

Módulo 1 - Complexidade da tecnologia

Uma evolução contínua

Há pouco mais de 40 anos, a Informática era vista como uma forma eficiente de processar dados e possibilitar a automação de funções repetitivas como as executadas pelos departamentos administrativos e contábeis das organizações. Nos anos posteriores, seu casamento com a eletrônica, também chamada de mecatrônica ou automação industrial, contribuiu para aumentar a eficiência e produtividade no chão de fábrica das indústrias. Em pouco tempo, outras importantes e radicais mudanças transformariam o mundo e, fundamentalmente, o setor corporativo.

A bem-sucedida aliança entre Informática e telecomunicações permitiu tornar realidade o conceito de globalização, expandindo as fronteiras das empresas para o mundo todo por meio de um simples toque no mouse. O passo seguinte é a convergência tecnológica, reunindo num único dispositivo funções de telefone, computador, Internet, agenda eletrônica, games, televisão, música, entre outras facilidades.

Se para uma pessoa comum já é difícil assimilar tantas mudanças em tão curto espaço de tempo, para um gestor da área de Tecnologia da Informação (TI) de uma empresa isso representa um enorme e constante desafio. A complexidade dos atuais parques de máquinas, redes e sistemas instalados é muito grande e está em contínua evolução. Soma-se a isso a necessidade cada vez mais premente de entender não apenas de bits e bytes, mas também da estratégia de negócios da companhia, de forma a responder rapidamente às necessidades dos clientes e do mercado e estabelecer com fornecedores e demais parceiros uma troca de informações eficiente e em tempo real.

De outro lado, os usuários internos da Tecnologia (funcionários dos diversos departamentos da empresa) também passaram a ter voz ativa para a escolha de ferramentas e soluções, obrigando o gestor de TI a considerar o fator humano entre as suas atribuições e responsabilidades. Nesse novo contexto, o profissional de TI precisou e precisa reinventar-se, tornando-se mais flexível e aberto, e menos técnico e fechado, como era imprescindível num passado nem tão distante.

O ambiente centralizado

Retrocedendo no tempo, verificamos que, até o final dos anos 50, os computadores eram tidos como obra da imaginação humana ou como uma fantasia extraída dos livros e filmes de ficção científica. Praticamente apenas alguns poucos segmentos, como as áreas acadêmica, militar e governo, aventuravam-se na experimentação das então grandiosas e complexas máquinas. No Brasil, o governo do Estado de São Paulo foi pioneiro ao adquirir, em 1957, um Univac -120 para calcular o consumo de água na capital paulista. O equipamento era formado por 4.500 válvulas, realizava 12 mil somas e subtrações por minuto e 2.400 multiplicações ou divisões por minuto.

No setor privado, uma das primeiras empresas a investir nesse sentido foi a Anderson Clayton, que comprou um Ramac 305 da IBM, em 1959. A máquina tinha cerca de 2 metros de largura e 1,80 de altura, com mil válvulas em cada porta de entrada e de saída da informação, ocupando um andar inteiro da empresa. Considerado, na época, o supra-sumo da inovação, esse computador levava 5 minutos para procurar uma informação e a impressora operava com uma velocidade de 12,5 caracteres por segundo.

Em pouco menos de 10 anos, essas fabulosas máquinas evoluíram e conquistaram o interesse das empresas de grande porte, órgãos do governo federal e universidades. Eram os anos 60, em que reinavam absolutos os CPDs - Centros de Processamento de Dados, ambientes climatizados, cercados por paredes de vidro, como uma verdadeira redoma, e preparados para abrigar as grandes máquinas – os mainframes.

GERENCIAMENTO DE TI

Em geral, o CPD era uma área à parte na empresa, à qual tinham acesso apenas os profissionais diretamente envolvidos com os computadores, como analistas de sistemas, técnicos de manutenção, programadores, operadores, entre outros. Inacessível aos funcionários de outros departamentos, o único elo entre essas ilhas de Informática e o resto da companhia eram as pilhas de formulários contínuos contendo informações processadas, as quais haviam sido requisitadas pelos usuários de alguma área específica.

Até o final dos anos 70, predominou o que se convencionou chamar de a Era dos CPDs, ou ainda a Era do Computador, em que todas as decisões referentes à Tecnologia estavam a cargo do gerente de processamento de dados e de sistemas de informações gerenciais. Esse profissional se reportava à hierarquia financeira da empresa, e era imprescindível que tivesse conhecimento e competência essencialmente técnicos. O foco da tecnologia, então, era a produtividade, e a tendência organizacional da área de Informática era de centralização.

Nesse ambiente, o enfoque administrativo era o de controle e os investimentos em Tecnologia eram conservadores e tinham de passar pelo crivo da área financeira da organização. Confinados e isolados no ambiente fechado dos CPDs, o gerente e demais profissionais de Informática ficavam alheios às necessidades dos funcionários dos vários departamentos e também à estratégia de negócios da empresa. Todo o tempo era dedicado à criação de algoritmos, rotinas, linguagens de programação, desenvolvimento de aplicativos e demais funções técnicas.

Quando precisavam justificar novos investimentos na área, os gerentes de Informática preocupavam-se em demonstrar os ganhos de custos do sistema, da mão-de-obra e de manutenção, e não os benefícios propiciados pela Tecnologia para a empresa como um todo. A maior dificuldade, nessa época, era convencer a diretoria financeira da real necessidade dos investimentos requeridos para aumento da capacidade dos sistemas, manutenção e desenvolvimento de novos aplicativos. A área de Informática era vista basicamente como um setor gerador de gastos e tida como “um mal necessário”.

O ambiente cliente/servidor

No começo da década de 80, os avanços da microeletrônica possibilitaram o desenvolvimento de computadores menores, que ocupavam menos espaço e, ao mesmo tempo, tornavam-se mais poderosos no que tange ao aumento da capacidade de processamento, agilidade e memória, ficando também mais acessíveis em termos econômicos. A partir de 1975, todas as funções necessárias para o funcionamento de um computador já estavam integradas num único chip. A capacidade de memória passou a dobrar a cada ano. Gradativamente, o processamento de informações deixava de ser feito em lotes de transações (em tempo posterior ou batch) e passava a ser on-line (em tempo real), ou seja, as atualizações dos arquivos eram feitas à medida que as transações eram efetuadas.

Mas foi a partir dos anos 90, com a evolução da microinformática, que as mudanças se tornaram mais significativas e visíveis. A Era dos CPDs chegava ao fim para dar início à “Era da Informação”. Aos poucos, os grandes mainframes, complexos demais para os usuários comuns e que exigiam pessoal altamente especializado para operá-los e encarregar-se da sua manutenção, e ainda eram altamente dispendiosos, começaram a ser substituídos por máquinas servidoras de aplicações, num processo batizado de downsizing e rightsizing. Em muitas empresas, no entanto, os mainframes foram mantidos para operações mais complexas e estratégicas.

Novas máquinas e periféricos foram sendo agregados ao parque das empresas. As redes de terminais “burros” ligadas ao mainframe foram sendo substituídas pelas estações cliente e pelos computadores de mesa – os personal computers (PC) – munidos com interfaces gráficas e aplicativos que tornaram sua operação mais fácil e amigável às pessoas sem nenhum conhecimento de tecnologia.

GERENCIAMENTO DE TI

Começava a vigorar o modelo cliente-servidor, proporcionando a todas as esferas da empresa o acesso à informação. O ambiente centralizado e fechado do mainframe e dos antigos CPDs cedeu o lugar a plataformas heterogêneas. Nessa época, começam a proliferar as software houses, disponibilizando e aumentando a oferta de software básico e pacotes aplicativos, decretando o final da era da arquitetura proprietária e abrindo caminho para o ambiente aberto e a compatibilidade entre os diferentes sistemas.

As aplicações empresariais

A Informática começa a ser entendida como Tecnologia da Informação e empresas de médio e pequeno portes entram para o rol das usuárias. Nas grandes companhias, surge um novo tipo de profissional, o CIO - Chefe Information Officer, definido como o mais alto executivo, cuja principal responsabilidade é a de gerenciar a informação. O gerente essencialmente técnico sai de cena e entra o executivo que precisa ser, antes de tudo, um homem de negócios, com capacidade de gerenciar os recursos de informação e atuar como um estrategista da tecnologia.

A competência requerida para o cargo é a de gerência de negócios. O CIO passa a reportar-se ao CEO - Chief Executive Officer ou Diretor Executivo, e situa-se no nível de alta gerência. O foco da Tecnologia passa a ser a vantagem competitiva da empresa em face à concorrência, a missão é a inovação tecnológica e os investimentos na área são agressivos. A área de Informática deixa de ser vista como um setor meramente gerador de custos, mas como fator essencial para possibilitar à empresa manter-se ágil, competitiva e inserida na nova ordem econômica ditada pela globalização.

No mesmo compasso das inovações do hardware, surgem as ondas tecnológicas e os respectivos pacotes aplicativos voltados a integrar toda a empresa e a aumentar a produtividade e facilitar a comunicação e a transmissão de dados em diferentes níveis. Os sistemas de gestão empresarial, conhecidos pela sigla ERP (Enterprise Resource Planning) são adotados inicialmente pelas empresas de grande porte e, em seguida, pelo middle market. A oferta de novos aplicativos para todos os tipos de usuários prolifera-se em escala exponencial. A Informática está em toda parte e ganha novas e poderosas aliadas: a Internet e as inovações no campo das telecomunicações.

Nas indústrias, o emprego da TI permite não apenas agilizar a produção, mas também facilitar o contato direto com fornecedores e parceiros de negócios. O foco são as redes internas e externas, troca eletrônica de documentos (EDI, que vem sendo substituído pelo Web EDI), código de barras, e soluções que permitam a perfeita integração com a cadeia de suprimentos (supply chain).

No setor financeiro, a atenção se volta para a segurança e armazenagem dos dados e para as aplicações de missão crítica. As operadoras de telecomunicações e empresas de varejo e da área de serviços priorizam os pacotes que permitem identificar e selecionar os clientes, como as soluções de Customer Relationship Management (CRM), ou gerenciamento do relacionamento com o cliente. As soluções de Business Intelligence, que permitem a análise dos dados sob as mais variadas e inusitadas perspectivas, começam a chamar a atenção das empresas de diversas áreas. A oferta de produtos diversifica-se ainda mais e se mantém em contínua evolução.

Em todos os tipos e portes de empresas, os usuários passam a ter participação ativa na escolha e implementação de novas ferramentas. Sua colaboração torna-se imprescindível para o sucesso dos novos projetos de tecnologia.

O futuro

Paradoxalmente, ao mesmo tempo em que a Tecnologia se tornou mais acessível a um maior número de pessoas, o seu gerenciamento ficou cada vez mais complexo. Além de orquestrar ambientes heterogêneos compostos por máquinas de diferentes épocas e fabricantes, intranets, extranets, redes locais (LAN), redes de longa distância (WAN), redes e dispositivos sem fio (notebooks, handhelds, palmtops, etc) , comunicação por satélite, software para diferentes aplicações, firewall, antivírus, política de segurança e mais uma série de questões puramente tecnológicas, o gerente de TI ainda precisa se preocupar com outros aspectos. Saber ouvir, respeitar e atender as necessidades dos profissionais de todas as áreas da empresa, integrar hardware e software novos com o legado, avaliar as inovações tecnológicas, não descuidar dos aspectos relativos à segurança, preocupar-se em reduzir e controlar custos, alinhar a TI com a estratégia de negócios da empresa, e comprovar os benefícios propiciados, são apenas algumas das suas novas atribuições.

Gerir a TI na atualidade significa saber trabalhar as idéias e os problemas de modo a analisar a questão sob diferentes aspectos que se integram: os fatores estratégicos, funcionais, técnicos, tecnológicos e de custos. Também se torna importante saber administrar terceiros, uma vez que cresce a tendência de se transferir boa parte das funções de TI para empresas externas e especializadas.

No futuro, o gerente de TI provavelmente deverá lidar com novos desafios como o grid computing, também chamado de utility computing e computação sob demanda – uma maneira de organizar os recursos de TI da mesma forma que as concessionárias públicas usam as redes elétricas para disponibilizar seus serviços. O conceito, até agora mais usado em comunidades técnicas e científicas do que em negócios comerciais, permite aos usuários compartilhar energia, armazenamento de dados, base de dados e outros serviços em tempo real. Essa tendência, no entanto, segundo afirmam os consultores de mercado, ainda levará de 10 a 15 anos para se tornar realidade. Abordaremos essa questão com maior profundidade nos demais módulos.

Alvin Toffler, consultor e jornalista norte-americano, autor de vários livros e respeitado como “futurólogo”, salienta que estamos vivendo o que convencionou chamar de Sociedade de Informação da Terceira Onda, em que o conhecimento passou a ser o ativo mais importante das empresas e não a produção. O desafio dos gestores em todo o mundo, segundo acredita, será o de criar redes de conhecimento capazes de interligar os elementos monetários de seus negócios aos fatores não-monetários, como a articulação da sociedade civil, que questiona o comportamento ambiental das empresas.

Toffler destaca três pontos-chave para a gestão do futuro. O primeiro deles é o efeito da velocidade, que significa a capacidade de acompanhar todas as informações que afetam direta ou indiretamente os negócios. O segundo é o efeito da complexidade, que implica administrar a diversidade de necessidades criadas por uma sociedade informada, ou seja, a capacidade de oferecer produtos customizados para cada cliente. E, finalmente, o efeito da constelação, que se refere à capacidade de perceber as inúmeras redes que estão interligadas em um negócio. Isso não se restringe a identificar áreas de negócios, fornecedores e consumidores, mas também exige um cuidado especial com a estratégia, que precisa ser capaz de coordenar as várias pontas que compõem a atividade econômica.

Módulo 2 - Métricas e metodologias

Padrões de mercado

“O que não se pode medir não se pode gerenciar.” A frase é de Peter Drucker, conceituado professor, consultor e um dos papas da administração moderna, e traduz bem a necessidade, cada vez maior, que os atuais gestores de TI (Tecnologia da Informação) têm de se servir de metodologias e indicadores que lhes permitam estabelecer objetivos, monitorar os resultados e verificar, de forma objetiva, como e se as metas propostas foram atingidas. A experiência tem mostrado que os antigos manuais de procedimentos utilizados no passado já não atendem mais aos requisitos das empresas.

O turbulento ambiente empresarial, que se apóia na Tecnologia e vive em constante mutação, exige formas mais ágeis e flexíveis de gerenciamento. É dentro dessa nova ótica que ganha força o que se convencionou chamar de governança de TI, que nada mais é do que uma estrutura bem definida de relações e processos que controla e dirige uma organização. O principal foco é permitir que as perspectivas de negócios, de infra-estrutura, de pessoas e de operações sejam levadas em consideração no momento de definição do que mais interessa à empresa, alinhando TI à sua estratégia.

Dentro desse contexto, além das métricas e metodologias que permitem mensurar a capacidade (em uso e em potencial) dos sistemas, ganha cada vez mais importância a adoção de padrões que assegurem e imprimam à infra-estrutura tecnológica corporativa maior flexibilidade. Esses padrões têm um papel crítico no gerenciamento de ambientes heterogêneos, sem os quais não seria possível facilitar a integração e a interoperabilidade entre os diferentes sistemas e soluções.

Atualmente, diante da complexidade e diversidade tecnológica presente nas corporações, já não basta gerenciar desktops, servidores, redes, dados e software de forma isolada. Todos esses componentes precisam interagir uns com os outros, para possibilitar a conectividade e os serviços, e o gerenciamento deve contemplar essas questões. Nesse sentido, as fornecedoras de Tecnologia estão adotando padrões em seus produtos para lhes imprimir maior facilidade de integração e, ao mesmo tempo, para permitir aos usuários um gerenciamento mais eficaz, com menores custos. De sua parte, as empresas usuárias de Tecnologia também começam a prestar atenção a esses detalhes e a escolher produtos com base nisso.

Uma das principais organizações que tem como foco a criação, emprego, manutenção e divulgação de padrões e iniciativas para o gerenciamento de ambientes de TI é a Distributed Management Task Force (DMTF – www.dmtf.org), que reúne em seu rol de afiliados e colaboradores os principais fornecedores de Tecnologia da Informação, além de grupos e entidades de padronização. O resultado dessa união de forças foi a criação de uma série de padrões, entre os quais se destacam o CIM (Common Information Model), WBEM (Web-Based Enterprise Management), DEN (Directory Enabled Networking), ASF (Alert Standard Format) e DMI (Desktop Management Initiative).

CIM, WBEM, DEN, ASF e DMI

Em termos simples, o CIM pode ser entendido como um modelo conceitual para a descrição dos ambientes computacionais e de rede das corporações – seus componentes, configurações, operações, relacionamentos, etc –, sem se referir a uma implementação em particular.

Sua utilização visa endereçar o gerenciamento ponto a ponto das estações-clientes para os servidores e pela rede, ou seja, permitir o intercâmbio de informações de gerenciamento entre sistemas e aplicações.

GERENCIAMENTO DE TI

O CIM é composto por duas partes: o CIM Specification, que descreve a linguagem, nomenclatura e técnicas de mapeamento para outros modelos de gerenciamento (como os SNMP MIBs e DMTF MIFs, entre outros), apresentando também o Meta Schema, que é a definição formal do modelo; e o CIM Schema, que fornece uma série de classes com propriedades e associações que propiciam o melhor entendimento conceitual do framework no qual é possível organizar a informação disponível sobre o ambiente gerenciado. O CIM propicia uma semântica padronizada, parecida com um dicionário de termos de gerenciamento, descrevendo os ambientes de TI e de rede da corporação. O modelo foi concebido para auxiliar a minimizar os impactos da introdução de novas tecnologias, facilitando a integração e a interoperabilidade com os demais sistemas já instalados.

Outro padrão desenvolvido pela DMTF é o Web-Based Enterprise Management (WBEM), voltado para acoplar o CIM aos protocolos da Internet como XML e HTTP. A arquitetura do WBEM incorpora o CIM Server e vários provedores de dados de gerenciamento. O CIM Server atua como um corretor (broker) de informação entre os provedores de dados de instrumentação e os clientes/aplicações de gerenciamento. O WBEM pode ser entendido como um set de tecnologias de gerenciamento e de padrões Internet desenvolvidos para unificar a administração de um ambiente corporativo de TI.

Já o Directory Enabled Networks (DEN) foi inicialmente definido como um modelo de informações baseado numa extensão do CIM. Sua função é descrever como utilizar o CIM e um diretório para localizar e acessar informações de gerenciamento. O DEN está focado em comunicar os benefícios, usos e estrutura de um diretório, tido como um componente de um ambiente completo de gerenciamento. O DEN também especifica os mapeamentos low-level LDAP para os releases CIM. Isso permite a criação de uma template para troca de informações entre diretórios e possibilita aos fornecedores de Tecnologia compartilhar uma definição comum (mas extensível) tanto de entidades como de sistemas, aplicações e serviços.

Outro padrão que vem despertando o interesse dos fornecedores de TI e também das empresas é o Alert Standard Format (ASF), que permite ao administrador de TI responder de forma proativa e reativa a problemas ocorridos num sistema em particular, ou em vários sistemas, quando um sistema operacional não estiver presente ou disponível. Historicamente esses problemas eram resolvidos com o emprego de tecnologias proprietárias e muito caras. Com o ASF é possível reduzir substancialmente esses custos.

O ASF consiste num sistema cliente (ou num servidor ou vários sistemas), definido como “cliente”, e um console de gerenciamento que o controla e monitora. Um computador ASF permite realizar o gerenciamento remoto num cenário de sistema operacional ausente e uma série de ações, tais como transmitir mensagens pelo sistema ASF incluindo alertas de segurança; recebimento e processamento de pedidos remotos de manutenção enviados pela console de gerenciamento; capacidade de descrever as características de um sistema cliente ao console de gerenciamento; e capacidade de descrever o software utilizado para configurar ou controlar o sistema cliente em uma situação em que o sistema operacional estiver presente.

O ASF adiciona importantes medidas de segurança, as quais definem interfaces de alerta e de controle remoto, permitindo o gerenciamento proativo de elementos da rede quando seus sistemas operacionais (OS) estiverem ausentes. A especificação ASF define o Remote Management Control Protocol (RMCP), que permite ao administrador da rede responder a um alerta remotamente em diferentes formas: ativando os sistemas, desativando os sistemas, ou forçando um reboot. Essa funcionalidade possibilita ao administrador economizar um tempo valioso, na medida em que reduz as visitas ao ambiente de desktop, já que terá a habilidade de solucionar os problemas de forma remota por meio de um console de gerenciamento. O ASF também define um protocolo de quatro fases que inclui descoberta, autenticação, comando de transferência e conclusão. Com essas capacidades de autenticação, é possível ao administrador atender, também de forma remota, as necessidades de segurança que a corporação requer.

GERENCIAMENTO DE TI

O OS-absent (sistema operacional ausente) é definido como um estado do ambiente computacional em que o sistema operacional não está disponível. Isso pode ocorrer por problemas de boot ou erros, ou porque o sistema está num estado de dormência (baixo poder). Com a especificação ASF, o administrador da rede será alertado das falhas em componentes específicos, minimizando a manutenção on-site e, ao mesmo tempo, aumentando a visibilidade e acesso remotos aos sistemas locais. Sem o ASF, os problemas de sistema operacional ausente precisam de uma intervenção manual para poder reativar os sistemas ou forçar um reboot.

As principais fornecedoras de soluções de TI, entre as quais se incluem a Intel, 3Com, HP e IBM, entre outras, desempenharam um papel ativo no desenvolvimento do ASF, trabalhando em conjunto com a DMTF. Essas empresas apostam nesse padrão como forma de assegurar aos respectivos clientes do setor corporativo uma forma mais eficiente de gerenciar seus ambientes distribuídos, auxiliando inclusive a maximizar o uptime (disponibilidade) dos sistemas. De outra parte, as corporações usuárias de Tecnologia já começam a exigir esse padrão nos produtos. Um exemplo foi o da Caixa Econômica Federal, que no edital para aquisição de desktops (cerca de 150 mil máquinas) inseriu o ASF como um dos requisitos para as fornecedoras que se candidataram na licitação.

Outro padrão desenvolvido pela DMTF é o Desktop Management Interface (DMI) Specification, que estabelece um framework padrão para gerenciar desktops, notebooks e servidores ligados em rede. O DMI foi o primeiro padrão para gerenciamento de desktop e coexiste nos ambientes atuais com o WBEM. A especificação inicial, criada em 1993, envolvia o gerenciamento remoto por uma interface e dispunha de um modelo para filtragem de eventos. A versão 2.0, veiculada em 1996, estendeu a especificação original com a definição de um mecanismo que envia as informações de gerenciamento através da rede para clientes não locais ou para um site central.

Metodologias e indicadores

A árdua tarefa de gerenciamento do ambiente de Tecnologia também pode ser facilitada com a adoção de ferramentas, indicadores e metodologias que auxiliam os profissionais a dimensionar o uso efetivo e o potencial de uso dos sistemas. O rol de produtos é vasto e variado. Atualmente, somam-se às soluções conhecidas e tradicionais, como Balanced ScoreCard, Return on Investment (ROI), TCO (Total Cost of Ownership), Economic Value Added (EVA), e Activity Based Costing, outros modelos que começam a ser empregados pelo setor corporativo, como o CobiT, ITIL e CMM. Em seguida, uma breve descrição das principais ferramentas de medição para auxiliar no gerenciamento empresarial que estão sendo utilizadas pelo mercado.

Desenvolvida nos Estados Unidos, a metodologia CobiT – Control Objectives for Information and Related Technology foi criada pelo Information System Audit and Control Association (Isaca) em 1996, a partir de ferramentas de auditoria, funcionando como uma espécie de guia para a gestão da TI nas empresas. O CobiT inclui uma série de recursos como sumário executivo, framework, controle de objetivos, mapas de auditoria e um conjunto de processos de trabalho já estabelecidos e empregados pelo mercado, entre os quais se incluem o CMM (Capability Maturity Model), a ISO 9000 (para qualidade), BS7799/ISSO 17799 (normas para segurança da informação) e o ITIL (para gestão do departamento de TI).

O CobiT independe das plataformas de TI adotadas pelas empresas e seu uso é orientado a negócios, no sentido de fornecer informações detalhadas para gerenciar processos. A metodologia é voltada para três níveis distintos: gerentes que necessitam avaliar os riscos e controlar os investimentos de TI; os usuários que precisam assegurar a qualidade dos serviços prestados para clientes internos e externos; e auditores que necessitam avaliar o trabalho de gestão da TI e aconselhar o controle interno da organização. O foco principal é apontar onde devem ser feitas melhorias.

GERENCIAMENTO DE TI

Complementar ao CobiT, o ITIL - Information Technology Infrastructure Library é uma biblioteca que descreve as melhores práticas de gestão, especificamente elaborada para a área de TI. Criado no final dos anos 80 pela Central Computing and Telecommunications Agency para o governo britânico, o ITIL reúne um conjunto de recomendações, sendo dividido em dois blocos: suporte de serviços (service support), que inclui cinco disciplinas e uma função; e entrega de serviços (service delivery), com mais cinco disciplinas. Os pontos focados apresentam as melhores práticas para a central de atendimento, gerenciamento de incidentes, gerenciamento de problemas, e gerenciamento financeiro para serviços de TI.

Voltado a auxiliar as empresas a melhorar a produtividade dos processos de desenvolvimento de software e a organizar o funcionamento de seus ambientes de Tecnologia da Informação, o CMM - Capability Maturity Model é uma metodologia que mostra as metas a serem alcançadas, atuando como um modelo de orientação e qualificação dos estágios de maturidade. O CMM define cinco níveis de maturidade para os ambientes de desenvolvimento de software (inicial, repetível, definido, gerenciado e otimizado), sendo que cada um deles é composto por um conjunto de áreas-chave de processo (KPA – Key Process Areas) que descrevem as questões e grandes temas que devem ser abordados e resolvidos para se atingir um determinado nível.

Metodologias tradicionais

Uma das metodologias mais visadas na atualidade é o Balanced ScoreCard, criada no início da década de 90 por Robert Kaplan e David Norton, ambos professores da Harvard University (EUA). Seu emprego permite a uma empresa obter uma base mais ampla para a tomada de decisão, considerando quatro perspectivas: a financeira (segundo a visão dos acionistas), a dos clientes, a de processos internos de negócios, e a de inovação.

Na prática, a metodologia consegue mostrar o que é mais crítico, possibilitando direcionar os recursos para os processos que de fato adicionarão valor à empresa. A Tecnologia é uma peça importante para colocar o BSC em funcionamento, mas não é suficiente porque a metodologia interage com a cultura da corporação. Por ser complexa e envolver toda a estrutura empresarial, a adoção desse modelo deve partir da alta direção ou mesmo do próprio presidente da empresa.

O projeto de construção do BSC se aplica a qualquer empresa, independente do ramo de atividade e porte, levando em média de 8 a 12 semanas para ser concluído, mas os benefícios começam a ser percebidos um ano após a implementação. O emprego dessa metodologia possibilita uma visão ampla, geral e integrada da empresa, por meio de diversos painéis. Trata-se de um modelo flexível, que permite ajustes ao longo do tempo.

O Balanced ScoreCard cria uma linguagem para comunicar a missão e a estratégia da empresa a todos os funcionários e utiliza indicadores para informar sobre os vetores de sucesso alcançados no momento e os pretendidos no futuro. Dessa forma, é possível canalizar as energias e esforços das pessoas para atingir os objetivos de longo prazo.

Outro indicador de desempenho fundamental no setor corporativo é o Return on Investment - ROI -, utilizado para apoiar e justificar novos investimentos em tecnologia. O ROI é calculado considerando o benefício anual proveniente do investimento dividido pelo montante investido, sendo expresso em porcentagem e, portanto, facilmente comparável a outras taxas, por exemplo, à de juros e de custo do capital. Esse indicador, no entanto, não leva em consideração os riscos envolvidos e nem outras variáveis durante um determinado período. Nesse sentido, não é muito indicado para a avaliação de projetos de longa duração, em que os custos e benefícios venham a passar por grandes alterações com o tempo. Mesmo assim, o ROI é um dos indicadores preferidos pelos principais executivos das empresas na medida em que oferece um valor quantificável e bem definido.

TCO, TVO e CAPT

Uma das grandes preocupações do setor corporativo é verificar até que ponto os gastos estão sendo feitos de forma inteligente e quais os reais ganhos obtidos. O mais importante não é saber quanto se investe em TI, mas ter uma compreensão geral do seu impacto na organização. Entre as metodologias existentes, uma das mais conhecidas e que se tornou padrão no mundo todo é o TCO -Total Cost of Ownership - desenvolvida em 1987 pelo Gartner Group, atual Gartner Incorporated –, que está evoluindo para um conceito ainda mais amplo batizado de TVO – Total Value of Opportunity.

O TCO começou a ser amplamente considerado à medida que a computação distribuída se desenvolvia e as empresas perceberam que, apesar de o modelo cliente/servidor oferecer uma série de benefícios muito válidos, em contrapartida, trazia uma série de desafios que o modelo centralizado anterior, de certa maneira, não trazia, por ser mais controlado. Entre esses desafios, os principais eram a gestão de custos e a questão da segurança. Inicialmente a metodologia foi desenvolvida para medir apenas os custos relativos aos PCs. Depois, o conceito amadureceu, sendo expandido para abarcar todo o resto da computação distribuída, como redes LAN (Local Area Network), bridges, hubs, roteadores, periféricos, etc.

A principal idéia que se procurava passar para o setor corporativo, no final dos anos 80, por meio da análise do TCO, era a de que o custo de se possuir um ativo de TI não se restringia ao valor de aquisição. A quantia paga na compra da solução ou do equipamento representava apenas uma pequena parte de uma equação muito mais complexa, que incluía também os custos relativos à manutenção e uso desse ativo ao longo do tempo. Similar a um plano de contas contábil, o plano de contas do TCO inclui todos os custos de se manter uma solução de TI – tanto os custos diretos e orçados (como aquisição de hardware e software, operação e administração), como os indiretos e não orçados (como tempo de inatividade dos sistemas e operações dos usuários finais).

Analisar os custos de TI de forma mais abrangente, no entanto, ainda não é considerado por muitas empresas como totalmente satisfatório. Muitas desejam comprovar os reais benefícios propiciados pela Tecnologia em uso. Com base nisso, o Gartner passou a fazer também pesquisas para usuários de negócio, resultando na criação de uma divisão nova, batizada de G2, composta por analistas especializados em análise de negócios, que desenvolveram o Gartner Business Performance Framework (GBPF) – um framework de métricas de oferta, demanda e suporte.

O GBPF constitui uma parte importante de uma nova ferramenta do Gartner batizada de TVO – Total Value of Opportunity. Baseada na Web, a ferramenta auxilia o cliente a construir um business case consistente dos projetos que pretende implementar na sua empresa. A espinha dorsal do TVO é formada por sete perguntas – as Seven Business Value Questions. São questões simples, tais como a descrição da iniciativa pretendida; onde essa iniciativa causará impacto no negócio; quanto custa, facilidade e dificuldade de implementação, entre outras.

Outra metodologia para se medir o custo total de propriedade é o Custo Anual por Teclado - CAPT, criado por volta de 1998 pelo CIA/ FGV (Centro de Informática Aplicada da Fundação Getúlio Vargas de São Paulo). O método se caracteriza pela simplicidade e facilidade de aplicação, e consiste, basicamente, em levantar todos os valores direcionados para a área de TI (investimentos e gastos com hardware, software, manutenção, suporte, atualização, treinamento de funcionários e tudo o mais que estiver sob a rubrica de TI), chegar a um único valor e dividir essa quantia pelo número de “teclados” ou de equipamentos existentes na empresa. A facilidade está justamente no fato de que toda empresa dispõe dessas informações. A proposta do CAPT é de ser um indicador que fornece uma visão bastante clara de como a empresa se encontra naquele momento ou, no mínimo, como está a administração dos recursos de tecnologia.

GERENCIAMENTO DE TI

O CAPT não foi baseado em nenhum modelo pré-existente, mas resultou de um trabalho de investigação, feito pela equipe de pesquisadores do CIA, que inclui professores e alunos da Fundação Getúlio Vargas, e que visava identificar quais eram as informações importantes e que precisavam ser elencadas para se poder medir, de forma eficiente, os custos da TI.

A metodologia da FGV fornece apenas uma parte da radiografia sobre os custos da TI de uma empresa. Os próprios criadores do método reconhecem a sua limitação. Ele permite obter poucas informações, exigindo o uso de outros indicadores para fornecer uma melhor percepção sobre o direcionamento dos gastos e investimentos em TI.

Especificamente quanto ao uso de aplicativos, existe a metodologia denominada Total Cost of Application Ownership (TCA), que se aplica especialmente para a avaliação dos custos relativos à computação baseada em rede. Com a proliferação do uso de redes nas companhias, muitas aplicações são disponibilizadas para usuários fixos, móveis e para os que se encontram dispersos geograficamente. Os aplicativos devem estar acessíveis através de uma grande variedade de opções de conectividade, como redes LAN, WAN, VPN, wireless e Web based, entre outras.

Também o número e a variedade de dispositivos fixos e móveis, como PCs, notebooks, PDAs, etc. têm crescido muito nas companhias. O TCA tem como foco a análise dos custos associados aos dispositivos específicos de computação, e leva em consideração como os aplicativos são disponibilizados, a localização dos usuários, as opções e a variedade de conectividade e a variedade de tipos de dispositivos-cliente.

Indicadores tradicionais

Além das metodologias e métricas específicas para a área de TI, os gestores de informática podem se valer de outros sistemas que já vinham sendo utilizados pelas empresas antes do uso maciço da tecnologia. O método Activity Based Costing (ABC), por exemplo, foi adotado inicialmente pelo setor industrial, usado como uma poderosa ferramenta para o gerenciamento dos custos de produção, sendo posteriormente empregado também em outras áreas, como a de serviços.

A idéia básica é a de que todas as atividades de uma empresa voltadas a suportar a produção e distribuição de bens e serviços devem ser consideradas como custos do produto. O ABC integra várias atividades distintas, entre as quais a análise de valor, a análise de processos, controle de custos e controle da qualidade. As abordagens baseadas em atividades geram informações importantes para apoio à decisão, na medida em que fornecem aos gerentes um panorama claro de como se comportam os custos e quais as formas de controlá-los eficientemente para otimizar o desempenho dos negócios.

Alguns gestores também fazem uso do Economic Value Added (EVA), ou Valor Econômico Agregado -, método de desempenho corporativo desenvolvido pela consultoria norte-americana Stern Stewart, na década de 80, que corresponde à subtração do lucro operacional do custo do capital.

Existem ainda outras metodologias e métricas que constituem importantes ferramentas para auxiliar os gerentes de Tecnologia a monitorar e controlar custos e para avaliar benefícios. O emprego desses sistemas, de forma individual ou combinado, está se tornando obrigatório para as corporações manterem-se ágeis e assegurar seu poder de competitividade.

Módulo 3 - Gerenciamento de desktops

Dos “terminais burros” aos Pcs

Durante décadas, o Diretor de Informática limitou-se a administrar a Tecnologia de forma tática e técnica. O ambiente centralizado, baseado na Tecnologia proprietária que vigorou nos anos 60 e 70, embora apresentasse grande complexidade, era mais fácil de ser gerenciado. A atenção do gestor da área estava basicamente focada no desenvolvimento de aplicativos, análise de sistemas, cuidados com a sua equipe, manutenção, atendimento às solicitações dos diferentes departamentos da empresa e atividades técnicas.

A diversidade de máquinas e software era pequena, se comparada aos dias atuais. Ao mainframe estavam ligados alguns periféricos e os então chamados "terminais burros", que permitiam acesso aos dados a limitado número de usuários. Nesse período, a escolha de novas tecnologias era de certa forma facilitada, na medida em que havia poucos fornecedores no mercado.

Esse modelo deixou de vigorar com a proliferação do ambiente cliente-servidor e da computação distribuída. Em curto espaço de tempo, novas empresas fornecedoras de hardware e software ampliaram consideravelmente a oferta de opções, tornando mais complicado o processo de escolha. De outro lado, os usuários de diferentes departamentos da corporação passaram a ter acesso a ferramentas de Tecnologia, resultando no aumento do número de estações de trabalho, de computadores de mesa (desktops, os conhecidos PCs) e devices móveis (notebooks) em uso.

Com isso, o ambiente de informática tornou-se múltiplo e bem mais complexo. Muitas empresas passaram a dispor de um parque heterogêneo, composto por máquinas de diferentes fabricantes, portes e datas de fabricação, executando diferentes sistemas operacionais e utilizando diferentes versões de software. Velhas e novas gerações de ferramentas de TI ligadas em redes passaram a conviver num mesmo ambiente, o qual passou a estar em constante transformação. Gerenciar Tecnologia da Informação deixou de ser uma atividade puramente técnica. Hoje, significa direcionar recursos para atingir objetivos estratégicos.

Novos desafios

A dinâmica da evolução tecnológica gerou um efeito colateral. Os altos custos diretos e indiretos relacionados à manutenção de todo o aparato computacional levaram as empresas a reavaliar sua infraestrutura de TI e a buscar identificar, medir e comprovar os benefícios propiciados em termos de disponibilidade, confiabilidade, acessibilidade e eficiência dos sistemas. Diante dessa variedade de mudanças, cabe ao diretor da TI a difícil tarefa de imprimir eficiência aos processos de negócios, e ao mesmo tempo, reduzir os custos operacionais. O bom gerenciamento e a melhor utilização do aparato computacional instalado passaram a ser fundamentais e também o principal desafio do administrador de TI.

No que se refere especificamente ao parque de PCs (desktops), estudos do Instituto de Pesquisa Gartner mostraram que as empresas que não mantêm um gerenciamento adequado de hardware e software distribuídos podem registrar um aumento anual da ordem de 7% a 10% no custo total de propriedade. Por monitoramento impróprio, essas corporações acabam acessando informações inadequadas para planejar upgrades de hardware ou sistemas operacionais. Além de aumentar os custos, o mau gerenciamento colabora para que os gestores da área tracem previsões incorretas sobre os equipamentos que os usuários de fato têm e para os quais devem desenvolver aplicações.

O Instituto de Pesquisa Gartner também concluiu que, ao contrário, quando o gerenciamento é adequado e bem executado, pode-se reduzir o TCO (custo total de propriedade) em cerca de 30%. A estratégia se resume em focar a redução de custos de todas as fases do ciclo de vida do PC, levando em consideração também o ambiente de TI do qual faz parte. Centralizar o controle da TI e optar pela adoção de um ambiente

GERENCIAMENTO DE TI

padronizado (com produtos de um único fabricante ou de poucos fornecedores) são outras atitudes que podem trazer grandes benefícios, entre os quais facilitar o suporte, agilizar a resolução de problemas, facilitar a atualização de antivírus e programas aplicativos e otimizar o treinamento de usuários, além de reduzir custos. Uma pesquisa feita pelo Giga Information Group mostrou que a padronização de PCs pode gerar reduções da ordem de 15 a 25% no custo da TI durante o ciclo de vida dos sistemas.

Planejamento da capacidade

O ciclo de vida dos PCs é dividido em quatro fases principais: avaliação, distribuição/migração, gerenciamento e desativação/renovação. Para evitar erros simples, como fornecer uma máquina com um processador de alta potência, grande capacidade de memória e recursos sofisticados para um funcionário que apenas irá utilizar um processador de textos e uma planilha eletrônica, ou dar a um engenheiro um equipamento que não lhe permita rodar aplicativos mais pesados e necessários para o seu trabalho, é fundamental que se faça uma avaliação prévia da base de usuários para se definir a configuração dos PCs a eles destinados, de forma a atender as suas reais demandas.

O planejamento da capacidade (sizing) dos desktops deve levar em conta duas vertentes. A primeira delas refere-se à análise do perfil de uso de cada funcionário, para que o equipamento e aplicativos apresentem as características e funcionalidades na medida exata das necessidades de trabalho daquele profissional. Nesse sentido, o gerenciamento pode ser facilitado se os usuários forem agrupados em categorias, de acordo com suas áreas de atuação: vendas, engenharia, administração, marketing, etc.

Também é importante considerar as características de trabalho de cada usuário, por exemplo, verificar a necessidade de mobilidade dos profissionais de campo e que costumam participar de reuniões externas com clientes e fornecedores, ou os que viajam com grande frequência; funcionários que utilizam aplicativos que requerem maior poder de processamento, como os da área de engenharia e de desenvolvimento de produtos, e assim sucessivamente.

O segundo cuidado diz respeito ao dimensionamento do volume de processamento de cada máquina. Esse cálculo é feito com base nos dados históricos de uso de cada máquina e de projeções de uso futuro dos sistemas. O mundo dos negócios não é estático. Ao contrário, vive em constante transformação, e isso deve ser levado em conta pelo gestor da TI.

É preciso avaliar e acompanhar ritmo das mudanças dentro da corporação e, conseqüentemente, das necessidades de cada usuário. Verificar continuamente a necessidade de ampliar a capacidade de memória, a capacidade dos discos, a velocidade do processamento, upgrade de software, mobilidade, recursos multimídia, recursos para trabalho em grupo, entre outros elementos, é fundamental para otimizar o parque de desktops e adequar seu uso.

Atualmente, existem ferramentas que auxiliam o gestor na tarefa de fazer esse levantamento, compor um inventário sobre o número de máquinas instaladas (inclusive notebooks, PDAs e dispositivos wireless) e monitorar suas respectivas configurações, software utilizado, métricas de performance e nível de integração com outros sistemas.

A distribuição/migração é outra questão importante. Em geral, os usuários acabam requerendo horas do pessoal técnico da área de suporte e help desk para configurar software nos seus equipamentos. Mas esse trabalho pode ser feito de forma remota por meio de ferramentas específicas baseadas em rede. A configuração automatizada reduz os riscos de erros humanos e estabelece maior padronização e confiabilidade. Em princípio esse processo permite carregar nos novos PCs o sistema operacional e aplicativos que foram configurados num sistema de referência.

GERENCIAMENTO DE TI

No que tange ao gerenciamento dos desktops, outros dois elementos são importantes: a atualização de software e a resolução de problemas. São processos que também podem ser feitos remotamente, mediante ferramentas específicas e por processos de monitoração. Falhas nos PCs significam queda de produtividade dos funcionários, por isso é recomendável a adoção de ferramentas que, combinadas com aplicações de help desk, permitam aos técnicos controlar os sistemas pela rede e providenciar a resolução das falhas de forma rápida e eficiente.

A determinação do tempo de vida útil dos equipamentos é atualmente uma prática recomendada pelos institutos de pesquisa e por consultores como forma de reduzir custos com suporte e manutenção, além de facilitar o gerenciamento. O Giga Information Group recomenda que a cada 3 anos o parque de desktops deve ser renovado e, a cada dois, o de notebooks, considerando que em termos monetários é mais caro para a empresa manter operantes equipamentos ultrapassados do que investir na sua substituição por produtos de última geração. Quanto mais antigo for o parque, maiores são os custos de manutenção e de suporte, além do aumento dos riscos de falhas nos sistemas e de uma baixa velocidade de processamento, o que pode comprometer os níveis de produtividade da empresa.

Estabilidade da plataforma

Estima-se que apenas em termos de PCs existam, no mundo, 500 milhões de máquinas com vida útil superior a quatro anos, sendo que, desse contingente, 50% são utilizados no setor corporativo. A maioria desses equipamentos está equipada com sistemas operacionais mais antigos como Windows 95 e 98. Quanto aos demais aplicativos, também exigem renovação, até porque muitos fornecedores de produtos, encabeçados pela Microsoft, param de fornecer suporte para versões antigas de suas soluções. Não acompanhar essa tendência do mercado pode significar para as corporações a obrigação de arcar com custos adicionais expressivos.

Investir em novas plataformas e em software de última geração pode representar um investimento inicial maior, mas os ganhos de performance e a redução da necessidade de manutenção demonstram, na ponta do lápis, que se trata de uma prática a ser seguida. Em termos comparativos, renovar o parque de TI equivale à compra de um carro novo. Quanto mais anos de uso tiver o automóvel, mais visitas à oficina mecânica serão necessárias, gerando gastos com manutenção. No caso da TI ocorre o mesmo. Além de ficarem mais sujeitos a falhas, os sistemas podem apresentar baixa performance e ficar mais vulneráveis a tentativas de invasão por hackers e vírus.

De acordo com alguns consultores, na prática, o número de empresas que opta pela estratégia de renovar o parque instalado é grande nos Estados Unidos e em países do primeiro mundo, que têm mecanismos financeiros e de mercado favoráveis a isso. Mas o mesmo não acontece em países como o Brasil e os da América Latina. Nesses locais, verifica-se que a atualização tecnológica não é mandatória, e sim limitada a alguns segmentos da empresa, especialmente nos que têm interface com o mundo externo. No Brasil, não é difícil encontrar indústrias que ainda utilizam soluções ultrapassadas, por exemplo, linguagem Cobol e sistema operacional DOS, e que não querem investir em inovação porque essas tecnologias antigas ainda as atendem de forma satisfatória.

No que se refere a novos investimentos em TI em países emergentes, a realidade mostra que os gestores precisam verificar como a informática flui nos diferentes departamentos da sua empresa e qual o grau de maturidade dos usuários para lidar com ela. Outra questão importante é verificar que resultados se obterão com as novas ferramentas e quanto a atualização tecnológica impactará na evolução dos negócios da corporação.

GERENCIAMENTO DE TI

O que apresenta maior peso, principalmente na redução dos custos diretos e indiretos, que hoje constitui a maior pressão sofrida pelos gestores da TI por parte da alta direção, são as práticas de gerenciamento. Fazer um inventário do parque de hardware e software instalado possibilita efetuar maior controle sobre os ativos, além de combater a pirataria, na medida em que é feito o levantamento da quantidade de licenças instaladas, e ainda contribui para disciplinar o uso desses recursos dentro da organização.

Também é importante contar com um programa eficiente de segurança e proteção de dados, de forma a disciplinar o uso dos ativos de TI, impedindo a instalação e remoção de software pelos usuários. Optar pela padronização do ambiente também é uma atitude inteligente, na medida em que facilita a utilização dos recursos por parte dos usuários, além de reduzir os custos com treinamento e minimizar o trabalho de help desk. São práticas que, no conjunto, contribuem para reduzir os custos totais em até 30%.

Gerenciamento da mobilidade

Atualmente, a força de trabalho está muito mais móvel e distribuída do que nunca, e esse processo deverá se acentuar nos próximos anos. Os sistemas operacionais modernos e as aplicações de gerenciamento oferecem um largo espectro de ferramentas que permitem monitorar e gerenciar os sistemas cliente de forma remota, controlando o inventário, solucionando problemas e instalando ou renovando software.

As soluções que possibilitam o gerenciamento remoto da base de usuários móveis facilitam, principalmente, as tarefas de manutenção e help desk. Se um usuário tiver problemas com um aplicativo, o pessoal técnico poderá visualizar o problema e solucioná-lo remotamente. Segundo o Instituto de Pesquisa Gartner, as corporações podem registrar uma economia da ordem de US\$ 21 a US\$ 77 por máquina, por ano, dos custos de help desk apenas adotando essa prática.

Outra forma de cortar custos e otimizar o gerenciamento dos ambientes distribuídos é espalhar pela corporação estações de reserva pelas quais os funcionários podem fazer backups e repor componentes dos sistemas conforme as suas necessidades. Desse modo, são criadas estações de serviços voltadas para atender os usuários de notebooks e ajudá-los a solucionar problemas de forma rápida e eficiente.

Em resumo, as melhores práticas para o bom gerenciamento da base de PCs recomendam que sejam tomadas algumas atitudes simples, como substituir PCs de forma proativa, simplificar e padronizar o ambiente, segmentar a base de usuários, manter os software atualizados, otimizar o processo de distribuição de sistemas, e monitorar o ambiente móvel por meio de soluções distribuídas.

Resultados na prática

Muitas empresas já estão obtendo ganhos consideráveis com a otimização do gerenciamento do parque de desktops. Um exemplo é o da Dedic, do Grupo Portugal Telecom, uma das maiores empresas de Contact Center do Brasil. O negócio da Dedic é fornecer uma solução completa de relacionamento com clientes para as empresas do mercado brasileiro, disponibilizando, para isso, dois sites próprios localizados em São Paulo, além de administrar três sites de clientes, em São Paulo, Campinas e Londrina.

Gerenciar a infra-estrutura técnica que suporta o Contact Center é, portanto, essencial para os seus negócios. Nesse sentido, a empresa optou por adotar as soluções da Altiris, especializada em auxiliar as organizações a gerenciar o ciclo de vida de desktops, notebooks, handhelds, servidores Windows, Linux e Unix, além de ativos fixos, providenciando a integração completa e soluções de gerenciamento de sistema para clientes, dispositivos móveis e servidores, com rápido retorno de investimento.

GERENCIAMENTO DE TI

Para automatizar a implantação, manutenção e suporte, de acordo com os padrões dos sistemas instalados nos desktops da Dedic, foi utilizada a solução Client Management Suite (CMS), da Altiris. Pelo módulo Deployment Solution, foi possível automatizar todo o serviço de configuração, resultando numa grande economia de tempo e dinheiro na realização da tarefa. Uma máquina foi preparada manualmente por um técnico com as configurações do cliente. A partir desse equipamento, foi criada uma imagem, a qual foi usada no processo de clonagem – feito pela solução da Altiris – que configurou os demais computadores.

O procedimento, em cada computador, levou menos de 10 minutos. A solução foi considerada vital para o negócio da Dedic porque a distribuição de softwares – principal etapa do processo de configuração – precisa ser feita de maneira ágil e confiável, mantendo a qualidade. Com o CMS, o padrão de softwares distribuídos foi mantido, e a ferramenta possibilitou reduzir de imediato o custo mensal de contratação de mão-de-obra para execução de tarefas. Com isso, foi aumentada a produtividade da equipe interna, refletindo imediatamente na satisfação e tranquilidade tanto da empresa quanto dos clientes.

Antes de implementar a solução, a Dedic havia feito uma pesquisa no mercado e testes com pilotos de soluções similares de outros fornecedores. A qualidade, performance e facilidade do uso demonstrada pela ferramenta da Altiris fizeram com que a empresa optasse pela sua adoção, a qual está em uso há mais de um ano e meio.

Redução de custos

Outra empresa que espera obter benefícios pelo gerenciamento adequado é a BMW, uma das companhias líderes do setor automotivo, que optou por seguir as melhores práticas para renovar o seu parque de PCs. A companhia introduziu centenas de equipamentos munidos com o Processador Intel® Pentium® 4 e Tecnologia Hyper-Threading, com sistema operacional Windows XP. Cerca de 20% desses novos computadores são notebooks equipados com o processador Pentium M. O objetivo da BMW é analisar como as várias categorias de funcionários irão se beneficiar da tecnologia móvel. O acesso desses usuários à rede corporativa da empresa se dará pela rede WWAN. Leia o case completo na área de complemento de módulo.

Módulo 4 - Gerenciamento de servidores

Os benefícios da consolidação

A opção pelo modelo de computação distribuída vem sendo feita pelas corporações desde o início da década de 80. Esses ambientes de Tecnologia podem dispor de um único computador com maior capacidade, utilizado como servidor de várias estações cliente (desde PCs comuns a estações de trabalho). O mais comum, no entanto, é as empresas contarem com um ambiente heterogêneo, com vários servidores distribuídos ou ligados em cluster (vários servidores ligados em rede). Esse modelo requer maiores cuidados de gerenciamento para que a infra-estrutura não se torne complexa demais, ineficiente, cara e necessitando de contínuos investimentos em equipamentos, componentes e pessoal.

Devido às limitações do hardware e software no passado, muitos operadores e administradores ainda permanecem presos a alguns conceitos e regras, por exemplo, a de que cada aplicação de missão crítica deve ficar num único servidor dedicado, o qual nunca pode utilizar mais do que 80% da capacidade da CPU (unidade central de processamento). Com a evolução tecnológica, isso não faz mais sentido.

Atualmente, a grande preocupação dos gestores de TI refere-se à proliferação do número de servidores. Cada vez mais as empresas investem em novos equipamentos, em busca de aumentar a produtividade e atender às crescentes necessidades dos negócios o que, ao contrário, pode causar graves transtornos e dificuldade de gerenciamento. A diversidade de plataformas operacionais e de gerações tecnológicas num único ambiente provoca problemas de operação, manutenção, atualização e, conseqüentemente, influi nos custos.

Um dos fatores que tem contribuído para o aumento do número de servidores nas empresas é a redução do custo do hardware, a cada ano, embora esse valor represente apenas 20% do custo total de propriedade. Apesar de a opção de instalar vários servidores possa parecer uma alternativa barata, cada nova máquina que chega, no entanto, adiciona custos ocultos significativos, requerendo dedicação dos técnicos especializados em atividades de depuração, otimização e gerenciamento. Além disso, é necessária a manutenção de diferentes configurações como scripts operacionais, versões de sistemas, utilitários de apoio, procedimento de backup e disaster recovery.

Manter todo esse aparato sob controle requer a adoção de algumas medidas, entre as quais se incluem as seguintes consolidações: geográfica, física, de dados e aplicações. Entende-se por consolidação geográfica a redução do número de sites, concentrando os servidores em um número menor de máquinas. Na prática, isso possibilita reduzir custos de administração, na medida em que diminui a necessidade de técnicos remotos. Também os níveis de serviço acabam sendo otimizados, por meio da adoção de procedimentos e regras operacionais.

Consolidação física significa transferir a carga de vários servidores de menor porte para máquinas de maior porte, o que melhora a utilização geral dos recursos. Em média, um servidor distribuído utiliza de 20% a 30% de sua capacidade, o que equivale ao uso do pleno potencial de um único servidor a cada três máquinas.

Outra medida recomendável refere-se à consolidação de dados e aplicações, o que exige ações mais sofisticadas e planejamento preciso para combinar diversas fontes de dados e plataformas em uma única.

Para compreendermos melhor esses conceitos, vamos imaginar que uma empresa disponha de um parque com 200 servidores, mesclando tecnologias Intel e RISC, de diversos fornecedores e gerações tecnológicas, os quais operam com sistemas operacionais distintos, como Unix, Linux e versões variadas de Windows e NetWare. Administrar esse ambiente heterogêneo implica custos de pessoal especializado para operação e suporte, além de gastos com as inúmeras versões de software e de soluções de gerenciamento e de segurança.

GERENCIAMENTO DE TI

Todas essas questões podem ser minimizadas se a empresa optar por uma simples consolidação em termos geográficos e físicos, substituindo estas máquinas por 30 ou 40 de maior porte, obtendo como resultado a redução do número de técnicos, dos custos de instalação física e operacionais, e ainda registrando ganhos em disponibilidade, segurança, nível de serviço e aproveitamento dos recursos computacionais.

O planejamento da capacidade dos servidores é outra tarefa que deve ser feita de forma contínua pelo gestor da TI, de acordo com a demanda e volume de processamento dos sistemas para que as variações de uso que ocorrem no ambiente não comprometam a performance desejada e apropriada. A periodicidade com que esse trabalho deve ser feito pode ser diária, semanal ou mensal, de acordo com as características de demanda das máquinas, do volume das informações processadas e da criticidade do ambiente.

Podem ser empregadas ferramentas que auxiliem a analisar o histórico de uso dos sistemas e a realizar cálculos para projetar necessidades de expansões futuras, levando em consideração aspectos como número de usuários simultâneos que acessam o servidor, aumento de velocidade de processamento, aumento da capacidade de memória, ampliação do número de estações clientes ligadas aos servidores, novos periféricos e aplicativos agregados.

O gerenciamento da mudança

O principal propósito do gerenciamento é preservar e assegurar a confiabilidade e a boa performance dos sistemas, aos menores custos possíveis de propriedade e de manutenção. A plataforma de aplicação escolhida deve levar em consideração cinco fatores principais: flexibilidade, escalabilidade, performance, confiabilidade e segurança. Para evitar problemas futuros, o gestor da TI precisa estar atento à garantia da qualidade das ferramentas empregadas na corporação.

As melhores práticas do mercado recomendam que, no caso de servidores, se busque obter dos fornecedores garantia de, no mínimo, 99,9% de confiabilidade. Os procedimentos para assegurar o bom desempenho dos servidores devem ser os mesmos que os aplicados a computadores de maior porte, como mainframes, com monitoramento e manutenções periódicas e planejamento do desempenho e uso dos sistemas.

Nos casos em que a TI suporta operações importantes para a empresa, mas esta ainda se vale de equipamentos de menor porte para isso, é recomendável que se opte pela adoção de servidores em cluster, assegurando a redundância do ambiente e, com isso, garantindo a manutenção dos serviços mesmo no caso de pane em algum dos equipamentos. Também é importante dispor de um sistema de backup para prevenir eventuais problemas de perda dos dados ou de indisponibilidade dos sistemas.

Também se faz necessária a adoção de algum tipo de gerenciamento das mudanças, que pode ser feito manualmente ou de forma automatizada. Quando os primeiros servidores começaram a ser empregados pelo setor corporativo, o software era instalado de forma manual, por vários tipos de mídia, como discos e os atuais CD-ROMs. Naquela época, o software instalado no servidor costumava ser estático, necessitando de alteração apenas uma ou duas vezes por ano. E quando precisavam ser modificados, o processo era realizado por técnicos que gastavam horas para concluir o serviço.

Com o passar dos anos e os avanços tecnológicos, as empresas começaram a adquirir um número maior de servidores e, com isso, surgiu a necessidade de realizar gerenciamento remoto. Algumas organizações utilizavam scripts desenvolvidos internamente e software utilitários para distribuir os aplicativos para servidores remotos e, depois, recorriam a ferramentas de administração e controle para instalação dos mesmos. Essa sistemática não oferecia escalabilidade e ainda necessitava de intervenção manual e profissionais especializados. Com o crescimento da Web e do conseqüente aumento do uso de aplicativos baseados em rede, também aumentou a frequência de alterações em códigos e conteúdos, sendo que ao mesmo tempo as arquiteturas de TI se tornavam cada vez mais complexas.

GERENCIAMENTO DE TI

Para atender a essas novas necessidades, surgiram novas soluções de gerenciamento das mudanças, que em termos simples são produtos indicados para simplificar o gerenciamento de aplicativos e dados, reduzindo a necessidade de administração local e, conseqüentemente, diminuindo a quantidade de chamados ao help desk. Hoje, a maioria das soluções para gerenciamento de mudanças em servidores é formada por uma mescla de sistema de distribuição de aplicativos e de conteúdo, e de instalação de arquivos, a partir de repositórios principais para pontos na rede, cujo objetivo é e oferecer controle em tempo real e disponibilidade de recursos.

TI em regime 24 x 7

Algumas corporações já começam a adotar ferramentas que lhes permite controlar melhor seus ativos de TI. A BM&F (Bolsa Mercantil & de Futuros) inclui-se nesse rol. As metas da empresa eram ambiciosas: internacionalizar as operações por meio do ingresso na Aliança Globex (formada pelas bolsas de Chicago, Paris, Cingapura, Madri e Montreal); lançar novos contratos visando o aumento do volume de negócios e da liquidez, automatizar os diferentes departamentos internos e preparar-se para tornar disponível ao mercado novos serviços de clearing de câmbio, além de automatizar os tradicionais processos de clearing de derivativos.

Para conseguir atender a esse elenco de metas propostas pela diretoria, garantindo os níveis de serviços, a BM&F precisou revitalizar toda a sua infra-estrutura tecnológica. O processo resultou na construção de dois centros de Tecnologia totalmente espelhados e operacionais, integrados por fibra óptica redundante, com três links de 2,5 GBPS. Todo esse aparato computacional é gerenciado e monitorado pela plataforma Unicenter, da Computer Associates (CA).

A definição da arquitetura de gerenciamento do ambiente de Tecnologia da Informação (TI) da BM&F levou em consideração uma série de requisitos, visando especificamente reduzir os riscos operacionais. O objetivo era avançar do conceito de gerenciamento de componentes da infra-estrutura para um modelo de gerenciamento das linhas de negócios e de processos críticos, de forma a assegurar o bom desempenho das operações.

Com base nisso, foi preparada uma Request For Proposal, contendo todas as especificações funcionais, técnicas, comerciais e de níveis de serviço desejados. A plataforma de gerenciamento teria de, necessariamente, suportar um ambiente heterogêneo (composto por plataformas mainframe, Windows/NT e Unix) e de alta criticidade, com diferentes bancos de dados e software aplicativos, possibilitando a consolidação das informações por linhas de negócio ou por processos críticos, além de garantir a integração e a interoperabilidade.

Outro item importante foi a flexibilidade para a contratação e expansão das licenças, assegurando o crescimento contínuo das plataformas e o compromisso com a entrega efetiva da solução. Os projetos de gerenciamento, em geral, possuem um fator de risco muito grande e muitas vezes não são conclusivos, apesar de estratégicos para a garantia da qualidade. Por isso, deveria haver um compromisso rigoroso para o cumprimento dos cronogramas e acompanhamento permanente.

A TI é fundamental para a BM&F – não é admissível nenhuma falha de operação, segurança e integridade dos dados. Também se faz necessária a garantia do funcionamento ininterrupto do aparato computacional, 24 horas por dia, sete dias por semana.

GERENCIAMENTO DE TI

Por essa razão, foram criados os dois centros tecnológicos – um deles instalado no prédio da BM&F, no centro velho da capital paulista, e o outro no datacenter da Optiglobe, no bairro de Santo Amaro, em São Paulo, empresa com a qual foi firmado um acordo de "colocation" (os equipamentos, sistemas e gerenciamento são da BM&F, cabendo à Optiglobe o fornecimento do local físico e da infra-estrutura de redes e links) . A iniciativa faz parte do plano de contingência da BM&F. Se houver algum problema em um dos prédios que comprometa o pleno funcionamento do Centro de Tecnologia, o outro centro assume, garantindo que as operações não sejam interrompidas.

Também foi feita toda a consolidação da base de dados para simplificar a sua recuperação, em caso de necessidade. Os dois CPDs são espelhados, mas ambos são operacionais e tudo é atualizado em tempo real. Para facilitar o gerenciamento da infra-estrutura e reduzir os riscos, foram montadas sete centrais de operação (de rede, servidores/processos, atendimento, armazenamento, segurança, administração predial, e mudanças/continuidade). Tudo foi sintetizado em dois conjuntos de painéis de controle e de monitoração, um dos quais voltado para negócios e o outro, para infra-estrutura. O gerenciamento de todo esse aparato,, além das redes intranet e extranet e todos os links de integração com outras empresas, está a cargo do Unicenter.

Todos os resultados projetados foram atingidos e a empresa passou a ter um controle mais efetivo do parque de TI, desde o registro de ocorrências no help desk, passando pelos painéis de monitoração e coleta em tempo real de comportamentos de performance, chegando à detecção de falhas e de consumo de todos os componentes.

Módulo 5 - Gerenciamento das redes

A evolução das redes

O surgimento das redes está intimamente relacionado à disseminação de computadores pessoais, estações de trabalho, servidores e outras ferramentas. Elas foram projetadas, inicialmente, para possibilitar o compartilhamento de recursos caros, como alguns programas aplicativos específicos e bancos de dados, além de impressoras e demais periféricos. As primeiras redes locais surgiram nas universidades americanas no início dos anos 70, mas foi a partir da década de 80, com o lançamento comercial da Ethernet (que se tornou padrão de redes locais de PCs, sendo ainda hoje uma das tecnologias mais utilizadas) e da proliferação do modelo cliente/servidor, que esse processo se difundiu nas empresas.

Nos anos subseqüentes, a evolução das ferramentas de informática e das telecomunicações, aliada à redução de custos dos recursos computacionais, somada ao crescimento da Internet e às tecnologias mobile e wireless (sem fio), possibilitou a criação de diferentes tipos e tamanhos de redes, as quais se mantêm em constante evolução.

A lógica é muito simples: a partir do momento em que passamos a usar mais de um micro, seja dentro de uma grande empresa ou num pequeno escritório, fatalmente surge a necessidade de transferir arquivos e programas, compartilhar a conexão com a Internet e periféricos de uso comum entre os sistemas. Adquirir uma impressora, um modem e um drive de CD-ROM para cada micro, por exemplo, e ainda usar disquetes, ou mesmo CDs gravados para trocar arquivos, não seria produtivo, além de elevar os custos em demasia.

Com os micros ligados em rede, transferir arquivos, compartilhar a conexão com a Internet, assim como com impressoras, drives e outros periféricos, contribui não apenas para melhor aproveitamento dos investimentos feitos nesse ferramental, mas também otimiza a comunicação entre os usuários, seja através de um sistema de mensagens ou de uma agenda de grupo, entre outras possibilidades.

Numa empresa na qual várias pessoas necessitem operar os mesmos arquivos, por exemplo, num escritório de arquitetura, onde normalmente muitos profissionais trabalham no mesmo desenho, centralizar os arquivos em um só lugar é uma opção interessante, na medida em que há apenas uma versão do arquivo circulando pela rede e, ao abri-la, os usuários estarão sempre trabalhando com a versão mais recente.

Centralizar e compartilhar arquivos também permite economizar espaço em disco, já que, em vez de haver uma cópia do arquivo em cada máquina, existe uma única cópia localizada no servidor de arquivos. Com todos os arquivos no mesmo local, manter um backup de tudo também se torna muito mais simples.

Além de arquivos individuais, é possível compartilhar pastas ou até uma unidade de disco inteira, sempre com o recurso de estabelecer senhas e permissões de acesso. A sofisticação dos recursos de segurança varia de acordo com o sistema operacional utilizado.

Um sistema que permita enviar mensagens a outros usuários pode parecer inútil numa pequena rede, mas numa empresa com várias centenas de micros, divididos entre vários andares de um prédio, ou mesmo entre cidades ou países diferentes, pode ser vital para melhorar a comunicação entre os funcionários. Além de texto (que pode ser transmitido por e-mail comum), pode-se montar um sistema de comunicação viva-voz, ou mesmo de videoconferência, economizando os gastos em chamadas telefônicas, pela Internet (Voz sobre IP – VoIP).

GERENCIAMENTO DE TI

Originalmente projetado para a transmissão de dados, o protocolo IP tornou-se padrão da Internet e vem se destacando no tráfego de voz, dados e imagens, sendo cada vez mais empregado pelo setor corporativo. Hoje as empresas buscam integrar suas redes à Web para permitir que clientes, parceiros de negócios e os próprios funcionários tenham acesso às informações em qualquer lugar.

Atualmente as opções em produtos, arquiteturas, protocolos, tipos de transmissão, entre outros elementos que compõem uma rede são inesgotáveis e cabe ao gestor da TI saber escolher e agregar novos componentes e orquestrar todo esse aparato, de modo que funcione em perfeita harmonia. E, à medida que aumenta a quantidade de usuários das aplicações corporativas, o volume de informações e a necessidade de administração dos dados crescem na mesma proporção.

Dessa forma, aumenta a necessidade de monitorar o consumo de banda e programar sua expansão ou, ainda, estudar o emprego de tecnologias que permitam comprimir os dados. Também se faz necessário controlar a disponibilidade dos recursos computacionais, verificando se os servidores e desktops estão funcionando adequadamente e se as aplicações estão disponíveis quando os usuários necessitam delas. A análise da performance é outro elemento fundamental para, no caso de se verificar alguma queda, identificar onde está o problema, se na rede, nos computadores ou nos aplicativos.

Tipos de rede

Genericamente falando, existem dois tipos de rede: as locais, também chamadas de LAN (Local Area Network) e as remotas ou de longa distância, batizadas de WAN (Wide Area Network). A LAN une os micros de um escritório, de um edifício, ou mesmo de um conjunto de prédios próximos, usando cabos ou ondas de rádio, e a WAN interliga micros situados em cidades, países ou mesmo continentes diferentes, usando links de fibra óptica, microondas ou mesmo satélites. Geralmente uma WAN é formada por várias LANs interligadas.

Determinada pela abrangência geográfica limitada e também por estar restrita a uma organização, as redes locais não devem ser entendidas como uma mera interligação de equipamentos para possibilitar o uso compartilhado de recursos, uma vez que preservam a capacidade de processamento individual de cada usuário e possibilitam que os micros se comuniquem com equipamentos de outras redes ou com máquinas de maior porte, sem perder autonomia.

Em termos simples, uma LAN pode ser classificada como rede de dados de alta velocidade, com baixa taxa de erros de transmissão, cobrindo uma área geográfica relativamente pequena e formada por servidores, estações de trabalho, sistema operacional de rede e link de comunicações. O planejamento desse sistema, ou arquitetura, inclui hardware (placas, conectores, micros e periféricos), software (sistema operacional, utilitários e aplicativos), meio de transmissão, método de acesso, protocolos de comunicação, instruções e informações.

A transferência de mensagens é gerenciada por um protocolo de transporte como IPX/SPX, NetBEUI e TCP/IP. Uma LAN pode ter duas ou várias centenas de estações, cada qual separada por metros de distância, possibilitando aos seus usuários o compartilhamento de recursos como espaço em disco, impressoras, unidades de CD-ROM etc., que é feito pelos NOS (Network Operation System - software de rede) e por placas de rede.

GERENCIAMENTO DE TI

Já a WAN permite a ligação entre computadores que estão distantes uns dos outros. Essa necessidade de transmissão remota de dados entre computadores surgiu com os mainframes, e as primeiras soluções eram baseadas em ligações ponto a ponto, feitas através de linhas privadas ou discadas. Com a proliferação do uso de PCs e das LANs, aumentou a demanda por transmissão de dados em longa distância, o que levou à criação de serviços de transmissão de dados – e também em redes de pacotes – nos quais, a partir de um único meio físico, pode-se estabelecer a comunicação com vários outros pontos.

Um exemplo de serviços sobre redes de pacotes são aqueles oferecidos pelas empresas de telecomunicações e baseados em tecnologia Frame Relay. Existem várias arquiteturas de rede WAN, entre as quais as baseadas no protocolo TCP/IP (Transmission Control Protocol), que é o padrão para redes Unix, Novell, Windows NT e OS/2 e também a utilizada na Internet.

Com o desenvolvimento da tecnologia sem fio, surgiram as WLAN (wireless local area network) que fornecem conectividade para distâncias curtas, geralmente limitadas a até 150 metros. Nelas, os adaptadores de redes dos computadores e os dispositivos de rede (hubs, bridges) se comunicam através de ondas eletromagnéticas. Seu emprego é ideal em ambientes com alta mobilidade dos usuários e em locais onde não é possível o cabeamento tradicional.

Reunindo os mesmos conceitos das redes WAN (Wide Area Network), empregadas para permitir a conexão de sistemas que se encontram em longa distância, as WWANs diferem destas por utilizarem antenas, transmissores e receptores de rádio, em vez de fibras ópticas e modem de alta velocidade, entre outras formas de conexão. Em termos de tecnologias de transmissão, as WWANs podem empregar as mesmas usadas pelas LANs sem fio. Mas também pode ser utilizada a tecnologia de telefonia móvel celular.

A influência da Internet

O surgimento da Internet, entendida como o conjunto de redes de computadores interligadas no mundo inteiro, tendo em comum um conjunto de protocolos e serviços, foi um fator que, sem dúvida, trouxe muito impacto às empresas e potencializou o uso dos recursos internos. A Internet propiciou a criação de outros tipos de redes, como as de uso exclusivo interno (intranets) e as destinadas ao relacionamento da empresa com seus parceiros de negócios (extranets), configurando-se como o meio eficiente para agilizar e facilitar o intercâmbio de informações e de documentos (via WebEDI). Além disso, ampliou as vulnerabilidades: riscos (vírus, acessos não-autorizados, invasões ao sistema, pirataria, etc.) e proporcionou o excesso do tráfego de dados (por e-mails e mensagens instantâneas), levando ao questionamento da dimensão da capacidades das máquinas e, conseqüentemente, tornando o gerenciamento mais complexo.

A Internet também tem se mostrado a infra-estrutura ideal para conectar redes privadas como as VPNs (Virtual Private Network), de acesso restrito. Em vez de usar links dedicados ou redes de pacotes, como Frame Relay, as VPNs usam a infra-estrutura da Internet para conectar redes remotas. A principal vantagem é o baixo custo, bem inferior se comparado ao dos links dedicados, especialmente quando as distâncias são grandes.

Gerenciamento

Independentemente do tipo e tamanho da rede, dos seus componentes, arquiteturas e protocolos utilizados, se conectadas fisicamente via cabo, ou remotamente via satélite, ondas de rádio, ou infravermelho, o que permanece imutável e comum a todas elas é a necessidade de controlar cada elemento, de tal forma que seja possível maximizar a sua eficiência e produtividade, e assegurar o seu funcionamento. O gerenciamento de todo esse aparato, seja uma simples rede composta por poucos computadores, seja a mais complexa das composições, compreende um conjunto de funções integradas, provendo mecanismos de monitoração, análise e controle dos dispositivos e recursos.

GERENCIAMENTO DE TI

Os principais objetivos de se gerenciar esses ambientes são, basicamente, reduzir custos operacionais, minimizar os congestionamentos da rede, detectar e corrigir falhas no menor tempo possível de forma a diminuir o downtime (indisponibilidade) dos sistemas, aumentar a flexibilidade de operação e integração, imprimir maior eficiência e facilitar o uso para a organização como um todo. A realização dessas tarefas requer metodologias apropriadas, ferramentas que as automatizem e pessoal qualificado. Atualmente existem no mercado diversos tipos de ferramentas que auxiliam o administrador nas atividades de gerenciamento. Estas ferramentas são divididas em quatro categorias principais:

- Ferramentas de nível físico, que detectam problemas em termos de cabos e conexões de hardware.
- Monitores de rede, que se conectam às redes supervisionando o tráfego.
- Analisadores de rede, que auxiliam no rastreamento e correção de problemas encontrados nas redes.
- Sistemas de gerenciamento de redes, os quais permitem a monitorização e controle de uma rede inteira a partir de um ponto central.

Dentre a gama de soluções possíveis para o gerenciamento de redes, uma das mais usuais consiste em utilizar um computador que interage com os diversos componentes da rede para deles extrair as informações necessárias ao seu gerenciamento.

Evidentemente é preciso montar um banco de dados neste computador, que será o gerente da rede, contendo informações necessárias para apoiar o diagnóstico e a busca de soluções para problemas. Isto envolve esforço para identificar, rastrear e resolver situações de falhas. Como o tempo de espera do usuário pelo restabelecimento do serviço deve ser o menor possível, tudo isto deve ser feito eficientemente.

Os sistemas de gerenciamento de redes apresentam a vantagem de ter um conjunto de ferramentas para análise e depuração. Eles podem apresentar também uma série de mecanismos que facilitam a identificação, notificação e registro de problemas, por exemplo:

- Alarmes que indicam, por meio de mensagens ou bips de alerta, anormalidades na rede.
- Geração automática de relatórios contendo as informações coletadas.
- Facilidades para integrar novas funções ao próprio sistema de gerenciamento.
- Geração de gráficos estatísticos em tempo real.
- Apresentação gráfica da topologia das redes.

Outro ponto que merece a atenção do gestor da TI são os serviços de telecomunicações, que figuram como os gastos mais difíceis de serem administrados. Hoje o desafio é ainda maior, pois é necessário reduzir custos sem, no entanto, comprometer a solidez da infra-estrutura da rede da corporação.

Existem ferramentas de gerenciamento de serviços de comunicação que facilitam uma série de tarefas, como a realização de inventário central, que inclui os aspectos técnicos e de bilhetagem de cada circuito; gerenciamento de dados e ferramentas para produção de relatórios e controle de contas, contratos e gerenciamento de circuito; integração de outras plataformas de TI, como sistemas help desk, plataformas para gerenciamento de desktop e rede, planejamento de recursos empresariais e contabilidade; e links para operadoras e outros provedores de serviços via XML ou extranet. O gerenciamento de telecomunicações corporativas permite uma administração contínua das operações da empresa. Mas é necessário determinar qual nível resultará no melhor retorno sobre o investimento.

O gerenciamento de rede na prática

Devido à grande complexidade dos ambientes de TI e das pressões não só para reduzir custos, mas também para justificar a real necessidade de investimentos, hoje é praticamente impossível ao diretor da área fazer um gerenciamento eficaz sem o auxílio de metodologias e ferramentas que permitam automatizar o processo. As empresas, e principalmente as altamente dependentes da tecnologia, estão cada vez mais conscientes dessa necessidade.

Seguindo essa lógica, o banco Santander Banespa optou por adotar as ferramentas Tivoli e contratou a IBM Global Services (IGS) para implementação da solução. A meta era gerenciar e monitorar 12 áreas de atuação (SPB Banespa e Santander, Netbanking, Site Institucional, Homebanking, Conexão Agências, ALTAIR, Cartão de Crédito, Transferência de Arquivos, Intranet, Segurança Perimetral e Empresas Externas), além dos serviços de disponibilidade de redes. Com a adoção da solução, foi possível identificar problemas na origem, agilizar suas soluções e, conseqüentemente, ampliar o grau de satisfação dos usuários.

A solução Tivoli foi implementada por um parceiro IBM como projeto-piloto de solução de gerenciamento de sistemas, abrangendo a monitoração de alguns elementos de TI e a verificação da disponibilidade das agências. O objetivo foi a centralização dos diversos tipos de eventos em uma console única e num único ponto focal.

Após a compra do Banespa pelo Santander, por um acordo da ELA (Enterprise License Agreement) com a IBM, ampliou-se a quantidade de licenças de disciplinas Tivoli. A partir daí, em janeiro de 2002, iniciou-se um projeto de expansão e reformulação do sistema de gerenciamento. Foram 18 meses de trabalho com o envolvimento de uma equipe formada pelo Santander Banespa e IBM Global Services, que reuniu 21 pessoas entre gerentes de projeto, coordenador, arquitetos, especialistas, administradores, consultores do Brasil e dos EUA.

A solução otimizou a carga de trabalho, mediante o uso de automações e da conseqüente redução dos procedimentos manuais, além de propiciar a padronização das interfaces e da monitoração. Segundo a equipe responsável pela administração da solução, a implementação dos produtos Tivoli possibilitou a determinação dos problemas na sua origem, proporcionou maior rapidez para resolução dos mesmos e melhorou a qualidade do atendimento. O acompanhamento dos serviços prestados pelas concessionárias de telecomunicações é feito em tempo real.

Módulo 6 - Ferramentas de gerenciamento

Monitoramento e controle

Foi-se o tempo em que era possível gerenciar o ambiente de TI de forma empírica e manual. Com a adoção em massa do modelo de computação distribuída, pelas empresas, e a crescente dependência da tecnologia para atingir metas de negócios, é cada vez maior a necessidade de dispor de ferramentas que permitam monitorar e controlar os sistemas em todos os níveis e camadas. Não é de se estranhar, portanto, a tendência de crescimento do mercado de software de gerenciamento que, segundo dados da International Data Corporation (IDC), deverá movimentar algo próximo a US\$ 11,5 bilhões em 2006.

De todos os fatores que contribuíram para essa realidade, a Internet, sem dúvida, teve um grande peso, na medida em que criou uma rede que possibilita um nível de interação nunca antes imaginado entre a empresa, clientes, fornecedores e demais parceiros de negócio. Gerenciar a infra-estrutura que suporta as transações no mundo virtual tornou-se essencial.

Monitorar e azeitar a rede é importante, assim como seus principais atores (desktops e servidores) individualmente, e ainda analisar a disponibilidade de aplicações e base de dados, planejar a capacidade dos sistemas, administrar o uso de software, falhas, conteúdo e pessoas, sem descuidar da segurança. Existem ferramentas de gerenciamento para cada uma dessas áreas, que se adaptam às mais complexas e diferentes plataformas, sejam as baseadas em Unix e Linux, sejam as baseadas em Windows e ambiente Intel.

Uma das formas de prever a viabilidade de utilização das ferramentas de gerenciamento é desenhar workflows para cada processo presente na empresa. Podem ser adotadas soluções que atendam, inicialmente, às áreas mais críticas e, em seguida, expandir o uso. Não existe, no entanto, nenhuma fórmula a ser seguida. Podem ocorrer, também, problemas de integração posterior das diferentes soluções, embora isso costume ser contornado pelos fornecedores que conseguem customizar o software para cada cliente e situação específica.

Evolução das ferramentas

Nos últimos 30 anos, o segmento de ferramentas de gerenciamento diversificou-se e está muito pulverizado hoje. No início do processo de amadurecimento dessa tecnologia, a era do framework dominou o mercado. O chassi, como ficou conhecido o dispositivo, servia como base das aplicações, mas dificultava a integração entre diferentes marcas de produtos. Atualmente, no entanto, a maioria das ferramentas disponíveis é mais amigável, aberta e modular, permitindo o desenho de um projeto de longo prazo e a mescla de produtos de diferentes fornecedores e até mesmo de soluções caseiras, desenvolvidas pela própria empresa.

É recomendável que as corporações analisem seus processos internos para determinar o que é crítico ou não para o core business antes de partir para a escolha da ferramenta. Deve-se ainda testar a infra-estrutura para verificar se as condições são favoráveis para receber o novo aplicativo. Caso a rede não esteja preparada, o software de gerenciamento poderá gerar mais problemas do que resultados. Um teste-piloto é fundamental, uma vez que é nesse momento que se define o monitoramento necessário. Outro cuidado vital é treinar as pessoas para que elas saibam exatamente o que estão fazendo. Se a equipe não estiver preparada e o projeto for mal dimensionado, o resultado pode demorar a aparecer ou mesmo frustrar expectativas.

Gerenciamento de redes

Os programas de gerenciamento de rede reúnem várias ferramentas de monitoração e controle – no sentido de fornecer uma única interface de operação – e são executados em servidores, hubs e placas de rede. Sua função é coletar estatísticas do movimento dos dados e vigiar as condições que excedem o limite dos programas.

GERENCIAMENTO DE TI

Ao detectarem algum problema, alertam o programa de gerenciamento central, o qual pode desencadear algumas ações de reinicialização ou roteamento e pedir ajuda humana mediante alarmes ou avisos.

Em geral, os fabricantes de equipamentos para redes adotam conjuntos de padrões que permitem a operação de programas gerenciadores. O mais conhecido e utilizado é o Gerenciador de Protocolos de Rede Simples (SNMP – Simple Network Management Protocol), que se aplica a todos os sistemas. Esse protocolo foi projetado em meados dos anos 80 como resposta aos problemas de comunicação entre os diversos tipos de rede. A idéia básica era oferecer um modo de fácil implementação, com baixo overhead para o gerenciamento de roteadores, servidores, workstations e outros recursos de redes heterogêneas. O SNMP é um protocolo de nível de aplicação da arquitetura TCP/IP, operando tipicamente sobre o UDP (User Datagram Protocol).

Sob o SNMP, pequenos programas de gerenciamento, conhecidos como agentes, são executados num processador especial contido numa variedade de dispositivos ligados em rede. Esses programas monitoram os dispositivos e coletam os dados estatísticos no formato conhecido como Management Information Base (MIB – base de informações de gerenciamento). Um programa central, denominado Management Console Program (programa console de gerenciamento), ordena os agentes em uma base regular e descarrega o conteúdo dos seus MIBs.

O local ideal para um agente de gerenciamento é o hub, dispositivo no centro do sistema de cabos. Dessa forma, o agente pode monitorar o nível de atividade e o tipo de dado que vai e volta para cada estação cliente e para cada servidor. Em geral, os servidores têm seus próprios agentes, que reportam detalhes das condições do equipamento e das ações das máquinas cliente. Os agentes de gerenciamento também estão disponíveis para certos modelos de placas de rede e para produtos especializados.

Para redes corporativas constituídas de diversas LANs (redes locais) conectadas por WAN (rede de longa distância), é utilizado o protocolo RMON (Remote Monitoring) – uma capacidade de gerenciamento remoto do SNMP. Isso porque os enlaces de rede de longa distância, por operarem a taxas de transmissão inferiores às das LANs que as interconectam, passam a ter grande parte da sua banda de transmissão ocupada por informações de gerenciamento. O protocolo RMON oferece suporte para a implementação de um sistema de gerenciamento distribuído. Cada elemento RMON tem como tarefa coletar, analisar, tratar e filtrar informações de gerenciamento de rede e apenas notificar à estação gerente os eventos significativos e situações de erro.

Modelos de gerenciamento

Existem alguns modelos para gerência de redes. Um deles é o modelo Internet, que adota uma abordagem gerente/agente. Os agentes mantêm informações sobre recursos, e os gerentes requisitam essas informações aos agentes. Outro modelo é o OSI, da ISO, que se baseia na teoria de orientação a objeto. Esse modelo gera agentes mais complexos de serem desenvolvidos, consumindo mais recursos dos elementos de rede e liberando o gerente para tarefas mais inteligentes. Há também sistemas de gerenciamento baseados em Java, que consistem em browser gerenciador no Network Management System (NMS) e uma máquina Java no agente.

Independentemente do modelo escolhido, dos protocolos e das ferramentas empregadas, o gerenciamento permite monitorar a disponibilidade e performance de cada elemento da rede, medir o nível de utilização do parque de software, consumo de banda, e uma série de fatores que asseguram a continuidade das operações e o melhor uso da infra-estrutura de TI.

GERENCIAMENTO DE TI

Também podem ser utilizadas ferramentas que irão gerenciar elementos específicos e pontuais como servidores, desktops, storage, e-mails, entre outros. Em geral, as soluções de gerenciamento de servidores permitem avaliar a performance das máquinas, planejar sua capacidade de processamento, fazer inventário de hardware e software e monitorar os bancos de dados e demais aplicativos (como ERP, CRM, BI, etc).

No caso dos desktops, um dos principais benefícios propiciados pelos sistemas de gerenciamento é fornecer ao diretor da área de TI maior controle sobre o parque de máquinas e, especialmente, sobre as licenças de software. Como em geral, nas grandes empresas, a decisão sobre o uso de software é do usuário final, é grande o risco de utilização de programas piratas, licenças não-autorizadas ou mesmo aplicativos não-autorizados pela empresa. Isso tudo, além gerar complicações legais, contribui para aumentar o custo causado pelo excesso de programas sendo executados em uma rede. O grande desafio das ferramentas de gestão não está exatamente no controle, mas no auxílio ao usuário, para que ele entenda o que pode ou não ser usado.

Gerenciamento de dados e e-mail

Com o maior uso da Internet, intranets e extranets, se faz necessário também outro tipo de gerenciamento: o de storage. Especialmente na empresas de maior porte ou nas que contam com grande parque tecnológico, o crescimento do volume de dados requer a tomada de medidas apropriadas para seu correto armazenamento. Alguns analistas avaliam que no mercado brasileiro ainda falta maturidade nessa área. Isso porque, mesmo com a vasta oferta de ferramentas de gerenciamento de storage, os executivos de TI acabam optando pela compra de discos de armazenamento que, na prática, não atendem aos interesses e dificultam o controle.

Mas, esse panorama já está mudando, devido à necessidade de se colocar dados on-line e armazenar dados com critério. O bom uso das ferramentas pode permitir, por exemplo, que a quantidade de dados que cada profissional de tecnologia gerencia salte de 1,5 TB para 15 TB. Isso significa que a redução de custo não ocorre apenas nos equipamentos de storage, mas no Departamento de Recursos Humanos.

Outra questão que preocupa as empresas, em geral, refere-se ao gerenciamento de e-mails e de acessos à Web. Transformada em ferramenta de trabalho indispensável, a Internet, se de um lado traz uma série de benefícios e facilidades, de outro requer iniciativas para normatizar seu uso. Há falhas na utilização tanto de e-mails quanto de sites, o que implica redução de produtividade, destruição de informações e maior exposição a vírus e ataques indesejados.

Mas existem normas que, associadas a ferramentas de controle, são simples de implementar e solucionam os problemas. A Glaxo SmithKline (GSK), por exemplo, criou um comitê de segurança da informação, composto por representantes de várias áreas da companhia. Esse grupo definiu a política de uso da Web. Na prática, o documento estabeleceu critérios para uso de e-mails e os tipos de sites que podem ser acessados e os que estão proibidos: pornográficos, racistas e de cunho informativo duvidoso. A ferramenta escolhida para efetuar esse controle foi um software da Aker, instalado antes do firewall. O aplicativo bloqueia qualquer tentativa de acesso a conteúdo não-autorizado. Quanto aos e-mails, foi proibida a realização de downloads de aplicativos, por firewalls e customizações internas. Com essas medidas, o consumo de banda caiu 20%.

Web Services

O mercado dispõe de um amplo leque de opções para todos os tipos de gerenciamento e voltadas a atender às necessidades de empresas de diferentes portes e ramos de atividade. Segundo o Gartner Inc., nos próximos anos os fornecedores de software de gerenciamento deverão basear suas aplicações em Web Services, em vez de adotar arquiteturas proprietárias, ou reestruturar os sistemas com foco nos modelos primários de comunicação entre os módulos pelo uso de protocolos abertos.

GERENCIAMENTO DE TI

Conceituados como componentes de software utilizados para integração entre aplicações corporativas, assim como para realizar a conexão entre empresas, clientes e parceiros, os Web Services estão cada vez mais recebendo atenção de fornecedores de soluções que os vêem como uma tecnologia voltada para a interoperabilidade. Alguns já começam a adotá-la, como é o caso da Automatos, empresa especializada em soluções de gerenciamento remoto de TI. Na concepção da empresa, as ferramentas de gerenciamento existentes são eficazes, mas o problema é que, na realidade, constituem mais um software para rodar na rede das corporações. Na tentativa de se gerenciar o legado, na prática, acaba-se por aumentá-lo.

Com essa visão, a Automatos apostou na tecnologia Web Services e a tomou como base para desenvolver suas soluções. Dessa forma, o cliente acessa a solução de gerenciamento requerida pela Internet – ou por uma rede privada – e adquire as funcionalidades de que necessita, sem precisar instalar o software na máquina e pagando apenas pelo que utilizar. O custo pode ficar cerca de 10 vezes mais baixo em comparação à compra do software, além de ser 5 vezes mais rápido e 3 vezes mais fácil de usar.

Sob esse formato, a Automatos disponibiliza soluções para gerenciamento de desktops, servidores e de rede. O DeskPS (Desktop Performance Solution), por exemplo, é uma solução voltada para determinar as reais necessidades de atualização dos parques de desktops e notebooks. Entre as funcionalidades há: análise de performance (o quanto cada computador está consumindo em termos de CPU, memória, disco e rede), análise de dimensionamento, planejamento de capacidade, elaboração de relatórios para planejamento de evolução do parque instalado, análise do tempo de resposta, controle de licenças, distribuição de arquivos e software, entre outras.

No caso de servidores, o Banco Opportunity conseguiu obter uma economia efetiva ao contratar serviços para gestão de inventários de hardware e software, e análise de desempenho e disponibilidade dos servidores. O contrato de 3 anos fechado com a Autômatos demandou investimento anual de R\$ 60 mil. Mesmo com crescimento de 300% da infra-estrutura, nos últimos 7 anos, que resultou em 180 estações e 50 servidores e volume de dados 10 vezes superior, chegando a 200 gigabites, o Opportunity conseguiu manter uma equipe de TI reduzida. Quando se descobriu ser possível usar a Internet para agregar valor ao processo de gerência de servidores, o software instalado para monitorar a atividade das máquinas possibilitou ao banco planejar novos investimentos em TI, evitando problemas de desempenho.

A maior vantagem disso foi dispensar a compra de servidores para o controle das máquinas o que reduziu as variáveis a serem controladas. Mesmo sendo sensível a questões de segurança, o banco aceitou bem a solução, porque foram usados mecanismos de criptografia para a transmitir os dados que trafegam na rede de forma tão segura quanto a do sistema usado pelo home banking.

Principais Players

Atualmente há muitos fornecedores disputando uma fatia desse mercado, que tende a ficar cada vez mais promissor. Entre as líderes destacam-se: Computer Associates, HP, IBM Tivoli, BMC Software, Compuware e Peregrine. Veremos a seguir, um resumo das principais famílias de ferramentas.

Computer Associates

O carro-chefe é o Unicenter, base de gerenciamento da empresa, que realiza 43% de seus negócios, a partir dessa tecnologia. Sob o guarda-chuva do Unicenter, abrigam-se 6 modalidades principais: network and systems, automated operations, IT resources, database, Web infrastructure e applications, todas baseadas em arquitetura de inteligência distribuída. A CA também dispõe de soluções para gerenciamento sem fio: o Wireless Network Management (WNM) e o Mobile Device Management (MDM). As soluções são modulares e podem ser implementadas aos poucos. A empresa já lançou seus primeiros produtos voltados para o gerenciamento de Web Services, dando um grande passo num mercado dominado por pequenas companhias e startups.

GERENCIAMENTO DE TI

O Unicenter Web Services Distributed Management monitora a performance dos aplicativos, notificando os administradores de sistema. O produto controla a construção das interfaces de software de acordo com os padrões Web Services.

HP

Depois da fusão da HP com a Compaq, a plataforma de gerenciamento OpenView ganhou um reforço: o Temp, voltado para centrais telefônicas e infra-estrutura de telecomunicações. O OpenView se baseia em camadas: análise de falhas, de performance e gerenciamento do serviço. As ferramentas podem gerenciar as aplicações, apontando, em seguida, onde estão as falhas. Os usuários podem optar por saber primeiro onde está o problema ou qual processo foi afetado.

IBM Tivoli

A empresa oferece soluções que suportam as linhas de negócios e não apenas a infra-estrutura. É um amplo portfólio de produtos que, juntos, possibilitam aos clientes selecionar, integrar e implementar software de gerenciamento em ambientes complexos. Os módulos principais são: gerenciamento da performance e disponibilidade, configuração e operações, segurança, armazenamento e serviços. Entre os produtos, destacam-se o Service Level Advisor, baseado em algoritmos complexos; o Enterprise Data Warehouse, desenvolvido sobre a tecnologia DB2 para arquivamento de dados de gerenciamento de sistemas; e o Switcher Analyzer, para monitoramento de redes.

BMC Software

As áreas cobertas pelas soluções disponibilizadas pela empresa são dados, aplicações, armazenamento e segurança. Denominadas Patrol (para ambiente distribuído) e MainView (para mainframe), os módulos que as compõem podem ser implementados de forma gradativa, de acordo com a necessidade dos clientes. O Patrol controla níveis de serviço, otimiza a performance e prevê a ocorrência de problemas antes que afetem os processos de negócios. O módulo Application Centric Network Management provê o gerenciamento de redes por meio da perspectiva da aplicação. Entre suas funcionalidades, incluem-se a análise de desempenho da rede e dos seus dispositivos, o planejamento da capacidade e a visualização gráfica da topologia e do tráfego. Outra família de produtos é a Incontrol, que gerencia e integra soluções corporativas pela simplificação do gerenciamento da produção, automação e segurança a partir de um único ponto central.

Compuware

A solução Vantage administra toda a infra-estrutura e aplicações. Podem ser gerenciados: servidor, rede, estações de trabalho, aplicações, intranets e o balanceamento de carga. A ferramenta também utiliza arquitetura em 3 camadas, que permitem aos servidores gerenciados e aos componentes de controle operarem de forma independente, recuperando-se de falhas na rede ou nos sistemas.

Peregrine

Fornecedora de software para gerenciamento consolidado de ativos, serviços e gestão de TI. Suas soluções têm foco nas metodologias de medição de TCO do Instituto de Pesquisa Gartner e implementação de processos ITIL, que auxiliam as empresas a reduzir custos e melhorar a produtividade, acelerando o retorno de investimento e assegurando acordos de níveis de serviço. No Brasil, os clientes utilizam as soluções Peregrine para realizar a gestão de serviços e ativos, sejam ou não de tecnologia, dentro dos padrões das melhores práticas definidas pelo ITIL (Information Technology Infrastructure Library).

Veja mais detalhes sobre essas famílias e outros produtos para gerenciamento nos sites:

www.ca.com – www.ibm.com.br – www.compuware.com.br
www.bmc.com – www.peregrine.com – www.automatos.com.br

Módulo 7 - Segurança

Continuidade dos negócios

Não resta dúvida de que o calcanhar de Aquiles do setor corporativo é a segurança. Quanto mais dependente da Tecnologia da Informação uma empresa é, mais vulnerável ela se torna. Spams, vírus, worms, invasões por hackers, acessos a sites impróprios, pirataria e acessos remotos não-autorizados são apenas alguns dos problemas que precisam ser equacionados pelos administradores de TI.

Mas a questão da segurança não se resume a isso apenas. Depois do atentado ao World Trade Center, em 11 de setembro de 2001, nos EUA, o mundo corporativo acordou para a importância de estabelecer um plano de emergência para assegurar a continuidade das operações, no caso de acidentes e incidentes que comprometam suas instalações físicas. É necessário, além disso, assegurar a disponibilidade dos sistemas, contar com um sistema de backup eficiente, manter a documentação dos sistemas atualizada, treinar pessoas e mais outras tantas providências.

O uso da tecnologia Web fez com que o enfoque dado à segurança mudasse. Até há pouco tempo, a grande preocupação dos gestores de Tecnologia era perder informações, em função das invasões e de ataques de vírus. Os investimentos concentravam-se na aquisição de soluções que limpassem e protegessem as máquinas, como antivírus e firewalls.

Hoje a preocupação ampliou-se. As ações quanto à segurança devem estar associadas à continuidade dos negócios, não se restringindo aos aspectos puramente tecnológicos, mas também a outras áreas como o treinamento de pessoas para o uso correto de informações, controle de acesso aos sistemas e aspectos relacionados à segurança do ambiente físico. O grande desafio do gestor é saber quantificar o impacto que uma falha na segurança, em qualquer nível, pode trazer à empresa e a seus parceiros de negócios, uma vez que qualquer paralisação pode interromper uma cadeia produtiva em nível mundial, resultando em exorbitantes prejuízos financeiros.

O gerenciamento da segurança

Antes de tudo, é importante que o gestor da TI tenha consciência de que o conceito de segurança é muito amplo e começa antes do emprego puro e simples de ferramentas. A tendência natural é querer colocar cadeados em tudo, até onde não é necessário. Com isso, podem ocorrer distorções como elevar excessivamente os investimentos, implementar soluções em áreas que não precisam tanto de proteção e deixar vulneráveis algumas áreas importantes.

Uma empresa, por exemplo, que disponibiliza para o público em geral uma página na Internet voltada para receber currículos, se tiver algum problema de violação por hackers, não sofrerá grandes perdas. Óbvio que terá prejuízos, principalmente quanto à sua imagem e perda de informações, mas nada que seja comprometedora. Nesse caso, não se aplicam soluções altamente sofisticadas como as de biometria, por exemplo, que também são muito caras, porque essas informações não são essenciais para a empresa, e o investimento não se justificaria.

Por isso, é fundamental que o primeiro passo seja identificar quais são as fragilidades da empresa e pontuar as áreas que requerem maior nível de proteção, tendo certeza do risco (risk assessment) para que não haja investimentos maiores que o necessário. Esse planejamento tem que ser feito sob a óptica do negócio e não da Tecnologia. O segundo passo refere-se à verificação dos processos da empresa e ao estabelecimento de políticas de segurança. Depois dessas definições, parte-se para a escolha e emprego de ferramentas e soluções para prevenir e evitar violações aos sistemas.

GERENCIAMENTO DE TI

Finalmente, deve ser feito um trabalho interno de conscientização. Todos os funcionários devem ser treinados e orientados sobre as medidas de segurança adotadas. De nada adianta dispor de vários mecanismos sofisticados de senhas, reconhecimento de usuários, etc., se depois de todos os cuidados um profissional se descuidar e deixar sobre a sua mesa um relatório confidencial que pode acabar sendo visto por pessoas não-autorizadas.

A adoção das especificações ISO 177-99 pode ajudar os gerentes de TI na difícil tarefa de administrar a segurança. Essas especificações têm as 10 áreas de controle:

1. Política de segurança
2. Segurança organizacional
3. Controle e classificação de ativos
4. Segurança das pessoas
5. Segurança do ambiente
6. Gerenciamento e controle das operações de comunicação
7. Controle de acesso aos sistemas
8. Desenvolvimento de sistemas e manutenção
9. Gerenciamento de continuidade dos negócios
10. Especificações de segurança

Apenas 40% dessas especificações são relativas à Tecnologia da Informação. As 60% restantes referem-se a pessoas, processos e treinamento. Se uma empresa estiver atenta a tudo isso, terá 80% das suas necessidades de segurança atendidas.

Quanto aos aspectos tecnológicos, há 3 áreas que merecem atenção do gerente. A primeira é a área de defesa da corporação. Algumas empresas instalam antivírus e firewall e acham que, com isso, estão protegidas, esquecendo que existem outras formas de invasão que não são bloqueadas com essas ferramentas, como o spam. É preciso administrar as vulnerabilidades decorrentes do próprio crescimento do ambiente computacional. A segunda área é a de gerenciamento da identidade. É necessário implementar soluções que permitam identificar e reconhecer o usuário, para que se tenha certeza de quem está acessando as informações e aplicativos é, de fato, o funcionário autorizado para isso.

O gestor também precisa levar em consideração que o perfil das pessoas muda com o decorrer do tempo. Um Diretor de Marketing que tinha acesso a informações e sistemas específicos pode vir a assumir outra função dentro da empresa. Por exemplo, passar a Diretor Financeiro. Em geral, ele acaba sendo autorizado a acessar outras informações e sistemas, acumulando os anteriores, quando o correto seria a desabilitação de alguns acessos que ele já não necessita. Deve-se ainda ter o cuidado de bloquear os acessos aos sistemas, quando o funcionário deixar a empresa.

E, finalmente, a terceira área refere-se ao controle de acesso aos sistemas corporativos, tanto quanto a funcionários internos (definir quem pode acessar o quê), quanto a parceiros (clientes, fornecedores, etc.). É importante que o gestor tenha uma visão de fora para dentro para determinar quais parceiros terão acesso a quais informações e sistemas da empresa, para que possa traçar as normas de permissão e de restrição aos acessos. Depois, cabe ao gestor da TI aplicar os conceitos dessas 3 áreas nas arquiteturas de desktops, servidores e redes da corporação.

Brechas

Uma das principais portas de entrada para incidentes de segurança no setor corporativo é a Internet. Isto porque a maioria das empresas permite a seus funcionários acesso total e também a terceiros, por extranets e e-business, o acesso por links dedicados ou pela Web. Apesar do uso de conexões criptografadas e outros cuidados, na prática, as portas podem não estar trancadas devidamente, facilitando o ataque de hackers e de acessos indevidos aos sistemas.

Em pesquisa realizada com empresas de diversos setores de atividade, ficou comprovado que mais de 78% delas registraram perdas financeiras em virtude da invasão dos sistemas, mas 56% do total não souberam quantificar os prejuízos. Mesmo sabendo dos riscos e acreditando que os ataques devem aumentar, as empresas não costumam ter qualquer plano de ação para impedi-los. O maior empecilho não é tecnológico, mas cultural. A falta de consciência do público interno, sejam executivos ou funcionários em geral, é o que pode colocar tudo a perder. Para minimizar esse problema, as empresas devem se preocupar em adotar uma política de segurança que seja compreensível para todos e divulgá-la amplamente.

É importante que a empresa avalie, no mapa do rede, todos os pontos que devem ser cobertos por processos seguros. Isso pode ser feito começando pela avaliação da infra-estrutura de TI e utilização do diagrama da arquitetura da rede para determinar como e onde os usuários internos e externos podem acessar a planta. Em seguida, recomenda-se que os sistemas da corporação sejam testados contra invasões, com ferramentas específicas, e assim as vulnerabilidades na rede podem ser visualizadas. Dispor de uma lista com todos os servidores e sistemas críticos para a empresa constitui outra boa iniciativa, complementada pela relação dos funcionários que instalaram e/ou desenvolveram aplicações.

Também é fundamental criar uma lista para todos os administradores de rede, especificando quem são os responsáveis pelos sistemas, um a um. Para os funcionários, deve ser estabelecida uma política que explique como utilizar de forma adequada as informações corporativas. Por exemplo, podem ser enumeradas as medidas que devem ser tomadas quando houver suspeita de invasão ou infecção na rede ou no desktop. Esses profissionais também devem ser instruídos sobre como lidar com suas senhas de acesso aos sistemas e se podem, ou não, deixar suas estações ligadas ao saírem, para evitar a exposição das informações internas a pessoas não- autorizadas.

Uma das principais brechas para incidentes de segurança é o sistema de e-mail. Apesar de na maioria dos casos as empresas contarem com ferramentas para monitoramento de e-mails, antivírus e firewall, todo dia surgem novas pragas virtuais que são transmitidas por e-mail e podem infestar os sistemas e causar graves transtornos. No Banespa, por exemplo, uma das formas de contornar o problema foi limitar o tamanho dos arquivos que são anexados nas mensagens que chegam aos usuários por e-mail. Esses arquivos não podem ter mais que 500 Kb e, em determinado nível, mais do que 3 Mb. Também foram adotadas medidas que excluem arquivos com extensões como.exe, .tif, .pdf, e .scr diretamente no servidor, assim como adoção de firewall e antivírus.

Na Brasmetal Waelzholz, empresa fornecedora de fitas de aço relaminadas a frio, que conta com um parque de 120 estações de trabalho e concluiu o seu sistema de segurança de rede há pouco mais de 3 anos, até meados da década de 90, o acesso à Internet era permitido a apenas 10 pessoas e, dessas, só 5 usavam e-mail. Na época, a companhia tinha absoluto controle de todas as informações que circulavam na rede. Em 1998, a empresa trocou o seu link de linha discada (a mesma usada em residências) por um de banda larga. A troca possibilitou que mais pessoas tivessem acesso a e-mail e à Internet. Com isso, houve um crescimento significativo no volume de acessos, e a empresa perdeu o controle do que trafegava pela rede.

Inicialmente, o maior receio era de uma invasão por vírus. Como o backup (cópia) de dados sempre foi um hábito da empresa, o principal problema seria a perda de horas de trabalho até que a infecção fosse resolvida.

GERENCIAMENTO DE TI

A Brasmetal optou por criar uma regra única para acessar a Internet e o e-mail e contratou a Lintec, integradora de soluções. Juntas, desenvolveram um projeto abrangendo servidores, antivírus, firewalls, entre outras ferramentas de segurança como forma de prevenção. A Lintec também orientou a empresa a investir em um sistema de detecção de intrusos e, com isso, foi implementado o eTrust Intrusion Detection, da Computer Associates, que garantiu o cumprimento das normas internas de acessos.

Para divulgar a política de acesso a dados e de utilização de e-mail e Internet, a Brasmetal elaborou um regulamento com regras detalhadas, além de um novo site interno (na intranet) contemplando as principais orientações de segurança para o treinamento de funcionários. Apesar de todos os sistemas complexos de segurança que foram implementados, a empresa está ciente de que não há como se proteger 100% dos ataques. Há backdoors, por exemplo, que não são detectados pelos sistemas de segurança e são instalados nas estações dos usuários. Devido à ingenuidade, este tipo de ataque é conhecido como "engenharia social", e, se o usuário não estiver treinado para não "cair" nesta "lábria", de nada adiantará todo o investimento feito em segurança da informação, pois, uma vez o backdoor instalado descoberto, o hacker já terá feito a festa.

Segurança em redes sem fio

Com a evolução da tecnologia móvel e o aumento do seu uso pelas empresas, alguns cuidados também devem ser tomados com relação às redes wireless. Todas as ferramentas de proteção convencionais usadas em redes cabeadas se aplicam ao ambiente sem fio. Mas, além delas, as redes wireless exigem cuidados adicionais e específicos. O padrão de criptografia para redes locais sem fio, denominado WEP (Wired Equivalent Privacy), é bastante seguro, mas ainda apresenta algumas restrições, por isso é recomendável que as empresas não se limitem a ele. É fundamental também fazer uma configuração confiável da rede wireless, utilizando recursos de segurança inerentes aos pontos de acesso e instalação de firewall, sendo que, nos casos mais complexos, vale a pena adquirir equipamentos, software e serviços especializados.

Para garantir a segurança desse ambiente, são lançados constantemente novos padrões. A Aliança Wi-Fi já divulgou o padrão WPA (Wi-Fi Protected Access) para o acesso de PDAs, com melhorias na criptografia dos dados e na autenticação do usuário em relação ao WEP. O consórcio desenvolveu também uma nova ferramenta, batizada de Zone, destinada a encontrar pontos de acesso Wi-Fi entre os 12 mil hot spots (pontos de acesso públicos) instalados no mundo.

Em junho de 2004, o IEEE ratificou o padrão IEEE 802.11i, que traz, de forma intrínseca, as primitivas de segurança aos protocolos IEEE 802.11b, 802.11a e 802.11g de Wireless LAN (WLAN). (transcrito de <http://www.netsix.com.br/Netsix/Netsix2.nsf/0/e7f49b993709a90a83256f79004af9f0?OpenDocument>)

Em geral, as soluções compatíveis com o padrão 802.11 incluem mecanismos de segurança, mas é necessário que as empresas implementem projetos de proteção de dados. A maior fragilidade das redes wireless está no chipset do ponto de acesso. Por isso, é importante tornar confiável a comunicação entre ele e os demais dispositivos autorizados. O envio de um pacote UDP (User Datagram Protocol) para uma determinada porta, por exemplo, faz com que o sistema retorne informações como o nome da rede (SSID- Service Set Identifier), a chave de criptografia e até a senha do administrador do próprio access point. O cuidado inicial, portanto, é evitar que o SSID, que faz a identificação do nome da rede entre os usuários, seja conhecido por um possível intruso. Para isso, é necessário desabilitar o envio por broadcast dessa sequência.

Em seguida, deve-se tornar confiável a comunicação entre o access point e os demais dispositivos autorizados. Para isso, é importante que o servidor central saiba exatamente quais os números seriais das placas de rede de cada máquina autorizada a compartilhar o ambiente. Os chamados MAC Address de todas elas devem estar cadastrados. Esse trabalho, mesmo feito de forma manual, pode evitar que computadores se liguem à rede com facilidade, apenas se aproximando da região de cobertura.

GERENCIAMENTO DE TI

Mas somente esse cuidado não é suficiente para garantir segurança. Existem vários programas disponíveis na Internet que simulam o endereço de qualquer placa de rede, fazendo-se passar por um dispositivo autorizado na hora de uma conexão. Se alguém com más intenções obtiver o código de uma determinada estação autorizada a usar a rede, poderá entrar facilmente e usar indevidamente esse acesso.

Uma vez fechada essa primeira brecha, é hora de cuidar da inviolabilidade da informação que trafega entre as estações e o ponto central de rede. Como todos os sinais estão trafegando num ambiente público, a única maneira de salvaguardar os dados é codificá-los e embaralhá-los de uma forma ordenada, ou seja, criptografá-los. Para desembaraçar a informação do outro lado, é preciso abri-la com uma chave criptográfica. As informações estão, dessa forma, seguras – isto é, até o momento em que um estranho tenha acesso à chave criptográfica ou quebre seu código.

Para garantir a inviolabilidade dos dados, são recomendáveis outros recursos, como os de uma rede virtual privativa. O uso do protocolo IPSec permite a criação de um túnel seguro entre a estação e o Access Point. Exemplo disso é o VPN-1 Security Client, da Check Point. Para proteger conexões wireless com até 10 mil usuários simultâneos, existe também a plataforma Cisco VPN3000, com escalabilidade e facilidade de upgrade.

Caso se queira níveis mais elaborados de criptografia, os padrões AES (Advanced Encryption Standard) e o DES (Data Encryption Standard) são opções interessantes. As empresas com operações mais críticas podem até implementar aplicações que usem o 3DES. No entanto, é preciso um certo senso de medida para evitar gastos desnecessários.

Outro cuidado refere-se à encriptação dos dados e à monitoração em tempo real, por meio de ferramentas específicas, muitas delas distribuídas gratuitamente pela Internet.

A seguir, algumas recomendações para gestor da TI, visando tornar a rede corporativa mais segura:

- Não mencionar o nome da rede para qualquer pessoa.
- Desabilitar, no access point, a emissão automática de informações como o nome da rede, a chave criptográfica e a senha do administrador de rede.
- Fazer uma lista dos computadores confiáveis,
- A autenticação do computador à rede deve ser feita usando o MAC Address da placa de cada dispositivo. Essa ação impede que máquinas estranhas ao ambiente possam se conectar à rede.
- Não deixar o sinal vaziar.
- O posicionamento do access point e a potência da antena podem ter um alcance que ultrapasse as fronteiras geográficas da empresa. O vazamento do sinal é perigoso. É preciso implementar mecanismos de autenticação e criptografia.
- Agir rápido se o notebook for roubado ou perdido. Roubo e perda de equipamentos têm consequências sérias para a segurança da rede corporativa. Deve-se estabelecer com antecedência as medidas a serem tomadas nesses casos, desde o registro de um Boletim de Ocorrência na delegacia até o corte da permissão de acesso da referida máquina.
- Definir que tipo de informação trafega na rede. É importante que o usuário do canal sem fio saiba o que pode e o que não pode ser trafegado pela rede wireless. Por exemplo, detalhes de um projeto estratégico que pode mudar os rumos do mercado não devem ser mencionados em e-mails, principalmente se não forem criptografados.
- Criptografar para não dar o mapa ao bandido. Dados estratégicos, e-mails profissionais, modelos de vendas, lista de clientes preferenciais e planos de novos negócios podem cair em mãos inimigas. O estrago do vazamento desse tipo de informação pode ser fulminante.

- Autenticação de quem entra na rede. Além de garantir que determinado dispositivo é autorizado para entrar na rede, devem ser usados métodos de autenticação forte de usuário, por meio de tokens e senhas dinâmicas.
- Erguer “muralhas de fogo”. A ligação com a rede local cabeada deve estar sempre protegida por firewall, como qualquer porta aberta para o mundo exterior.
- Realizar monitoração freqüente de todas as atividades da rede sem fio para verificar falhas e flagrar intrusos. Esse procedimento traz uma série de benefícios, como permitir a descoberta de instalação de placas não autorizadas nos equipamentos pelos usuários, checagem de dispositivos que não estão usando criptografia, detecção de ataques contra clientes wireless que não sabem que estão sendo hackeados; e visualização de acessos não autorizados, o que permite tomar providências imediatas que impeçam o intruso de chegar aos dados estratégicos da empresa.

Segurança dos dados

O ativo mais precioso das empresas, sem dúvida, são as informações. Portanto, os cuidados com relação aos dados devem ser redobrados. Estudos da International Data Corporation (IDC) revelaram que o volume de informações dentro das empresas cresce 34% ao ano, chegando a 60% em algumas empresas, o que exige mais espaço em armazenamento e gerenciamento otimizado. O que se observa atualmente é uma grande preocupação, da parte dos fornecedores de soluções, em oferecer sistemas de gerenciamento capazes de trabalhar não apenas com equipamentos de diferentes marcas, como também com topologias distintas, como as redes SAN (Storage Area Network) – voltadas para um volume grande de dados estruturados, com elevada quantidade de acessos e número limitado de usuários – e NAS (Network Attached Storage) – que coloca os discos como dispositivos da rede e não como periféricos de um único servidor. Há ainda o CAS (Content Addressed Storage), destinado a guardar dados de baixa utilização e arquivamento por um longo período, como as informações fiscais.

O gerenciamento da rede de storage é realizado por meio de soluções de SRM (Storage Resource Management), que mostram o comportamento de cada dispositivo conectado na rede, quantidade e tipos de dados guardados, a origem das informações, quantidade de espaço livre e registro de problemas nos discos. É possível criar regras para cada tipo de arquivo e fazer a transferência automática para o disco adequado. Há ainda outras opções, como os conceitos Information Lifecycle Management (ILM), para classificar os dados conforme a periodicidade com que são acessados e a data do armazenamento, e o Hierarchical Storage Management (HSM), que estabelece um limite para cada usuário armazenar arquivo, variando conforme a atividade e o cargo de cada um. O HSM pode ser usado também dentro de aplicações, como e-mail e banco de dados.

O gerenciamento de storage costuma ser complexo porque, em geral, as empresas têm vários sistemas na rede que não se integram perfeitamente. Alguns fabricantes de soluções defendem o conceito de virtualização, segundo o qual é possível ter acesso aos dados independentemente do servidor e sistema operacional utilizado. Com isso, os usuários podem criar camadas de armazenamento entre sistemas de diferentes fornecedores, tendo uma visão unificada e consolidada da capacidade de storage. Em vez de acessar a informação diretamente da base, isso é feito pelo servidor de virtualização, eliminando cópias e o espaço livre em disco.

O gerenciamento de dados envolve a realização de backup, restore e business continuity. É importante que a empresa saiba recuperar tanto os dados que foram gravados há 5 minutos, quanto os que foram gravados há 1 ano, por exemplo. Para isso, precisam adotar metodologias específicas e realizar testes periódicos. Uma administração malfeita pode trazer prejuízos imensos para as empresas, além do risco de se perder informações valiosas. Os softwares de gerenciamento representam uma solução importante, na medida em que automatizam a operação de backup e diminuem a necessidade de manutenção.

GERENCIAMENTO DE TI

Existem boas opções de ferramentas disponíveis, como as listadas a seguir.

- Computer Associates BrightStor SRM – Oferece capacidade de gerenciar storage, a partir de um ponto único, oferecendo informações como a capacidade de storage do sistema.
- EMC ControlCenter StorageScope: – Voltado para relatórios de capacidade e gerenciamento de recursos, possui total integração como a família ControlCenter.
- Fujitsu Softek Storage Manager – Oferece um ponto único para visualizar os recursos de storage em mainframe e plataforma distribuída.
- HP OpenView Builder – Software de gerenciamento de capacidade para direct-attached storage (DAS), SAN-attached storage e NAS.
- IBM Tivoli Storage Resource Manager: oferece integração com o Tivoli Inventory e monitoramento de aplicações do DB2.
- Sun StorEdge Resource Management Suite – Automatiza a descoberta, relatórios de estatísticas, monitoração e alerta sobre a capacidade de storage em uso.
- Veritas SANPoint Control/Storage Reporter – Com o SANPoint Control 3.5, a Veritas expandiu seu gerenciamento de aplicações de storage, incluindo o RDBMS da Oracle e o Exchange da Microsoft.

Apenas com a implementação de uma rede de storage centralizada, usando soluções da HP, o Detran do Rio de Janeiro conseguiu reduzir o número de servidores de 6 para 4, e a equipe dedicada a administrar a infraestrutura caiu de 11 para 2 pessoas. Outro exemplo é o da PUC Paraná, que optou por centralizar o armazenamento no equipamento Thunder 9200, da Hitachi Data Systems. Houve expressivo aumento do desempenho em comparação à estrutura anterior, além de ter sido eliminada a necessidade de backup de cada servidor, resultando numa redução de custos significativa.

Contingência

O setor corporativo mostra-se cada vez mais inclinado a adotar uma política de contingência. Como dissemos acima, o atentado ao World Trade Center, em 11 de setembro de 2001, serviu para ampliar o interesse, mas muitas empresas, principalmente as que lidam com grandes volumes de dados e dependem muito da Tecnologia, como as do setor de finanças e de telecomunicações, já se preocupam com a questão há algum tempo. Foi o caso do J.P.Morgan, que contratou a Peregrine para auxiliá-lo a elaborar e executar um projeto de emergência, logo após o primeiro atentado, um ano antes da explosão das Torres Gêmeas. Percebendo o risco, a empresa não perdeu tempo e tomou as iniciativas adequadas, o que a salvou e permitiu a continuidade das operações quando suas dependências foram totalmente destruídas naquele fatídico 11 de setembro.

Uma política de proteção não pode ser efetivada da noite para o dia e nem existe uma fórmula-padrão que sirva para todas as empresas. É preciso, inicialmente, fazer uma análise interna e determinar o que é vital para a companhia, quais são os maiores riscos e vulnerabilidades de seus sistemas, os cuidados básicos que devem ser tomados e as ferramentas de hardware e software mais apropriadas para proteger a empresa em todos os sentidos. Outro aspecto a ser considerado é que um plano de segurança não pode ser rígido, ou seja, precisa ser flexível e dinâmico para suportar as necessidades que surgirem em virtude da velocidade de mudança de fatores físicos, tecnológicos e humanos.

Conscientizar os funcionários e envolvê-los no processo também constitui um elemento importante para o sucesso de uma política de segurança. Cada funcionário precisa entender o seu papel nesse processo e deve ser treinado. A empresa, de sua parte, precisa agir com transparência para que a equipe de trabalho atue como uma aliada. Outra medida fundamental é fazer reavaliações periódicas do plano de segurança para verificar, por meio de testes, pontos ainda vulneráveis.

GERENCIAMENTO DE TI

A questão de contingência está diretamente relacionada à necessidade de manter a disponibilidade dos sistemas, principalmente nos ambientes de missão crítica. É a partir da identificação do custo decorrente das interrupções e do tempo em que os sistemas ficam indisponíveis (downtime) que se determina a estratégia a ser adotada. Quanto menor for o downtime e o tempo de recuperação da informação, maior será o custo do projeto.

Para bancos, operadoras de cartão de crédito e empresas nas quais apenas alguns minutos do sistema fora do ar podem acarretar prejuízos de milhões de dólares, sem contar o risco de ter a sua imagem de credibilidade abalada, os riscos são minimizados com a adoção de máquinas redundantes à falha (espelhadas) e também de um outro site totalmente espelhado, que entra em atividade no caso de haver uma pane no sistema principal. São alternativas extremamente caras e que só se justificam pela criticidade das operações. As empresas com menos recursos podem usar como opção os sistemas de alta disponibilidade, compostos geralmente por vários servidores ligados em cluster.

Deve-se considerar, ainda, que uma parte das interrupções e problemas nos sistemas pode ocorrer por erros humanos de operação. É indispensável contar com ferramentas adequadas e apoio especializado para quantificar as perdas ocasionadas por essas paradas não planejadas e também para tomar medidas eficazes para evitar, ou ao menos minimizar, suas ocorrências.

CIOs, CTOs e CSOs

Cuidar da segurança passou a ser mandatório. Mas a quem cabe essa responsabilidade dentro das empresas? Nos Estados Unidos e na Europa, muitas empresas optaram por admitir especialistas, como os CTOs (Chief Technology Officers) e CSOs (Chief Security Officers), para cuidarem das políticas de segurança e da aquisição de tecnologias específicas, deixando aos CIOs (Chief Information Officers) os assuntos relacionados à gestão dos negócios e a responsabilidade pela integração das áreas executivas com a área de TI.

No Brasil e outros países da América Latina, esse panorama é um pouco diferente. Em geral, o CIO acumula o papel de gerente dessas áreas com o de executivo de negócios e tomador de decisões. Em grande parte das empresas, as funções dos CTOs e CSOs são executadas por gerentes operacionais que se reportam ao CIO. São subordinados que assumem tarefas importantes, como a de "fechar as portas" da organização para impedir ataques externos, mas quase sempre não passam do primeiro nível da gestão corporativa.

Esses profissionais, na verdade, cuidam dos produtos adquiridos (como firewalls, roteadores, switches e software de gerenciamento) para verificar se a infra-estrutura está funcionando de acordo com o previamente estabelecido. Apenas em algumas empresas esses gerentes operacionais têm um status maior e coordenam a política de segurança, não apenas na área de TI, mas em todos os níveis corporativos.

O grande problema é que a maioria das empresas ainda vê a segurança como um centro gerador de custos e se questiona se realmente precisa investir continuamente altas cifras e tomar todos os cuidados. Os investimentos necessários, de fato, costumam ser expressivos e a expectativa é de que nada aconteça. No entanto, não há segurança à prova de absolutamente tudo. Os níveis de segurança variam de empresa para empresa e para cada processo de negócios.

GERENCIAMENTO DE TI

Para conseguir convencer a alta direção de que as medidas de segurança são fundamentais, os administradores de TI acabam se valendo das técnicas de marketing que consistem em difundir o medo, exaltando os desastres que poderiam ser causados caso houvesse um problema nos sistemas. Esse apelo, baseado na emoção e não na razão, no entanto, mostra-se como uma faca de dois gumes. A abordagem pode funcionar em situações reais de crise, mas acaba não se sustentando ao longo do tempo. Outro efeito colateral indesejado é o desperdício de dinheiro, na medida em que são implementadas soluções que nem sempre são as mais indicadas, além de mostrarem-se mais difíceis de serem gerenciadas e analisadas em termos de resultados práticos.

A atitude mais acertada é condensar as informações relativas às necessidades de segurança da empresa de forma clara para transmitir um cenário que os executivos da alta gerência (principalmente o presidente da empresa e o diretor financeiro) possam compreender. Em geral, esses executivos consideram que segurança é um problema tecnológico e não de negócios, por isso acabam não aprovando os investimentos necessários para a área.

Mostrar os riscos que essa decisão pode trazer para a empresa, sem no entanto apelar para a técnica do terror, é um dos desafios do administrador da TI. Cabe ao CIO fazer os executivos de negócios entenderem que um excelente firewall não resolve tudo. São necessárias outras medidas que devem funcionar como um todo, uma vez que novas ameaças surgem no mesmo compasso da evolução tecnológica, o que requer, portanto, constante atenção e a implementação de novas soluções e ações que permitam manter a empresa com o maior nível de proteção possível.

Módulo 8 - O futuro do gerenciamento

O futuro da Tecnologia da Informação

A Tecnologia da Informação evoluiu rapidamente. Em menos de 30 anos, deixou de ser um privilégio apenas das grandes empresas, para se tornar uma ferramenta indispensável para grandes, médias ou pequenas. Hoje não se discute mais a sua aplicabilidade para o alcance das metas de negócios. O grande questionamento dos analistas de mercado e dos gestores da TI é avaliar até que ponto, no futuro, valerá a pena ser pioneiro em inovação tecnológica, ou se a melhor estratégia será esperar o amadurecimento das soluções para então investir na sua aquisição. Hardware e software já viraram commodities? De fato, será possível comprar tecnologia sob demanda? A terceirização será inevitável?

O futuro da TI nas empresas esteve particularmente em evidência em 2003, devido ao artigo de Nicholas Carr, publicado em maio na revista Harvard Business Review, que causou polêmica no mundo inteiro. O escritor, jornalista e consultor norte-americano, especializado na interseção entre estratégia de negócios e Tecnologia da Informação, ganhou notoriedade por seu artigo intitulado “IT doesn’t matter” (a TI não tem importância) em que convidava os executivos a analisar o papel da Tecnologia da Informação. O tema rendeu reportagens em jornais e revistas de negócios e de TI, como o The New York Times, Washington Post, Financial Times, Business Week, USA Today, Fortune, Computerworld, entre outras.

Embora veementemente contestados, os argumentos apresentados por Carr não puderam ser ignorados, propiciando boa reflexão. Entre os principais pontos abordados, ele ressaltou que, para ter valor estratégico, a tecnologia precisa permitir que as companhias a usem de forma diferenciada. Mas, como a evolução da TI é muito rápida e em pouco tempo torna-se acessível a todos, fica cada vez mais difícil obter vantagem apenas pelo seu emprego.

Carr acredita que a infra-estrutura de TI (hardware e software), entendida como um processo de armazenamento e transmissão de dados, está se transformando em commodity, assim como as ferrovias se transformaram em parte da infra-estrutura das empresas do século XIX, ocorrendo o mesmo com a eletricidade, no começo do século XX.

“TI é essencialmente um mecanismo de transporte, na medida em que carrega informação digital da mesma forma que os cabos elétricos transportam eletricidade. E é mais valiosa quando compartilhada, do que se usada isoladamente. Além disso, a quase infinita escalabilidade de muitas tecnologias, combinada com a velocidade de padronização tecnológica, significa que não há nenhum benefício em ser proprietário das aplicações. Ninguém mais desenvolve seu próprio e-mail ou processador de texto. E isso está se movendo rapidamente para aplicações mais críticas, como gerenciamento da cadeia produtiva e gerenciamento do relacionamento com o cliente. Sistema genéricos são eficientes, mas não oferecem vantagens sobre os concorrentes, pois todos estão comprando os mesmos tipos de sistema. Com a Internet, temos o canal perfeito para a distribuição de aplicações genéricas. E à medida que nos movemos para os Web Services, dos quais podemos comprar aplicações, tudo nos levará a uma homogeneização da capacidade da Tecnologia.”

Neste trecho da entrevista concedida ao Computerworld, Nicholas Carr reitera a idéia de que hoje a Tecnologia não representa mais um diferencial competitivo para as empresas. No passado, o panorama era outro. Apenas as grandes empresas tinham poder de fogo para investir no desenvolvimento de Tecnologia, esperando (e conseguindo) obter vantagem sobre os concorrentes. Atualmente, no entanto, com a evolução tecnológica ocorrendo em espaços de tempo cada vez mais curtos, essa vantagem deixa de existir. Não vale mais a pena investir altas cifras em desenvolvimento de sistemas e soluções e correr os riscos do pioneirismo, porque até se pode obter uma vantagem sobre os concorrentes, mas rapidamente isso deixa de ser um diferencial.

GERENCIAMENTO DE TI

Como exemplo, Carr cita que em 1995, nos EUA, grandes bancos varejistas criaram redes proprietárias para oferecer serviços de home banking a seus clientes e investiram milhões de dólares nesse sentido. Percebendo esse nicho, software-houses logo passaram a oferecer soluções do tipo e a Internet banking virou commodity, possibilitando a outros bancos menores disponibilizar esse serviço com investimentos e riscos infinitamente inferiores aos das instituições que foram pioneiras.

O grande risco das empresas na atualidade, segundo Carr, é gastar em excesso em TI e continuar querendo obter vantagens sobre a concorrência, o que fatalmente levará a um desperdício de dinheiro e ao desapontamento. Essas afirmações provocaram diferentes reações no mercado e entre os executivos de TI, mesclando indignações acaloradas com concordâncias discretas.

As principais críticas evidenciaram que as empresas pioneiras, que apostam no desenvolvimento tecnológico, têm sucesso porque também contam com uma estratégia de negócios bem orquestrada. Mas a TI desempenha um papel primordial e contribui significativamente para a obtenção dos bons resultados. A dinâmica do mercado sofre a ação de vários agentes, além das pressões dos concorrentes. Isso deve ser complementado por um conjunto de processos, o que requer aplicações e sistemas inovadores, além de níveis de serviço para suportar a estratégia de negócios.

Polêmica à parte, o fato inegável é que atualmente as empresas estão mais reticentes em realizar novos investimentos em Tecnologia, inclusive as que são extremamente dependentes desses recursos. Muitos fatores contribuem para isso, entre os quais as oscilações na política e na economia mundial e o conseqüente enxugamento da produção dos bens e serviços. Mas também não se pode ignorar o fato de que grande parte das empresas investiu em tecnologia de ponta, subutiliza o aparato computacional de que dispõe e se questiona se deve partir para novas aquisições ou voltar-se ao melhor aproveitamento dos seus ativos.

Computação sob demanda

Conceitos batizados de computação on demand, grid computing, utility computing e adaptive computing, que na prática significam quase a mesma coisa, têm sido apresentados como o futuro da computação. O movimento tem à frente as fornecedoras líderes da indústria de TI, como a IBM, HP e Sun Microsystems. Cada uma à sua maneira, elas defendem a idéia de que o desafio do setor corporativo é não se basear em cenários, porque eles mudam muito rapidamente. Ou seja, as empresas precisam ter a capacidade de responder a essas mudanças, com a mesma agilidade.

Parafraseando Charles Darwin, as espécies que sobrevivem não são as mais fortes, mas as que melhor conseguem se adaptar às mudanças. O mesmo princípio se aplica às empresas que cada vez mais precisam ser hábeis para gerenciar a TI, reduzindo custos sem comprometer a qualidade dos serviços, defendendo a máxima de fazer mais com menos. Daqui para frente, o que fará toda a diferença não será o tipo de tecnologia empregada, mas a forma como a empresa a utiliza.

Hoje, algumas funções de processamento são limitadas pelas restrições dos computadores. O conceito de computação sob demanda pressupõe um cenário em que será possível obter uma capacidade extra de processamento, na medida em que ela for necessária, pela rede, sem que o usuário precise conhecer a complexidade da infra-estrutura e pagando apenas pelo que for efetivamente utilizado. Também chamado de grid computing, é um conceito de processamento distribuído que envolve o uso de vários computadores interconectados através de redes locais ou de longa distância, ou mesmo a Internet. Sua operação requer também o emprego de muitos protocolos, padrões e ferramentas de software.

Na concepção da IBM, on demand não se refere apenas à tecnologia, mas também de mudar a forma de fazer negócios, por meio do desenvolvimento de novas capacidades para responder a tudo o que o mercado apresenta, tornando a empresa mais eficiente e obtendo vantagens sobre os concorrentes. On demand terá

GERENCIAMENTO DE TI

diferentes alcances em diferentes indústrias. Na farmacêutica, por exemplo, as soluções on demand poderão ajudar as empresas a reduzir o tempo para lançar novos medicamentos, o que lhes trará vantagens em relação aos competidores mais lentos. Já no setor automobilístico, auxiliarão a melhorar o gerenciamento da cadeia de distribuição e de pedidos, além de otimizar a fabricação de peças, seus processos de desenvolvimento de projetos e fabricação, e a administração de produtos através de seus ciclos de vida.

A IBM já disponibiliza serviços para prover acesso remoto a aplicações de servidores, cobrados de acordo com o volume de uso. A estratégia é atender às empresas que precisam lidar com grande volume de servidores, o que torna caros a aquisição, gerenciamento e manutenção. Com isso, as companhias passam a utilizar o poder dos servidores da própria IBM, que ficam instalados nos data centers da fabricante. O acesso é feito remotamente, e o usuário paga carga que utilizou por mês. No mesmo modelo de negócio, a IBM colocou à disposição o gerenciamento dos serviços de servidores e rede, como conectividade com Internet, armazenamento, backup e firewall.

Adaptive Enterprise

Seguindo na mesma direção, mas ressaltando que o modelo proposto é um pouco diferente, a HP disponibiliza pacotes de serviços, software, soluções e uma arquitetura de referência – tudo sob o que batizou de “Adaptive Enterprise”. A idéia é auxiliar os usuários dos produtos a medir, projetar e gerenciar mudanças na estrutura de TI, atendendo à demanda de negócios. O objetivo é trabalhar com o que já existe no cliente, preservando os investimentos feitos e preparando-o para avançar gradualmente para um novo patamar.

Na prática, o conceito defendido pela fornecedora prevê a virtualização gradual do processamento de aplicativos, começando dentro das próprias empresas e chegando à terceirização total em alguns anos. Existem, na verdade, estágios entre o modelo atual e o de empresa adaptável que são mensuráveis e podem ser divididos em 3 níveis:

1. Segurança e continuidade de negócios.
2. Consolidação e gerenciamento.
3. Virtualização, processamento sob demanda e outsourcing.

Outsourcing

Na avaliação de consultores de mercado, a computação sob demanda ainda está levando alguns anos para amadurecer. O que deverá ganhar cada vez mais impulso é o processo de terceirização da TI. O outsourcing, como também é conhecido, não representa nenhuma novidade e há muitos anos vem sendo adotado, em maior ou menor escala, pelas empresas de diferentes ramos de atividade. Mas recentemente começou-se a perceber que as desconfianças e resistências das áreas usuárias, que eram muito elevadas no passado recente, já não constituem empecilho para a maturação desse modelo. Motivadas pela necessidade de reduzir custos e por terem concluído que fazer tudo em casa, além de muito caro, é pouco produtivo, as empresas de grande, médio e pequeno portes estão gradativamente aumentando o repasse de algumas funções da TI para terceiros.

Há, no entanto, necessidade de seguir alguns critérios, a fim de alcançar os objetivos pretendidos. Tão importante quanto a escolha da empresa prestadora, é fundamental elaborar o melhor acordo de nível de serviço (SLA – Service Level Agreement), que se caracteriza por ser bem mais detalhista do que os contratos convencionais na descrição dos serviços acordados entre as partes, estabelecendo uma série de parâmetros e métricas a serem atingidos (tempo médio entre falhas, disponibilidade dos sistemas, performance, etc) e contendo cláusulas com penalidades previstas para os casos de não cumprimento.

GERENCIAMENTO DE TI

Espera-se também o crescimento do Business Process Outsourcing (BPO), que não se restringe a uma simples terceirização, na medida em que exige do prestador do serviço a participação nos riscos dos negócios do cliente. O BPO pressupõe a terceirização da gestão de um processo de negócio de uma empresa, por exemplo, a área de recursos humanos, em que são ofertados toda a infra-estrutura de hardware, os software aplicativos, suporte e mão-de-obra especializada. Isso requer que o prestador tenha profundo conhecimento do negócio do cliente. Se o negócio for bem, o provedor será bem remunerado; se for mal, os prejuízos terão que ser divididos entre as partes.

No âmbito geral do outsourcing, as estimativas da IDC Brasil são de que esse mercado, no Brasil, continuará crescendo a taxas bem superiores às de outros segmentos de Tecnologia, devendo movimentar cerca de R\$ 14,7 bilhões em 2007. No entanto, existem ainda alguns obstáculos. Enquanto a terceirização de redes de dados e voz e o gerenciamento de infra-estrutura são considerados serviços consolidados, outras propostas de outsourcing de infra-estrutura ainda precisam quebrar barreiras. É o caso do segmento de armazenamento de dados, em que os data centers se apresentam como grandes propulsores do serviço, oferecendo a possibilidade de alocar servidores e equipamentos do cliente, ou mesmo cedendo espaço em suas máquinas e disponibilizando uma gama ampla de serviços. Por enquanto, as empresas que mais investem em outsourcing de armazenamento são as dos setores financeiro, varejo e manufatura.

O CIO do futuro

Não se pode afirmar com certeza os caminhos e tecnologias que irão prevalecer no futuro, mas outsourcing, computação sob demanda, mobilidade, convergência, consolidação de sistemas, segurança e software livre são as vertentes mais prováveis. Diante de um cenário que prevê o aumento da comoditização da TI e da sua operação por terceiros, qual será o papel do CIO no futuro? Hoje, esse profissional ainda é o melhor integrador de soluções dentro das corporações. O próximo passo será tornar-se o melhor gerenciador dessas necessidades. Além do óbvio conhecimento da Tecnologia, o novo CIO também precisará ter visão estratégica e familiaridade com o board da companhia, seja para reportar-se a ele, seja para dele fazer parte. Também caberá ao CIO decidir o que deverá ou não, ser terceirizado, mantendo o controle sobre o gerenciamento dos serviços e contratos, e ainda distinguir onde a inovação tecnológica se fará necessária e onde se poderá optar pela comoditização.

Os mais pessimistas acreditam que, num futuro não muito distante, o cargo de CIO deixará de existir porque a Tecnologia será tão simples de usar que não haverá necessidade de um profissional específico para comandá-la. Os otimistas sustentam que o CIO provavelmente deixará de ser o grande mentor da informática, mas continuará sendo responsável pela manutenção da infra-estrutura tecnológica como um todo e pelo gerenciamento de terceiros. Nesse sentido, a governança de TI terá de crescer muito. Qual das duas correntes está certa só o tempo dirá.