UNIDADE 3 – A GESTÃO DO CONHECIMENTO – CAPTURANDO, CRIANDO, MANTENDO E DISSEMINANDO O CONHECIMENTO DA EMPRESA DIGITAL.

MÓDULO 1 – GESTÃO ESTRATÉGICA DO CONHECIMENTO NA EMPRESA DIGITAL

01

1 - GESTÃO DO CONHECIMENTO

Na economia moderna, o maior bem da empresa é o conhecimento sobre os serviços exclusivos que oferece ou sobre produtos que fabrica. Se uma empresa consegue oferecer um serviço por um preço inferior ao da concorrência, ela detém um conhecimento que os seus concorrentes não possuem. Da mesma forma, se a empresa fabrica um produto de excelente qualidade por um preço competitivo ela também detém um conhecimento que é fundamental para a sua permanência no mercado.

Neste contexto competitivo, as empresas devem ser únicas, e a diferenciação pode ser feita, por exemplo, pela inovação, pela marca, pela utilização de ferramentas e processos únicos para a estrutura organizacional da empresa e para a gestão de pessoas. Portanto, essa competência organizacional, que, na verdade, é algo intangível, pois não pode ser mensurado, cria valor para a sociedade se constituindo como uma fonte de lucros para a empresa.

À medida que o conhecimento é uma fonte de lucros para empresa, ele tem uma importância estratégica essencial para a sobrevivência da empresa, o seu sucesso dependerá diretamente da capacidade da empresa em gerar, organizar e disseminar o conhecimento. A gestão do conhecimento então aumenta a capacidade da empresa de produzir conhecimento, incorporando esse conhecimento aos seus negócios.

Gestão do conhecimento é um processo sistemático, organizado, apoiado na geração, codificação, disseminação e apropriação de conhecimentos, com o propósito de atingir a excelência organizacional.

02

A tecnologia da informação tem um papel chave na gestão do conhecimento, pois oferece o suporte para que a gestão do conhecimento seja realizada. Para que a gestão do conhecimento realmente gere valor, é necessário que a empresa:

- identifique quais são os conhecimentos importantes;
- quais benefícios que trazem para a empresa.

© 2011 - AIEC - Associação Internacional de Educação Continuada

Uma vez determinados esses dois aspectos, a empresa pode realmente partir para um programa de gestão do conhecimento. Este programa, quando implementado em grandes empresas, é geralmente liderado por um profissional específico – CKO – executivo chefe do conhecimento que se encarrega de reunir, armazenar e disseminar o conhecimento.

O conhecimento está disperso dentro de uma empresa. Todos os sistemas de informação descritos anteriormente são úteis para a gestão do conhecimento. Entretanto, a base de conhecimento utilizada na gestão do conhecimento deve ser bem mais abrangente.

A base de conhecimento envolve:

Conhecimento interno estruturado (conhecimento explícito)	Conhecimento mais voltado ao uso de tecnologias de informação e comunicação (chats, intranet, data warehouse, manuais de produtos, relatórios, etc.). É o conhecimento mais fácil de ser codificado.
Conhecimento informal interno (Conhecimento tácito)	Vivência e experiência dos empregados.
Conhecimento externo de concorrentes, produtos e mercados	Sites dos concorrentes, jornais , revistas, periódicos e empresas transmissoras de notícias (Reuters, Down Jones, etc.)

Esses três tipos de conhecimento então devem ser reunidos e organizados para que possam ser disseminados dentro da empresa.

03

Disseminação do conhecimento - A maioria do trabalho que utiliza o conhecimento é realizado dentro dos escritórios. São utilizados então sistemas de escritório que têm por finalidade aumentar a produtividade dos trabalhadores da informação dentro do escritório. Esses sistemas permitem o gerenciamento de documentos (criação, armazenagem, recuperação e disseminação), a gestão de agendas (agendamento de reuniões), os contatos (dados referentes a funcionários, fornecedores e clientes), as ferramentas de comunicação e os dados do escritório.

O grande problema enfrentado pelas organizações na implantação de programas de gestão do conhecimento é que a maioria da documentação está armazenada em papéis, exigindo a utilização de **sistemas de digitalização de documentos**. Entretanto, mesmo com a utilização desses sistemas, ainda é preciso manter uma grande quantidade de papéis, pois documentos digitalizados não possuem valor legal reconhecido. De qualquer forma, a grande vantagem da digitalização de dados é reduzir a circulação de documentos em papel na empresa e a facilidade de pesquisa e consulta desses documentos dentro por meio da *intranet* da empresa.

Além dessas funcionalidades básicas de gestão de documentos, existem alguns sistemas que permitem o controle de alterações e versões de documentos, possibilitando ainda a pesquisa de documentos pelo seu conteúdo. Sem dúvida, a aquisição de um sistema em rede com essas funcionalidades como os

© 2011 - AIEC - Associação Internacional de Educação Continuada

da *IntraNet solutions* e da *Open Text* pode ser interessante e, em alguns casos, quase indispensável para grandes empresas.

Entretanto, empresas pequenas e de médio porte podem utilizar o próprio Microsoft Word para funcionalidades, como o controle de alterações. Ferramentas como o *Google Desktop* também permitem a indexação de documentos e a pesquisa por documentos que tenham palavras-chave específicas em seu conteúdo.

04

Criação do Conhecimento - Nós vimos como os sistemas de informação podem nos ajudar a reunir e disseminar o conhecimento. Agora iremos tratar dos sistemas de trabalhadores do conhecimento (STC). São sistemas específicos para trabalhadores que lidam com a criação do conhecimento, como os pesquisadores, projetistas e analistas. Esses profissionais precisam de sistemas específicos com alta capacidade de processamento que permitam o manuseio de gráficos, informações multimídia, a realização de cálculos complexos e simulações. Esses sistemas são bem específicos ao tipo de necessidade do profissional. Assim o sistema utilizado por um analista financeiro deve ser completamente diferente do sistema utilizado por um designer de carros.
Captura do conhecimento - As organizações estão utilizando cada vez mais sistemas que utilizam técnicas de inteligência artificial (IA). A inteligência artificial é definida no dicionário Houass como "ramo da informática que visa dotar os computadores da capacidade de simular certos aspectos da inteligência humana, tais como, aprender com a experiência, inferir a partir de dados incompletos, tomar decisões em condições de incerteza e compreender a linguagem falada, entre outros."

Os sistemas que utilizam esses conceitos de IA são os chamados sistemas especialistas. A finalidade desses sistemas especialistas é sintetizar o conhecimento de um especialista para que determinadas ações e procedimentos possam ser realizados de forma automatizada.

Esse conceito é utilizado, por exemplo, em sistemas bancários para avaliar o crédito de um cliente. Esse tipo de sistema é utilizado também para detectar possíveis irregularidades nas compras dos cartões de crédito e na emissão de cheques. Compras que fogem ao padrão de consumo do cliente são detectadas e procedimentos administrativos podem ser realizados para validar a compra e o cheque do cliente.

05

Sistemas especialistas são utilizados até mesmo na área de produção, como é o caso da Indústria de cimento. Os sistemas especialistas são utilizados para ajustar o tempo de cozimento dos ingredientes que forma o cimento, avaliando vários fatores como qualidade da matéria-prima, temperatura e pressão do forno; são utilizados com sucesso para resolver problemas não estruturados, em que a quantidade de variáveis de entrada é muito grande, ou quando a relação entre as variáveis não é bem definida, ou ainda quando o problema é muito complexo e não se conhecem bem todas as variáveis relacionadas ao problema.

Os sistemas especialistas utilizam como base quatro técnicas:

Regras de negócios	As regras de negócios são regras do tipo SE-ENTÃO. Como exemplo, poderíamos criar regras para a concessão de financiamento do carro, como segue:

© 2011 - AIEC - Associação Internacional de Educação Continuada

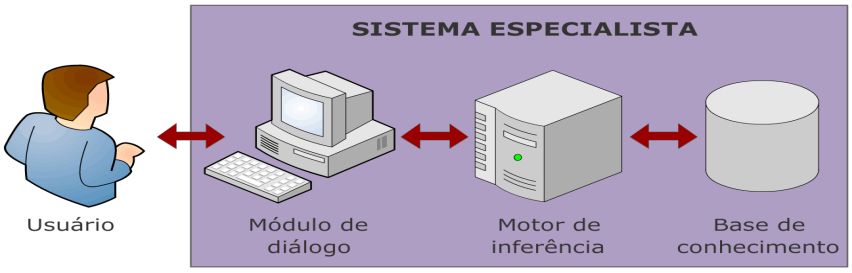
	Se renda>3 prestações então *perguntar sobre casa própria.* *Se possuir casa for própria então* *Perguntar se possui outros financiamentos* *Se não possuir outros financiamentos então* *Conceder o empréstimo.* Sistemas especialistas podem utilizar milhares de regras para apresentar um diagnóstico ou fornecer uma resposta a uma solicitação.
Lógica fuzzy	Esta técnica também utiliza regras de negócio, mas são regras mais imprecisas. Por exemplo, um exemplo é uma sala com ar condicionado. Uma pessoa que está dentro da sala pode classificar a temperatura da sala como quente, agradável e fria, sem necessariamente conhecer com exatidão a temperatura da sala. Então as regras de negócio poderiam ser: Se a sala estiver fria então Aqueça Se a sala estiver quente Esfrie a sala Se a sala estiver com temperatura agradável Mantenha a temperatura Portanto, a lógica fuzzy é uma técnica que permite que os projetistas e sistemas trabalhem com estados imprecisos da mesma forma como os homens trabalham.
Redes neurais	As redes neurais se baseiam no modelo físico do cérebro, que consiste em uma grande rede de células simples (neurônios) interconectadas. No caso dos programas, é possível simular o funcionamento de uma rede neural possibilitando o "aprendizado" do programa. Esse tipo de técnica não utiliza as regras de negócios e sim dados históricos com os resultados obtidos. A rede se encarrega de "aprender" e, quando uma situação similar ocorrer, ela fornecerá o resultado apropriado.
Algoritmos genéticos	A técnica baseada em algoritmos genéticos utiliza o conceito de evolução de Darwin que afirma que ao longo das gerações os seres vivos sofrem mutações aleatórias e sofrem a seleção natural. Os sistemas baseados em algoritmos genéticos procuram solucionar problemas utilizando essa técnica "selecionar" a melhor solução.

06

2 - COMPONENTES DOS SISTEMAS ESPECIALISTAS

Um sistema especialista pode ser dividido em três módulos: módulo de diálogo, base de conhecimento e motor de inferência:

© 2011 - AIEC - Associação Internacional de Educação Continuada

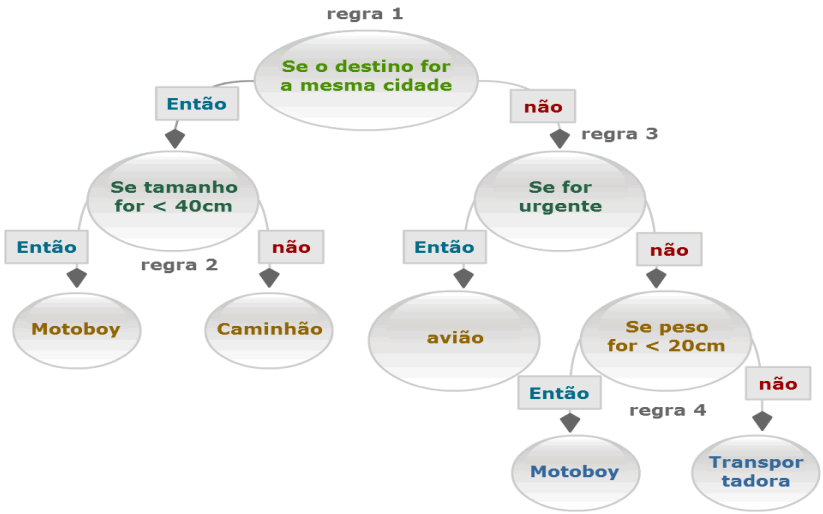


O **módulo de diálogo** tem por finalidade oferecer uma interface para a consulta e apresentação do resultado para o usuário. Esse módulo de diálogo pode oferecer também um **shell IA** para que o sistema seja programado por meio da introdução de regras de negócio, para que se possa alterar e pesquisar dados na base de conhecimento e gerar interfaces gráficas para o usuário.

Nos sistemas especialistas baseados em regras, o **motor de inferência** se encarrega de receber as informações do usuário, analisá-las, fazendo associações com as regras definidas na **base de conhecimento**, aplicando-as corretamente, de forma a obter a solução do problema. Os sistemas especialistas podem ser implementados seguindo duas estratégias: encadeamento para frente e encadeamento para trás. No **encadeamento progressivo ou encadeamento à frente**, o usuário entra com dados de entrada, o motor analisa os dados aplicando as regras e o resultado é apresentado ao usuário. No **encadeamento regressivo**, ou **encadeamento dirigido por objetivos**, o motor de inferência parte de uma hipótese e segue em frente questionando o usuário ou verificando os dados de entrada até que chegue a uma conclusão.

07

A figura abaixo apresenta um exemplo de regras de negócio simplificadas para um sistema especialista utilizado no departamento de logística de uma empresa Paulista, que determina qual é o meio de transporte mais adequado para o envio de uma carga.



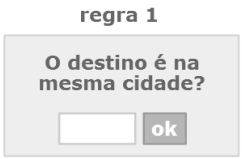
Segundo o sistema acima, qual seria o meio de transporte ideal para o envio para a carga abaixo:

© 2011 - AIEC - Associação Internacional de Educação Continuada

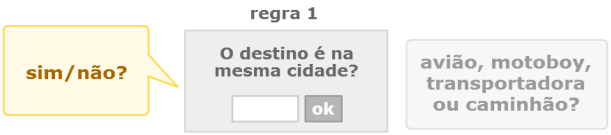
Destino: Brasília
Urgente: não
Tamanho: 30cm
Peso: 55Kg

Se o sistema de inferência utilizasse o encadeamento progressivo, o sistema testaria a primeira regra: O destino da carga é na mesma cidade da empresa? A resposta é não. Então passaríamos para a avaliação da regra 3. Como o peso da carga é superior a 20Kg, então a carga seria enviada por meio de uma transportadora.

08



No caso do encadeamento regressivo, o sistema iria eleger primeiramente um meio de transporte e verificar se esse meio poderia ser utilizado por meio da validação de todas as regras que o antecedem. Assim o motor de inferência iria primeiramente testar a hipótese: “A carga deve ser enviada pelo motoboy?”. Pela regra 2, poderia, mas pela regra 1 não, pois a carga não é urgente. Logo o sistema passaria a testar a próxima hipótese: “A carga deve ser enviada por caminhão?”. E assim sucessivamente até testar a hipótese verdadeira: “A carga deve ser enviada pela transportadora?”.



O tipo de encadeamento normalmente é definido de acordo com o tipo de problema a ser resolvido. O encadeamento progressivo é utilizado para resolver problemas de planejamento, projeto e classificação. O encadeamento regressivo é utilizado para resolver problemas de diagnóstico, pois possui um grande número de dados de iniciais e poucas saídas que geralmente utilizam.

09

Quando utilizar um sistema especialista?

Sistemas especialistas devem ser utilizados quando o problema que se deseja resolver tiver as seguintes características:

- não for trivial
- não for estruturado
- ser frequente
- existir um especialista disponível

Para que seja interessante partir para a implantação de sistemas especialistas, o problema que se deseja resolver não deve ser trivial e nem estruturado, pois problemas triviais e problemas estruturados podem

© 2011 - AIEC - Associação Internacional de Educação Continuada

ser resolvidos por sistemas de informações tradicionais. Para que o benefício supere os custos de implantação, o problema deve ocorrer com frequência e é importante que exista um especialista dentro da empresa que poderá ajudar o CKO a construir a base de conhecimento e as regras de inferência que devem ser utilizados no SE.

10

RESUMO

Na economia moderna, o maior bem da empresa é o conhecimento que esta possui sobre os serviços exclusivos que oferece ou dos produtos que fabrica. O sucesso da empresa digital depende então diretamente da capacidade da empresa em criar, organizar e disseminar o conhecimento.

O conhecimento está disperso dentro de uma empresa. Todos os sistemas de informação são úteis para a gestão do conhecimento. Entretanto, a base de conhecimento utilizada na gestão do conhecimento deve ser bem mais abrangente envolvendo: conhecimento interno estruturado (*chats*, *intranet*, data *warehouse*, manuais de produtos, relatórios, etc.), conhecimento informal interno (vivência e experiência dos funcionários) e conhecimento externo do mercado, dos concorrentes e do ambiente de negócios.

Um dos meios mais eficientes para disseminar a informação é utilizar os chamados **sistemas de escritório**, que têm por finalidade aumentar a produtividade dos trabalhadores da informação dentro do escritório. Esses sistemas permitem o gerenciamento de documentos (criação, armazenagem, recuperação e disseminação), a gestão de agendas (agendamento de reuniões), os contatos (dados referentes a funcionários, fornecedores e clientes), as ferramentas de comunicação e os dados do escritório.

São utilizados sistemas de trabalhadores do conhecimento (STC) para ajudar na criação do conhecimento. Esses sistemas são específicos para trabalhadores que lidam com a criação do conhecimento como pesquisadores, projetistas e analistas.

E por fim, vimos os sistemas especialistas que têm por finalidade sintetizar o conhecimento de um especialista para automatizar a solução de um problema. Esses sistemas são baseados em conceitos de inteligência artificial e utilizam tipicamente quatro técnicas: aplicação de regras de negócios, redes neurais, lógica fuzzy e algoritmos genéticos. Os sistemas especialistas são compostos por: base de conhecimento, motor de inferência e módulo de diálogo. O motor de inferência é o módulo responsável pela aplicação das regras de negócio e definição da solução.

Os sistemas especialistas são indicados para a resolução de problemas não triviais, não estruturados e que ocorrem com frequência na empresa. Além disso, devem ser avaliados os benefícios que o sistema trará para a empresa em relação ao custo de projeto e implantação do sistema. Recomenda-se que a empresa só desenvolva um SI se já possuir um especialista na área que dará suporte e ajudará na construção da base de conhecimento.

© 2011 - AIEC - Associação Internacional de Educação Continuada

UNIDADE 3 – A GESTÃO DO CONHECIMENTO – CAPTURANDO, CRIANDO, MANTENDO E DISSEMINANDO O CONHECIMENTO DA EMPRESA DIGITAL. MÓDULO 2 – SISTEMAS DE APOIO À DECISÃO

01

1 - BANCO SANTANDER

O banco Santander Banespa consolidou-se como o quarto banco privado por volume de ativos e primeiro entre os bancos internacionais. Fechou o ano de 2005 com uma base de clientes que ultrapassa os 6,7 milhões e conta com 1.897 pontos de venda e 7.119 caixas eletrônicos.

Criado em 1982, o Banco começou, em 1997, a aumentar a atuação no Brasil com a aquisição do Banco Geral do Comércio S.A. Nos anos seguintes, foram mais três aquisições. Em 1998, comprou o Banco Noroeste S.A., em janeiro de 2000, foi anunciada a aquisição do Conglomerado Financeiro Meridional - formado pelos bancos Meridional e Bozano, Simonsen. E, em novembro do mesmo ano, o Santander comprou o controle do Banco do Estado de São Paulo S.A. - BANESPA.

O conglomerado financeiro Santander Banespa foi formado em 2001, após a reestruturação societária realizada no primeiro semestre daquele ano, envolvendo as operações contábeis para a transferência das ações do Banco do Estado de São Paulo S.A. - Banespa, naquela época de propriedade do Banco Santander Central Hispano, S.A., para o Banco Santander S.A.

Após todas essas aquisições, o conglomerado precisou uniformizar a gestão de dados dos clientes e melhorar o processo de avaliação de crédito dos clientes.

02

Em novembro de 2005, o banco contratou uma empresa Fair Isaacs, que unificou o cadastro de clientes do conglomerado e implementou uma ferramenta de apoio à decisão chamada de StrategyWare para a avaliação de crédito de clientes.

O sistema utiliza um modelo baseado em pontuação e em árvores de decisão para permitir o crédito ao cliente. Levou sete meses para ser implementado, e em menos de um ano já mostrava resultados expressivos. A taxa de inadimplência caiu em 40% nos créditos de curto prazo. O processo de avaliação do crédito é agora completamente automatizado, sendo que o gerente pode verificar a sua disponibilidade de forma rápida pelo próprio terminal.

O próximo passo será implementar esse sistema nos caixas eletrônicos e também no Internet Banking

© 2011 - AIEC - Associação Internacional de Educação Continuada

para que os próprios usuários possam solicitar e receber resposta instantânea pelo sistema, reduzindo os custos operacionais do banco e aumentando a satisfação do cliente.

O Banco Santander então precisou de um sistema que ajudasse a avaliar o crédito de um cliente. Para isso utilizou o chamado sistema de apoio à decisão que são sistemas que fornecem suporte computacional interativo Ad Hoc (consultas de informações únicas de um problema não programado e específico à situação) direto e imediato aos gerentes auxiliando-os durante o processo de decisão. São por exemplo, dados, tabelas, planilhas de custos, gráficos, fatos e informações de texto. Os SAD são úteis, por exemplo, quando o gerente de uma empresa deseja saber o melhor local para a implantação de uma nova filial.

2 - O PROCESSO DE TOMADA DE DECISÃO

O administrador precisa tomar decisões quando encontrar mais de uma alternativa viável para resolver um problema. Quando temos mais de uma solução para um problema, a dificuldade será escolher a melhor decisão, aquela que trará mais benefício para a empresa e menos consequências negativas.

O grande pesquisador americano Herbert Simon, laureado em 1978, descreveu em seu livro **"The New Science of Management Decision"** que o processo de tomada de decisões possui três estágios: inteligência, concepção e seleção.

- **Inteligência** - nesse estágio o administrador deverá identificar o problema e quais são os fatores envolvidos no problema e qual o seu efeito sobre a organização. Neste estágio os administradores devem coletar dados dentro e fora da organização. Nesta fase o SIG poderá ajudar a identificar os problemas da organização por meio da elaboração de relatórios.
- **Concepção** – nesse estágio o administrador deve pensar em todas as soluções viáveis para o problema. Para isso os dados coletados no estágio anterior devem ser processados utilizando métodos, modelos, fórmulas e outras ferramentas para avaliar as alternativas e reduzir o número de soluções. Neste estágio um sistema SAD de pequeno porte poderá ajudar no processamento dos dados de forma a apontar quais os caminhos que poderão ser tomados.
- **Seleção** – quando já temos um número reduzido de alternativas, o administrador deve então realizar a escolha. Nesse estágio o administrador deverá aprofundar o seu conhecimento sobre as possíveis soluções do problema que foram definidas na etapa de concepção. Nesta fase então devemos utilizar modelos mais complexos e simulações para identificar quais seriam os efeitos da aplicação de cada uma das soluções na empresa. Nesse estágio um sistema SAD de grande porte com a possibilidade de realizar simulações complexas poderia ser de grande ajuda. De posse dos resultados dessas simulações, o administrador teria os todos os elementos para selecionar a melhor solução.

Entretanto, o processo de tomada de decisões nem sempre é assim linear seguindo os três passos descritos acima. Por exemplo, as informações obtidas na fase de inteligência podem ser incompletas fazendo com que o problema seja mal compreendido e, portanto, levarem a soluções ineficientes. Ou os

© 2011 - AIEC - Associação Internacional de Educação Continuada

modelos utilizados no processamento de dados não foram adequados e, após a implementação, constatou-se que solução escolhida trouxe consequências inesperadas.

04

Este processo de tomada de decisão é válido para qualquer tipo de problema, mas a quantidade de dados e a complexidade do processamento dependerão diretamente da natureza do problema.

Os problemas são classificados em:

Problemas estruturados - Os problemas totalmente estruturados são aqueles problemas que podem ser resolvidos pelo uso de uma série definida de passos. Em matemática chamamos esses passos de algoritmo. Nesse tipo de problema, caso tenhamos os mesmos dados de entrada, teremos sempre a mesma solução. Geralmente os problemas físicos e matemáticos são estruturados, por exemplo: qual a temperatura de congelamento da água, qual a área do prédio, etc.

Os problemas estruturados são, usualmente, chamados de problemas programáveis, porque como a solução se baseia em uma sequência de passos repetitivos a solução é muito fácil de ser programada.

Problema não estruturado - O problema não estruturado é aquele em que não existe um algoritmo a ser seguido para chegarmos a solução, seja porque não existem dados suficientes para a formulação de uma solução, seja porque existem tantos fatores que fica difícil processar os dados e termos uma única solução. Os problemas não-estruturados são problemas incertos, por exemplo: qual será o preço da ação de amanhã, qual será o tempo que fará daqui a um mês, etc.

Problemas semiestruturados - O problema semiestruturado é aquele que nem é totalmente estruturado e nem totalmente não estruturado. Neste tipo de problema só uma parte do problema possui uma resposta clara e objetiva. Por exemplo, qual seria a reação do consumidor se reduzirmos o peso do produto em 5%? Quais seriam os benefícios de abrirmos mais uma loja na cidade?

Os problemas estruturados exigem uma baixa complexidade de processamento tornando a implementação do SAD mais simples e rápida. A resolução de problemas semiestruturados ou não estruturados necessita de SAD mais elaborados que geralmente são mais caros e menos precisos, exigindo bom senso e mais experiência do administrador.

05

3 - Sistemas de apoio à decisão – SAD

Como vimos, os sistemas de apoio à decisão são muito úteis nos estágios de concepção e seleção de soluções no processo de tomada de decisões da empresa. Esses sistemas permitem que o administrador tenha os elementos necessários para escolher uma solução dentre as várias possibilidades. Os SAD podem ajudar a empresa a melhorar a participação no mercado, aumentar a lucratividade, reduzir custos e melhorar a qualidade do produto. Os sistemas de apoio à decisão podem, a exemplo do que vimos no caso Banespa, automatizar o processo de tomada de decisões, analisando rapidamente uma grande quantidade de dados e oferecendo uma solução imediata para a demanda de clientes e funcionários.

© 2011 - AIEC - Associação Internacional de Educação Continuada

A maioria dos SAD possui três componentes básicos: módulo de gerenciamento de dados, módulo de gerenciamento do modelo e módulo de diálogo.

- **Módulo de gerenciamento de dados** - é composto por uma base de dados ou por uma data *warehouse* que permite ao administrador realizar o estágio de inteligência do processo de tomada de decisões. Um investidor pode, por exemplo, querer investir em uma companhia. Antes de aplicar o dinheiro na empresa, o investidor poderá procurar dados históricos da empresa, resultados, balanços para decidir se vai ou não investir.

Muitos SAD são completamente conectados aos outros sistemas da empresa facilitando assim a coleta de internos da empresa. Os dados devem apresentar as seguintes características principais: Idade adequada à situação de decisão em questão e Confiabilidade e relevância no processo decisório.

06

- **Módulo de gerenciamento de modelos** - Para transformar os dados coletados em informações úteis, é preciso que o administrador escolha um modelo do módulo de gerenciamento de modelos que descreverá o processamento que será aplicado aos dados. O Modelo pode ser descrito em três aspectos:
- Representação – descreve os tipos de dados necessários.
- Tempo – identifica se está sendo considerado um instante no tempo ou o mesmo fenômeno em diferentes períodos de tempo.
- Metodologia – considera como os dados são coletados e processados.

Os modelos são baseados em pesquisas matemáticas e na experiência. Por exemplo, poderemos predizer as vendas da organização em virtude da publicidade, aplicando um modelo fundamentado em regressão linear aplicado aos dados históricos da organização. Para isso, seria aplicada a técnica de regressão linear aos dados obtidos nos anos anteriores de forma a obter a equação que descreve a relação publicidade x vendas da empresa.

Ano	Publicidade milhões/mês	Vendas milhões/mês
1995	5	23,4
1996	6	25
1997	2	10,3
1998	3	15,1
1999	4	17,2
2000	5	21,2
2001	5	21,5
2002	7	28,4
2003	7	27,2
2004	8	30,9

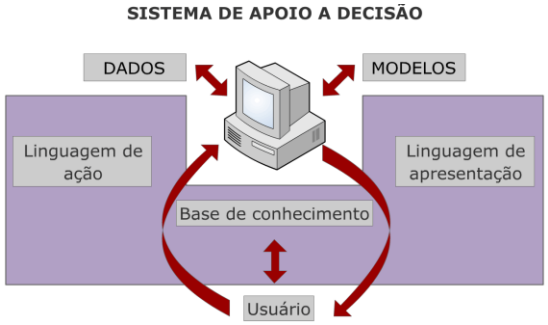
Aplicando o modelo de regressão linear aos dados históricos, obteve-se, no exemplo acima, que a relação entre publicidade (variável X do gráfico) e vendas (variável Y do gráfico) é dada pela equação Y=3,3484X+4,5817, o administrador poderia estimar quanto seria vendido caso a empresa resolvesse investir 10 milhões em publicidade, o que daria uma venda estimada de Y=3,3484x10.000.000+4,5817,

© 2011 - AIEC - Associação Internacional de Educação Continuada

ou seja, R$33.484.004,58. É interessante lembrarmos que simulações simples como essa que foi mostrada podem ser realizadas por meio de planilhas eletrônicas, como o Microsoft Excel.

07

- **Módulo de diálogo** – Interface – é a forma como o usuário interage com o sistema. Esse módulo utiliza a linguagem de apresentação e permite ao usuário determinar quais os dados que serão processados e também permite escolher qual o modelo que será utilizado no processamento. Por fim, esse módulo é responsável pela apresentação dos dados, seja em formato textual, ou tabelas, ou gráficos ou mesmo simulações gráficas. A Interface engloba três aspectos:
- Banco de Conhecimento – considera o conhecimento que o usuário possui em relação à situação de decisão e à utilização do sistema.
- Linguagem de Ação – refere-se ao modo como o usuário se comunica com o sistema (teclado, mouse, entre outros).
- Linguagem de Apresentação – diz respeito à forma de saída dos resultados (textos, tabelas, gráficos, entre outros).



Com ênfase na tomada de decisão em grupo, surgiram os Sistemas de Apoio à Decisão em Grupo (SADG), que possibilitam o trabalho conjunto de profissionais, cada um em seu computador. A eficácia desse tipo de sistema depende muito da forma como o evento é planejado e conduzido.

08

4 - Quando desenvolver um SAD para a empresa?

Um SAD é um investimento que possui um custo que pode ir de milhares a milhões de reais para a empresa. A empresa pode adquirir sistemas prontos ou então desenvolver sistemas específicos, caso seus problemas sejam únicos. Entretanto, quais situações justificam tal investimento? O questionário abaixo ajudará a avaliar em que um SAD poderia ser útil para a organização e em que medida a sua aquisição seria recomendável.

a) Qual é o tipo de problema que deverá ser resolvido? De modo geral, quanto menos estruturado for o problema, mais análise será requerida e mais útil será o SAD para o administrador. Devemos ter em mente que alguns problemas podem ser resolvidos simplesmente verificando os dados e utilizando o bom senso.

b) Os dados necessários ao SAD estão disponíveis no banco de dados da empresa? Quanto mais

© 2011 - AIEC - Associação Internacional de Educação Continuada

dados forem usados diretamente do banco de dados da empresa, mais rápido será o desenvolvimento do sistema.

c) Qual é a frequência em que o problema ocorre? Quanto maior a frequência do problema, mais útil é a implementação de um SAD.

d) Quem usará o sistema? Quanto mais funcionários precisarem do sistema, maior o benefício para a empresa.

e) Os usuários do sistema podem gastar tempo e dedicação para ajudar no desenvolvimento do sistema? O desenvolvimento do sistema exige que uma parte dos usuários gaste tempo e dedicação para ajudar no projeto. Portanto, é preciso que os administradores estejam cientes que os seus funcionários dedicarão menos horas em suas atividades cotidianas.

09

RESUMO

Vimos, nesse módulo, que o processo de tomada de decisões é muito importante para o sucesso das organizações, sendo uma das principais atividades do administrador.

O processo de tomada de decisões é composto de três fases: inteligência, concepção e seleção. A fase de inteligência consiste na coleta de dados sobre o problema e sobre as suas possíveis soluções. O administrador poderia se servir de SIG para coletar os dados. A fase de concepção busca identificar as soluções viáveis para o problema e por meio do processamento dos dados coletados, reduzir o número de soluções. Na fase de seleção as soluções viáveis são analisadas com bastante profundidade de forma a identificar quais os seus efeitos e resultados que seriam obtidos com a adoção de cada solução. Essa análise será a base da seleção da solução a ser implementada pelo administrador. As duas últimas fases da decisão poderão ser beneficiadas com o uso de SAD.

Existem basicamente três tipos de problema: problemas estruturados, problemas não estruturados e problemas semiestruturados. O problema é dito estruturado quando pode ser resolvido por meio de passos (algoritmo). Os problemas não estruturados e problemas semiestruturados não podem ser resolvidos por meio de algoritmos, exigindo análises mais complexas, exigindo bom senso e perspicácia por parte do administrador para a sua resolução.

Devido ao fato de os custos de aquisição e desenvolvimento de SAD serem caros, o administrador deverá avaliar bem a sua necessidade. Para isso o administrador deverá responder as seguintes questões: Qual o tipo de problema deve ser resolvido? O quanto ele é estruturado? Quais são os dados que estão disponíveis no banco de dados? Quantos funcionários vão usar o sistema? Os funcionários poderão ajudar no desenvolvimento do sistema cedendo tempo e dedicação do trabalho? Pois o envolvimento dos funcionários no desenvolvimento do sistema é essencial.

© 2011 - AIEC - Associação Internacional de Educação Continuada

UNIDADE 3 – A GESTÃO DO CONHECIMENTO – CAPTURANDO, CRIANDO, MANTENDO E DISSEMINANDO O CONHECIMENTO DA EMPRESA DIGITAL.

MÓDULO 3 – COMÉRCIO ELETRÔNICO E INTERNET

01

1 - UMA HISTÓRIA DE SUCESSO

A Internet teve um enorme desenvolvimento nos últimos anos. A integração de novas tecnologias de comunicação com softwares revolucionou a forma das pessoas e empresas se comunicarem e fazerem negócios. Você agora pode fazer compras sem sair de casa em lojas que se encontram em outro país. Agora as empresas não estão competindo apenas com seus concorrentes locais, mas com todas as empresas interconectadas na WEB. Por isso a importância de o administrador conhecer o funcionamento e as aplicações disponíveis na Internet para que suas empresas participem dessa revolução e marquem presença no mundo virtual.

AMERICANAS.COM

No final dos anos 90, o modelo das “Lojas Americanas” era visto com pessimismo pelos especialistas que acreditavam que o avanço dos hipermercados acabaria ameaçando a sua sobrevivência. Devemos nos lembrar que empresas tradicionais como a Mesbla e o Mappin haviam fechado as suas portas. Em 1999 a Lojas Americanas decidiu entrar no mundo virtual e criou a Americanas.com junto com um grupo de investidores do mercado financeiro: Chase Capital Partners, Flatiron Partners, AIG Capital Partners, Next Internacional, Mercosul Internet e Global Bridge Ventures. As Lojas Americanas é acionista majoritária, embora a Americanas.com seja completamente independente e possua seu próprio conselho de administração e diretoria. O objetivo original da Americanas.com era alavancar os ativos e a marca Lojas Americanas.

02

A Americanas.com fechou o ano de 1999, após dois meses de operação, com um total de vendas de R$56 mil reais e mil clientes cadastrados. No ano de 2000, o lucro bruto foi de R$2,9 milhões, ou 15% da venda líquida, entretanto, o resultado operacional acumulado foi negativo em R$45,4 milhões. Ao final do ano de 2000, a loja possuía 175 mil clientes cadastrados e um mix diversificado de produtos com aproximadamente 25 mil unidades de produtos em estoque. Em julho de 2000, a empresa também decidiu criar quioques-internet dentro das próprias lojas físicas para melhorar o acesso de clientes que não tinham acesso à internet. Ao final de 2000, as vendas nos quiosques internet representavam 10% do total de vendas da loja virtual, sendo que o sistema de televendas representava 21%.

Em 2003, a receita bruta ficou em R$274 milhões e com lucro de R$115,9 milhões. Em 2004, a loja virtual faturou R$434 milhões e obteve um lucro de R$64,1 milhões, uma queda de mais de 40% em

© 2011 - AIEC - Associação Internacional de Educação Continuada

relação ao ano anterior. No ano de 2005, a empresa faturou R$864,8 milhões, com um lucro líquido superior a R$100 milhões. Um resultado muito expressivo, pois devemos considerar que o patrimônio líquido da empresa está avaliado em R$150 milhões. Atualmente a Americanas.com possui um fluxo de 3 milhões de usuários ao mês.

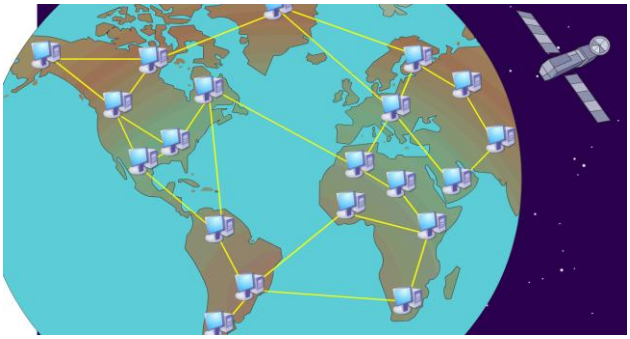
O caso de sucesso das Lojas Americanas não é um fenômeno isolado. Para se ter ideia do potencial da internet nos negócios, basta analisarmos o avanço do comércio eletrônico nos últimos cinco anos. Neste período, o faturamento do comércio eletrônico nacional aumentou cerca de 400%; o valor médio das compras cresceu 63% no período; o volume de vendas aumentou 254% e o número de consumidores aumentou de 700 mil adeptos em 2001 para 3,25 milhões em 2005 (dados da e-bit - www.e-bit.com.br). Portanto, vale a pena conhecermos como funciona a internet para aproveitarmos desse mercado em expansão.

03

2 - COMO FUNCIONA A INTERNET

Internet é uma gigantesca rede mundial de computadores, que inclui supercomputadores, servidores, computadores pessoais atuais com processadores Intel Pentium IV e AMD Athlon 64, há microcomputadores antigos ainda em uso como PC 386 ou 486.

Esses equipamentos são interligados por linhas comuns de telefone, linhas de comunicação privadas, cabos submarinos, canais de satélite e diversos outros meios de telecomunicação. Os computadores que compõem a Internet podem estar localizados, por exemplo, em empresas, universidades, cooperativas, prefeituras e nas próprias residências.



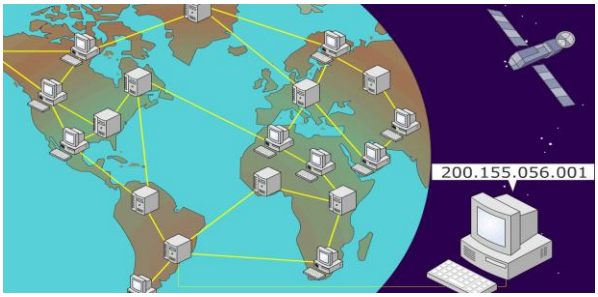
Fazendo paralelo com a estrutura de estradas de rodagem, a Internet funciona como uma rodovia pela qual a informação contida em texto, som e imagem pode trafegar em alta velocidade entre qualquer computador conectado a essa rede. É por essa razão que a Internet é muitas vezes chamada de "super rodovia da informação".

04

A Internet é considerada por muitos como um dos mais importantes e revolucionários desenvolvimentos da história da humanidade. Pela primeira vez no mundo, um cidadão comum ou uma pequena empresa pode (facilmente e a um custo muito baixo) não só ter acesso a informações

© 2011 - AIEC - Associação Internacional de Educação Continuada

localizadas nos mais distantes pontos do globo como também - e é isso que torna a coisa revolucionária - criar, gerenciar e distribuir informações em larga escala, no âmbito mundial, algo que somente uma grande organização poderia fazer usando os meios de comunicação convencionais.



Todo computador na Internet possui um número de identificação único que é o chamado de endereço IP. As aplicações e os protocolos de Internet permitem então que um computador localize e seja conectado a outro computador na internet. É isso que acontece quando você digita um endereço WEB (URL – Uniform Resource Locator) no navegador como http://www.google.com.br. A URL especifica então o protocolo utilizado para a comunicação entre o seu computador e o servidor, nesse caso http (Hypertext Transfer Protocol) e o nome de domínio www.google.com.br especifica o endereço do servidor. É um nome que serve para localizar e identificar conjuntos de computadores na Internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet. Sem ele, teríamos que memorizar uma sequência grande de números.

O endereço IP é formado por uma sequência de quatro de números separados por pontos, por exemplo: 123.234.12.2 ou 245.254.125.128. Os números da sequência estão necessariamente entre 0 e 255.

05

Mas como localizamos o endereço IP do servidor a partir do endereço URL? É simples, existem servidores específicos chamados de servidores DNS (*Domain Name System*) que possuem uma grande tabela que armazena a URL e o respectivo endereço IP do computador. Assim quando digitamos o endereço no navegador, o nosso computador se conecta com um servidor DNS e solicita o endereço IP associado a uma determinada URL. De posse do endereço IP, o computador poderá se conectar ao computador desejado.

Para se obter um domínio no Brasil, deve ser efetuado um registro junto ao Núcleo de Informação e Coordenação do Ponto BR - NIC .br que controla o site Registro.br. No caso de domínios internacionais, o registro deve ser feito nos respectivos órgãos.

O primeiro requisito para obter um domínio no Brasil é de que o nome não esteja registrado, reservado pelo Comitê Gestor, nem que seja uma marca notória do INPI.

Para registrar um domínio, é necessário ser uma entidade legalmente representada ou estabelecida no Brasil como pessoa jurídica ou física que possua um contato em território nacional.

© 2011 - AIEC - Associação Internacional de Educação Continuada

As regras sintáticas que o domínio deve seguir são:

- Tamanho mínimo de 2 e máximo de 26 caracteres, não incluindo a categoria.
- Caracteres válidos (A-Z;0-9) e o hífen.
- Nenhum tipo de acentuação.
- Não pode conter somente números.
- O hífen vale como separador sintático interno de palavras, sendo que os domínios já registrados com ou sem o mesmo só poderão ser registrados com esta diferença pelo detentor do primeiro registro.

06

O nome de domínio está estruturado em níveis hierárquicos. Ele é composto de duas partes: um nome fantasia que pode ser o nome da empresa, por exemplo, seguido por um ponto e um especificador do tipo de domínio. Por exemplo, o nome de domínio google.com.br tem como nome "google" , o primeiro especificador do tipo é ".com" que é o tipo específico para sites de empresa de comércio em geral e o último especificador é ".br", que informa que é um site brasileiro.

O nome de domínio também é chamado de domínio de primeiro nível (DPN). Cabe ao órgão Registro.Br definir e classificar os DPN do brasil (.br). Apresentamos, abaixo, uma tabela de DPN definidos para as instituições aqui no Brasil.

DPNs para Instituições (Somente para pessoas jurídicas)	
AGR.BR	Empresas Agrícolas, fazendas
AM.BR	Empresas de radiodifusão sonora
ART.BR	Artes: música, pintura, folclore
EDU.BR	Entidades de ensino superior
COM.BR	Comércio em geral
COOP.BR	Cooperativas
ESP.BR	Esporte em geral
FAR.BR	Farmácias e drogarias
FM.BR	Empresas de radiodifusão sonora
G12.BR	Entidades de ensino de primeiro e segundo grau
GOV.BR	Entidades do governo federal
IMB.BR	Imobiliárias
IND.BR	Indústrias
INF.BR	Meios de informação (rádios, jornais, bibliotecas, etc.)
MIL.BR	Forças Armadas Brasileiras
NET.BR	Detentores de autorização para o serviço de Rede e Circuito Especializado da Anatel e/ou detentores de um Sistema Autônomo conectado à Internet conforme o RFC1930
ORG.BR	Entidades não governamentais sem fins lucrativos
PSI.BR	Provedores de serviço Internet

© 2011 - AIEC - Associação Internacional de Educação Continuada

REC.BR	Atividades de entretenimento, diversão, jogos, etc.
SRV.BR	Empresas prestadoras de serviços
TMP.BR	Eventos temporários, como feiras e exposições
TUR.BR	Entidades da área de turismo
TV.BR	Empresas de radiodifusão de sons e imagens
ETC.BR	Entidades que não se enquadram nas outras categorias

07

A Internet é somente uma infraestrutura na qual as aplicações podem rodar. Geralmente, classifica-se a grande quantidade de informações disponíveis na Internet pela forma como a informação é organizada, pesquisada e transmitida. As aplicações mais comuns são:

- **Envio e recebimento de e-mails (Correio eletrônico)** – sendo possível não apenas a troca de mensagens de texto, mas a inclusão de arquivos multimídia. Os programas mais conhecidos são Outlook e Eudora.
- **Transferência de arquivos** - geralmente utilizam o protocolo **FTP**: (File Transfer Protocol).
- **Troca de Mensagens instantâneas** ou também chamada de **IRC** (Internet Relay Chat) - permite a interação em tempo real entre usuários. Também evoluiu bastante nesses últimos anos e os últimos aplicativos permitem não apenas a troca de mensagens de texto, mas a troca de arquivos e mesmo a videoconferência com o envio de som e imagem. Os aplicativos mais conhecidas são Messenger e ICQ.
- **Telefonia Internet (VoIP)** – a evolução nas técnicas de compactação de voz, ligados ao aumento da velocidades da rede permitiram o crescimento da utilização da voz sobre IP, ou seja, a utilização da internet para a realização das chamadas telefônicas. O aplicativo mais conhecido é o Skype.
- **Navegação Web** – aplicação que permite o acesso a documentos multimídia, com texto, som, imagens e animações. Hoje em dia, o mercado de aplicativos de navegação Web, os chamados Navegadores ou Browsers, é dominado pelo Internet Explorer, entretanto, existem outros aplicativos como Firefox e Netscape.

08

3 - INTERNET, INTRANETS E EXTRANETS

A internet tornou-se uma ferramenta importante para aumentar a produtividade da empresa. A empresa poderá utilizá-la para divulgar os seus produtos, receber, processar pedidos, efetuar pagamentos e realizar pesquisas.

Com a internet, as empresas perceberam que essa nova tecnologia não apenas possibilitou a divulgação de seus produtos, a sua comercialização, mas também possibilitou um acesso privilegiado ao seu cliente. O cliente poderia conhecer rapidamente informações sobre a empresa, seus produtos. De forma análoga, a empresa tem um canal direto com o cliente permitindo um maior conhecimento de seus anseios, desejos, suas opiniões sobre a empresa e sobre os seus produtos. Mas se isso funciona com os

© 2011 - AIEC - Associação Internacional de Educação Continuada

clientes externos, por que não funcionaria com os seus clientes internos? Seus funcionários? Daí surgiu a ideia das intranets.

A intranet é uma rede privada (só acessível pelos funcionários) que serve para disseminar informação de interesse dos funcionários dentro da empresa e também pode servir como ponto de acesso aos sistemas de gerenciamento e controle. Ela utiliza a mesma tecnologia da Internet podendo ser acessada da maioria das plataformas de computação, sendo fácil de utilizar visto que utiliza o próprio navegador Web.

A intranet também melhora sensivelmente o trabalho colaborativo, permitindo a troca interna de mensagens e documentos, reduzindo os custos de distribuição da informação. A tecnologia permite também que a intranet seja acessada de casa ou de qualquer outro lugar pelo funcionário, utilizando a tecnologia de **redes privadas virtuais** (VPN – *virtual private Network*). Essa tecnologia permite que se crie, por meio de técnicas de criptografia, um túnel virtual entre o computador do funcionário ligado à Internet e o computador da empresa conectado a Intranet para que as informações trafeguem de forma confiável. Esse sistema permite que funcionários em trânsito possam consultar dados disponíveis na intranet de maneira segura.

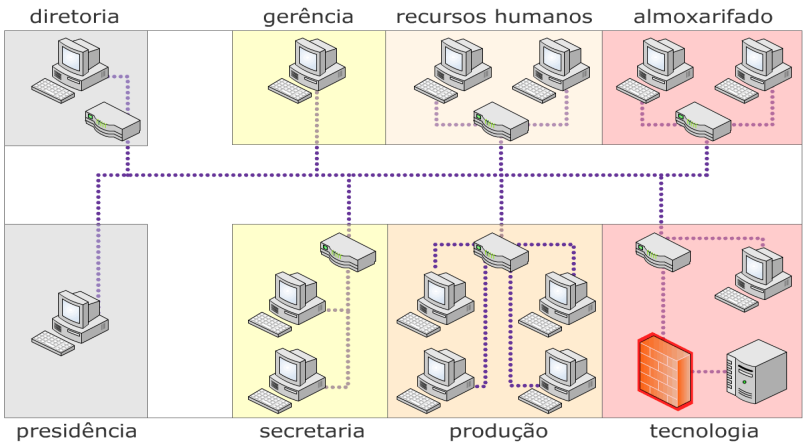
09

Outra rede muito utilizada hoje em dia é a chamada extranet. Essa rede liga a empresa a fornecedores, a empresas clientes ou a empresas parceiras. Esse tipo de rede é usado principalmente para melhorar a gestão da cadeia de suprimentos reduzindo o tempo do fluxo de informação do pedido, o tempo de entrega dos produtos e os custos. Além disso, as extranets também desempenham um papel importante no desenvolvimento de projetos comuns em empresas parceiras facilitando a comunicação entre os agentes envolvidos como engenheiros, projetistas, marketing e produção.

As empresas podem assim trabalhar de modo mais eficiente, reduzindo custos e lançando produtos mais rapidamente no mercado. Se os fornecedores são ligados diretamente à empresa por meio da Extranet, podem acelerar o prazo de entrega dos produtos.

É claro que para que essa sinergia entre as empresas aconteça é necessário que as empresas tenham se preparado para a integração. A empresa também deve se preparar para atender à nova forma de trabalho voltada para o atendimento da demanda do cliente. Processos de negócios devem ser reavaliados, principalmente aqueles ligados a cadeia de suprimentos. As empresas devem criar políticas de compartilhamento de informações para decidir que informações compartilhar, o formato e critérios de segurança.

© 2011 - AIEC - Associação Internacional de Educação Continuada



10

4 - B2B E B2C

Existem diferentes formas de classificar as transações de comércio eletrônico. A mais conhecida é a que leva em consideração a natureza dos participantes da transação que podem ser essencialmente de dois tipos: de empresa para empresa e de empresa para consumidor.

No comércio eletrônico de empresa para empresa, também chamado de B2B (*business to business*), a venda é de bens e serviços entre empresas. Estima-se que o volume de transações entre empresas na internet seja superior a dez vezes o volume de transações entre empresas e consumidores finais.

As transações comerciais entre empresas concentram-se em duas modalidades: a troca de informações, que se refere a preços, contratos, envio de documentos eletrônicos, e pagamentos.

A modalidade de transação são os mercados e os leilões virtuais. No caso dos e-marketplaces, as empresas se cadastram em sites especializados que permitem aos seus associados disponibilizarem os seus produtos e comprarem produtos de outras empresas associadas. Nesse caso, as empresas interessadas podem negociar diretamente o preço dos produtos.

Nos leilões, a oferta é pública e é a empresa que pagar mais ou a que cobrar menos que ganhará a concorrência. Atualmente o governo está incentivando a aplicação de pregões eletrônicos, principalmente em compras de baixo valor de forma a reduzir o custo da licitação e aumentar a transparência para a sociedade. Aliás, o pregão eletrônico acabou impulsionando o mercado de pequenas e médias empresas que no sistema de licitação tradicional, acabavam ficando de fora, devido aos complexos e caros trâmites burocráticos.

11

No comércio eletrônico de empresa para consumidor, chamado de B2C (*business to consumers*), a venda de bens e serviços é realizada no varejo diretamente ao consumidor final. Essa modalidade só tende a aumentar na medida em que o acesso à Internet for sendo ampliado.

© 2011 - AIEC - Associação Internacional de Educação Continuada

Uma vez conectado, o internauta pode acessar a milhares de lojas virtuais, comparar preços, se informar sobre o produto e concretizar a sua compra, e isso tudo sem sair de dentro de casa. Existem inclusive sites especializados em comparação de preços (www.bondfaro.com.br) que aceleram ainda mais o processo de comparação de preços e a decisão do usuário.

No intuito de fidelizar o cliente, as empresas também têm investido bastante em tecnologias de personalização, que permitem a customização da navegação e/ou de itens do site específicos para o cliente. Um exemplo é o site Submarino, que, uma vez cadastrado no site, a cada novo acesso, você recebe a mensagem de boas-vindas. O site da Amazon registra as suas últimas compras e sugere produtos similares. Outra forma de conquistar clientes é a chamada lista de desejos que permite que você selecione produtos que você gostaria de adquirir. No site Yahoo, o usuário pode escolher a interface que deseja no site e disponibiliza o tipo de informação que ele tem interesse.

Vemos então que a tecnologia está tornando o comércio eletrônico cada vez mais simples, fácil e atrativo para os clientes, trazendo conveniência, poupando tempo e dinheiro, visto que o cliente pode comparar os preços em diferentes lojas para tomar decisão de compra. Entretanto, um fator que ainda afasta uma parcela dos consumidores do comércio eletrônico é o sistema de pagamento.

O pagamento por meio eletrônico (cartão de crédito ou débito) é considerado seguro, mas alguns consumidores ainda desistem de comprar quando o único meio de pagamento é o cartão. Para driblar essa relutância, as empresas tiveram que se adaptar e hoje todas as grandes empresas possibilitam o pagamento de compras utilizando outros meios de pagamento, como boletos bancários, depósitos em conta ou mesmo via televendas.

Alguns autores costumam incluir mais um tipo, o chamado consumidor para consumidor (C2C – consumer to consumer), que seria o caso dos leilões como o mercadolivre, entretanto, podemos verificar que existem sempre empresas intermediando a transição, logo essencialmente consiste de uma transação de empresa para consumidor (B2C).

12

5 - WEB DATABASES

Quando você procura um produto na Internet, não é suficiente acessar a página principal da loja, você quer saber detalhes sobre o produto, saber preço, disponibilidade e pesquisar outras informações. Se você está com dúvidas sobre a utilização de um produto, você acessa o site do fabricante e procura catálogos, ou então consulta a FAQ, ou mesmo procura fóruns de usuários que tiveram o mesmo problema.

Em todos esses casos, está acessando bancos de dados. Assim, se você quer que sua empresa disponibilize informações que ajudem os seus clientes a conhecerem melhor os seus produtos, obterem informações que o ajudem a optar por seus produtos, que melhorem a comunicação entre a empresa e

© 2011 - AIEC - Associação Internacional de Educação Continuada

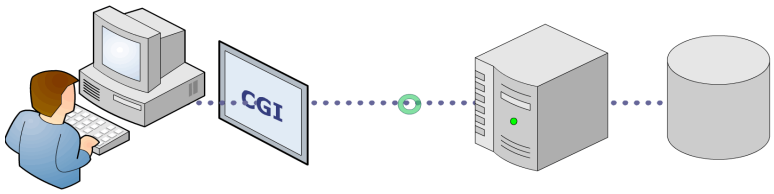
o cliente, então a empresa deve conectar o seu sistema de banco de dados da empresa à Internet. Isso permite que os clientes tenham acesso ao banco de dados por meio do Browser do PC. Os usos mais comuns para os bancos de dados na Web são:

- Disponibilização de catálogos online: utilizado para a apresentação de produtos, normalmente permitindo que o cliente realize buscas por palavras-chave e código de itens.
- Lista de Contatos: lista de nomes, telefones e e-mails importantes.
- Cadastro de clientes: esse cadastro implementado por meio de formulários disponíveis no site permite que a empresa conheça melhor os seus clientes e pode servir para o envio de mensagens eletrônicas de interesse do cliente: novidades, atualizações, etc.
- Rastreamento de encomendas: uma ferramenta importante pós-venda que permite que o usuário consulte a tramitação da sua encomenda até a sua recepção. Por exemplo, o cliente poderá saber se a controladora do cartão já liberou a compra, se o produto já foi enviado, pontos de verificação ou parada antes da chegada e a data provável de entrega.
- Transações financeiras: em todas as transações bancárias, é necessário acessar o registro do cliente.

13

O grande benefício das bases de dados estabelecidos na Web é que permitem que o cliente acesse os bancos de dados por meio de navegadores, como o Internet Explorer ou Firefox. Entretanto, para que isso seja possível, é necessário que seja criada uma interface entre o navegador e a base de dados que permita a interatividade entre a página Web vista pelo usuário e a aplicação SGDB, que está no servidor.

As páginas Web que utilizam apenas HTML ou XHTML não permitem tal interatividade, por isso deve ser criada uma interface entre o navegador e o SGDB. As interfaces mais comuns utilizam: **scripts CGI** (Common Gateway Interface), **java server pages** (JSP), **java servlets** ou **ASP** (Active Servers Pages). Um exemplo de funcionamento utilizando o CGI para o acesso a um banco de dados é mostrado na figura a seguir.



O CGI especifica como os dados vindos do cliente WEB serão passados ao programa (script CGI) e como este programa deve retornar o resultado ao servidor WEB. Quando o usuário terminar de preencher um formulário na Web, o navegador acessará uma página com um script CGI. O servidor executa o script CGI (um programa) que verifica os valores inseridos no formulário e o CGI faz as solicitações em linguagem DML (*data manipulation language*) ao SGDB. Os dados solicitados ao SGDB são recuperados pelo CGI, que formata os resultados em formato HTML para serem apresentados no navegador.

© 2011 - AIEC - Associação Internacional de Educação Continuada

14

O profissional de TI deve considerar alguns pontos importantes antes de disponibilizar a base de dados na Web que são:

- Que aplicação será usada.
- Como assegurar que não haja conflitos entre os dados que estão sendo acessados por diferentes usuários na internet.
- Como manter a segurança.

Este último ponto é de extrema importância, pois a empresa deve ter consciência que, a partir do momento em que um banco de dados é disponibilizado na Internet, existe um risco que usuários não autorizados consigam acessá-lo e alterá-lo.

Ambiente jurídico do comércio eletrônico - Outro aspecto que deve ser discutido é a questão legal. Hoje em dia ainda não existem leis específicas para o comércio eletrônico. Os organismos ainda estão se adaptando a essa nova modalidade de comércio. Ainda se discute tópicos como o valor jurídico dos contratos eletrônicos e a validade da assinatura digital. Entretanto, parece haver um consenso de que até o momento não houve um prejuízo importante pelo fato do arcabouço jurídico ainda não ter sido concluído.

15

RESUMO

A Internet teve um enorme desenvolvimento nos últimos anos. A integração de novas tecnologias de comunicação com softwares revolucionou a forma de as pessoas e empresas se comunicarem e fazerem negócios. Por isso a importância de o administrador conhecer o funcionamento e as aplicações disponíveis na Internet para que suas empresas participem dessa revolução e marquem presença no mundo virtual.

Internet é uma gigantesca rede mundial de computadores interligados por linhas comuns de telefone, linhas de comunicação privadas, cabos submarinos, canais de satélite e diversos outros meios de telecomunicação. Todo computador na Internet possui um número de identificação único que é o chamado de endereço IP. As aplicações e os protocolos de Internet permitem então que um computador localize e seja conectado a outro computador na internet. As aplicações mais comuns são: navegação Web, envio e recebimento de e-mails (Correio eletrônico), transferência de arquivos, troca de Mensagens instantâneas e telefonia Internet (VoIP).

Além da internet, as empresas têm utilizado outras duas redes: as intranets e as extranets. A intranet é uma rede privada (só acessível pelos funcionários), que serve para disseminar informação de interesse dos funcionários dentro da empresa e também pode servir como ponto de acesso aos sistemas de gerenciamento e controle. A chamada extranet é uma rede que liga a empresa a fornecedores, a empresas clientes ou a empresas parceiras.

A internet impulsionou o comércio eletrônico que, geralmente, é classificado segundo a natureza dos participantes da transação, que podem ser essencialmente de dois tipos: de empresa para empresa (B2B - business to business) e de empresa para consumidor (B2C - business to consumers). Mas, para que

© 2011 - AIEC - Associação Internacional de Educação Continuada

esse comércio eletrônico seja possível, é preciso conectar as bases de dados das empresas à Internet, que é o conceito de Web Databases. O grande benefício das bases de dados baseadas na Web é que se permite que o cliente acesse os bancos de dados por meio de navegadores, como a Internet Explorer ou Firefox. Por fim, foram discutidas as questões legais ligadas ao comércio eletrônico. Ressaltando que ainda não existem leis específicas para o comércio eletrônico no Brasil, e os organismos ainda estão se adaptando a essa nova modalidade de comércio.

UNIDADE 3 – A GESTÃO DO CONHECIMENTO – CAPTURANDO, CRIANDO, MANTENDO E DISSEMINANDO O CONHECIMENTO DA EMPRESA DIGITAL.

MÓDULO 4 – SEGURANÇA

01

1 - A IMPORTÂNCIA DA SEGURANÇA

"A segurança é um processo. Pode-se aplicar o processo seguidamente à rede e à empresa que a mantém e, dessa maneira, melhorar a segurança dos sistemas. Se não se iniciar ou interromper a aplicação do processo, sua segurança será cada vez pior, à medida que surgirem novas ameaças e técnicas."
Wadlow (2000).

As empresas possuem variados sistemas de informações que executam funções vitais para seu processo administrativo. Esses sistemas operam nas áreas de contabilidade, financeira, de controle de material, de produção, de recursos humanos, de faturamento, de atendimento ao cliente, entre outras, exercendo atividades em praticamente todos os setores. Assim, a empresa mantém uma relação de dependência grande com os serviços prestados por seus sistemas de informação.

As informações processadas e armazenadas constituem um bem precioso da organização, pois além de servirem ao funcionamento e à gestão da empresa, dizem respeito a aspectos confidenciais de clientes e da própria empresa. Por isso é tão importante a proteção dessas informações contra eventuais danos ou para evitar o acesso por pessoas alheias aos interesses da empresa.

As informações processadas e armazenadas nas organizações, além de serem fundamentais ao seu funcionamento e gestão, podem ser confidenciais de cliente. Nesse caso, um esforço dobrado deve ser envidado em questões de segurança. Um exemplo disso é o caso de informações bancárias de clientes: o saldo de clientes não pode ser acessado por pessoas não autorizadas, que podem planejar ações com

© 2011 - AIEC - Associação Internacional de Educação Continuada

base nessa informação – de estelionato a sequestro.

No caso de um hospital, por exemplo, o sistema contém todo o acompanhamento do paciente. É crucial que somente pessoas relacionadas com a efetiva prestação do serviço médico acessem o sistema e atualizem as informações.

Um caso verídico de falta de segurança nas informações – especificamente no tráfego via correio eletrônico – é o do laboratório farmacêutico Eli Lilly. O site www.ITWeb.com.br publicou em 2001 o caso do laboratório, que, inadvertidamente, no início de julho de 2001, divulgou os endereços eletrônicos de alguns pacientes com depressão, bulimia ou desordem obsessivo-compulsiva. Isso ocorreu devido a uma mensagem de 27 de junho, que listava os endereços eletrônicos de cerca de 600 pessoas que assinaram um serviço de Internet da empresa que enviava mensagens para que as pessoas se lembrassem de tomar o antidepressivo Prozac.

Ao longo dos últimos dois anos, as mensagens foram dirigidas apenas aos indivíduos. Em junho daquele ano, foi enviada uma mensagem aos participantes - por causa de uma falha de programação, com todos os endereços eletrônicos - anunciando o fim do programa. Foi prejudicada a imagem da empresa, que está respondendo a diversos processos judiciais. O transtorno poderia ter sido evitado se um mecanismo de segurança averiguasse as operações via correio eletrônico.

02

Como dar segurança aos Sistemas de Informação?
- Para garantir a segurança das informações, são necessários controles de segurança lógica, por intermédio de senhas, e controles de segurança física, que restringem o acesso aos equipamentos de processamento de dados apenas para pessoas autorizadas.

Muitas empresas desprezam a questão da segurança, porque:

- Acreditam que os sistemas são invulneráveis ("um sistema com esse custo é imune a problemas").
- Acham que problemas de acesso não autorizado ou desastres nunca atingirão sua organização ("isso nunca vai acontecer na minha empresa").
- Desconhecem os transtornos causados por falta de segurança.
- Imaginam que investir em segurança custa muito caro.

É necessário um planejamento consistente para proteger o sistema contra possíveis invasões e contra problemas provenientes do tempo, como desastres naturais. Deve-se investir em prevenção para controlar também riscos oriundos do desenvolvimento tecnológico.

Será que é tão grave perder informações**?**
- É preciso, antes de tudo, que a empresa tenha consciência da importância dos procedimentos de

© 2011 - AIEC - Associação Internacional de Educação Continuada

segurança, e do transtorno que a perda das informações* traz à empresa. É preciso refletir sobre as seguintes questões:

- O que se quer proteger?
- Contra o quê ou quem?
- Quais as ameaças prováveis?
- Qual a importância de cada recurso?
- Qual o grau de proteção desejado?
- Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança?
- Quais as expectativas dos usuários e clientes em relação à segurança de informações?
- Quais serão as consequências para a instituição, se suas informações forem corrompidas ou roubadas?

03

World Trade Center - Após luto, desafio será a recuperação dos dados

O Vale do Silício foi particularmente atingido pelo ataque da terça-feira, 11 de setembro de 2001, não apenas porque muitas empresas tinham escritórios em Nova York e nas torres do World Trade Center (WTC), mas também porque contavam com empresas da Wall Street e arredores entre seus clientes. Para dificultar a situação, nas torres estavam localizados os sistemas chamados de back-office e suporte, que são essenciais para a operação de Wall Street. "Esse poderá ser o evento mais desafiador da história dos negócios nos Estados Unidos", disse William Malik, especialista em segurança de informações na Gartner Group. Todas as empresas, disse ele, têm seus planos de emergência para salvar dados e sistemas em caso de incêndios ou terremotos. E boa parte desses dados e sistemas, acredita ele, devem estar salvos. O problema principal seria a perda de vidas - a perda de funcionários que sabiam tudo sobre esses sistemas e dados. Outro analista, Howard Rubin, vice-presidente executivo do Meta Group, não concorda. Ele pondera que ninguém se prepara para um desastre dessas proporções. "Ninguém se planeja para a eventualidade do desaparecimento total do prédio onde o sistema está instalado", disse.

Em desastres anteriores - no atentado ao WTC em 1993, por exemplo -, uma média de 40 empresas transferiu o núcleo de suas operações eletrônicas para centros de recuperação de desastres.

© 2011 - AIEC - Associação Internacional de Educação Continuada

O Meta Group ligou para alguns desses centros no final da tarde de terça-feira e constatou que o número de transferências havia triplicado. Segundo John Jackson, presidente da Comdisco (uma empresa que oferece tais centros de recuperação), a maioria das companhias que o procurou é formada por bancos, seguradoras e outras empresas de serviços financeiros.

A imensa tarefa a que se defrontam agora as empresas do Vale do Silício é o suporte a clientes que precisam recuperar sistemas e dados perdidos no desastre. Não há estimativa, ainda, dos danos causados nessa área fundamental para a economia americana. E, nas empresas, ninguém ainda está preparado para falar do assunto: estão todas concentradas em localizar o paradeiro de funcionários que trabalhavam em Nova York ou estavam em visita de negócios à cidade.
"Não podemos e não devemos fechar nossas portas", escreveu Larry Ellison, o presidente da Oracle, maior fabricante mundial de bases de dados, em e-mail aos funcionários na terça-feira. Ellison lembrou a todos que "agora é mais importante do que nunca prover serviços críticos a todas as instituições que compõem a infraestrutura essencial do país". A Oracle perdeu "alguns" funcionários, um deles como passageiro de um dos aviões sequestrados.

A Sun Microsystems, fabricante de estações de trabalho e servidores de alta performance, demorou a localizar todos os seus 340 funcionários. Todos eles ocupavam dois andares - o 25º e o 26º - da torre Sul do World Trade Center (WTC). Nenhum deles morreu. Mas Phil Rosenzweig, diretor da Sun Software e funcionário desde 1991, estava no voo 11 da American Airlines, um dos seqüestrados, e morreu.

A empresa manteve as portas abertas mesmo na terça-feira, operando principalmente os serviços de suporte a sistemas do tipo missão crítica, "que são agora mais importantes do que nunca". A porta-voz Jo Chun não quis informar quais clientes da Sun precisaram de um suporte de urgência naquele momento.

Na Cisco Systems, maior fabricante de equipamentos para redes de computadores, também demorou o trabalho de localização de funcionários que estivessem viajando ou em Nova York por ocasião dos atentados. O maior fabricante de chips para computador, a Intel, também baseada no Vale, não temeu a perda de funcionário, mas redobrou a segurança em 30 instalações ao redor do mundo, inclusive três em Israel, onde a empresa tem um total de 5 mil funcionários.

O CEO Craig Barrett, que tem uma intensa agenda de viagens, por sorte, estava na sede, em Santa Clara, no Vale do Silício, por ocasião dos atentados.

Já a Hewlett-Packard tinha a maior parte de seus executivos cruzando o país de leste a oeste para explicar a investidores a decisão de comprar a Compaq. A principal executiva, Carly Fiorina, estava em

© 2011 - AIEC - Associação Internacional de Educação Continuada

Palo Alto, onde a empresa tem sede mundial, e todos os demais executivos ficaram bem. "A segurança das instalações da HP em todo o mundo está no mais alto nível de alerta", explicou o porta-voz Dave Berman, sem dar mais detalhes.

04

As respostas para essas perguntas delineiam uma política de segurança adequada à situação da empresa, com suas expectativas. A informação é um ativo que precisa ser protegido adequadamente. O objetivo da segurança é evitar qualquer ameaça à informação, garantindo a continuidade dos negócios, minimizando as consequências dos danos nos sistemas de informação e maximizando o retorno dos investimentos.

Conjunto de valores representado pelas aplicações de patrimônio e de capital de uma empresa ou pessoa (Dicionário Hoauiss da Língua Portuguesa, 2001)

Uma política de segurança consiste em uma série de decisões que determinarão a postura de uma organização em relação à segurança. Esse conjunto de ações, que visa a prover segurança, deve determinar os limites de tolerância e os níveis de controle para violações que possam eventualmente ocorrer.

A segurança da informação tem como finalidade a preservação da informação no que se refere a:

- Confidencialidade: acesso à informação somente por pessoas autorizadas.
- Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.
- Disponibilidade: garantia de que os usuários autorizados tenham acesso à informação sempre que necessário.

É importante saber que a segurança deve fazer parte da cultura da empresa e de seus procedimentos de rotina. Só uma ação de todos os funcionários, dos diversos níveis hierárquicos, pode assegurar a integridade das informações da empresa.

© 2011 - AIEC - Associação Internacional de Educação Continuada

05

2 - AMEAÇAS À SEGURANÇA

Quais são as principais ameaças ao SI?

Os principais problemas relacionados à segurança nos sistemas de informações organizacionais decorrem de erros humanos, falta de procedimentos de segurança e má configuração dos sistemas.

Gil (1994) definiu a natureza das agressões que os recursos de informática podem sofrer:

Interrupção de operação de hardware, o software, insumos e componentes de informática.

Avaria de máquinas, equipamentos e insumos.

Avaria de máquinas, equipamentos e dispositivos de processamento eletrônico de dados e paralisação total ou parcial dos aplicativos de informática.

Compreensão do funcionamento das redes de informática, com fins de sabotagem.

Subtração de recursos materiais, desestabilizando a continuidade operacional e causando danos ao patrimônio organizacional. Em muitos casos, as ameaças à segurança das informações acontecem dentro da própria empresa.

O site www.intermanagers.com.br divulgou, em 2000, um fato ocorrido com a Companhia Telefônica de Estado de São Paulo: a lista telefônica da companhia estava à venda nos camelôs da cidade, em CD-ROM, por R$ 10. No CD-ROM podiam ser encontrados inclusive os dados dos anunciantes que optaram por não divulgar o número do seu telefone, entre políticos, artistas e outras pessoas famosas.
A apropriação indébita de todo o banco de dados de assinantes não pôde ser resultado da ação de um hacker, via Internet. O banco de dados de assinantes certamente foi copiado por um funcionário da companhia, que provavelmente revendeu estes dados a terceiros, que fizeram as cópias e as

© 2011 - AIEC - Associação Internacional de Educação Continuada

entregaram para venda pelos camelôs.

Além da divulgação de um patrimônio sigiloso da organização, a companhia pode ser processada pelas pessoas que tiveram a sua privacidade invadida, por meio da revelação do número do telefone.

Destruição dos recursos computacionais.

Avaria parcial ou total dos recursos computacionais.

Espontâneo ou por má conservação de instalações, pode provocar avaria parcial ou total dos recursos computacionais.

Destruição ou avaria aos equipamentos e insumos de informática.

06

Os principais problemas em relação à falta de segurança lógica em sistemas de informação são:

- Centralização física dos dados - tanto os dados quanto os backups ficam no mesmo local físico, o que concentra o risco.
- Fraco treinamento dos profissionais de informática e dos usuários com a tecnologia de segurança, inclusive com barreiras culturais (‘isso nunca vai acontecer comigo!’).
- Dificuldades na repreensão por ações erradas, dolosas e inadequadas.
- Descaso com a segurança em informática, falta de determinação explícita de responsabilidades e falta de especialista na tecnologia de segurança do ambiente computacional.
- Falta de um plano de contingência.

A Internet aumentou ainda mais as preocupações com segurança das informações nas organizações. Os hackers podem invadir os sistemas das empresas pela Internet, acessar informações e mudar o conteúdo dos sites.

O Plano de Contingência é um conjunto de procedimentos que orienta os membros das organizações em situações adversas, como incêndio, desastre, roubo de um equipamento importante, entre outros. Assim como agir corretamente no socorro a uma vítima de acidente é fundamental para a sua sobrevivência, agir corretamente em situações de sinistro também é fundamental para a recuperação das informações da empresa.

© 2011 - AIEC - Associação Internacional de Educação Continuada

Indivíduos hábeis em burlar os mecanismos de segurança de sistemas de computação e em conseguir acesso não autorizado aos seus recursos, geralmente a partir de uma conexão remota (em local físico diferente), em uma rede de computadores.

Possibilidade de um evento, no caso, um problema de segurança, acontecer ou não.

07

A Internet facilitou a ação dos hackers. As ameaças por meio da Internet podem ser:

- Perda de integridade de dados: a informação é criada, modificada ou apagada por um intruso.
- Perda de privacidade de dados: a informação é acessada por pessoas não autorizadas .
- Perda de serviço: um serviço é interrompido devido à ação de um hacker.
- Perda de controle: os serviços são usados por pessoas autorizadas de um modo não controlado.

Algumas empresas, mesmo tendo mecanismos de segurança, são atacadas por intrusos. Como isso é possível? Os ataques podem ser feitos por meio de:

- Monitoração de comunicação entre duas partes que estejam trocando informações.
- Roubo do software e/ou hardware.
- Interceptação da saída eletromagnética do monitor - o intruso pode reproduzir em seu microcomputador uma operação que está sendo feita por um usuário autorizado, e assim ter acesso a dados importantes como número do cartão de crédito, senhas, entre outras.
- Utilização de 'cavalos de tróia'.
- Falsificação (spoofing) de IP.
- Recursos de mídia descartados pela empresa, como, por exemplo, disquetes.
- Suborno do pessoal de segurança, para que facilitem a entrada do intruso.

Além das ameaças de acesso por pessoas não autorizadas, os vírus representam outro grande problema para as organizações. Mesmo com a instalação de programas antivírus, é possível ter o computador atacado, pois novos vírus cada vez mais destruidores e complexos de combater são criados diariamente.

Cada microcomputador conectado a rede possui um endereço de IP – Internet protocol, composto por 10 dígitos (Ex.: 193.123.42), que o individualiza na rede. Sua falsificação se dá da seguinte forma: alguns sites só podem ser acessados por determinados endereços IP. Falsificando o IP de um micro, o hacker consegue acessar uma área que não acessaria pelo seu endereço de IP.

Programa estranho ao sistema de computador capaz de copiar e instalar a si mesmo, geralmente concebido para provocar efeitos nocivos ou estranhos à funcionalidade do sistema ou aos dados nele armazenados.

08

São pequenos softwares que parecem inofensivos, mas que coletam informações do sistema ou do

© 2011 - AIEC - Associação Internacional de Educação Continuada

usuário e as enviam via Internet ou rede ao intruso ou hacker.
Talvez ainda não tenha ouvido falar sobre eles. Talvez já, mas sem dar muita importância. Mas está na hora de se tomar cuidado com esses programas. Cavalos de Tróia são programas que vêm causando danos a determinados usuários da Internet. Saiba como eles funcionam e como podemos nos manter fora da área de risco.

Atualmente, muitos recursos têm sido amplamente utilizados para invadir máquinas ligadas à Internet. A tática é simples: envia-se um programa, como por exemplo, um screensaver, que na verdade contém um outro programa que dá ao hacker acesso remoto à máquina em que o cavalo de Troia foi instalado. Esses programas são portas de acesso ao conteúdo do computador.

Independentemente do sistema operacional, os Cavalos de Troia permitem que outra pessoa tenha controle sobre a sua máquina, por meio do protocolo TCP/IP da Internet.

Testes demonstraram que o administrador remoto é capaz de acessar os dados e efetuar tarefas com mais eficiência do que o próprio usuário que está em frente à máquina.

Geralmente os Cavalos de Troia não são vírus. Eles apenas permitem que uma pessoa execute, a distância, as mesmas tarefas disponíveis para quem senta em frente do computador. Sozinhos, não causam danos aos programas. É preciso que haja alguém (um hacker) trabalhando com o sistema de forma remota. São pequenos softwares que parecem inofensivos, mas que coletam informações do sistema ou do usuário e as enviam via Internet ou rede ao intruso ou hacker.
Talvez ainda não tenha ouvido falar sobre eles. Talvez já, mas sem dar muita importância. Mas está na hora de se tomar cuidado com esses programas. Cavalos de Tróia são programas que vêm causando danos a determinados usuários da Internet. Saiba como eles funcionam e como podemos nos manter fora da área de risco.

Atualmente, muitos recursos têm sido amplamente utilizados para invadir máquinas ligadas à Internet. A tática é simples: envia-se um programa, como por exemplo, um screensaver, que na verdade contém um outro programa que dá ao hacker acesso remoto à máquina em que o cavalo de Troia foi instalado. Esses programas são portas de acesso ao conteúdo do computador.

Independentemente do sistema operacional, os Cavalos de Troia permitem que outra pessoa tenha controle sobre a sua máquina, por meio do protocolo TCP/IP da Internet.

Testes demonstraram que o administrador remoto é capaz de acessar os dados e efetuar tarefas com mais eficiência do que o próprio usuário que está em frente à máquina.

Geralmente os Cavalos de Troia não são vírus. Eles apenas permitem que uma pessoa execute, a

© 2011 - AIEC - Associação Internacional de Educação Continuada

distância, as mesmas tarefas disponíveis para quem senta em frente do computador. Sozinhos, não causam danos aos programas. É preciso que haja alguém (um hacker) trabalhando com o sistema de forma remota.

09

Há diferentes tipos de vírus:

- Vírus de setor de boot: reside no setor de boot da máquina e, toda vez que o computador é inicializado, o vírus é ativado, infectando os arquivos no disco rígido.
- Vírus de programa executável: trabalha infectando arquivos executáveis (por exemplo, programas e bibliotecas).
- Vírus de macro: na maioria dos casos, infectam o Microsoft Word e o Excel, são aplicações muito adotadas no seu gênero.

De acordo com a complexidade do vírus, ele pode trazer diferentes danos ao usuário:

- Aborrecedor: exibe mensagens na tela, mas não causa dano real.
- Pouco ofensivo: exibe mensagens em sua tela e impede a execução de programas, mas não causa nenhum dano permanente.
- Prejudicial: destrói dados do programa infectado, mas todos os outros dados do microcomputador permanecem intactos.
- Destrutivo: destrói todos os dados e impede o funcionamento do computador.

É preciso ter programas antivírus instalados em todos os microcomputadores e fazer a atualização periódica destes programas, para se ter mais sucesso na proteção do microcomputador.

Programas que combatem vírus. Um bom programa antivírus deve ter três procedimentos:

- **Scanner: verifica todos os arquivos nos discos rígidos locais, disquetes e *drives* de rede.**
- **Proteção: procura por vírus quando são carregados softwares da Internet, ou é inserido um disquete.**
- **Limpador: remove o vírus localizado, por intermédio do uso de vacinas (*Programas elaborados para a neutralização de vírus de computador. Cada vírus precisa de uma vacina específica*.).**

10

3 - Implementando segurança de dados e informações

Como definir uma política de segurança? O ponto fundamental para o desenvolvimento de uma política de segurança é a consciência das ameaças que o sistema pode sofrer e do transtorno – muitas vezes irreversível – que podem causar.
É preciso definir políticas de segurança e torná-las conhecidas, contribuindo, assim, para a formação de uma cultura de segurança.

A segurança de dados é fundamental para fornecer às organizações:

© 2011 - AIEC - Associação Internacional de Educação Continuada

- Confidencialidade: é necessária para controlar quem lê as informações e para impedir o acesso de pessoas não autorizadas.
- Integridade: precisa assegurar que as informações e programas são alterados somente de maneira prevista e autorizada, e que os dados apresentados são genuínos e não foram alterados durante a transmissão.
- Disponibilidade: precisa garantir que usuários autorizados continuem tendo acesso a informações e recursos.
- Legitimidade: recursos não podem ser usados por pessoas ou de forma não autorizadas.

As preocupações com segurança podem ser divididas em três grupos: infraestrutura, recursos humanos e recursos técnicos.

Separação física de ambientes com atividades diferentes	A separação de locais onde são executadas atividades de natureza muita diversa protegem a informação. Por exemplo, em uma indústria, deixar em local mais elevado a parte administrativa e em local mais baixo a industrial.
Energia	É importante a existência de geradores ou de *no-breaks*, para que as operações sejam salvas em caso de falta de energia elétrica.
Ar condicionado	Para o bom funcionamento de alguns equipamentos de informática, como servidores ou supercomputadores, a temperatura média e constante é fundamental.
Radiação eletromagnética	Equipamentos como disquetes e winchesters podem perder os dados se ficarem próximos à radiação eletromagnética proveniente de ímãs, autofalantes, entre outros objetos.
Proteção física	Barreiras físicas, como leitoras de cartão magnético, de retina, de impressão digital, para garantir o acesso aos equipamentos de informática apenas por pessoas autorizadas.

© 2011 - AIEC - Associação Internacional de Educação Continuada

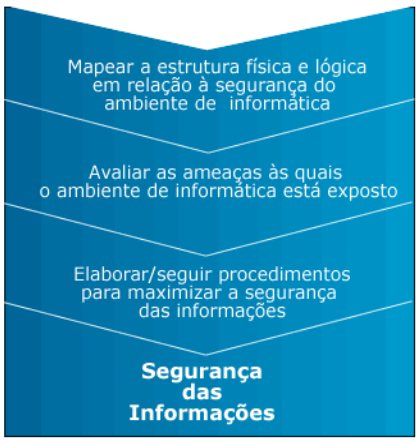
Equipamento dotado de bateria, que se destina a suprir falhas na alimentação da rede elétrica, mantendo o fornecimento de eletricidade por determinado período de tempo e evitando interrupção no funcionamento dos aparelhos a ele conectados.

Proteção lógica	Barreiras lógicas, tais como senhas, para garantir o acesso aos equipamentos de informática apenas por pessoas autorizadas.
Controle de acesso	É preciso saber que o sistema foi acessado indevidamente, por quem, em que data, em que horário, quais as operações efetuadas, se alguma informação foi enviada por *e-mail*.
Conscientização	Deve-se criar uma cultura de segurança. As pessoas precisam se conscientizar da importância da segurança e dos transtornos causados pela falta dela.

Integridade dos dados	Fornecer meios para que os dados da empresa estejam sempre corretos.
Confiabilidade	Proteger o sistema de modo que os dados da empresa não sejam modificados indevidamente.
Integridade dos sistemas	Desenvolver sistemas que não permitam invasões.
Integridade das redes	Configurar as redes de forma que não permitam invasões, já que os ataques sempre ocorrem por meio das redes, seja interna da empresa, Internet ou intranet.

11

Segurança é coisa séria.
A figura abaixo resume o que é preciso fazer para implementar segurança das informações na empresa.



© 2011 - AIEC - Associação Internacional de Educação Continuada

Uma maneira muito usada de dificultar a leitura de informações por intrusos é a criptografia. Foi criada durante a segunda guerra mundial, quando os exércitos usavam estórias e senhas para impedir a decifração de mensagens por inimigos que as conseguissem interceptar.

Arte de escrever em cifra ou em código, utilizando um conjunto de técnicas que permitem codificar informações, como mensagens escritas, dados armazenados ou transmitidos por computador, tornando possível sua compreensão apenas por quem tem a chave de decifração do código.

12

4 - POLÍTICA DE SEGURANÇA

Temos de buscar prever tudo o que pode acontecer...

Política de segurança consiste em uma série de decisões que determinam a postura de uma organização em relação à segurança.

Esse conjunto de ações que se propõem a prover segurança deve determinar os limites de tolerância e os níveis de controle para violações que possam eventualmente ocorrer (SUAVÉ et alii, 1999).

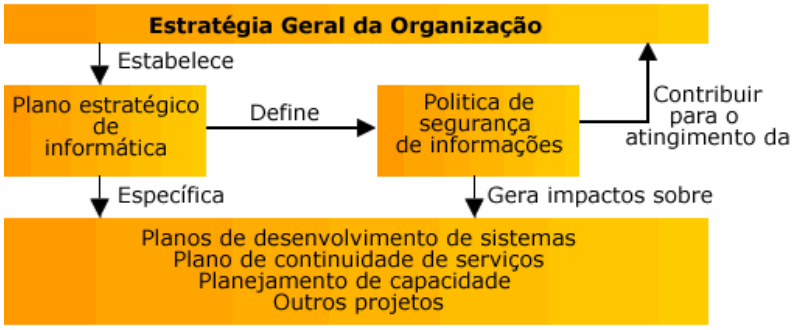
Uma política de segurança deve atender aos seguintes propósitos, segundo Wadlow (2000):

- Definir o que está sendo protegido, e por quê.
- Definir prioridades de proteção e custos.
- Fornecer ao departamento de segurança motivos válidos para as restrições.
- Conceder ao departamento de segurança a autoridade necessária para sustentar as ações de segurança.
- Estabelecer um acordo explícito com as várias partes da empresa em relação à importância da segurança.

De novo, todos têm de estar envolvidos...
É importante que toda a organização esteja envolvida na definição da política de segurança, pois ela faz parte da estratégia geral da organização.

13

Na verdade, a política de segurança afeta e é afetada pela organização, conforme se pode observar:



© 2011 - AIEC - Associação Internacional de Educação Continuada

Para definir adequadamente uma política de segurança, é preciso:

- Fazer uma lista de todos os recursos que precisam ser protegidos.
- Definir quem tem acesso físico ao hardware e acesso lógico ao software.
- Catalogar as ameaças para cada um dos recursos.
- Realizar uma análise de risco, mostrando a probabilidade de cada ameaça.
- Avaliar que ameaças podem ser ignoradas em curto prazo, e quais precisam ser consideradas.
- Fazer constantes avaliações e atualizações em busca de novas ameaças ou falha na segurança.

14

5 - NORMAS DA SEGURANÇA DE DADOS E INFORMAÇÕES

Há normas oficiais de segurança?

A segurança em tecnologia da informação é tão importante que já há um código de prática para a gestão da segurança da informação.

A NBR ISO/IEC 17799, elaborada pela Associação Brasileira de Normas Técnicas (ABNT), é a tradução da ISO/IEC 17799 *Information technology - Code of Practice for information security management.*

O objetivo da NBR ISO/IEC 17799 é fornecer recomendações para a gestão da segurança da informação, servindo como base para que se desenvolvam normas de segurança organizacional.

A segurança da informação é obtida com a implementação de controles implementados por políticas, procedimentos, práticas e estruturas organizacionais, de acordo com a NBR ISO/IEC 17799 (2001).

As organizações e os seus sistemas são colocados à prova constantemente por diversos tipos de ameaças à segurança das informações. Essas ameaças podem ser fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo ou inundação, problemas causados por vírus e hackers, segundo a NBR ISO/IEC 17799.

Quais são os requisitos de segurança?

Essa norma também define que é importante para a organização identificar os seus requisitos de segurança. Existem três fontes principais:

- A primeira é derivada de uma avaliação de risco dos ativos da organização, para que sejam identificadas as ameaças, as vulnerabilidades e sua probabilidade.
- A segunda é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais aos quais a organização, seus parceiros, contratados e prestadores de serviço têm que atentar.
- A terceira são os objetivos e requisitos de processamento de informação que uma organização tem que estabelecer para apoiar suas operações.

15

A avaliação dos riscos de segurança é uma consideração sobre o impacto nos negócios causado por falha de segurança, e da probabilidade dessa falha ocorrer, considerando as ameaças e as vulnerabilidades

© 2011 - AIEC - Associação Internacional de Educação Continuada

mais frequentes e os controles já implementados.

Também há fatores críticos de sucesso?
A implementação da segurança da informação dentro de uma organização possui alguns fatores críticos de sucesso:

- Política de segurança, objetivos e atividades, que reflitam os objetivos do negócio.
- Enfoque para a implementação da segurança coerente com a cultura organizacional.
- Comprometimento e apoio da direção.
- Bom entendimento dos requisitos de segurança, avaliação e gerenciamento de risco.
- Divulgação eficiente da segurança para todos os gestores e funcionários.
- Distribuição das diretrizes sobre as normas e política de segurança da informação para todos os envolvidos.
- Educação e treinamento adequados.

A área de segurança é relativamente nova e carece de profissionais com qualificação adequada para o exercício de suas atividades. A NBR ISO/IEC 17799, além de definir procedimentos e metas em relação à segurança das informações, orienta o trabalho desses profissionais.

16

RESUMO

As informações processadas e armazenadas constituem um bem precioso da organização, pois além de servirem ao funcionamento e à gestão da empresa, dizem respeito a aspectos confidenciais de clientes e da própria empresa. Por isso é tão importante a proteção dessas informações contra eventuais danos ou para evitar o acesso de pessoas alheias aos interesses da empresa.
Para garantir a segurança das informações, são necessários controles de segurança lógica, por intermédio de senhas, e controles de segurança física, que restringem o acesso aos equipamentos de processamento de dados apenas para pessoas autorizadas.

Muitas empresas desprezam a questão da segurança por acreditar que os sistemas são invulneráveis, por achar que problemas de acesso não autorizado ou desastres nunca atingirão sua organização, por desconhecer os transtornos causados pela falta de segurança e por supor que é muito caro investir em segurança. Por tudo isso, é necessário que seja desenvolvida uma consciência da importância dos procedimentos de segurança e dos transtornos que a perda das informações pode causar.

A organização pode sofrer ameaças à sua segurança como sabotagem, terrorismo, espionagem, roubo e furto, acidente, explosão, desabamento, incêndio e inundação. No que se refere à segurança lógica, muitos problemas decorrem da centralização física dos dados, do treinamento insuficiente dos envolvidos nas questões de segurança, da dificuldade de repreender ou punir responsáveis por atos dolosos, do descaso e da falta de um plano de contingência. A Internet tornou-se mais uma porta de acesso para hackers, que podem provocar danos à integridade das informações, perda de privacidade, interrupção de serviços e perda do controle das funções dos sistemas. Mesmo adotando procedimentos de segurança, a empresa pode ser atacada de diversas formas.

© 2011 - AIEC - Associação Internacional de Educação Continuada

Programas antivírus devem ser rotineiros na empresa, para evitar os diferentes danos que podem ser provocados por vírus. A segurança de dados é fundamental para proporcionar às organizações confidencialidade, integridade, disponibilidade e legitimidade.

As preocupações com segurança podem relacionar-se à infraestrutura, recursos humanos e recursos técnicos. Por infraestrutura entende-se separar fisicamente ambientes com atividades diferentes, instalar bom ar condicionado, evitar radiação eletromagnética, garantir a fonte de energia com no-breaks e proteger fisicamente o acesso aos equipamentos de informática. No que concerne a recursos humanos, pode-se implantar proteção lógica, controle de acesso e incentivar a formação de uma cultura de segurança. Já no caso de recursos técnicos, pode-se garantir a integridade e a confiabilidade dos dados e a integridade dos sistemas e das redes. Um recurso amplamente utilizado é a criptografia, que usa técnicas que codificam as informações que trafegam na rede, tornando-as compreensíveis somente a quem tem a chave de decifração do código.

Nesse panorama, é essencial que a organização defina uma política de segurança que faça parte de sua estratégia geral, e que relacione recursos a serem protegidos, que defina funcionários que poderão ter acesso lógico e físico aos sistemas, que liste as possíveis ameaças e respectivas probabilidades que avalie as chances de as ameaças ocorrerem em curto prazo. Constantes atualizações nesse processo garantem uma boa política de segurança.

A questão da segurança já mobilizou diferentes setores organizacionais e já há um código de prática para a gestão da segurança da informação, a NBR ISO/IEC 17799, elaborada pela Associação Brasileira de Normas Técnicas (ABNT). Seu objetivo é fornecer recomendações para a gestão da segurança da informação, servindo como base para que se desenvolvam normas de segurança organizacional.

© 2011 - AIEC - Associação Internacional de Educação Continuada