, S. "Electricity Grid in U.S. Penetrated by Spies". *The Wall Street Journal*, 8 abr. 2009.
- GORMAN, S.; RAMSTAD, E. "Cyber Blitz Hits U.S., Korea". *The Wall Street Journal*, 9 jul. 2009.
- _____. "FAA's Air-Traffic Networks Breached by Hackers". *The Wall Street Journal*, 7 maio 2009.
- _____. COLE, A.; DREAZEN, Y. "Computer Spies Breach Fighter-Jet Project". *The Wall Street Journal*, 21 abr. 2009.
- GROW, B.; EPSTEIN, K.; TSCHANG, Chi-Chu. "The New E-spyionage Threat". *Business Week*, 10 abr. 2008.
- HOOVER, J. N. "Cybersecurity Balancing Act". *Information Week*, 27 abr. 2009.
- HOUSLEY, R.; ARBAUGH, W. "Security Problems in 802.11b Networks". *Communications of the ACM*, 46, n. 5, maio 2003.
- IVES, B.; WALSH, K. R.; SCHNEIDER, H. "The Domino Effect of Password Reuse". *Communications of the ACM*, 47, n. 4, abr. 2004.
- JAGATIC, T.; JOHNSON, N.; JAKOBSSON, M.; MENCZER, F. "Social Phishing". *Communications of the ACM*, 50, n. 10, out. 2007.
- JAVELIN Research. "2009 Identity Fraud Survey Report". 9 fev. 2009.
- KIRK, J. "MySpace Users Struggle to Overcome Cybervandalism". *PC World*, 30 jun. 2008.
- MARKOFF, J.; SHANKER, T. "Panel Advises Clarifying U.S. Plans on Cyberwar". *The New York Times*, 30 abr. 2009.
- MARKOFF, J. "Tracking Cyberspies Through the Web Wilderness". *The New York Times*, 12 maio 2009.

- _____. "Vast Spy System Loots Computers in 103 Countries". *The New York Times*, 29 mar. 2009.
- McDOUGALL, P. "High Cost of Data Loss". *Information Week*, 20 mar. 2006.
- MECKBACH, G. "MasterCard's Robust Data Centre: Priceless". *Computerworld Canada*, 26 mar. 2008.
- MERCURI, R. T. "Analyzing Security Costs". *Communications of the ACM* 46, n. 6, jun. 2003.
- MILLS, E. "Facebook Disables Rogue Data-Stealing, Spamming Apps". *CNET News*, 20 ago. 2009.
- MITCHELL, D. "It's Here: It's There; It's Spyware". *The New York Times*, 20 maio 2006.
- NARAINA, R.; PRINCE, B. "Data Breaches Cause Concern". *eWeek*, 7 abr. 2008.
- NARAINA, R. "ActiveX Under Siege". *eWeek*, 11 fev. 2008.
- _____. "Inside a Modern Malware System". *eWeek*, 7 jan. 2008.
- NULL, C. "WPA Cracked in 1 Minute". *Yahoo! Tech*, 27 ago. 2009.
- PANKO, R. R. *Corporate Computer e Network Security* 2e. Upper Saddle River, NJ: Pearson Prentice Hall, 2010.
- PASZTOR, A.; MICHAELS, D. "Computer Failures Are Probed in Jet Crash". *The Wall Street Journal*, 27 jun. 2009.
- PEREZ, J. C. "Facebook Stamps Out Malware Attack". *PC World*, 8 ago. 2008.
- PEREZ, S. "The Facebook Virus Spreads: No Social Network Is Safe". *The New York Times*, 11 dez. 2008.
- PRINCE, B. "The Growing E-Mail Security Challenge". *eWeek*, 21 abr. 2008.
- RICHARDSON, R. "2008 CSI Computer Crime and Security Survey". *Computer Security Institute*, 2008.
- ROBERTSON, J. "Hackers: Social Networking Sites Flawed". *Associated Press*, 3 ago. 2007.
- ROCHE, E. M.; NOSTRAND, G. V. *Information Systems, Computer Crime and Criminal Justice*. New York: Barracough Ltd., 2004.
- SAMPLE, C.; KELLEY, D. "Cloud Computing Security: Infrastructure Issues". *Security Curve*, 23 jun. 2009.
- SANGER, D. E.; SHANKER, T. "Pentagon Plans New Arm to Wage Wars in Cyberspace". *The New York Times*, 29 maio 2009.
- SCHMIDT, H. "Cyber Anxiety". *Optimize Magazine*, maio 2007.
- SCHWERHA IV, J. J. "Cybercrime: Legal Standards Governing the Collection of Digital Evidence". *Information Systems Frontiers* 6, n. 2, jun. 2004.
- SHANKER, T.; SANGER, D. E. "Privacy May Be a Victim in Cyberdefense Plan". *The New York Times*, 13 jun. 2009.
- SHANKER, T. "New Military Command for Cyberspace". *The New York Times*, 24 jun. 2009.
- SHIELDS, G. "Modern Malware Threats and Countermeasures". Sunbelt Software, 2008.
- SOFTWARE World. "U.S. Consumers Losing Billions in Cyber Attacks". 1 set. 2006.
- SOPHOS Plc. "Security Threat Report: 2009". 2008.
- STEEL, E. "Web Ad Sales Open Door to Viruses". *The Wall Street Journal*, 15 jun. 2009.
- STEELE, B. K. "Due Diligence". *Baseline*, mar. 2009.
- SYMANTEC Corporation. "Symantec Internet Threat Security Report". 2009.
- VAAS, L. "The Final 'Final' Nail in WEP's Coffin?". *eWeek*, 5 abr. 2007.
- VOLONINO, L.; ANZALDUA, R.; GODWIN, J. *Computer Forensics: Principles and Practices*. Upper Saddle River, NJ: Prentice Hall, 2007.
- WANG, H.; WANG, C. "Taxonomy of Security Considerations and Software Quality". *Communications of the ACM* 46, n. 6, jun. 2003.
- WARKENTIN, M.; LUO, X.; TEMPLETON, G. F. "A Framework for Spyware Assessment". *Communications of the ACM* 48, n. 8, ago. 2005.
- WESTERMAN, G. *IT Risk: Turning Business Threats into Competitive Advantage*. Harvard Business School Publishing, 2007.
- WIENS, J. "With Security, More Is Better". *Information Week*, 10 mar. 2008.

Principais aplicações de sistemas para a era digital

PARTE

III

Capítulo 8 Conquistando excelência operacional e intimidade com o cliente: aplicativos integrados

Capítulo 9 Comércio eletrônico: mercados digitais, mercadorias digitais

Capítulo 10 Como melhorar a tomada de decisão e a gestão do conhecimento

Esta terceira parte examina as principais aplicações de sistemas de informação que as empresas usam atualmente para aumentar a excelência operacional e melhorar a tomada de decisão. Entre as aplicações estão sistemas integrados; sistemas para gestão da cadeia de suprimentos, gestão do relacionamento com o cliente e gestão do conhecimento; aplicações de comércio eletrônico; sistemas de apoio à decisão; e sistemas de apoio ao executivo. Assim, esta parte responde a perguntas do seguinte tipo: como as aplicações integradas melhoraram o desempenho da empresa? Como as empresas usam o comércio eletrônico para ampliar o alcance de seus negócios? Como os sistemas melhoraram a tomada de decisão e ajudam as empresas a fazer bom uso de seus ativos de conhecimento?

Conquistando excelência operacional e intimidade com o cliente: aplicativos integrados

Capítulo

8

OBJETIVOS DE ESTUDO

Ao terminar este capítulo, você será capaz de responder às seguintes perguntas:

1. Como os sistemas integrados ajudam as empresas a conquistar a excelência operacional?
2. Como os sistemas de gestão da cadeia de suprimento coordenam o planejamento, a produção e a logística com os fornecedores?
3. Como os sistemas de gestão do relacionamento com o cliente conquistam a intimidade com o público?
4. Como as aplicações integradas são utilizadas em plataformas para novos serviços interfuncionais?

PLANO DO CAPÍTULO

Caso de abertura: *Aplicativos integrados ajudam a Severstal a criar uma plataforma global de produção*

Sistemas integrados

Sistemas de gestão da cadeia de suprimentos

Sistemas de gestão do relacionamento com o cliente

Aplicações integradas: novas oportunidades e desafios

Projetos práticos em SIG

Resolvendo problemas organizacionais — *Border States Industries incentiva o rápido crescimento com ERP*

APLICATIVOS INTEGRADOS AJUDAM A SEVERSTAL A CRIAR UMA PLATAFORMA GLOBAL DE PRODUÇÃO

A Severstal ("Northern Steel") é um dos maiores produtores de aço da Rússia. A empresa opera principalmente em seu país de origem, mas mantém instalações em locais como Ucrânia, Cazaquistão, Reino Unido, França, Itália, Estados Unidos e África. Com mais de 100 mil empregados ao redor do mundo e mais de 22,4 bilhões de dólares em receita no ano de 2008, a Severstal está redefinindo a produção global de aço.

Algumas empresas norte-americanas abandonaram o mercado de produção de aço porque o setor é de capital intensivo. A Severstal não está preocupada com isso. Os gerentes da empresa estão convencidos de que estão à frente de um líder em lucratividade global no setor de aço e mineração.

As estratégias corporativas da Severstal exigem a oferta de produtos com alta margem de valor agregado em mercados de nichos atrativos em todo o mundo, mantendo os custos baixos. A empresa está desenvolvendo uma plataforma global para compartilhamento de melhores práticas e desenvolvimento de competências. A Severstal deseja nivelar as melhores práticas e tecnologias em suas operações globais e aperfeiçoar as eficiências localizando suas fábricas próximo aos clientes automotivos. Em 2004, por exemplo, a Severstal da América do Norte adquiriu a Rouge Industries em Dearborn, Michigan, originalmente parte do grandioso complexo de manufatura River Rouge, de Henry Ford, para ganhar acesso ao mercado norte-americano de aço automotivo. Atualmente, a Severstal da América do Norte é a quarta maior produtora integrada de aço nos Estados Unidos.

A maior parte dos clientes da Severstal possui operações ao redor do mundo e deseja receber aço da mesma qualidade na América do Norte, na Europa e

na Rússia. Segundo Sergei Kuznetsov, diretor financeiro da Severstal da América do Norte, a estratégia da Severstal é "criar uma plataforma de produção global que possa fornecer aço de alta qualidade para clientes localizados em qualquer parte".

Todos esses planos exigem uma infraestrutura de TI flexível que seja ágil o suficiente para atender os requisitos de negócios globais em constante mudança e apoiar o crescimento eficiente. A infraestrutura de TI da Severstal da América do Norte era uma miscelânea de sistemas diferentes que incluíam Oracle PeopleSoft Enterprise para as finanças, Indus Enterprise PAC para compras e manutenção, e uma variedade de sistemas customizados. A informação não conseguia fluir livremente entre as diferentes áreas funcionais.

Em vez de atualizar suas aplicações existentes, a empresa padronizou os sistemas com a Oracle E-Business Suite 12, uma suíte de aplicativos com módulos para finanças, aquisições, gestão de ativos empresariais, manufatura e gestão de pedidos. As aplicações no software Oracle E-Business Suite são integradas, o que facilita o acesso aos dados de diferentes áreas funcionais para tomada de decisão, cria fluxos de trabalho mais eficientes e aumenta a produtividade. Em vez de otimizar processos de negócios individuais, a empresa consegue otimizar todos os processos. Os processos de aquisição-a-pagamento estão integrados ao novo sistema de aquisições.

O novo sistema também reduz o tempo necessário para encerramento dos livros da empresa de dez dias para cinco dias ou menos, oferecendo informações mais pontuais e de maior qualidade para as filiais da Severstal na Rússia. Oracle iSupplier Portal, Oracle iProcurement e Oracle Sourcing incluem recursos para



cotação eletrônica e aplicações 'self-service', facilitando a comunicação e a colaboração com os fornecedores e parceiros de negócios da Severstal da América do Norte. À medida que a empresa cresce organicamente ou por meio de aquisições, o software Oracle vai ajudar na integração de novas unidades à mesma plataforma.

Fontes: David A. Kelly, "Managing in a Global Economy: SeverStal", *Profit Magazine*, fev. 2008; Anna V. Schevchenko, "Severstal Global Master Data Project", 15-16 out. 2008; e www.severstalna.com, acessado em 5 jul. 2009.

Os esforços da Severstal para criar uma infraestrutura global de TI identificam algumas das questões a serem consideradas pelas empresas se elas quiserem utilizar sistemas globais e que abarquem toda a empresa. Para operar como um negócio global, precisou dispor de um conjunto apropriado de processos de negócios e sistemas de informação estabelecidos. Ela precisou acessar informações de toda a empresa a partir de todos os diferentes locais globais de operação e funções de negócios de modo que a gerência pudesse administrar a companhia como uma única entidade global.

A figura de abertura de caso nos chama a atenção para pontos importantes levantados pelo caso e pelo capítulo. A Severstal está tentando gerar lucros em um setor competitivo e de capital intensivo através da oferta de produtos que podem alcançar preços altos nos mercados de nicho, mas ainda precisa manter seus custos operacionais baixos. Para enfrentar esse desafio, a empresa adotou um modelo de produção global. A Severstal poderia ter atualizado seus sistemas existentes com tecnologia mais nova, mas esses sistemas de informação legados não suportavam processos de negócios e fluxos de informação globais. Em vez disso, a empresa substituiu esses sistemas com um conjunto de aplicativos integrados da Oracle. Os novos sistemas integram funções e processos de negócios dispares e permitem que a empresa crie novos processos interfuncionais que englobem toda a empresa.

Agora a Severstal consegue responder de forma flexível a oportunidades que surgem em todo o mundo.

Sistemas integrados

Em todo o planeta, as empresas estão se tornando cada vez mais conectadas, tanto internamente quanto externamente. Quando você administrar uma empresa, desejará ser capaz de reagir instantaneamente quando um cliente fizer um grande pedido, ou a remessa de um fornecedor se atrasar. Vai querer também saber o impacto desses eventos em cada parte da empresa e como está o desempenho da organização a cada momento, especialmente se estiver administrando uma grande companhia. Os sistemas integrados oferecem a solução que torna isso possível. Vamos ver como funcionam e o que podem fazer.

O que são sistemas integrados?

Imagine que você precise administrar uma empresa com base em informações provenientes de dezenas, ou mesmo centenas, de diferentes sistemas e bancos de dados, incapazes de se comunicar uns com os outros. Imagine que sua empresa tenha dez grandes linhas de produtos, cada uma delas produzida em uma fábrica diferente, e que cada fábrica tenha conjuntos independentes e incompatíveis de sistemas que controlam a produção, o armazenamento e a distribuição.

A Alcoa, por exemplo — maior produtora mundial de alumínio e produtos derivados, com operações espalhadas por 41 países e 500 locais —, inicialmente estava organizada em linhas de negócios nas quais cada uma dispunha de seu próprio conjunto de sistemas de informação. Muitos desses sistemas eram redundantes e ineficientes. Os custos para execução dos processos de aquisição-até-pagamento e financeiros eram muito mais altos e seus tempos de ciclo eram muito mais longos do que os das outras empresas do setor. (Os tempos de ciclo referem-se ao tempo total decorrido entre o início e o final do processo.) A empresa não podia operar como uma única entidade mundial.

Nessa situação, sem sistemas integrados, sua tomada de decisão baseia-se em relatórios impressos, frequentemente desatualizados, e é difícil entender o que realmente está acontecendo na empresa toda. O pessoal de vendas pode não conseguir dizer, no momento de registro de um pedido, se os produtos solicitados estão disponíveis no estoque, e é difícil para o departamento de manufatura utilizar os dados de vendas para planejar uma nova produção. Pois bem: agora você tem uma boa ideia de por que as empresas precisam de um sistema especial para integrar informações.

O Capítulo 2 introduziu os sistemas integrados, também conhecidos como sistemas de planejamento de recursos empresariais (ERP); eles se fundamentam em uma suíte de módulos de software integrados e um banco de dados central comum. Esse banco de dados coleta dados das diferentes divisões e dos departamentos da empresa, e de um grande número de processos de negócios centrais nas áreas de produção e manufatura, finanças e contabilidade, vendas, marketing e recursos humanos, e torna-os disponíveis para aplicações utilizadas em praticamente todas as atividades internas da organização. Quando um processo acrescenta novas informações, estas se tornam imediatamente disponíveis para outros processos de negócios (veja a Figura 8.1).

Se um representante de vendas lança no sistema um pedido de rodas, por exemplo, o sistema verifica o limite de crédito do cliente em questão, programa a remessa, identifica a melhor rota de expedição e deixa os artigos necessários reservados no estoque. Se o estoque for insuficiente para atender ao pedido, o sistema programa a produção de mais rodas, solicitando os materiais e componentes necessários aos fornecedores. As previsões de produção e vendas são imediatamente atualizadas. Os livros-razão e o caixa são automaticamente atualizados com as informações de entrada e saída referentes ao pedido. Os usuários podem consultar o sistema e saber, a qualquer momento, onde aquele pedido em particular se encontra. Do mesmo modo, a administração pode obter informações a qualquer instante sobre como a empresa está operando. O sistema pode ainda gerar dados referentes a toda a empresa para análises administrativas de lucratividade e custo por produto.

Software integrado

Um **software integrado** é desenvolvido em torno de milhares de processos de negócios predefinidos que refletem as melhores práticas. A Tabela 8.1 descreve alguns dos principais processos de negócios apoiados por softwares integrados.

Ao implantar esse tipo de software, as empresas precisam, antes de qualquer coisa, selecionar as funções do sistema que desejam usar e, depois, mapear seus processos de negócios de acordo com os processos predefinidos do software. Para implementar um novo software integrado, a

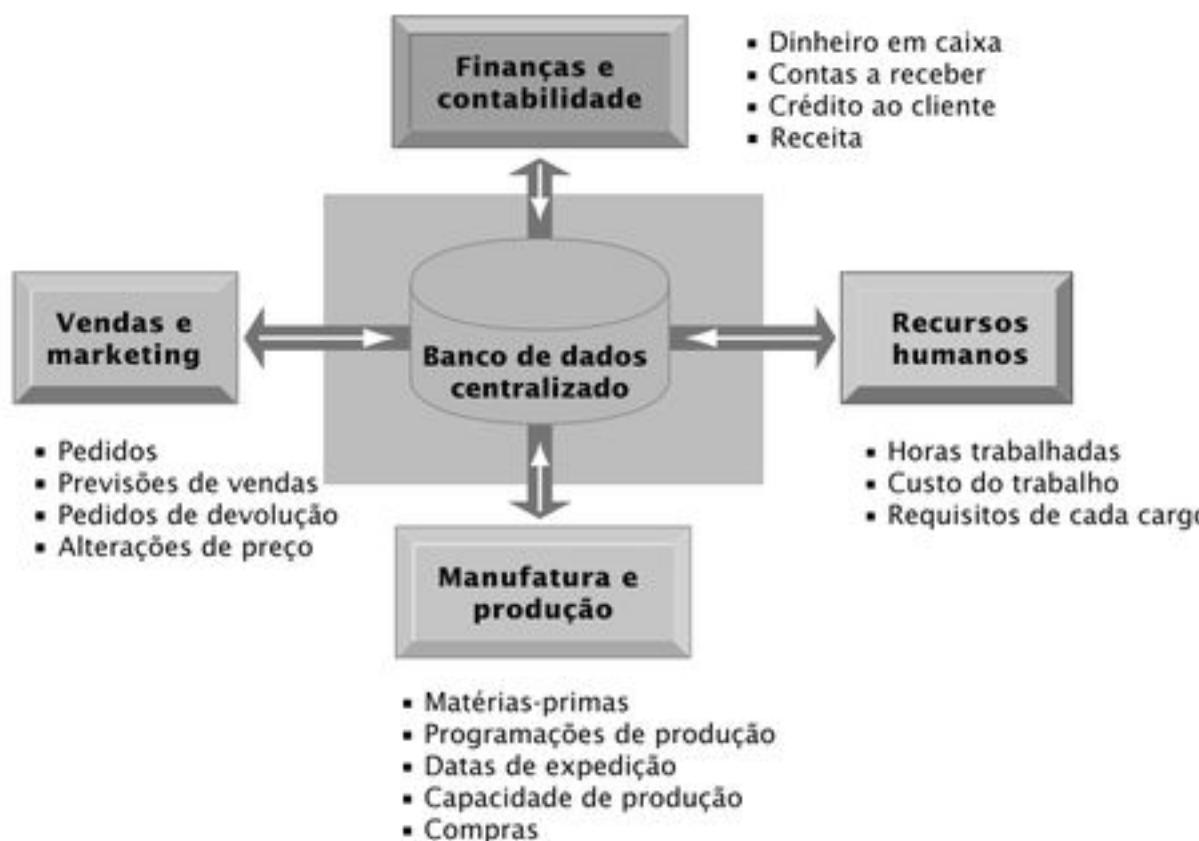


Figura 8.1

Como funcionam os sistemas integrados

Os sistemas integrados apresentam um conjunto de módulos de software integrados e um banco de dados central; este permite que os dados sejam compartilhados pelos diferentes processos de negócios e áreas funcionais de toda a empresa.

Tabela 8.1

Processos financeiros e contábeis, incluindo livro-razão, contas a pagar, contas a receber, ativos fixos, gerenciamento e previsão de caixa, contabilidade de custo de produto, contabilidade por centros de custos, contabilidade de ativos, contabilidade de impostos, gerenciamento de crédito e relatórios financeiros.

Processos de recursos humanos, incluindo gestão de pessoal, contabilização de horas trabalhadas, folha de pagamento, planejamento e desenvolvimento de pessoal, contabilidade de benefícios, acompanhamento de seleção de candidatos, administração do tempo, remuneração, planejamento de força de trabalho, gestão de desempenho e relatórios de despesas de viagem.

Processos de produção e manufatura, incluindo seleção de fornecedores, gestão de estoque, compra, expedição, planejamento e programação de produção, planejamento da necessidade de materiais, controle de qualidade, distribuição, execução de transporte e manutenção das instalações e dos equipamentos.

Processos de vendas e marketing, incluindo processamento de pedidos, cotações, contratos, configuração de produtos, determinação de preços, faturamento, verificação de crédito, gerenciamento de comissões e incentivos e planejamento de vendas.

Tasty Baking Company identificou seus processos existentes e os transformou em processos de negócios embutidos no software SAP ERP que havia selecionado. Uma empresa utilizaria tabelas de configuração fornecidas pelo software para adaptar determinado aspecto do sistema a sua forma de operação. A organização pode usar essas tabelas, por exemplo, para decidir se deseja controlar a receita por linha de produto, unidade geográfica ou canal de distribuição.

Se o software integrado não se adequar às operações empresariais, a empresa pode reescrever uma parte desse software segundo seus processos de negócio. Os softwares integrados são incrivelmente complexos, contudo, e uma customização profunda pode prejudicar o desempenho do sistema, comprometendo a integração de processos e informações, seu principal benefício. Se quiserem colher o máximo benefício do software integrado, as empresas precisam mudar sua maneira de trabalhar para se conformar aos processos de negócio do software. Para garantir esses benefícios, a Tasty Baking Company planejou deliberadamente a customização de menos de cinco por cento do sistema e realizou pouquíssimas modificações no próprio software SAP. A empresa utilizou o maior número de ferramentas possível e recursos já construídos no software. O SAP possui mais de 3 mil tabelas de configuração para seu aplicativo integrado. Costuma ser um grande esforço identificar os processos de negócios da empresa a serem incluídos no sistema e mapeá-los aos processos no software integrado.

Entre os principais fornecedores de software integrado estão SAP, Oracle-PeopleSoft e Infor Global Solutions. Existem versões de pacotes de software integrados baseados na Web especiais para pequenas empresas oferecidos por provedores de serviços de aplicação. Embora inicialmente elaborados para automatizar os processos de negócio de *back-office* internos, os sistemas integrados vêm se tornando mais orientados ao exterior da empresa e capazes de se comunicar com clientes, fornecedores e outras organizações.

Valor empresarial dos sistemas integrados

Os sistemas integrados oferecem valor ao elevar a eficiência operacional e fornecer informações sobre a empresa como um todo, ajudando os gestores a tomar melhores decisões. Grandes empresas com muitas unidades operacionais em diferentes lugares vêm usando sistemas integrados para aplicar práticas e dados padronizados, de maneira que todos conduzam os negócios da mesma maneira no mundo inteiro.

A Coca-Cola, por exemplo, implementou um sistema SAP integrado para padronizar e coordenar importantes processos de negócios em 200 países. A falta de processos de negócios padronizados e que englobassem toda a empresa evitaram que a empresa nivelasse seu poder de compra mundial para obter preços mais baixos para matérias-primas e que a fizeram reagir rapidamente às mudanças no mercado. A Severstal, descrita no caso de abertura do capítulo, implementou seu sistema integrado para padronizar processos globais de negócios por razões semelhantes.

Os sistemas integrados ajudam as empresas a responder rapidamente a pedidos de clientes por informações ou produtos. Como o sistema integra dados de pedidos, produção e entrega, a área de produção pode produzir apenas aquilo que os clientes já pediram, comprar a quantidade exata de componentes ou matérias-primas para atender aos pedidos, planejar a produção e minimizar o tempo que os componentes ou produtos finalizados permanecem em estoque.

Depois de implantar o software integrado da Oracle, a Alcoa eliminou muitos processos e sistemas redundantes. O sistema integrado ajudou a empresa a reduzir o tempo do ciclo de aquisição-até-pagamento (tempo total gasto entre o momento da geração da requisição de compra até o momento em que o pagamento da requisição é efetuado) através da verificação de recibos de produtos e geração automática de recibos de pagamento. O processamento das transações de contas a pagar da Alcoa caiu 89 por cento. A empresa conseguiu centralizar as atividades financeiras e de aquisições, o que ajudou a reduzir aproximadamente 20 por cento de seus custos mundiais.

Sistemas integrados oferecem informações valiosas para a melhoria da tomada de decisão. A alta gerência tem acesso a dados atualizados sobre vendas, estoque e produção, e usa essas informações para criar previsões mais precisas sobre vendas e produção. O software integrado inclui ferramentas analíticas para utilização dos dados capturados pelo sistema para avaliação do desempenho organizacional geral. Softwares integrados contêm ferramentas analíticas que usam os dados capturados pelo sistema para avaliar o desempenho organizacional geral. Os dados dos sistemas integrados têm definições e formatos comuns e padronizados, aceitos por toda a organização. Desse modo, números de desempenho significam o mesmo em qualquer parte da empresa. Os sistemas integrados permitem à administração sênior descobrir facilmente, a qualquer momento, o desempenho de uma unidade organizacional específica, determinar quais produtos são mais ou menos lucrativos e calcular os custos.

O sistema integrado da Alcoa, por exemplo, inclui funcionalidades para gestão de recursos humanos globais que mostram a correlação entre investimentos no treinamento e na qualidade dos empregados, avalia os custos de toda a empresa para distribuição de serviços aos empregados e mensura a eficiência das operações de recrutamento, compensação e treinamento.

Sistemas de gestão da cadeia de suprimentos

Se você administrar uma pequena empresa que fabrica apenas alguns produtos ou presta poucos serviços, provavelmente terá um pequeno número de fornecedores. Com um simples telefone e uma máquina de fax — as ferramentas mais usadas em microempresas para administrar fornecedores —, coordenará os pedidos e entregas desses fornecedores. Se, porém, administra uma empresa que produz itens e serviços mais complexos, ou uma companhia que opera em escala regional, nacional ou global, terá centenas de fornecedores e cada um deles terá seu próprio conjunto de fornecedores. De repente, você se verá em uma situação em que precisará coordenar as atividades de centenas, ou mesmo milhares, de outras empresas a fim de produzir seus produtos e serviços. Os sistemas de gestão da cadeia de suprimentos, já apresentados no Capítulo 2, são uma resposta a esses problemas de escala e complexidade da cadeia de suprimentos.

A cadeia de suprimentos

A **cadeia de suprimentos** de uma empresa é uma rede de organizações e processos de negócios para selecionar matérias-primas, transformá-las em produtos intermediários e acabados e distribuir os produtos acabados aos clientes. A cadeia interliga fornecedores, instalações industriais, centros de distribuição, varejistas e clientes com a finalidade de fornecer mercadorias e serviços desde a fonte até o ponto de consumo. Matérias-primas, informações e pagamentos fluem pela cadeia de suprimentos em ambas as direções.

As mercadorias começam como matérias-primas e, à medida que se movimentam pela cadeia de suprimentos, são transformadas em produtos intermediários (também chamados de componentes ou peças) e, finalmente, em produtos acabados. Estes são enviados a cen-

tos de distribuição e de lá expedidos para varejistas e clientes. Os itens devolvidos fluem na direção contrária, do comprador para o vendedor.

A título de exemplo, vamos examinar a cadeia de suprimentos dos tênis Nike. Ela projeta, distribui e vende tênis, meias, roupas esportivas e acessórios em todo o mundo. Seus fornecedores primários são fabricantes terceirizados com fábricas na China, Tailândia, Indonésia, no Brasil e em outros países. Essas empresas manufaturam os produtos acabados da Nike.

Os fornecedores da Nike não fabricam os tênis do nada. Eles adquirem componentes — caderços, ilhoses, cabedais e solados — de outros fornecedores e, depois, os reúnem em tênis acabados. Esses fornecedores de componentes, por sua vez, têm seus próprios fornecedores. Por exemplo, os fornecedores de solados têm fornecedores de borracha sintética, de produtos químicos usados para derreter a borracha nos moldes, e dos próprios moldes. Os fornecedores de caderços têm fornecedores de fios, tinturas e acabamentos plásticos.

A Figura 8.2 ilustra de maneira simplificada a cadeia de suprimentos dos tênis Nike; ela mostra o fluxo de informações e materiais entre os fornecedores, a Nike e os distribuidores, varejistas e clientes. Os fabricantes terceirizados são seus fornecedores primários. Os fornecedores de solas, cabedais e caderços são os secundários (camada 2). E os fornecedores desses fornecedores são os terciários (camada 3).

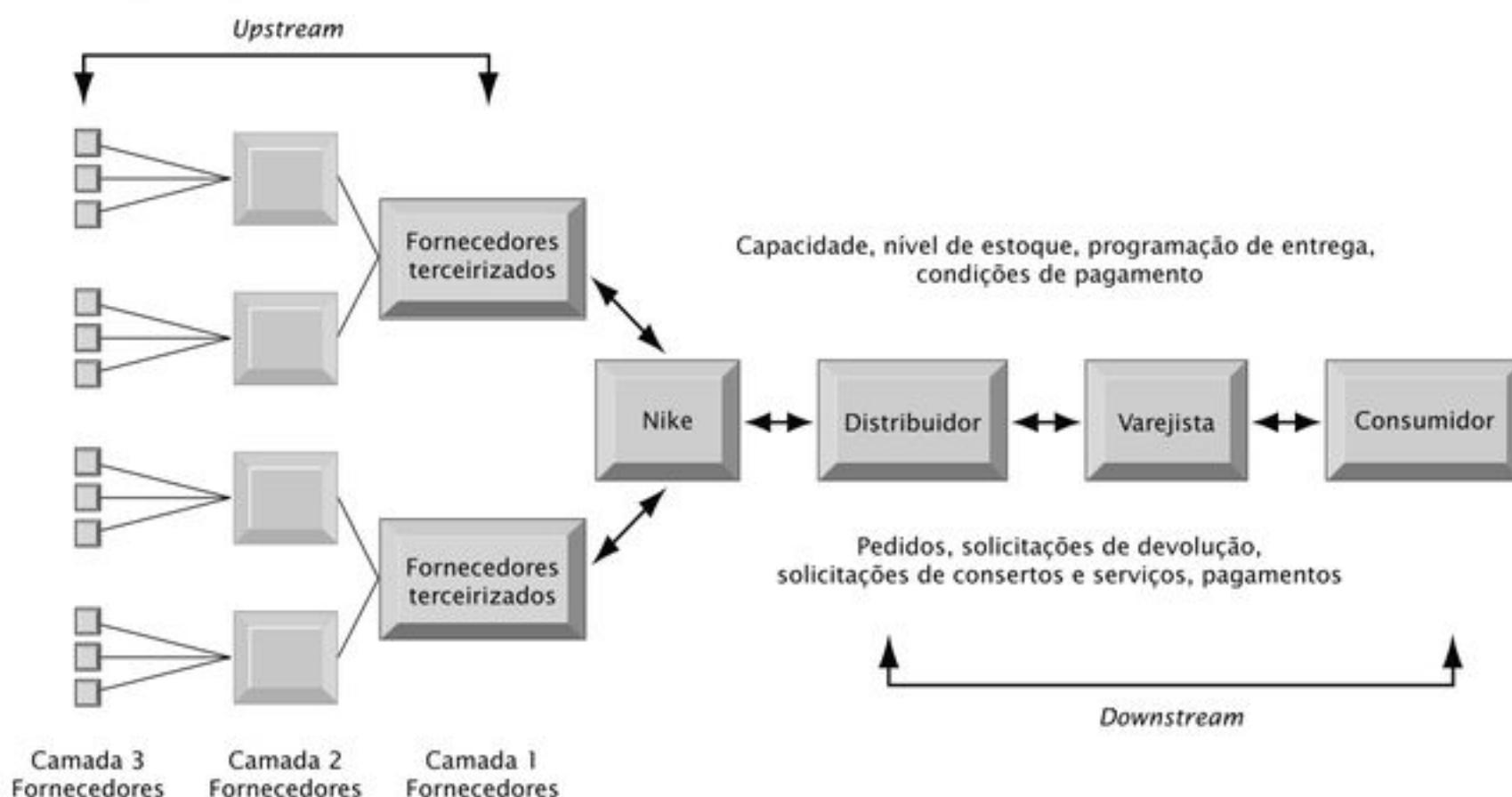
A parte *upstream* da cadeia de suprimentos inclui os fornecedores da empresa, os fornecedores dos fornecedores e os processos para gerenciar as relações entre eles. A parte *downstream* consiste nos processos e organizações envolvidos na distribuição e entrega de produtos ao consumidor final. As empresas fabricantes, como as fornecedoras de tênis contratadas pela Nike, também gerenciam seus próprios processos de *cadeia interna de suprimentos*, pelos quais transformam matérias-primas, componentes e serviços proporcionados por seus fornecedores em produtos acabados ou intermediários (componentes ou peças) a seus clientes, usando esses mesmos processos para gerenciar matérias-primas e estoque.

A cadeia de suprimentos ilustrada na Figura 8.2 foi simplificada. Ela mostra apenas dois fabricantes de tênis e apenas o fluxo *upstream* referente aos solados. A Nike tem centenas de fabricantes terceirizados que entregam tênis, meias e roupas esportivas acabadas, cada um com seu próprio conjunto de fornecedores. A parte *upstream* da cadeia de suprimentos da Nike compreende, na verdade, milhares de entidades. A Nike também tem inúmeros distribuidores e seus calçados são vendidos por milhares de varejistas; portanto, a porção *downstream* de sua cadeia de suprimentos é igualmente ampla e complexa.

Figura 8.2

Cadeia de suprimentos da Nike

Esta figura ilustra as principais entidades na cadeia de suprimentos da Nike e o fluxo de informações upstream (atividades a montante) e downstream (atividades a jusante) para coordenar as atividades envolvidas na compra, fabricação e transporte do produto. O que vemos aqui é uma cadeia de suprimentos simplificada, com a parte upstream focada apenas nos fornecedores de tênis e solados de tênis.



Gestão da cadeia de suprimentos e informações

Ineficiências na cadeia de suprimentos, como falta de peças, capacidade ociosa de produção, estoque excessivo de produtos acabados ou altos custos de transporte, são causadas por informações imprecisas e extemporâneas. Por exemplo, os fabricantes podem manter excesso de peças em estoque porque não sabem exatamente quando receberão a próxima remessa de seus fornecedores. Os fornecedores podem fazer pedidos insuficientes de matéria-prima porque não dispõem de informações precisas a respeito da demanda. Essas ineficiências da cadeia de suprimentos podem causar um desperdício de até 25 por cento dos custos operacionais de uma empresa.

Se um fabricante souber exatamente quantos produtos seus clientes desejam, quando desejam e em que momento esses produtos poderão ser fabricados, será possível implantar uma estratégia *just-in-time* ('na hora certa') altamente eficiente. Os componentes chegarão no exato momento em que se precisa deles, e os produtos acabados serão expedidos assim que deixarem a linha de montagem.

Sempre existem incertezas, contudo, em uma cadeia de suprimentos, porque muitos eventos não podem ser previstos: demanda incerta, atraso nas remessas dos fornecedores, peças ou matérias-primas defeituosas, ou ainda panes no processo de produção. Para satisfazer os clientes, os fabricantes muitas vezes lidam com essas incertezas e eventos imprevistos mantendo mais matérias-primas ou produtos em estoque do que eles acham que será realmente necessário. O *estoque de segurança* atua como um escudo contra a falta de flexibilidade na cadeia de suprimentos. Embora manter um estoque excessivo saia caro, taxas insuficientes de atendimento também são dispendiosas, pois a organização pode perder negócios caso cancele muitos pedidos.

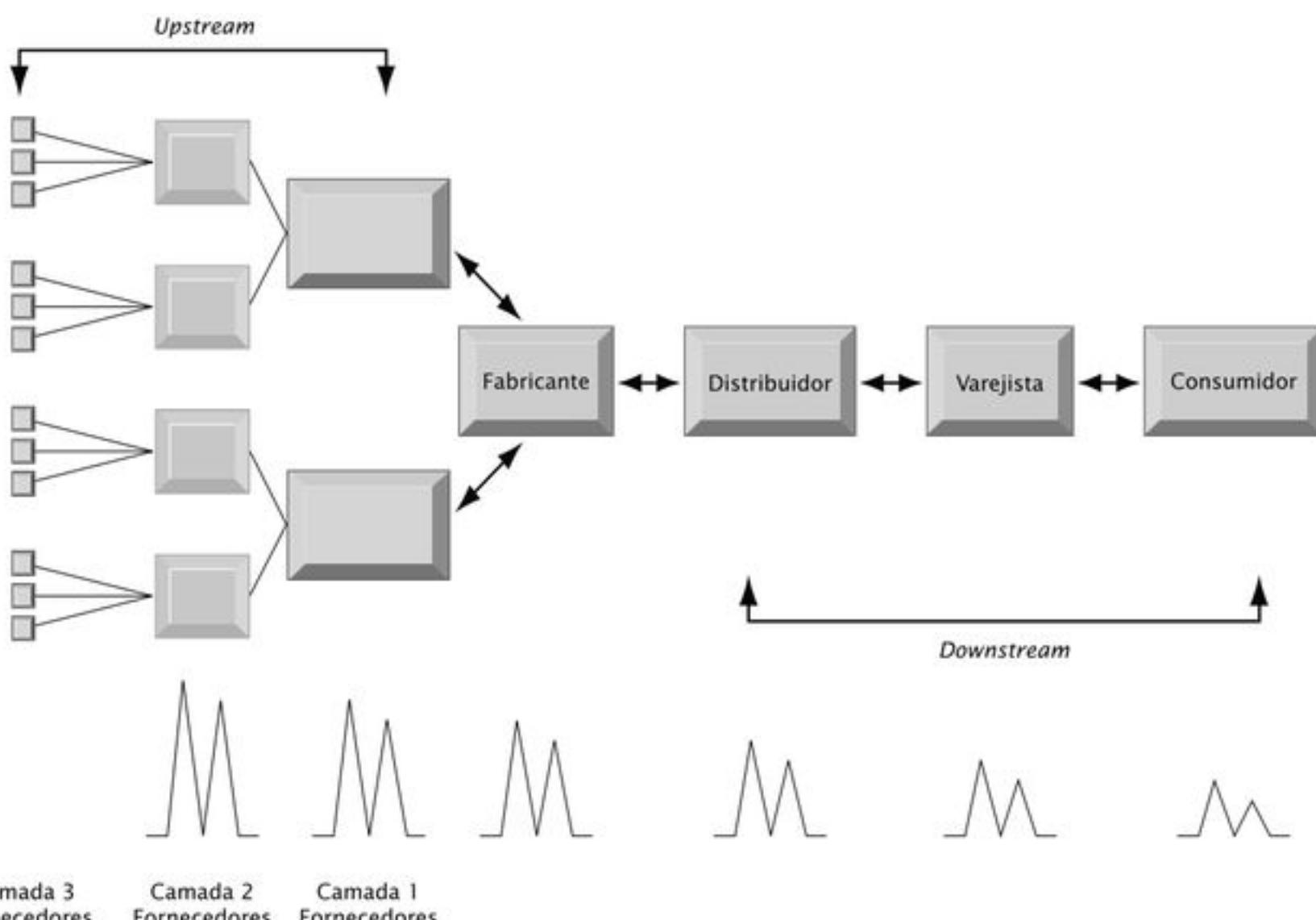
Um problema recorrente na gestão da cadeia de suprimentos é o **efeito chicote**, pelo qual a informação da demanda por um produto é distorcida à medida que passa de uma entidade à entidade seguinte na cadeia de suprimentos. Uma pequena elevação na demanda de um item pode fazer com que diferentes membros da cadeia de suprimentos — distribuidores, fabricantes, fornecedores, fornecedores secundários (fornecedores dos fornecedores) e terciários (fornecedores dos fornecedores dos fornecedores) — abarrotuem o estoque para ter o suficiente 'só por precaução'. Essas alterações se propagarão por toda a cadeia de suprimentos, ampliando o que tinha começado como uma pequena alteração nos pedidos previstos e criando custos excessivos de estoque, produção, armazenagem e expedição (veja a Figura 8.3).

A Procter & Gamble (P&G), por exemplo, descobriu que, devido a esse tipo de informação distorcida, tinha estoques excessivos de suas fraldas descartáveis Pampers em vários pontos ao longo de sua cadeia de suprimentos. Embora as compras nas lojas fossem razoavelmente estáveis, os pedidos dos distribuidores disparavam quando a P&G lançava promoções agressivas de preço. Assim, as Pampers e seus componentes acumulavam-se nos armazéns ao longo da cadeia de suprimentos para atender a uma demanda que na verdade não existia. Para eliminar esse problema, a P&G revisou seus processos de marketing, de vendas e da cadeia de suprimentos e passou a usar uma previsão de demanda mais acurada.

O efeito chicote pode ser controlado quando se reduzem as incertezas sobre a demanda e a oferta, e isso só ocorre quando todos os membros da cadeia de suprimentos contam com informações precisas e atualizadas. Se todos os membros da cadeia de suprimentos compartilharem informações dinâmicas sobre níveis de estoque, programações, previsões e embarques, terão uma ideia mais exata de como ajustar seus planos de aquisição de matérias-primas, fabricação e distribuição. Os sistemas de gestão da cadeia de suprimentos oferecem esse tipo de informação, que pode ajudar seus membros a tomar decisões de compra e programação mais acertadas. A Tabela 8.2 descreve como as empresas se beneficiam com esses sistemas.

Software de gestão da cadeia de suprimentos

Há dois tipos de software de cadeia de suprimentos: aqueles que ajudam as empresas a planejar suas cadeias de suprimentos (planejamento de cadeia de suprimentos) e aque-

**Figura 8.3****Efeito chicote**

Informações imprecisas podem fazer com que pequenas flutuações na demanda por produtos sejam amplificadas à medida que nos movemos para trás na cadeia de suprimentos. Pequenas flutuações nas vendas de varejo podem criar estoques excessivos para distribuidores, fabricantes e fornecedores.

les que as ajudam a executar as etapas da cadeia de suprimentos (execução da cadeia de suprimentos). **Sistemas de planejamento da cadeia de suprimentos** habilitam a empresa a gerar previsões de demanda para um produto e a desenvolver planos de aquisição de matérias-primas e fabricação para aquele item. Tais sistemas ajudam as empresas a tomar decisões operacionais, tais como: determinar a quantidade de um produto específico a ser fabricada em dado período; estabelecer níveis de estoque para matérias-primas, produtos intermediários e acabados; determinar onde armazenar os artigos acabados; e identificar o meio de transporte a ser usado para a entrega.

Por exemplo, se um grande cliente faz um pedido maior que o usual, ou o altera de última hora, isso pode ter um impacto tremendo em toda a cadeia de suprimentos. Pode ser necessário pedir aos fornecedores mais matéria-prima ou uma combinação diferente de matérias-primas. A manufatura terá de alterar sua programação de trabalho e o transportador talvez precise reprogramar suas entregas. É aí que entra em cena o software de planejamento da cadeia de suprimentos, que faz os ajustes necessários nos planos de produção e distribuição.

Tabela 8.2 Como os sistemas de informação facilitam a gestão da cadeia de suprimentos
As informações dos sistemas de gestão da cadeia de suprimentos ajudam as empresas a

- Decidir quando e o que produzir, armazenar e movimentar
- Comunicar rapidamente os pedidos
- Controlar o status dos pedidos
- Verificar a disponibilidade do estoque e monitorar seus níveis
- Reducir os custos de estoque, transporte e armazenagem
- Controlar a expedição
- Planejar a produção com base na demanda real do cliente
- Comunicar rapidamente as modificações no projeto do produto

As informações sobre as mudanças são compartilhadas entre os membros relevantes da cadeia de suprimentos, de maneira que eles possam coordenar seu trabalho. Uma das mais importantes — e complexas — funções do planejamento da cadeia de suprimentos é o **planejamento da demanda**, que determina a quantidade de produto que uma empresa precisa produzir para satisfazer a demanda de todos os seus clientes.

A Whirlpool Corporation, que produz máquinas de lavar, secadoras, refrigeradores, fogões e outros eletrodomésticos, utiliza sistemas de planejamento da cadeia de abastecimento para certificar-se de que o que produz atende à demanda dos clientes. A empresa usa software de planejamento da cadeia de abastecimento da i2 Technologies, que inclui módulos para cronograma-mestre, planejamento de execução e planejamento de estoque. A organização também instalou uma ferramenta da i2 baseada na Web para planejamento colaborativo, previsão e reabastecimento para compartilhar e combinar suas previsões de vendas com as previsões de seus principais parceiros de vendas. Melhorias no planejamento da cadeia de suprimentos combinadas aos modernos centros de distribuição ajudaram a Whirlpool a aumentar para 97 por cento a disponibilidade dos produtos no estoque quando os clientes precisam, e reduziu em 20 por cento o número excessivo de produtos acabados em estoque e em 50 por cento os erros de previsão (Barrett, 2009).

Os **sistemas de execução da cadeia de suprimentos** gerenciam o fluxo de produtos pelos centros de distribuição e depósitos para garantir que sejam entregues nos locais certos, da maneira mais eficiente possível. Eles monitoram a situação física dos produtos, a gestão de materiais, as operações de armazenamento e transporte e as informações financeiras referentes a todas as partes. O sistema de gestão de armazém (SGA) da Haworth Incorporated é um exemplo. A Haworth é líder mundial no projeto e na fabricação de móveis para escritórios, com centros de distribuição em quatro estados diferentes. O SGA rastreia e controla o fluxo dos produtos acabados dos centros de distribuição da Haworth até seus clientes. Agindo sobre os planos de expedição dos pedidos dos clientes, o SGA direciona a movimentação dos produtos com base nas condições imediatas para espaço, equipamento, estoque e pessoal. Manugistics e i2 Technologies (ambas compradas pela JDA Software) são os principais fornecedores de software de gestão da cadeia de suprimentos, ao passo que os fornecedores de software integrado SAP e Oracle-PeopleSoft oferecem módulos específicos para isso.

A Seção interativa sobre tecnologia descreve como o software de gestão da cadeia de suprimentos aprimora o desempenho operacional e a tomada de decisão na Procter & Gamble. Essa multinacional gerencia cadeias de suprimentos globais para mais de 300 marcas, cada uma com suas próprias configurações. Suas cadeias de suprimentos são numerosas e complexas, e a P&G possui muitas aplicações para geri-las. A cadeia descrita aqui é responsável pela otimização de estoque.

Cadeia de suprimentos global e a Internet

Antes da Internet, não era simples coordenar a cadeia de suprimentos: as informações não fluíam livremente entre os sistemas internos de compras, gestão de materiais, produção e distribuição. Também era difícil compartilhar informações com parceiros externos porque os sistemas de fornecedores, distribuidores e provedores de logística se baseavam em plataformas e padrões tecnológicos incompatíveis. Os sistemas integrados conseguiram, em certa medida, conectar os processos internos da cadeia de suprimentos, mas não foram projetados para lidar com processos externos.

Usando a tecnologia da Internet, é possível integrar um pouco mais a cadeia de suprimentos sem gastar muito. As empresas usam *intranets* para aumentar a coordenação entre seus processos internos da cadeia de suprimentos, e *extranets* para coordenar os processos compartilhados com os parceiros de negócios (veja a Figura 8.4).

Por meio de intranets e extranets, todos os membros da cadeia de suprimentos passam a ser instantaneamente capazes de se comunicar entre si, usando informações atualizadas para ajustar compras, logística, produção, embalagem e programações. Um gerente pode usar uma interface da Web para consultar os sistemas dos fornecedores e, assim, verifi-

SEÇÃO INTERATIVA: TECNOLOGIA

A Procter & Gamble tenta otimizar seu estoque

Os corredores de xampus e batons do Carrefour e do Walmart dificilmente parecem campos de batalha, mas costumam ser local para uma competição interminável entre empresas de produtos de consumo por espaço nas prateleiras. Nenhuma empresa sabe melhor disso do que a Procter & Gamble (P&G), uma das maiores companhias mundiais do ramo, com receita anual que ultrapassa 76 bilhões de dólares e 138 mil empregados espalhados em 80 países. A empresa vende mais de 300 marcas ao redor do mundo, incluindo os cosméticos Cover Girl, a linha Olay de cuidados com a pele, Crest, Charmin, Tide, Pringles e Pampers.

A variabilidade da demanda por produtos do departamento de cosméticos da P&G é muito grande. Uma cor popular de sombra ou batom pode rapidamente perder a popularidade, enquanto as tendências da moda exigem continuamente que novos produtos entrem na cadeia. As principais lojas de varejo, como Walmart e Carrefour, competem oferecendo produtos de marcas renomadas ao menor preço possível.

Em resposta a essas pressões, a P&G está sempre pesquisando novas formas de reduzir os custos da cadeia de suprimentos e aprimorar a eficiência em toda a sua rede de manufatura e distribuição. Recentemente, a empresa implantou um sistema multinível de otimização de estoque para gerenciar sua cadeia de suprimentos de modo mais eficiente.

As cadeias de abastecimento de uma empresa tão grande quanto a P&G são extremamente complicadas, com milhares de fornecedores, instalações de manufatura e mercados. Mesmo a mais simples das mudanças em qualquer ponto da cadeia causa efeitos significativos em todos seus participantes. Além disso, como as cadeias de abastecimento da P&G são muito extensas, as chances de ocorrerem erros ou ineficiências são maiores do que nas cadeias menores e mais compactas. Para uma empresa do porte da P&G, a otimização do estoque é crítica para a redução de custos e aumento das receitas. A empresa já era conhecida por sua gestão da cadeia de suprimentos, reduzindo de forma bem-sucedida seu estoque excedente com o planejamento de vendas e operações, melhores previsões, estratégias de distribuição just-in-time e atividade de estoque gerenciada por fornecedores. Mas a otimização multinível de estoque ofereceu à organização novas maneiras de alcançar níveis ainda mais altos de eficiência.

As redes multinível são aquelas nas quais os produtos estão armazenados em uma variedade de locais ao longo do percurso de distribuição, alguns dos quais estão em diferentes 'níveis', ou camadas, da rede de distribuição da empresa. As redes de distribuição de grandes varejistas, por exemplo, costumam ser compostas por um centro regional de distribuição e um grande número de centros para repasse. A presença de múltiplos níveis em uma rede de distribuição torna a gestão de estoque mais difícil porque cada nível está isolado dos outros e, portanto, as modificações no estoque

feitas em um nível podem ter efeitos imprevisíveis nos outros.

A otimização multinível de estoque procura minimizar o estoque total em todos os níveis da cadeia de suprimentos de uma empresa. Isso é mais complicado do que a otimização do estoque tradicional devido ao tempo de execução adicional, ao efeito chicote e à necessidade de sincronização dos pedidos e controle dos custos entre os níveis. Empresas com esse nível de complexidade em suas cadeias de abastecimento devem reabastecer e dividir seus estoques em cada ponto de distribuição ao longo da cadeia, diferentemente dos pontos de distribuição únicos ou mesmo do estoque do fornecedor inicial. Os pontos na cadeia de suprimentos também desconhecem os níveis de estoque dos pontos além daqueles com os quais mantêm contato, o que cria falta de visibilidade na cadeia de suprimentos.

A abordagem multinível de gestão de estoque consiste em: múltiplas atualizações independentes de previsões em cada nível; controle de todos os tempos de execução e de variações nesses tempos; gestão do efeito chicote; criação de visibilidade em toda a cadeia de demanda; estratégias de sincronização de pedidos; e modelagem apropriada dos efeitos das estratégias de abastecimento dos diferentes níveis sobre os outros.

A P&G prefere desenvolver suas próprias ferramentas analíticas, mas, neste caso, recorreu à Optiant e sua ferramenta PowerChain Suite para solução de otimização de estoque multinível. A Gillette, empresa adquirida pela P&G na época, já havia começado a utilizar o software da Optiant com fortes resultados.

O PowerChain Suite determina as configurações adequadas para o estoque que podem se adaptar sem problemas a uma demanda que se altera rapidamente. A solução utiliza modelos matemáticos, baseados em pesquisas premiadas do MIT, que equilibram custos, recursos e serviços aos clientes para chegar a essas configurações. As ferramentas do PowerChain agrupam o estoque de modo a minimizar os riscos entre produtos, componentes e clientes, além de coordenar a política de estoque entre diferentes itens. (A existência de estoque disponível ao mesmo tempo ajuda a reduzir o estoque inicial.) O PowerChain permite que as empresas projetem novas cadeias de abastecimento e modelem sua cadeia do início ao fim. Elas podem, assim, avaliar os custos e o desempenho de estruturas alternativas para a cadeia de suprimentos e para opções de fornecedores a fim de tomar decisões mais acertadas. A Optiant vem fornecendo sistemas de gestão da cadeia de suprimentos para os principais fabricantes, como Black & Decker, HP, IKEA, Imation, Intel, Kraft, Microsoft e Sonoco.

O departamento de produtos de beleza da P&G serviu como projeto-piloto para adoção do software da Optiant. Esse é o maior, mais complicado e mais rentável departamento da empresa. A P&G acreditou que, se as estratégias de otimização multinível pudessem

aumentar os lucros no departamento de produtos de beleza, então seriam capaz de funcionar em qualquer outra parte da empresa.

Primeiro, o software da Optiant foi configurado com a cadeia de suprimentos de cosméticos existente, registrando os últimos 18 meses de dados de demanda e utilizando a variabilidade na demanda dos últimos três meses. Em seguida, otimizou a estratégia de estoque dentro daquela cadeia de suprimentos, com o objetivo de alcançar níveis de serviço acima de 99 por cento. Uma terceira etapa identificou projetos alternativos para cadeias de abastecimento, e a etapa final criou um reprojeto ótimo da rede de abastecimento.

Os resultados foram impressionantes e o departamento de produtos de beleza da P&G reduziu seu esto-

que total entre três e sete por cento, mantendo seus níveis de serviço acima de 99 por cento. No primeiro ano fiscal da implantação do novo software, os ganhos do departamento aumentaram 13 por cento, e as vendas, sete por cento. O período de estoque disponível diminuiu para oito dias comparado ao ano fiscal anterior. Os resultados foram tão bons que a P&G começou a implantar estratégias de estoque multinível em todas as unidades de produção.

Fontes: "Optiant Adds New Inventory Optimization Capabilities and Centralized Administration Portal". Supply & Demand Chain Executive, 27 fev. 2009; John Kerr, "Procter & Gamble Takes Inventory Up a Notch", Supply Chain Management Review, 13 fev. 2008; Optiant, "Optiant Announces Multi-Echelon Inventory Optimization Enterprise Agreement with P&G", 17 out. 2007; e www.optiant.com. Acessado em 17 jul. 2009.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. Por que é mais difícil gerenciar as cadeias de abastecimento maiores? Liste diversos motivos.
2. Por que a gestão da cadeia de suprimentos é tão importante em uma empresa como a P&G?
3. Qual foi o impacto causado pela otimização do estoque sobre as operações e a tomada de decisões?
4. Por que uma empresa pequena não obteria tantos benefícios quanto uma empresa grande com a otimização de estoque multinível? Explique.

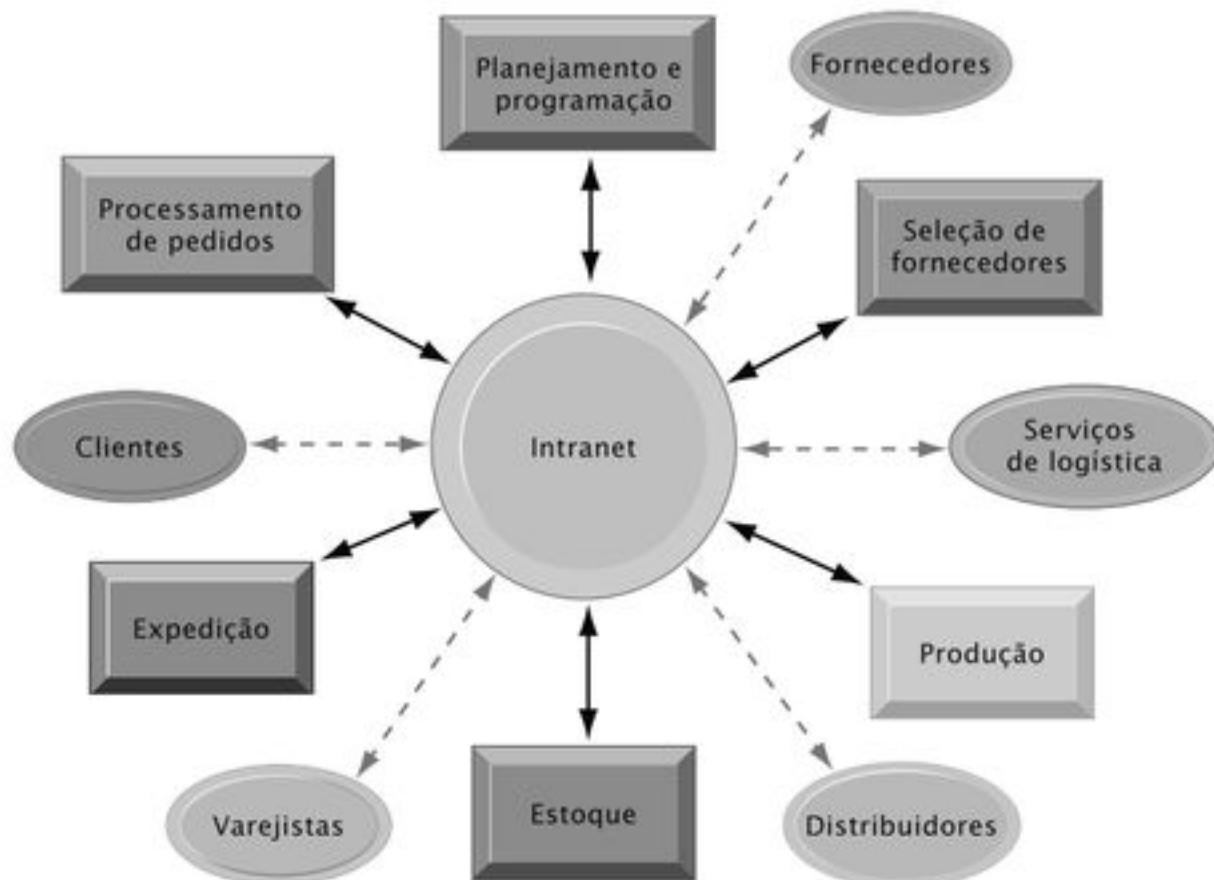


Figura 8.4

Intranets e extranets para gestão da cadeia de suprimentos

As intranets integram informações provenientes de processos de negócios isolados dentro da empresa, ajudando na gestão da cadeia de suprimentos interna. O acesso a essas redes privadas também pode ser estendido a certos fornecedores, distribuidores, serviços de logística e, às vezes, clientes de varejo, a fim de melhorar a coordenação dos processos externos da cadeia de suprimentos.

car se sua capacidade de produção e estoque atende à demanda pelos produtos da empresa. Parceiros de negócios podem usar ferramentas de gestão da cadeia de suprimentos baseadas na Web para fazer previsões conjuntas on-line. Representantes de vendas podem acessar informações dos fornecedores sobre logística e programação de produção para monitorar o andamento dos pedidos.

Questões relacionadas à cadeia de suprimentos global

Um número cada vez maior de empresas está entrando em mercados internacionais, terceirizando operações de manufatura, obtendo fornecedores em outros países e vendendo seus produtos internacionalmente. Suas cadeias de suprimentos estendem-se por muitos

países e regiões. Existem complexidades e desafios adicionais na gestão de uma cadeia de suprimentos global.

As cadeias de suprimentos globais costumam se estender por distâncias geográficas e fusos horários diferentes, mais amplos do que aqueles das cadeias nacionais, e possuem participantes em países variados. Embora o preço de compra de muitos produtos seja mais baixo em outros países, sempre existem custos adicionais de transporte, estoque (necessidade de um estoque de segurança maior) e taxas e impostos locais. Os padrões de desempenho podem variar de região para região ou de nação para nação. A gestão da cadeia de suprimentos pode precisar refletir regulamentações governamentais estrangeiras e diferenças culturais. Todos esses fatores causam impacto sobre a forma como a empresa registra pedidos, planeja distribuições, dimensiona armazéns e gerencia as logísticas interna e externa em todos os mercados globais que atende.

A Internet ajuda as empresas a gerenciar muitos aspectos de suas cadeias de suprimentos globais, incluindo aquisição, transporte, comunicações e finanças internacionais. A atual indústria de vestuário, por exemplo, baseia-se fortemente na terceirização para contratar fornecedores na China e em outros países de baixa renda. As empresas de vestuário estão começando a usar a Web para gerenciar sua cadeia de suprimentos global e as questões relacionadas a produtos.

A Koret of California, por exemplo, subsidiária da Kellwood Co., usa o software e-SPS baseado na Internet para ganhar visibilidade total da cadeia de suprimentos. O software oferece recursos para aquisição, rastreamento de trabalho em andamento, roteamento de produção, controle do desenvolvimento do produto, identificação de problemas e colaboração, projeções de datas de entrega, solicitações e relatórios relacionados à produção.

À medida que os produtos são adquiridos, produzidos e expedidos, é preciso que haja comunicação entre varejistas, produtores, fornecedores, agentes e provedores de serviços de logística. Muitas empresas, em especial as pequenas, ainda compartilham informações sobre produtos através de telefone, e-mail ou fax. Esses meios desaceleram a cadeia de suprimentos e também aumentam os erros e a incerteza. Com o e-SPS, todos os integrantes da cadeia de suprimentos se comunicam através de um sistema na Web. Se um dos fornecedores da Koret modifica o andamento de um produto, todos os outros na cadeia de suprimentos conseguem visualizar a modificação.

Além da fabricação terceirizada, a globalização encorajou a gestão da terceirização de armazenamento, do transporte e das operações relacionadas a fornecedores terceirizados de serviços de logística, como UPS Supply Chain Solutions e Schneider Logistics Services. Esses serviços de logística oferecem software baseado na Web para oferecer a seus clientes uma melhor visão de suas cadeias de suprimentos. Os clientes conseguem consultar um site Web seguro para monitorar estoque e expedição, ajudando-lhes a gerenciar de maneira mais eficiente suas cadeias de suprimentos globais.

Cadeias de suprimentos orientadas pela demanda: da produção push para a produção pull e resposta eficiente ao cliente

Além de reduzir custos, os sistemas de gestão da cadeia de suprimentos possibilitam uma resposta eficiente ao cliente, permitindo que o funcionamento da empresa seja direcionado segundo a demanda do consumidor. (Introduzimos os sistemas de resposta eficiente ao cliente no Capítulo 3.)

Os primeiros sistemas de gestão da cadeia de suprimentos eram direcionados por um modelo push ('empurrão'). No **modelo push**, as programações de produção baseiam-se em previsões ou nas melhores avaliações da demanda por produtos, que são 'empurrados' aos clientes. Com os novos fluxos de informação viabilizados por ferramentas baseadas na Internet, a gestão da cadeia de suprimentos pode seguir mais facilmente um **modelo pull**. No modelo pull, também conhecido como *modelo orientado pela demanda* ou **build-to-order (feito-para-pedido)**, os pedidos ou as compras reais do cliente disparam as etapas da cadeia de suprimentos. As transações necessárias para produzir e entregar apenas o que os clientes solicitaram ascendem pela cadeia, desde os varejistas até os distribuidores, destes aos fabricantes e, depois, aos fornecedores. Apenas os produtos destinados a atender a esses

pedidos voltam pela cadeia de suprimentos até o varejista. Os fabricantes usam apenas a informação de demanda efetiva para orientar suas programações de produção e a seleção de componentes e matérias-primas, conforme mostrado na Figura 8.5. O sistema de reposição contínua do Walmart e o sistema de montagem sob encomenda da Dell Computer Corporation, ambos descritos no Capítulo 3, são exemplos do modelo pull.

A Internet e a respectiva tecnologia permitem que se passe das cadeias de suprimentos sequenciais, em que informações e materiais fluem sequencialmente de empresa para empresa, para cadeias de suprimentos concomitantes, em que a informação flui em muitas direções, simultaneamente, entre os membros de uma rede de cadeias de suprimentos. Os membros da rede ajustam-se imediatamente a mudanças na programação e nos pedidos. Em última instância, a Internet pode criar um ‘sistema nervoso digital de logística’ que abrange toda a cadeia de suprimentos (veja a Figura 8.6).

Valor empresarial dos sistemas de gestão da cadeia de suprimentos

Você acabou de ver como os sistemas de gestão da cadeia de suprimentos permitem que as empresas rationalizem seus processos internos e externos da cadeia de suprimentos e, além disso, oferecem à administração informações mais precisas sobre o que produzir, esto-

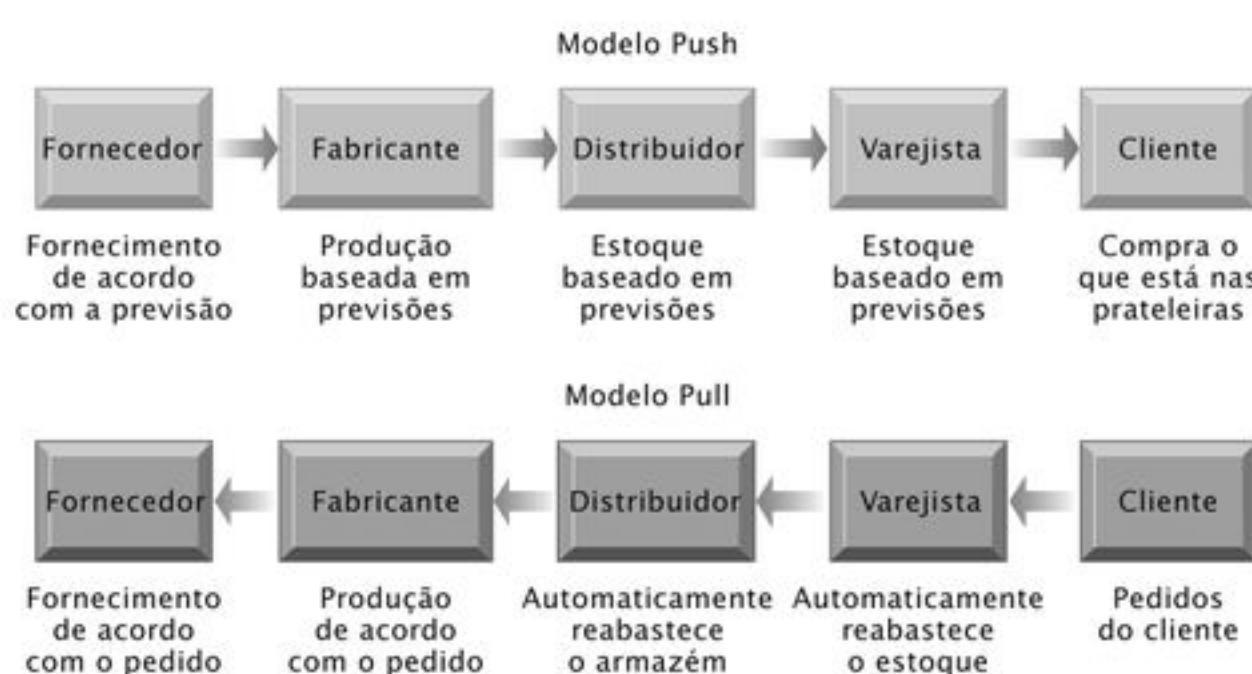


Figura 8.5

Modelos de cadeia de suprimentos push e pull

A diferença entre os modelos push e pull pode ser resumida nesta frase: “Vamos produzir o que vendemos, não vender o que produzimos”.

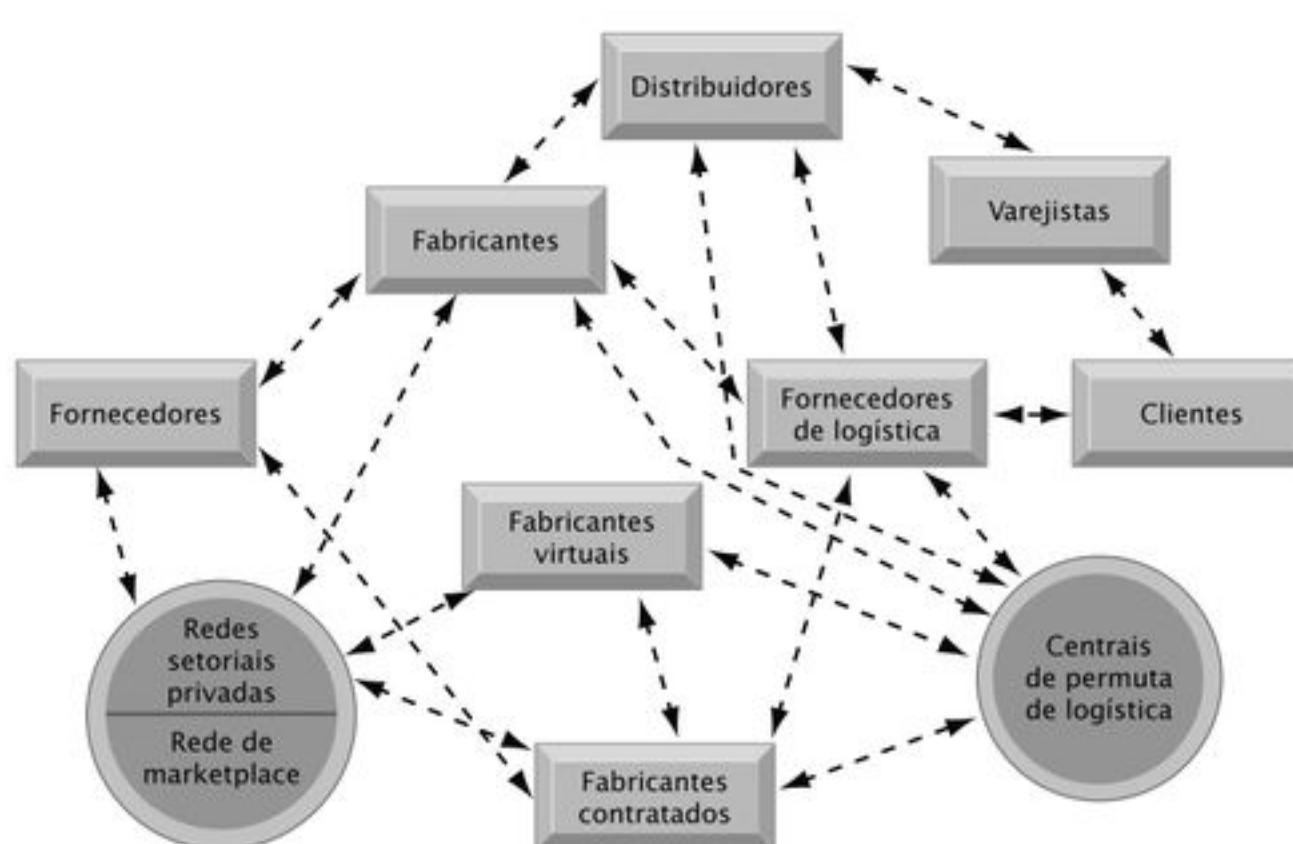


Figura 8.6

Futura cadeia de suprimentos orientada pela Internet

Esta cadeia opera como um sistema nervoso digital de logística. Provê comunicação multidirecional entre empresas, redes de empresas e e-marketplaces de mercado, de modo que redes inteiras de parceiros de cadeia de suprimentos possam ajustar estoques, pedidos e capacidades imediatamente.

car e transportar. Ao implantar um sistema de gestão da cadeia de suprimentos em rede e integrado, as empresas sintonizam oferta e demanda, reduzem níveis de estoque, melhoram o serviço de entrega, diminuem o tempo que o produto leva para chegar ao mercado e usam os ativos de maneira mais eficiente.

No caso de muitas empresas, os custos totais da cadeia de suprimentos respondem pela maior parte das despesas operacionais e, em alguns setores, chegam perto de 75 por cento do orçamento operacional total. Logo, reduzir tais custos pode ter um impacto significativo na lucratividade da empresa.

Além de reduzir custos, os sistemas de gestão da cadeia de suprimentos podem aumentar as vendas. Se um produto não estiver disponível quando o cliente o deseja, na maioria das vezes ele tentará comprá-lo de outro fornecedor. Um controle mais preciso da cadeia de suprimentos aumenta a capacidade da empresa de ter o produto certo disponível para o consumidor no momento adequado.

Sistemas de gestão do relacionamento com o cliente

Provavelmente você já ouviu bordões como “O cliente tem sempre razão”, ou “O cliente vem em primeiro lugar”. Atualmente, essas palavras soam mais verdadeiras do que nunca. Como a vantagem competitiva baseada em um produto ou serviço inovador tem, na maioria das vezes, um tempo de vida muito curto, as empresas estão percebendo que sua única força competitiva duradoura pode estar no relacionamento com os clientes. Alguns dizem que a base da concorrência deixou de ser quem vende mais produtos e serviços, para ser quem é o ‘dono’ do cliente, e que os relacionamentos com o público representam o ativo mais valioso de uma empresa.

O que é gestão do relacionamento com o cliente?

De que tipos de informação você precisaria para construir e cultivar relacionamentos sólidos e duradouros com os clientes? Você precisaria saber exatamente quem são eles, como contatá-los, se é dispensoso atendê-los, em quais tipos de produtos e serviços estão interessados e quanto dinheiro gastam com sua empresa. Se possível, seria bom que conhecesse bem cada um de seus potenciais compradores, tal como se administrasse uma lojinha de cidade pequena. E também precisaria fazer com que seus bons clientes se sentissem especiais.

Em uma pequena empresa de bairro, os proprietários e gerentes podem de fato conhecer seus clientes pessoalmente, face a face. Porém, em uma grande empresa que atua em escala metropolitana, regional, nacional ou mesmo global, é impossível ‘conhecer o cliente’ de maneira tão estreita. Nesses tipos de empresa existe uma quantidade imensa tanto de compradores quanto de maneiras pelas quais eles interagem com a organização (via Web, telefone, fax e face a face). Torna-se incrivelmente difícil integrar as informações de todas essas fontes para lidar com o grande número de clientes.

Um grande processo de negócios, que envolva vendas, serviços e marketing, tende a ser altamente compartmentado, e esses departamentos não compartilham muitas informações essenciais sobre clientes. Algumas informações sobre determinado cliente podem estar armazenadas e organizadas em relação à conta daquela pessoa com a empresa. Outras informações sobre o mesmo cliente podem estar organizadas segundo os produtos por ele adquiridos. Não há como consolidar todas as informações de modo a oferecer uma visão unificada de um cliente na empresa.

É aí que entram em cena os sistemas de gestão do relacionamento com o cliente (*customer relationship management* — CRM). Esses sistemas, introduzidos no Capítulo 2, capturam e integram dados do cliente provenientes de toda a organização, consolidam e analisam essas informações, e depois distribuem os resultados para vários sistemas e pontos de contato com o cliente espalhados por toda a empresa. Um **ponto de contato** é um canal de interação com o cliente, como telefone, e-mail, serviço de atendimento, correspondência convencional, site, dispositivo sem fio ou loja de varejo.

Sistemas CRM bem projetados oferecem uma visão única dos clientes que serve para melhorar tanto as vendas quanto o atendimento. Da mesma maneira, esses sistemas oferecem ao cliente uma visão única da empresa, independentemente de qual ponto de contato esteja usando (veja a Figura 8.7).

Os bons sistemas de CRM fornecem dados e ferramentas analíticas para responder a perguntas como: qual é o valor ao longo do tempo de determinado cliente para a empresa? Quem são os mais fiéis? (Custa seis vezes mais vender para um cliente novo do que para um já existente.) Quem são os mais lucrativos? E o que desejam comprar? As empresas podem então usar as respostas para conquistar novos clientes, oferecer melhores serviços e suporte aos atuais, personalizar suas ofertas com maior precisão em relação às preferências do comprador e oferecer valor contínuo para reter os clientes lucrativos.

Software CRM

Os pacotes de software CRM comerciais vão desde ferramentas de nicho que executam apenas algumas funções, como personalizar sites para clientes específicos, até aplicativos integrados de larga escala, que capturam inúmeras interações com os clientes, realizam análises com sofisticadas ferramentas de relatório e interligam-se a outros grandes aplicativos integrados, como sistemas integrados e de gestão da cadeia de suprimentos. Os pacotes CRM mais abrangentes contêm módulos para **gestão do relacionamento com o parceiro (partner relationship management — PRM)** e **gestão do relacionamento com o funcionário (employee relationship management — ERM)**.

O PRM usa, em grande parte, os mesmos dados, ferramentas e sistemas que a gestão do relacionamento com o cliente, mas seu objetivo é melhorar a colaboração entre a empresa e seus parceiros de venda. Se uma organização não vende diretamente aos clientes, mas por meio de distribuidores ou varejistas, o PRM ajuda esses canais na venda direta. Com ele, a empresa e seus parceiros podem intercambiar informações, bem como distribuir indicações de venda e dados sobre os clientes, integrando elementos como geração de indicações, determinação de preços, promoções, configurações de pedido e disponibilidade. O PRM também proporciona à empresa ferramentas para avaliar o desempenho de seus parceiros; assim, ela pode garantir que seus melhores parceiros recebam o apoio necessário para fechar mais negócios.

O ERM lida com assuntos de RH estreitamente relacionados ao CRM, tais como estabelecimento de objetivos, gestão do desempenho do funcionário, remuneração baseada no desempenho e treinamento. Entre os principais fornecedores de software aplicativo CRM estão Siebel e a Peoplesoft (adquiridos pela Oracle), SAP e Salesforce.com. Fornecedores de software integrado, como a SAP e a Oracle-PeopleSoft CRM, SAP, Salesforce.com e Microsoft Dynamics CRM.



Figura 8.7

Gestão das relações com o cliente (CRM)

Os sistemas CRM examinam os clientes sob uma perspectiva multifacetada. Usam um conjunto de aplicações integradas para abordar todos os aspectos do relacionamento com o cliente, inclusive atendimento, vendas e marketing.

Normalmente, os sistemas de gestão do relacionamento com o cliente oferecem softwares e ferramentas on-line para as áreas de vendas, atendimento ao cliente e marketing. Alguns desses recursos são comentados a seguir.

Automação da força de vendas

Os módulos de automação da força de vendas nos sistemas CRM ajudam a equipe de vendas a aumentar a produtividade, concentrando seus esforços nos clientes mais lucrativos, aqueles com maior probabilidade de adquirir produtos e serviços. Os sistemas CRM oferecem informações relativas a contatos e prospecção de vendas e aos produtos, além de recursos para configuração de produtos e geração de cotações. Tais softwares podem reunir informações sobre o histórico de compras de determinado cliente, ajudando o vendedor a fazer recomendações personalizadas. Os softwares CRM também permitem que os departamentos de vendas, marketing e entrega compartilhem facilmente informações sobre clientes e prospects. Isso aumenta a eficiência de cada vendedor, reduzindo tanto o custo por venda quanto o custo de conquistar e reter clientes. Softwares CRM também apresentam funções de previsão de vendas, gestão de território e venda em equipe.

Atendimento ao cliente

Os módulos de atendimento ao cliente nos sistemas CRM oferecem informações e ferramentas para aumentar a eficiência de *call centers*, help desks e da equipe de suporte. Possuem recursos para encaminhar e gerenciar solicitações de serviços feitas pelos clientes.

Um desses recursos é uma linha telefônica para consultas ou marcação de visitas: quando o comprador liga para determinado número de telefone, o sistema encaminha a chamada ao atendente adequado, que insere no sistema informações sobre aquele cliente uma única vez. Uma vez que os dados estejam no sistema, qualquer atendente pode conduzir o relacionamento com ele. Com acesso mais fácil a informações precisas e coerentes sobre o cliente, os *call centers* podem atender a mais chamadas por dia e passar menos tempo em cada. Dessa maneira, os telefonistas e os grupos de atendimento ao cliente conseguem maior produtividade, tempos de transação menores e serviços de qualidade mais elevada a um custo mais baixo. O cliente fica mais satisfeito porque gasta menos tempo na linha contando outra vez seu problema ao atendente.

A Seção interativa sobre organizações descreve outro recurso de CRM para melhoria do atendimento aos clientes e da eficiência operacional. A implementação do software da Enkata ajudou a JP Morgan Chase a aumentar sua taxa de resolução na primeira ligação, que acontece quando um atendente consegue resolver um problema do cliente na primeira ligação.

Os sistemas CRM também podem incluir recursos de autoatendimento baseados na Web: o site da empresa pode ser configurado para oferecer suporte personalizado, assim como a opção de contatar a equipe de atendimento ao cliente para assistência adicional.

Marketing

Os sistemas CRM colaboram com as campanhas de marketing direto, pois oferecem a possibilidade de capturar dados de clientes e prospects, fornecer informações sobre produtos e serviços, classificar indicações para marketing direcionado e programar e monitorar e-mails ou correspondência de marketing direto (veja a Figura 8.8). Os módulos de marketing também incluem ferramentas para análise de marketing e dados de clientes, com o objetivo de identificar clientes lucrativos ou não, projetar produtos e serviços que satisfazem as necessidades e os interesses de clientes específicos e identificar oportunidades para *cross-selling* (venda cruzada).

Cross-selling (venda cruzada) é o marketing de produtos complementares. Na área de serviços financeiros, por exemplo, pode-se vender a um cliente que tenha conta-corrente um título de capitalização ou um financiamento imobiliário. As ferramentas CRM também ajudam as empresas a gerenciar e executar todas as etapas de suas campanhas de marketing, desde o planejamento até a determinação da taxa de sucesso de cada campanha.

SEÇÃO INTERATIVA: ORGANIZAÇÕES

Se você possui um cartão de crédito norte-americano, existe uma boa chance de que ele seja da Chase. A Chase Card Services é uma divisão da JP Morgan Chase especializada em cartões de crédito que oferece uma gama de produtos deste nicho, a exemplo do cartão Chase Rewards Platinum Visa. Como uma das maiores administradoras de cartões de crédito dos Estados Unidos, a empresa recebe um volume igualmente grande de ligações de pessoas em busca de atendimento para suas contas de cartão de crédito. Diariamente, cada um dos 6 mil atendentes espalhados pelo mundo nas 11 centrais de atendimento da Chase atende até 120 ligações. A empresa contabiliza pouco menos de 200 milhões de chamadas por ano oriundas de uma base de 100 milhões de clientes.

Mesmo a pequena redução de um por cento no volume de ligações recebidas resulta em uma economia de milhões de dólares e na melhoria do atendimento ao cliente para a Chase. Entretanto, é mais fácil falar de tal redução do que alcançá-la. Em 2006, a Chase Card Services tentou realizar tal façanha através da melhoria da resolução na primeira ligação. A resolução na primeira ligação acontece quando um atendente da central de atendimento consegue resolver um problema do cliente durante a primeira ligação para o serviço de atendimento, sem que sejam necessárias ligações adicionais.

O problema era que a manutenção dos registros da empresa não contabilizava com precisão a taxa atual de resoluções na primeira ligação. A Chase já havia tentado controlar as resoluções na primeira ligação fazendo com que os atendentes registrassem o conteúdo e os resultados de cada ligação recebida. Entretanto, essa tarefa era demorada e não padronizada — os atendentes tendiam a registrar os resultados de forma subjetiva e não de maneira uniforme. As políticas da empresa para algumas solicitações dos clientes também estavam longe do ideal para que se aumentasse o número de resoluções na primeira ligação. Por exemplo, os atendentes somente conseguiam processar as transferências de saldo para os clientes que ligassem de casa, e a estrutura de pagamento passou por diversas mudanças em curto intervalo, o que estimulou a repetição de chamadas.

Para aumentar a eficiência da central de atendimento, a Chase contratou a Enkata Technologies para implantar sistema de gestão de desempenho e talentos.

O sistema monitora e identifica cada ligação com informações sobre o assunto e a duração da chamada, bem como o tempo que o atendente leva trabalhando no atendimento. Não há necessidade de os atendentes realizarem nenhuma tarefa adicional para que as informações sejam obtidas; o sistema controla automaticamente as ligações através do registro das teclas digitadas pelo atendente.

Assim que o atendente clica sobre o recurso da conta sobre o qual o cliente deseja informações, o sistema da Enkata automaticamente identifica o motivo da ligação.

Gestão do relacionamento com o cliente ajuda a Chase Card Services a gerenciar as ligações dos clientes

Algoritmos proprietários combinam a razão da chamada com a identificação de quem está ligando com o tempo predeterminado para cada tipo de ligação.

O sistema então monitora discrepâncias no tempo da ligação em função de seu motivo. Por exemplo, a ligação de um cliente solicitando a ativação de um cartão deve ser rápida; portanto, o sistema identificará as chamadas para ativação de cartão que durarem mais do que o normal, ou as ligações para discussão de taxas que forem mais curtas do que o normal. Algumas vezes, entretanto, os clientes possuem múltiplas razões para ligar, o que teria sido muito difícil de controlar antes da implantação do sistema da Enkata. Agora, o sistema separa cada razão individual para ligação e as organiza em sequência de modo que uma ligação para tratar de diversas questões seja analisada com base na estrutura de tempo apropriada.

Separando e organizando as razões para a ligação em diferentes categorias, a Chase consegue definir critérios para decidir se determinadas chamadas estão 'resolvidas'.

Por exemplo, uma ligação para ativar um cartão será considerada resolvida somente depois de alguns dias sem que haja ligação de retorno, mas uma reclamação de cobranças não será considerada resolvida até que o cliente receba outra fatura sem quaisquer reclamações. Esse método oferece à Chase dados muito mais precisos sobre resoluções na primeira ligação, feito considerado muito difícil e impressionante no setor.

A Enkata compila os dados e os distribui para a Chase Card Services em forma de relatórios semanais por tipo de ligação e duração, tempo de gestão da ligação, taxas de repetição de chamadas e outras medidas de desempenho que permitem que atendentes e supervisores monitorem seu desempenho. O sistema também conecta os relatórios com os registros de ligações para ajudar os gerentes no acompanhamento e na avaliação de seus atendentes. Quando o sistema ainda estava sendo implementado, a Enkata utilizou dados históricos coletados antes da implementação para criar os relatórios iniciais. Os executivos da Chase Card Services consideraram essa carga inicial de dados a parte mais demorada da implementação. Uma vez concluído o processo, a empresa esperava que as melhorias na interpretação e na gestão das informações levassem a melhorias no desempenho dos atendentes e na satisfação e retenção de clientes.

Os resultados falam por si. No primeiro ano após a implantação do sistema da Enkata, a Chase Card Services aumentou em 91 por cento sua taxa de resolução na primeira ligação — um aumento de três por cento —, o que representou uma economia total de 8 milhões de dólares. Aproximadamente 2,5 milhões da economia total foram um resultado direto da diminuição em dois segundos do tempo médio de duração de uma ligação.

A empresa espera alcançar sua meta de 95 por cento nos próximos anos. A taxa ideal de cem por cento de resoluções na primeira ligação não é possível porque, em determinadas circunstâncias, é aceitável que existam algumas ligações adicionais depois da primeira, como no caso de o cliente lembrar uma reclamação de cobrança previamente relatada.

Depois de três meses, 30 por cento dos atendentes que registraram taxa de atendimento abaixo do esperado nas resoluções na primeira ligação subiram para um nível aceitável. Após a implantação do sistema, embora o número de contas ativas de clientes tenha subido 5,2

por cento em seis meses, o volume de ligações diminuiu em 8,3 por cento durante o mesmo período.

Encorajados por esses casos de sucesso, a Chase Card Services está agora buscando a expansão dos recursos do sistema para classificar as ligações em um número ainda maior de categorias, e relacionar os dados coletados a programas de marketing para incentivar a venda cruzada e aumentar o volume de vendas.

Fontes: Marshall Lager, "Credit Where Due", *Customer Relationship Management*, abr. 2008; e Michele Heller "How Chase Got Control of Call-Center Expenses", *American Banker*, 26 fev. 2008.

PERGUNTAS SOBRE O ESTUDO DE CASO

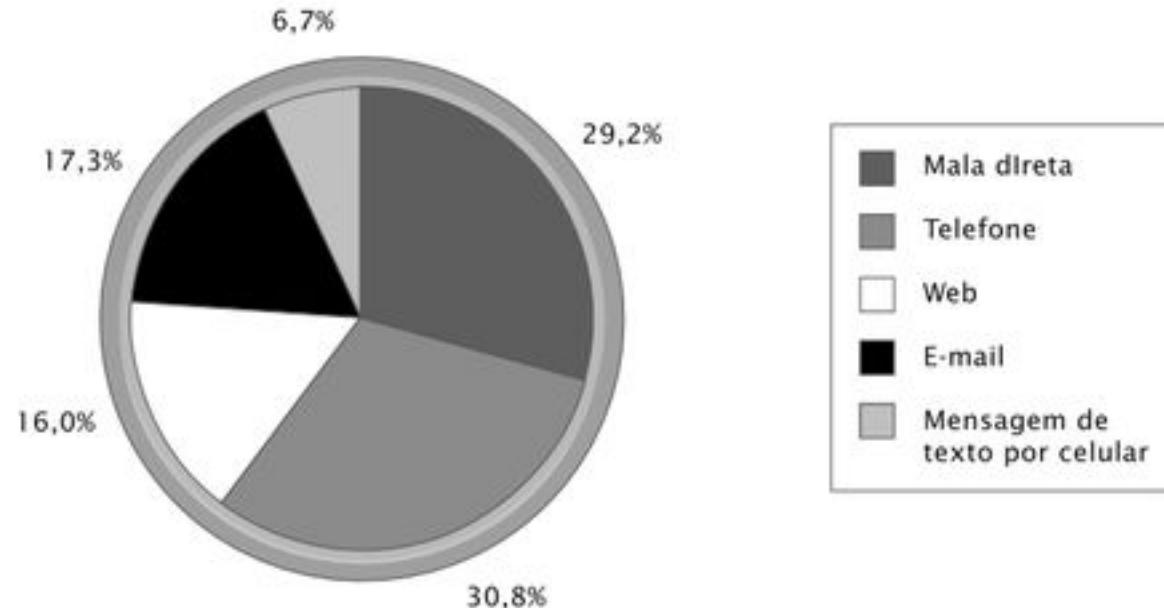
1. Que funções dos sistemas de gestão do relacionamento com o cliente são ilustradas nesse caso?
2. Por que a central de atendimento é tão importante para a Chase Card Services? Como a central de atendimento pode ajudar a Chase a melhorar seu relacionamento com os clientes?
3. Descreva o problema encontrado nas centrais de atendimento da Chase. Quais fatores gerenciais, organizacionais e tecnológicos contribuíram para o problema?
4. Como a utilização do sistema da Enkata ajudou a melhorar o desempenho operacional e a tomada de decisões? Dê exemplos.
5. Quais fatores gerenciais, organizacionais e tecnológicos tiveram de ser considerados na implementação da solução da Enkata?

Figura 8.8

Como os sistemas CRM colaboram com o marketing

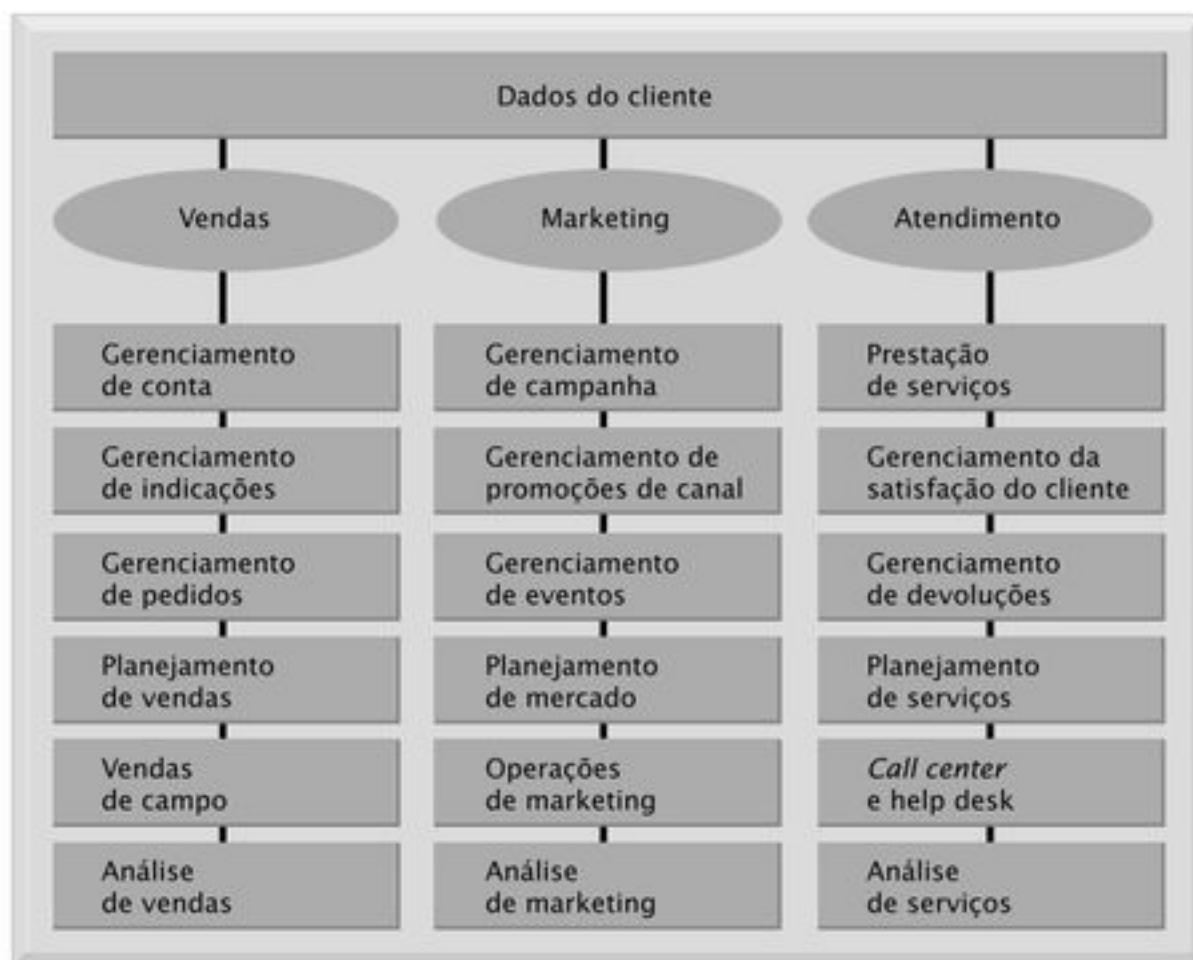
Com os softwares de gestão do relacionamento com o cliente, os usuários têm um único ponto para administrar e avaliar as campanhas de marketing realizadas em múltiplos canais, incluindo e-mail, mala direta, telefone, a Web e mensagens de dispositivos sem fio.

**Respostas por canal em janeiro de 2010
Campanha promocional**



A Figura 8.9 ilustra os recursos mais importantes para os processos de vendas, atendimento e marketing que podem ser encontrados nos principais produtos de software CRM. Assim como o software integrado, esse tipo de software é orientado segundo processos de negócios, incorporando centenas de processos de negócios considerados as melhores práticas em cada uma dessas áreas. Para extrair o máximo de benefício, as empresas precisam revisar e remodelar seus processos de negócios, a fim de que correspondam aos processos de negócios de melhores práticas de CRM.

A Figura 8.10 ilustra como uma melhor prática para aumentar a fidelidade do cliente por meio do atendimento pode ser remodelada pelo software CRM. Ao atender os clientes diretamente, as empresas ganham a oportunidade de aumentar a retenção deles, pois podem selecionar os clientes mais lucrativos no longo prazo e prestar-lhes atendimento preferencial. O software CRM pode atribuir a cada cliente uma 'nota' com base em sua fidelidade e seu valor para a empresa; com essa informação, os *call centers* podem direcionar uma solicitação de serviço

**Figura 8.9**

Recursos dos softwares CRM

Os principais produtos de software CRM apoiam os processos de negócios nas áreas de vendas, atendimento e marketing, integrando informações do cliente provenientes de diversas fontes. Aqui incluímos o apoio para os aspectos tanto operacionais quanto analíticos de CRM.

aos atendentes mais adequados para lidar com as necessidades daquele cliente. Em seguida, o sistema fornece automaticamente ao agente um perfil detalhado do cliente, incluindo sua ‘nota’ de valor e fidelidade. Essas informações servirão para o agente apresentar ofertas especiais ou serviços adicionais, estimulando esse cliente a continuar fechando negócios com a empresa.

CRM analítico e operacional

Todas as aplicações que acabamos de descrever apoiam tanto aspectos operacionais quanto analíticos da gestão do relacionamento com o cliente. O **CRM operacional** abrange as aplicações voltadas ao cliente, tais como ferramentas para automação da força de vendas, apoio ao atendimento e ao *call center* e automação do marketing. Já o **CRM analítico** abrange as aplicações que analisam os dados do cliente gerados pelas aplicações CRM operacionais, a fim de fornecer informações para que se gerencie melhor o desempenho da empresa.

Figura 8.10

Mapa de processo da gestão da fidelidade do cliente

Este mapa de processo mostra como uma melhor prática para aumentar a fidelidade do cliente por meio do atendimento poderia ser remodelada pelo software de gestão do relacionamento com o cliente. O software CRM ajuda as empresas a identificar aqueles com maior valor, a fim de oferecer atendimento preferencial.



As aplicações de CRM analíticas baseiam-se em *data warehouses* que consolidam os arquivos dos sistemas CRM operacionais e dos pontos de contato com o cliente, usando-os para processamento analítico on-line (OLAP), *data mining* e outras técnicas de análise de dados (veja o Capítulo 5). Os dados do cliente coletados pela organização podem ser combinados com os de outras fontes, como listas de clientes para campanhas de marketing direto adquiridas de outras empresas ou dados demográficos. A análise de tais dados visa identificar padrões de compra, a fim de criar segmentos para o marketing direcionado e distinguir clientes lucrativos e não lucrativos (veja a Figura 8.11).

Outro dado importante proporcionado pelo CRM analítico é o valor do cliente ao longo do tempo para a empresa. O **valor do cliente ao longo do tempo (customer lifetime value — CLTV)** baseia-se na relação entre a receita produzida por um comprador específico, as despesas decorrentes de conquistá-lo e atendê-lo e a duração esperada do relacionamento entre esse cliente e a empresa.

Valor empresarial dos sistemas de gestão do relacionamento com o cliente

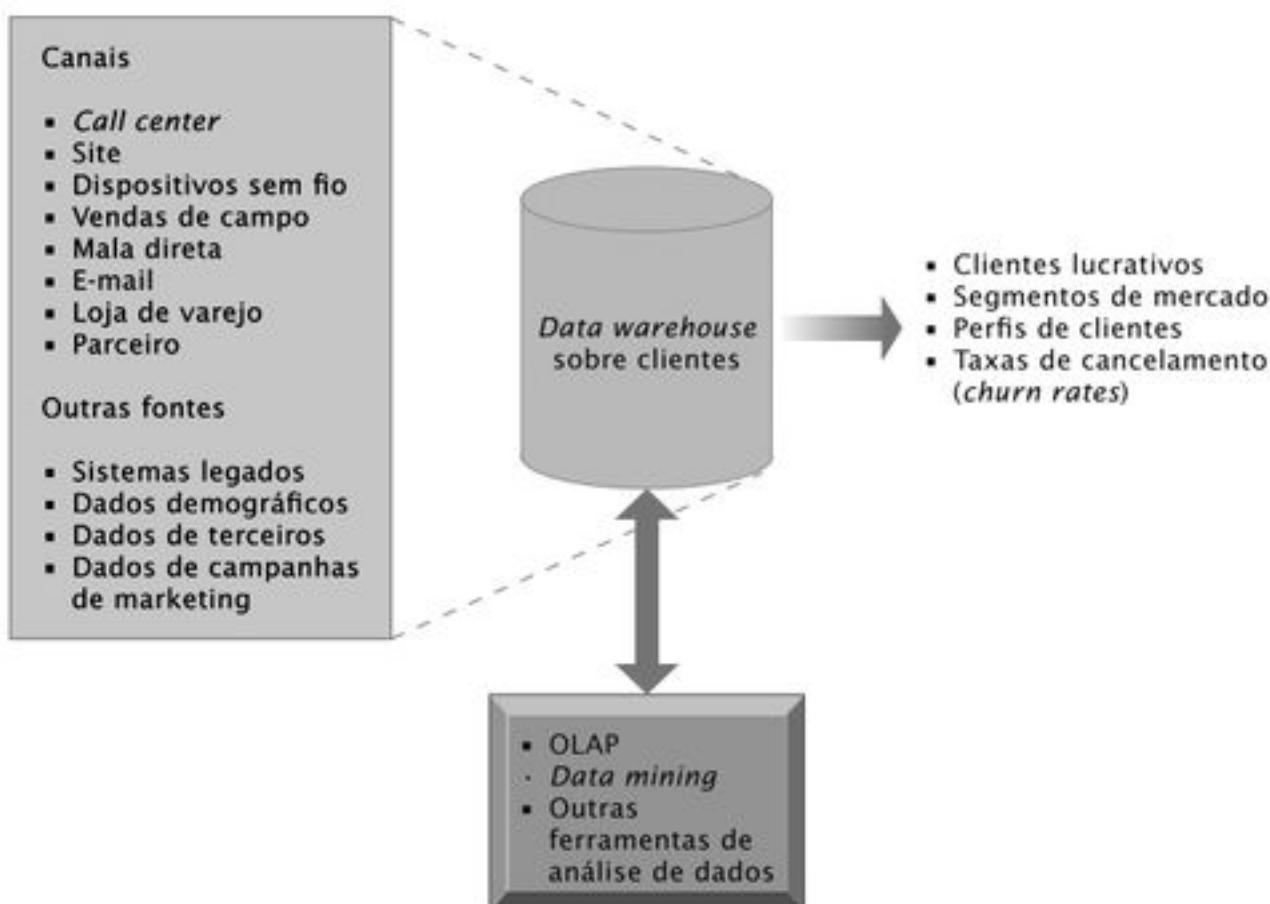
As empresas que usam sistemas eficientes de gestão do relacionamento com o cliente percebem muitos benefícios, entre eles maior satisfação do cliente, menores custos de marketing direto, marketing mais eficiente e menores custos de conquista e retenção do cliente. As informações fornecidas pelo sistema CRM aumentam a receita de vendas, pois permitem identificar os segmentos e clientes mais lucrativos para marketing focado e *cross-selling*.

Por outro lado, o cancelamento de contratos cai à medida que as áreas de vendas, atendimento e marketing ficam mais sintonizadas com as necessidades do cliente. A **taxa de cancelamento (churn rate)** mede o número de pessoas que param de usar ou adquirir os produtos ou serviços de uma empresa. É um importante indicador do crescimento ou declínio da base de clientes da empresa.

Figura 8.11

Data warehouse de CRM analítico

O CRM analítico usa um data warehouse sobre clientes, bem como ferramentas para analisar dados coletados nos pontos de contato da empresa com o cliente e em outras fontes.



Aplicações integradas: novas oportunidades e desafios

Muitas empresas vêm implementando sistemas integrados e sistemas para gestão da cadeia de suprimentos e gestão do relacionamento com o cliente, por serem eles instrumentos eficazes na conquista da excelência operacional e no aprimoramento da tomada de decisão. No entanto, justamente por serem tão eficazes em alterar o funcionamento da organização, sua implantação apresenta inúmeros desafios. Vamos examinar brevemente alguns desses desafios, assim como novas maneiras de extrair ainda mais valor desses sistemas.

Desafios das aplicações integradas

Promessas de redução radical nos custos de estoque e no tempo do pedido até a entrega, assim como resposta mais eficiente ao cliente e maior lucratividade por consumidor e por produto fazem dos sistemas integrados e para gestão da cadeia de suprimentos e do relacionamento com o cliente ferramentas muito atrativas. No entanto, para usufruir de todos esses benefícios, é preciso entender claramente como sua empresa deve mudar para usar tais sistemas com eficácia.

Aplicativos integrados envolvem partes complexas de software que são muito caras de comprar e implementar. Uma grande empresa pode levar anos para concluir uma implementação em larga escala de um sistema aplicativo ou de um sistema para CRM ou SCM. O custo total de implementação de um grande sistema, incluindo software, ferramentas de banco de dados, taxas de consultoria, custos pessoais, treinamento e, talvez, equipamentos, pode aumentar de quatro a cinco vezes o preço inicial de aquisição de um software.

As aplicações integradas não exigem apenas mudanças tecnológicas profundas, mas alterações fundamentais no funcionamento da empresa. Os processos de negócio mudam radicalmente, assim como a cultura e a estrutura organizacional. Os funcionários precisam aceitar novas funções e responsabilidades. Têm de aprender a realizar um novo conjunto de atividades e entender como as informações que inserem no sistema podem afetar outras partes da empresa. Tudo isso requer um novo aprendizado organizacional.

Os sistemas para gestão da cadeia de suprimentos exigem que as múltiplas empresas compartilhem informações e processos de negócios. Cada participante no sistema pode precisar alterar alguns de seus processos e o modo como usa as informações para criar um sistema que atenda melhor à cadeia de suprimentos como um todo.

Algumas empresas vivenciam grandes problemas e perdas organizacionais quando implementaram pela primeira vez aplicações integradas, pois não compreenderam o volume necessário de modificação organizacional.

- Kmart teve problemas na movimentação dos produtos para as prateleiras das lojas quando implantou o software de gestão da cadeia de suprimentos da i2 Technologies, em julho de 2000. O software da i2 não funcionou bem com o modelo de negócios direcionado a promoções da Kmart, que criou aumentos e quedas acentuados na demanda por produtos, e que não foi projetado para lidar com o número massivo de produtos armazenados nas lojas.
- Uma implantação da Oracle desenvolvida em outubro de 2005 e cercada de erros fez com que o sistema de rastreio da Overstock.com ficasse fora do ar durante a semana inteira e contribuisse para uma perda de 14,5 milhões de dólares. A Overstock.com tentou substituir um sistema nativo pelo sistema integrado da Oracle. A pressa para implementar foi a razão para os problemas iniciais de projeto. O novo sistema registrava uma a uma — e não em lote, como o antigo sistema — as transações de devolução aos clientes. A equipe de desenvolvimento ERP da Overstock não sincronizou adequadamente essa mudança com o sistema de contas a receber da empresa, e o balanço dessas contas não refletia com precisão todas essas devoluções. Em outubro de 2008, a Overstock teve de declarar novamente mais de cinco anos de ganhos, com uma redução na receita de 12,9 milhões de dólares, e prejuízo aumentado de 10,3 milhões de dólares.

As aplicações integradas também produzem ‘custos de mudança’. Se adotar uma aplicação integrada de um único fornecedor, como SAP, Oracle ou outros, será muito dispendioso substituí-la e, assim, sua empresa se tornará dependente desse fornecedor para manter e atualizar seus produtos.

Você também precisará dedicar algum tempo à gestão dos dados. As aplicações integradas baseiam-se em definições de dados válidas para toda a organização. Logo, é necessário entender exatamente como sua empresa usa essas informações e como elas podem ser organizadas em um sistema integrado, de gestão da cadeia de suprimentos ou de gestão do relacionamento com o cliente. Em particular, sistemas CRM normalmente exigem algum tipo de depuração de dados.

Em resumo, dá bastante trabalho fazer com que as aplicações integradas funcionem adequadamente. Todas as pessoas da empresa precisam estar envolvidas. Obviamente, para aquelas organizações com sistemas integrados, sistemas de gestão da cadeia de suprimentos e do relacionamento com o cliente bem-sucedidos, os resultados com certeza valem a pena.

Aplicativos integrados da próxima geração

Hoje em dia, fornecedores de aplicativos integrados estão distribuindo mais valor por tornarem seus produtos mais flexíveis, disponíveis na Web e capazes de integração com outros sistemas. Sistemas empresariais, de gestão da cadeia de suprimentos de CRM isolados estão se tornando coisa do passado.

Os principais fornecedores de software integrado criaram o que chamam de *soluções integradas, suites integradas ou suites para e-business* para fazer com que seus sistemas empresariais, de CRM e de cadeia de suprimentos funcionem bem próximos uns dos outros e se conectem a sistemas de clientes e fornecedores. SAP Business Suite, Oracle e-Business Suite e Microsoft Dynamics (cujo alvo são as empresas de médio porte) são exemplos que agora utilizam serviços da Web e arquitetura orientada a serviços (SOA, veja Capítulo 4).

A próxima geração de aplicativos integrados da SAP está baseada em sua arquitetura orientada a serviços que incorpora padrões SOA e usa a ferramenta NetWeaver como plataforma de integração que conecta as aplicações da própria SAP e também serviços da Web desenvolvidos por fornecedores independentes de software. O objetivo é tornar as aplicações integradas mais fáceis de serem desenvolvidas e gerenciadas.

A versão atual do software integrado da SAP, por exemplo, combina aplicações importantes para a administração de finanças, logística, aquisição e recursos humanos em um componente ERP principal. As empresas então estendem essas aplicações através de ligações a serviços da Internet com funções específicas, como recrutamento de funcionários ou gestão de coleções, oferecidos pela SAP e outros fornecedores. A SAP oferece mais de 500 serviços da Web em seu site.

A Oracle também incluiu recursos de SOA e de gestão de processos de negócios em seus produtos *middleware Fusion*. As empresas podem usar as ferramentas da Oracle para customizar as aplicações sem quebrá-las por inteiro.

As aplicações integradas da próxima geração também incluem soluções de código aberto e sob demanda. Comparados aos aplicativos integrados comerciais, os produtos de código aberto — como Compiere, Open for Business (OFBiz) e Openbravo — não são tão maduros, tampouco incluem tanto suporte. Entretanto, empresas como pequenos fabricantes estão escolhendo essa opção porque elas não precisam de taxas de licença. (Suporte e customização de produtos de código aberto têm custo extra.)

O crescimento mais explosivo nas ofertas de software como serviço (SaaS) tem sido para a gestão do relacionamento com o cliente. A Salesforce.com hoje é líder na hospedagem de soluções CRM; a Oracle e a SAP também desenvolveram recursos SaaS. As versões SaaS de aplicativos integrados estão disponíveis em pequenos fornecedores, como a Netsuite e a Plex Online.

Atualmente, a SAP oferece uma solução de aplicativo integrado sob demanda, denominada ByDesign, para pequenas e médias empresas de determinados países. Para grandes empresas, a versão local do software integrado da SAP é a única disponível. Entretanto,

a SAP está hospedando aplicações para funções específicas (como *e-sourcing* e gestão de despesas), disponíveis por meio de uma assinatura, que se integram aos sistemas locais SAP Business Suite dos clientes. Os principais fornecedores de aplicações comerciais também oferecem porções de seus produtos que funcionam em dispositivos móveis.

A Salesforce.com e a Oracle agora incluem alguns recursos da Web 2.0 que permitem às empresas identificar novas ideias mais rapidamente, melhorar a produtividade das equipes e aumentar a interação com os clientes. A Salesforce Ideas, por exemplo, permite que empregados, clientes e parceiros de negócios sugiram e votem novas ideias. A Dell Computer lançou essa tecnologia como Dell IdeaStorm (dellideastorm.com) para permitir aos clientes fazer sugestões e votar sobre novos conceitos e mudanças nos recursos dos produtos da empresa. As ideias sugeridas pelo serviço incentivaram a Dell a incluir telas de alta resolução no modelo 1530 de seus laptops (Greenfield, 2008).

Plataformas de serviços

Outra maneira de estender os aplicativos integrados é usá-los na criação de plataformas de serviços para novos processos de negócios, ou processos de negócios aprimorados, que integram informações de diferentes áreas funcionais. Essas plataformas de serviços que abrangem toda a empresa oferecem um maior grau de integração interfuncional do que os aplicativos integrados tradicionais. Uma **plataforma de serviços** integra múltiplas aplicações de diferentes funções de negócios, unidades de negócios ou parceiros de negócios para distribuir uma experiência perfeita a clientes, empregados, gerentes e parceiros de negócios.

Por exemplo, o processo de encomenda-até-pagamento envolve o recebimento de um pedido e seu percurso até que seu pagamento seja realizado. Esse processo começa com o fornecimento de informações sobre o produto, campanhas de marketing e chegada do pedido, que normalmente são tratadas pelos sistemas CRM. Uma vez que o pedido seja recebido, a manufatura é agendada e a disponibilidade de peças é verificada — processos que costumam ser suportados pelo software integrado. O pedido é então tratado por processos de planejamento de distribuição, armazenamento, preenchimento de pedido e expedição, que costumam ser suportados pelos sistemas de gestão da cadeia de suprimentos. Por fim, o pedido é cobrado ao cliente, etapa tratada por aplicativos financeiros integrados ou sistemas de contas a pagar. Se, em algum momento, a compra precisar de atendimento ao cliente, os sistemas de gestão de relacionamento com o cliente são solicitados.

Um serviço como o de encomenda-até-pagamento requer integração entre dados de aplicativos integrados e sistemas financeiros em um processo composto que contemple toda a empresa. Para isso, as empresas precisam de ferramentas de software que utilizem as aplicações existentes como blocos de montar para novos processos interempresariais (veja Figura 8.12). Os fornecedores de produtos integrados também oferecem ferramentas e *middleware* que usam XML e serviços da Web para integrar aplicações integradas com aplicações legadas e sistemas de outros fornecedores.

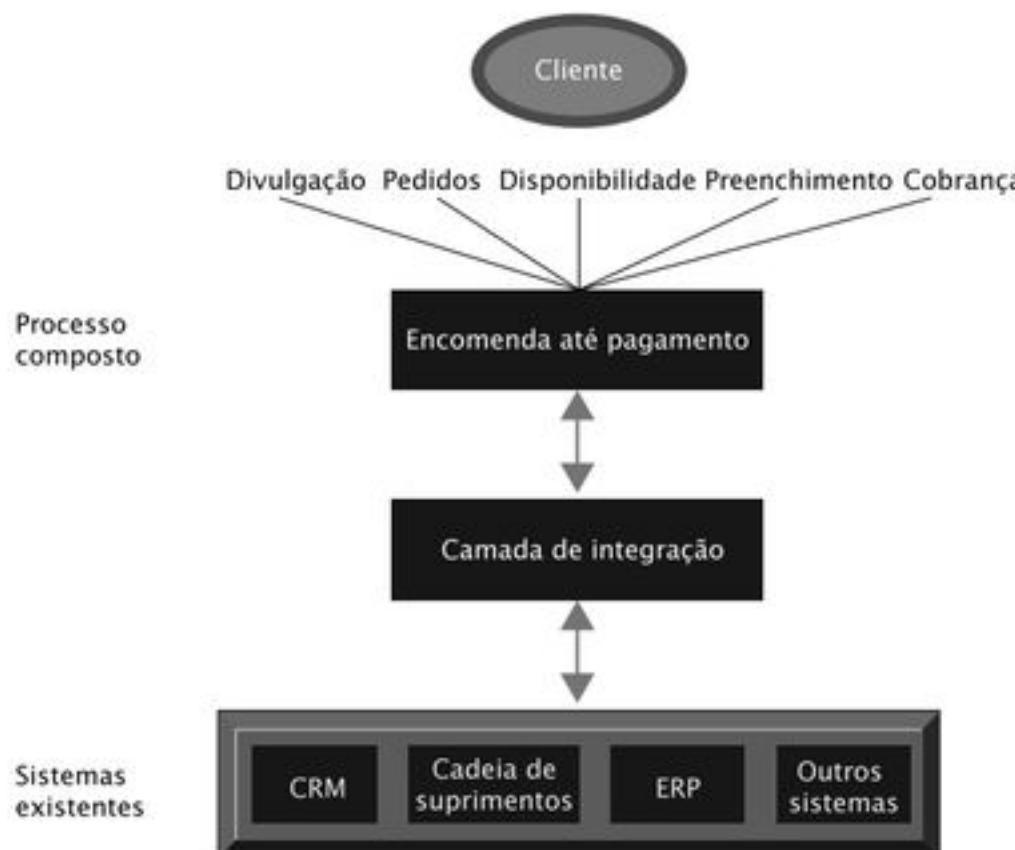
Cada vez mais, esses novos serviços são distribuídos através de portais. Software para portal integra informações de aplicativos integrados e sistemas legados dispare, apresentando essas informações aos clientes através de uma interface da Web que faz com que a informação pareça vir de uma única fonte. Por exemplo, a Valero Energy, maior refinador norte-americano, usou SAP NetWeaver Portal para criar um serviço que permitisse que clientes atacadistas visualizassem as informações de suas contas de uma única vez. O software oferece uma interface para dados de faturas de clientes, preços, fundos eletrônicos e transações com cartão de crédito armazenados no *data warehouse* do sistema de gestão do relacionamento com o cliente da SAP e em outros sistemas.

Projetos práticos em SIG

Os projetos nesta seção oferecem experiência prática em atividades como análise de integração de processos de negócios, sugestão de aplicativos para gerência da cadeia de

Figura 8.12**Serviço de encomenda-até-pagamento**

O processo de encomenda-até-pagamento é composto e integra dados de sistemas integrados individuais e aplicações financeiras legadas. O processo deve ser projetado e transformado em um sistema de software utilizando ferramentas de aplicativos integrados.



suprimentos e gerência do relacionamento com o cliente, utilização de banco de dados para gestão das solicitações dos clientes e avaliação dos serviços de negócios da cadeia de suprimentos.

Problemas de decisões gerenciais

1. A Mercedes-Benz de Toronto, no Canadá, possui uma rede de 55 concessionárias, mas não sabia muito sobre seus clientes. As concessionárias repassavam os dados dos clientes para a empresa de modo espontâneo. A Mercedes não exigia que elas relatassem essas informações, e o processo de controle das lojas que não repassavam os dados era complicado. Não havia incentivo real para que as concessionárias compartilhassem as informações com a empresa. Como os sistemas de CRM e de gestão do relacionamento com parceiros podem ajudar a resolver esses problemas?
2. A Office Depot vende uma gama de produtos e serviços de escritório nos Estados Unidos e no exterior, incluindo suprimentos para escritórios e computadores, máquinas empresariais (e seus suprimentos) e móveis de escritório. A empresa tenta oferecer uma vasta variedade de produtos de escritório a um custo menor do que o de outros varejistas utilizando o reabastecimento *just-in-time* e sistemas de controle de estoque. Ela usa informações de um sistema de provisão de demanda e dados de PDVs para reabastecer o estoque de suas 1.600 lojas de varejo. Explique como esses sistemas ajudam a Office Depot a minimizar os custos e cite qualquer outro benefício que possam oferecer. Identifique e descreva outras aplicações de gestão da cadeia de suprimentos que seriam especialmente úteis para a Office Depot.

Melhorando a tomada de decisão: usando software de banco de dados para gerenciar solicitações de serviço de clientes

Habilidades de software: projeto de banco de dados; consultas e relatórios

Habilidades organizacionais: análise do atendimento ao cliente

Neste exercício, você vai utilizar software de banco de dados para desenvolver uma aplicação que controle as solicitações de serviços e analise os dados dos clientes para identificar aqueles que merecem prioridade no atendimento.

A Prime Service, grande prestadora de serviços na área de consertos e manutenção, atende cerca de 1.200 empresas de todos os tamanhos em Nova York, Nova Jersey e Connecticut. Dentre os clientes estão empresas de todos os portes. Quando precisa de

serviços, o cliente telefona para o departamento de atendimento da Prime e faz sua solicitação, que pode ser um conserto de tubos de calefação, janelas quebradas, goteiras, canos rompidos etc. O representante da Prime atribui um número àquela solicitação e o registra, assim como o número de identificação da conta do cliente, a data da solicitação, o tipo de equipamento necessário para o conserto e uma breve descrição do problema. As solicitações de serviço são atendidas por ordem de chegada. Quando o conserto tiver sido feito, a Prime calcula o custo do serviço, insere o preço no formulário de solicitação e emite a fatura para o cliente.

A administração não está contente com esse modo de operação, pois os clientes mais importantes e lucrativos — aqueles com contas superiores a 70 mil dólares — são tratados exatamente como os clientes de contas pequenas. Eles gostariam de encontrar uma maneira de oferecer melhor atendimento aos melhores clientes. A administração também gostaria de saber quais tipos de problema ocorrem com mais frequência, para manter sempre em estoque os recursos mais adequados.

A Prime Service tem um pequeno banco de dados com informações das contas dos clientes. Esse banco contém campos relativos ao número de identificação da conta, ao nome da empresa (conta), seu endereço, cidade, estado, código postal, tamanho da conta (em dólares), sobrenome do contato, primeiro nome do contato e número de telefone do contato. Contato é a pessoa responsável, em cada empresa, por contatar a Prime quando necessário. Projete uma solução que permita aos atendentes da Prime identificar os clientes mais importantes e dessa forma lhes oferecer atendimento prioritário. Sua solução exigirá mais de uma tabela. Alimente seu banco de dados com pelo menos 15 solicitações de serviço. Crie vários relatórios que possam ser úteis à administração, tais como uma lista das contas de maior ou menor prioridade e um relatório mostrando os problemas mais frequentes. Crie, também, um relatório que mostre aos atendentes quais chamadas de serviço eles devem responder primeiro em uma data específica.

Alcançando excelência operacional: avaliando soluções de gestão da cadeia de suprimentos

Habilidades de software: navegador da Web e software para apresentação

Habilidades organizacionais: localizar e avaliar fornecedores

Empresas de transporte em caminhões não atuam mais somente carregando produtos de um lado a outro. Algumas delas também oferecem a seus clientes serviços de gestão da cadeia de suprimentos e ajudam na gestão da informação. Neste projeto, você vai utilizar a Web para pesquisar e avaliar dois desses serviços.

Visite o site de duas empresas, a UPS Logística e a Cometa Courier, para ver como seus serviços podem ser utilizados na gestão da cadeia de suprimentos. Em seguida, responda às seguintes perguntas:

- Que processos da cadeia de suprimentos cada uma dessas empresas pode suportar para seus clientes?
- Como os clientes podem usar os sites dessas empresas para ajudá-los na gestão da cadeia de suprimentos?
- Compare os serviços de gestão da cadeia de suprimentos oferecidos por essas empresas. Qual delas escolheria para ajudar sua empresa a gerenciar sua cadeia de suprimentos? Justifique.

Resumo

1. Como os sistemas integrados ajudam a conquistar a excelência operacional? Software integrado baseia-se em uma suite de módulos de software integrados e um banco de dados comum central que coleta dados de diversas aplicações que podem suportar quase todas as atividades de negócios internas da empresa e fornece outras. Quando novas informações são fornecidas por um processo, elas são disponibilizadas imediatamente para outros processos de negócios.

Sistemas integrados ajudam na centralização organizacional, pois aplicam processos de negócios e padrões de dados uniformizados em toda a empresa, além de utilizar uma única plataforma tecnológica. Válidos para toda a empresa, os dados gerados pelos sistemas integrados ajudam os gestores a avaliar o desempenho organizacional.

2. Como os sistemas de gestão da cadeia de suprimentos coordenam o planejamento, a produção e a logística com os fornecedores? Os sistemas de gestão da cadeia de suprimentos automatizam o fluxo de informações entre os membros da cadeia de suprimentos; com isso, esses membros podem usar essas informações para tomar decisões mais acertadas sobre quando e quanto comprar, produzir ou expedir. As informações mais precisas proporcionadas pelos sistemas de gestão da cadeia de suprimentos reduzem a incerteza e o impacto do efeito chicote.

Os softwares de gestão da cadeia de suprimentos dividem-se em softwares de planejamento e softwares de execução da cadeia de suprimentos. A tecnologia de Internet facilita a gestão de cadeias de suprimentos globais, pois permite que organizações de diferentes países se conectem e compartilhem informações. A melhor comunicação entre os membros da cadeia também facilita a resposta eficiente ao cliente e a transição para um modelo orientado pela demanda.

3. Como os sistemas de gestão do relacionamento com o cliente conquistam a intimidade com o cliente? Sistemas de gestão do relacionamento com o cliente (CRMs) integram e automatizam muitos processos vol-

tados ao cliente nas áreas de vendas, marketing e atendimento, proporcionando uma visão válida para toda a empresa. As organizações podem usar esse conhecimento sobre o cliente quando interagem com eles para oferecer melhores serviços ou vender novos produtos e serviços. Esses sistemas também identificam clientes lucrativos ou não lucrativos, bem como oportunidades para reduzir a taxa de cancelamento (*churn rate*).

Os principais pacotes de software de gestão do relacionamento com o cliente oferecem recursos tanto para o CRM operacional quanto para o CRM analítico. Muitas vezes, incluem módulos para gerenciar o relacionamento com parceiros de vendas (gestão do relacionamento com o parceiro) e para a gestão do relacionamento com o funcionário.

4. Quais os desafios e as novas oportunidades trazidos pelas aplicações integradas? É difícil implementar aplicações integradas. Elas exigem profundas mudanças organizacionais, pesados investimentos em novos softwares e cuidadosa avaliação de como esses sistemas melhorarão o desempenho organizacional. As aplicações integradas não podem agregar valor se forem implementadas sobre processos falhos ou se as empresas não souberem como usar esses sistemas para avaliar as melhorias no desempenho. Os funcionários precisam ser preparados para os novos procedimentos e papéis. A gestão de dados também merece atenção especial.

5. Como os aplicativos integrados são usados em plataformas para novos serviços interfuncionais? As plataformas de serviços integram informações e processos de diversos aplicativos integrados (sistemas empresariais, de gestão do relacionamento com o cliente e de gestão da cadeia de suprimentos), bem como de sistemas legados dispare, para criar novos processos de negócios compostos. Serviços da Web agrupam muitos sistemas. Os novos serviços são distribuídos através de portais corporativos, que podem integrar aplicações distintas para que as informações pareçam vir de uma única fonte. Já são disponibilizadas versões desses produtos de código aberto, móveis e para nuvem.

Palavras-chave

Cadeia de suprimentos, 257

CRM analítico, 271

CRM operacional, 271

Cross-selling, 268

Efeito chicote, 259

Gestão do relacionamento com o funcionário (ERM), 267

Gestão do relacionamento com o parceiro (PRM), 267

Just-in-time, 259

Modelo pull, 264

Modelo push, 264

Planejamento da demanda, 261

Plataforma de serviços, 275

Ponto de contato, 266

Sistemas de execução da cadeia de suprimentos, 261

Sistemas de planejamento da cadeia de suprimentos, 261

Software integrado, 255

Taxa de cancelamento, 272

Valor do cliente ao longo do tempo (CLTV), 272

Questões de revisão

1. Como os sistemas integrados alcançam excelência operacional?

- Defina o que é sistema integrado e explique como ele funciona.
- Descreva como os sistemas integrados agregam valor à empresa.

2. Como os sistemas de gestão da cadeia de suprimentos coordenam planejamento, produção e logística com fornecedores?

- Defina o que é cadeia de suprimentos e identifique quais componentes ela compreende.
- Explique como os sistemas de gestão da cadeia de suprimentos podem lidar com o efeito chicote e como agregam valor aos negócios.
- Defina e compare sistemas de planejamento da cadeia de suprimentos e sistemas de execução da cadeia de suprimentos.
- Descreva os desafios de cadeias de suprimentos globais e diga de que forma a tecnologia de Internet pode ajudar as empresas a gerenciar melhor.
- Faça a distinção entre um modelo pull e um modelo push de gestão da cadeia de suprimentos e explique como os sistemas de gestão da cadeia de suprimentos contemporâneos facilitam o modelo pull.

3. Como os sistemas de gestão do relacionamento com o cliente ajudam as empresas a se tornarem íntimas dos clientes?

- Defina o que é gestão do relacionamento com o cliente e explique por que as relações com o cliente são tão importantes hoje.

• Descreva como a gestão do relacionamento com o parceiro (PRM) e a gestão do relacionamento com o funcionário (ERM) estão relacionadas à gestão do relacionamento com o cliente (CRM).

- Descreva as ferramentas e recursos dos softwares de gestão do relacionamento com o cliente nas áreas de vendas, marketing e atendimento.

• Faça a distinção entre CRM analítico e operacional.

4. Quais os desafios impostos pelos aplicativos integrados?

- Liste e descreva os desafios impostos pelos aplicativos integrados.
- Explique como esses desafios devem ser abordados.
- Como os aplicativos integrados são usados em plataforma para serviços interfuncionais?
- Defina o que é uma plataforma de serviços e descreva as ferramentas para integração de dados nos aplicativos integrados.
- Como os aplicativos integrados estão tirando proveito da computação em nuvem, da tecnologia sem fio, da Web 2.0 e da tecnologia de código aberto?

Para discutir

1. Gerenciar a cadeia de suprimentos tem menos a ver com gerenciar o movimento físico de mercadorias do que com gerenciar as informações. Discuta as implicações dessa afirmação.

2. Se determinada empresa deseja implantar uma aplicação integrada, é bom fazer a 'lição de casa' direito. Discuta as implicações dessa afirmação.

Colaboração e trabalho em equipe

Analisando fornecedores de aplicações integradas

Forme um grupo de três ou quatro colegas. Usem a Web para pesquisar e avaliar os produtos de dois fornecedores de software de aplicações integradas. Vocês podem comparar, por exemplo, os sistemas integrados da SAP e da Oracle, os sistemas de gestão da cadeia de suprimentos da i2 e SAP, os sistemas de gestão do relacionamento com o cliente da Oracle-Siebel Systems e da Salesforce.com. Usem tudo o que encontrarem nos sites dessas empresas para comparar os pacotes de software selecionados em termos de: funções de negócios apoia-

das, plataforma de tecnologia, custo e facilidade de uso. Qual fornecedor vocês escolheriam? Por quê? Vocês escolheriam o mesmo fornecedor para uma microempresa e para uma empresa de grande porte? Se possível, usem o Google Sites para publicar links para páginas da Web, comunicados para a equipe e tarefas; para trocar ideias e para trabalhar no projeto de forma colaborativa. Tentem usar o Google Docs para desenvolver uma apresentação eletrônica a fim de comunicar suas conclusões à classe.

Resolvendo problemas organizacionais

Border States Industries incentiva o rápido crescimento com ERP

A Border States Industries Inc. (BSE) é um distribuidor atacadista para os mercados de construção, industrial, de utilidades e de comunicação de dados. A empresa tem sede em Fargo, Dakota do Norte, e possui 57 escritórios de vendas em estados ao longo das fronteiras dos Estados Unidos com Canadá e México, além de unidades em Dakota do Sul, Wisconsin, Iowa e Missouri. A BSE possui 1.400 empregados e pertence totalmente a seus funcionários através do plano de participação. Para o ano fiscal encerrado em 31 de março de 2008, a BSE obteve receitas de mais de 880 milhões de dólares.

A meta da BSE é oferecer aos clientes o que eles precisarem, sempre que precisarem, incluindo o fornecimento de serviços além da entrega de produtos. Assim sendo, a empresa não é somente um distribuidor atacadista, mas um fornecedor de soluções para cadeia de suprimentos, com amplas operações de serviços em logística, moradias para canteiro de obras e empacotamento (agrupamento de partes individuais separadas, embora relacionadas, como uma mesma unidade). A BSE possui acordos de distribuição com mais de 9 mil fornecedores de produtos.

Desde 1998, a BSE vinha confiando no Rigel, seu próprio sistema legado ERP, para apoiar seus principais processos de negócios. Entretanto, o Rigel foi projetado exclusivamente para atacadistas de produtos elétricos e, em meados da década de 1990, o sistema não conseguia suportar as novas linhas de negócios da BSE e o amplo crescimento da empresa.

Naquele ponto, a gerência da BSE decidiu implantar um novo sistema ERP e escolheu o software da SAP AG. A solução ERP incluía módulos SAP para vendas e distribuição, gestão de materiais, finanças e controle, e recursos humanos.

Inicialmente, a BSE havia reservado 6 milhões de dólares para o novo sistema, com data de início para 1º de novembro de 1998. A gerência sênior trabalhou em conjunto com a consultoria da IBM e da SAP para implementar o sistema. Embora o intenso envolvimento da gerência tenha sido um dos principais ingredientes para o sucesso do sistema, as operações diárias sofreram enquanto os gerentes trabalhavam no projeto.

A BSE também decidiu customizar extensivamente o sistema. Ela escreveu seu próprio software para permitir que o sistema ERP realizasse automaticamente uma interface com os sistemas de outros fornecedores, que incluíam Texware Systems, Inc., Innovis Inc. e TOPCALL International GmbH. O sistema da Texware permite que a BSE atenda às exigências relacionadas aos impostos sobre as vendas em todos os estados e municípios nos quais realiza negócios. O sistema da Innovis suporta o intercâmbio eletrônico de dados de modo que a BSE podia trocar eletronicamente transações de compras e pagamentos com seus fornecedores. O sistema da TOPCALL permite que a BSE envie faxes para clientes e fornecedores diretamente de seu sistema SAP.

Durante a implantação do sistema, a BSE não tinha experiência com o software SAP e dispunha de poucos con-

sultores familiarizados com a versão do software SAP que a BSE utilizava. Em vez de adotar os processos de negócios de melhores práticas embutidos no software SAP, a BSE contratou consultores para customizar o software e fazer com que seu novo sistema SAP se parecesse com o antigo sistema Rigel em determinadas áreas. A empresa tentou, por exemplo, fazer com que as faturas para os clientes lembressem aquelas produzidas pelo antigo sistema Rigel.

A implantação dessas mudanças exigiu tantas customizações no software SAP que a BSE teve de adiar seu lançamento para 1º de fevereiro de 1999. À época, a customização e otimização contínuas elevaram os custos de implementação para 9 milhões de dólares (um aumento de 50 por cento).

O procedimento de conversão e limpeza dos dados do sistema legado da BSE levou muito mais tempo do que o imaginado pela gerência. O primeiro grupo de 'usuários especialistas' foi treinado muito cedo e precisou ser ensinado novamente quando o sistema finalmente foi concluído. Antes que entrasse em funcionamento, a BSE nunca testou integralmente o sistema do modo como seria utilizado no ambiente de produção.

Nos cinco anos seguintes, a BSE continuou a utilizar seu sistema SAP/ERP de maneira bem-sucedida, adquiriu diversas pequenas empresas e expandiu sua infraestrutura de escritórios para 24 estados. À medida que o negócio crescia, aumentaram os giros de lucros e estoque. Contudo, a Internet trouxe a necessidade de mudanças adicionais, pois os clientes procuravam fazer negócios com a BSE através de um portal de comércio eletrônico. A BSE automatizou o processamento on-line de cartões de crédito e acordos especiais de preços com alguns clientes. Infelizmente, o software SAP existente não suportou essas modificações e a empresa teve de processar manualmente esses acordos.

Para processar uma transação de cartão de crédito em um escritório, os empregados da BSE tinham de levantar da cadeira, andar até um sistema dedicado de processamento de cartões de crédito no escritório dos fundos, digitar manualmente o número do cartão, esperar pela aprovação da transação e então retornar à estação de trabalho para continuar o processamento da transação de vendas.

Em 2004, a BSE começou a atualização de seu sistema ERP para uma versão mais recente do software SAP. A aplicação incluía novos recursos de cobrança de materiais e empacotamento que não estavam disponíveis no antigo sistema. Essa funcionalidade permitiu que a BSE oferecesse melhor suporte aos clientes, pois podia preparar kits que podiam ser entregues diretamente a um local.

Dessa vez a empresa manteve a customização em um nível mínimo e utilizou as melhores práticas para distribuição atacadista embutidas no software. Ela também substituiu o TOPCALL por um software da Esker para expedição por fax e e-mail de faturas, confirmações de pedidos e ordens de compra, e acrescentou recursos do Vistex Inc. para automatizar o processamento de reclamações de

desconto relacionadas aos acordos especiais de preços. A BSE processa mais de 360 mil reclamações desse tipo anualmente, e o software permitia que a empresa reduzisse o tempo de atendimento do desconto para 72 horas e diminuisse em 63 por cento o tempo de processamento de transações. No passado, a BSE levava de 15 a 30 dias para receber os abatimentos dos fornecedores.

A BSE estimou o gasto em 1,6 milhão de dólares e a duração da implementação em 4,5 meses, investimento e tempo considerados suficientes pela gerência para um projeto dessa magnitude. Dessa vez, não houve problemas. O novo sistema foi concluído na data prevista e custou apenas 1,4 milhão de dólares — 14 por cento abaixo do orçamento.

No final de 2006, a BSE adquiriu uma grande empresa tida como a razão para um aumento de 20 por cento nas vendas de cada ano. Essa aquisição acrescentou 19 novos escritórios capazes de rodar o software SAP da BSE um dia depois da conclusão da compra. Agora, a BSE controla 1,5 milhão de itens exclusivos com o software.

Desde a primeira utilização do software SAP, em 1998, as vendas da BSE aumentaram 300 por cento, os lucros subiram mais de 500 por cento, 60 por cento das transações de pagamento de contas são realizadas eletronicamente utilizando a transferência eletrônica de dados e o processamento do SPA foi reduzido em 63 por cento. A empresa gira seu estoque mais de quatro vezes por ano. Em vez de esperar de 15 a 20 dias para os relatórios financeiros mensais, resultados financeiros mensais e anuais estão disponíveis um dia após o fechamento dos livros. O trabalho manual de separar correspondência, preparar depósitos bancários e levar cheques fisicamente ao banco foi significativamente reduzido. Mais de 60 por cento das faturas de fornecedores chegam eletronicamente, o que reduziu o tamanho da equipe de contas a pagar e diminuiu a quantidade de erros em transações. Os custos das transações baixaram.

Na área de sistemas de informação, o número de empregados em tempo integral da BSE aumentou de modo a dar suporte ao software SAP. Inicialmente, a empresa esperava contar com três pessoas na equipe de TI para suporte ao sistema, mas precisou de oito empregados quando a primeira implementação foi concluída, em 1999, e de 11 profissionais em 2006 para dar suporte ao software SAP adicional e à nova aquisição. Os custos de TI da BSE subiram aproximadamente 3 milhões de dólares por ano após a primeira implementação SAP. Entretanto, as vendas expandiram durante o mesmo período e o aumento das despesas com a produção do sistema gerou um aumento nos custos de 0,5 por cento do total de vendas.

A gerência da BSE observou que a maior parte do trabalho automatizado pelos sistemas ERP se deu no departamento de contabilidade e nas atividades envolvidas, puramente transacionais. Essa medida liberou recursos para inclusão de mais empregados que trabalham diretamente com os clientes na tentativa de reduzir os custos e aumentar as vendas.

No passado, a BSE mantinha grande parte de seus dados fora de seus principais sistemas corporativos, utilizando um banco de dados Microsoft Access baseado em PC e planilhas eletrônicas em Excel. A gerência não dispunha de uma versão dos dados corporativos que abarcasse toda a empresa porque os dados estavam fragmentados em muitos sistemas. Agora, a empresa está padronizada em uma única plataforma comum e a informação está sempre atualizada e disponível. A gerência pode obter um panorama de como está o desempenho de toda a empresa a qualquer momento. Como o sistema SAP disponibiliza todos os dados de planejamento e orçamento on-line, a gerência consegue tomar decisões mais acertadas e com maior rapidez.

Em 2006, a Gartner Group Consultants realizou uma avaliação independente da implementação ERP da BSE. A Gartner entrevistou os principais executivos e analisou os dados da BSE sobre o impacto do sistema ERP sobre os custos de processos de negócios utilizando os custos como um percentual das vendas para medida final na avaliação do impacto financeiro do software SAP. As categorias de custo analisadas incluem custos de produtos vendidos, custos gerais e administração, custos de armazenagem, suporte de TI e distribuição.

A análise da Gartner confirmou que o custo de implementação do software SAP entre 1998 e 2001 realmente totalizou nove milhões de dólares e que, em dois anos e meio, esse investimento foi revertido em economias com o novo sistema ERP. Entre 1998 e 2006, o software SAP implantado pela BSE produziu economias totais de 30 milhões de dólares, aproximadamente um terço dos ganhos cumulativos da BSE no mesmo período. Como percentual das vendas, os custos de armazenagem diminuíram um por cento, os custos de distribuição baixaram 0,5 por cento, e os custos gerais totais caíram 1,5 por cento. A Gartner calculou que o retorno total sobre o investimento para o projeto realizado entre 1998 e 2006 foi de 3,3 milhões anuais, ou 37 por cento do investimento original.

Agora, a BSE está se concentrando na oferta de melhor suporte às vendas pela Internet, que incluem encomendas on-line, estoque, status de pedidos e revisão de faturas, tudo dentro do ambiente do software SAP. A empresa implementou a aplicação SAP NetWeaver Master Data Management para oferecer ferramentas para gestão e manutenção dos dados do catálogo e preparação dos dados para publicação on-line e na mídia impressa tradicional. A empresa está utilizando o ambiente de desenvolvimento da Web DynPro para permitir que as atividades sem fio de gestão de armazenamento e estoque possam interagir com o software SAP. Além disso, utiliza o software SAP NetWeaver Business Intelligence para aprender mais sobre clientes e seus hábitos de consumo, e sobre oportunidades para vendas cruzadas e aumento das vendas.

Fontes: Jim Shepherd e Aurelie Cordier, "Wholesale Distributor Uses ERP Solution to Fuel Rapid Growth". AMR Research, 2009; SAP AG, "Border States Industries: SAP Software Empowers Wholesale Distributor". 2008; www.borderstateselectric.com, acessado em 7 jul 2009; e "Border States (BSE)". 2008 ASUG Impact Award.

Questões

- À medida que se expandia, que problemas a Border States Industries enfrentava? Quais os fatores humanos, organizacionais e tecnológicos responsáveis por esses problemas?
- Foi fácil desenvolver uma solução utilizando software SAP e ERP? Explique.
- Liste e descreva os benefícios do software SAP.
- Como foi a transformação do negócio a partir da nova solução de sistema? Explique.
- Quão bem-sucedida foi a solução para a BSE? Identifique e descreva as métricas utilizadas para medir o sucesso da solução.
- Se tivesse sido responsável pela implementação do ERP da SAP, o que teria feito diferente?

Referências bibliográficas

- BARRETT, Joe. "Whirlpool Cleans Up Its Delivery Act", *The Wall Street Journal*, 24 set. 2009.
- CHICKOWSKI, Ericka. "5 ERP Disasters Explained", www.Baselinemag.com, acessado em 8 out. 2009.
- D'AVANZO, Robert; LEWINSKI, Hans von; WASSENHOVE, Luk N. Van. "The Link between Supply Chain and Financial Performance", *Supply Chain Management Review*, 1 nov. 2003.
- DAVENPORT, Thomas H. *Mission Critical: Realizing the Promise of Enterprise Systems*. Boston: Harvard Business School Press, 2000.
- DAY, George S. "Creating a Superior Customer-Relating Capability", *MIT Sloan Management Review* 44, n. 3, primavera 2003.
- DVORAK, Phred. "Clarity is Missing Link in Supply Chain", *The Wall Street Journal*, 18 maio 2009.
- EVANS, Bob. "Global CIO: LG Transforms Global Operations with Oracle ERP", *Information Week*, 24 ago. 2009.
- FERRER, Jaume; KARLBERG, Johan; HINTLIAN, Jamie. "Integration: The Key to Global Success", *Supply Chain Management Review*, 1 mar. 2007.
- FLEISCH, Elgar; OESTERLE, Hubert; POWELL, Stephen. "Rapid Implementation of Enterprise Resource Planning Systems", *Journal of Organizational Computing and Electronic Commerce* 14, n. 2, 2004.
- GARBER, Randy; SARKAR, Suman. "Want a More Flexible Supply Chain?", *Supply Chain Management Review*, 1 jan. 2007.
- GOODHUE, Dale L.; WIXOM, Barbara H.; WATSON, Hugh J. "Realizing Business Benefits through CRM: Hitting the Right Target in the Right Way", *MIS Quarterly Executive* 1, n. 2, jun. 2002.
- GREENBAUM, Joshua. "Is ERP Dead? Or Has It Just Gone Underground?", *SAP NetWeaver Magazine* 3, 2007.
- GUINIPERO, Larry; HANDFIELD, Robert B.; JOHANSEN, Douglas L. "Beyond Buying", *The Wall Street Journal*, 10 mar. 2008.
- HITT, Lorin; WU, D. J.; ZHOU, Xiaoge. "Investment in Enterprise Resource Planning: Business Impact and Productivity Measures", *Journal of Management Information Systems* 19, n. 1, verão 2002.
- KALAKOTA, Ravi; ROBINSON, Marcia. *E-Business 2.0*. Boston: Addison-Wesley, 2001.
- _____. *Services Blueprint: Roadmap for Execution*. Boston: Addison-Wesley, 2003.
- KANAKAMEDALA, Kishore; RAMSDELL, Glenn; SRIVATSAN, Vats. "Getting Supply Chain Software Right", *McKinsey Quarterly*, n. 1, 2003.
- KLEIN, Richard; RAI, Arun. "Interfirm Strategic Information Flows in Logistics Supply Chain Relationships". *MIS Quarterly* 33, n. 4, dez. 2009.
- KOPCZAK, Laura Rock; JOHNSON, M. Eric. "The Supply-Chain Management Effect", *MIT Sloan Management Review* 44, n. 3, primavera 2003.
- LEE, Hau; PADMANABHAN, L. V.; WHANG, Seugin. "The Bullwhip Effect in Supply Chains", *Sloan Management Review*, primavera 1997.
- _____. "The Triple-A Supply Chain", *Harvard Business Review*, out. 2004.
- LIANG, Huigang; SHARAF, Nilesh; HU, Qing; XUE, Yajiong. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management". *MIS Quarterly* 31, n. 1, mar. 2007.
- MALHOTRA, Arvind; GOSAIN, Sanjay; EL SAWY, Omar A. "Absorptive Capacity Configurations in Supply Chains: Gearing for Partner-Enabled Market Knowledge Creation". *MIS Quarterly* 29, n. 1, março 2005.
- MAYLETT, Tracy; VITASEK, Kate. "For Closer Collaboration, Try Education", *Supply Chain Management Review*, 1 jan. 2007.
- MCKAY, Lauren. "CRM and the iPhone". *Customer Relationship Management*, mar. 2009.
- _____. "Everything's Social Now", *Customer Relationship Management*, jun. 2009.
- ORACLE CORPORATION. "Alcoa Implements Oracle Solution 20% below Projected Cost, Eliminates 43 Legacy Systems", www.oracle.com, acessado em 21 ago. 2005.
- RAI, Arun; PATNAYAKUNI, Ravi; SETH, Nainika. "Firm Performance Impacts of Digitally Enabled Supply Chain Integration Capabilities", *MIS Quarterly* 30, n. 2, jun. 2006.
- RANGANATHAN, C.; BROWN, Carol V. "ERP Investments and the Market Value of Firms: Toward an Understanding of Influential ERP Project Variables". *Information Systems Research* 17, n. 2, jun. 2006.
- ROBEY, Daniel; ROSS, Jeanne W.; BOUDREAU, Marie-Claude. "Learning to Implement Enterprise Systems: An Exploratory Study of the Dialectics of Change", *Journal of Management Information Systems* 19, n. 1, verão 2002.
- SCHWARTZ, Ephraim. "Does ERP Matter-Industry Stalwarts Speak Out", *InfoWorld*, 10 abr. 2007.
- SCOTT, Judy E.; VESSEY, Iris. "Managing Risks in Enterprise Systems Implementations", *Communications of the ACM* 45, n. 4, abr. 2002.
- SLONE, Reuben E. "Leading a Supply Chain Turnaround". *Harvard Business Review*, out. 2004.
- SULLIVAN, Laurie. "ERPZilla", *Information Week*, 11 jul. 2005.
- VIOLINO, Bob. "The Next-Generation ERP", *CIO Insight*, maio 2008.
- WHITING, Rick. "You Look Marvelous!", *Information Week*, 24 jul. 2006.