Comunicado Técnico 86

Outubro, 2008
Campinas, SP

ISSN 1677-9274

Projeto e Implementação de um Modelo de Controle de Acesso para Aplicações Web

Alexandre Iakovlevitch Kopelevitch[1]
Stanley Robson de Medeiros Oliveira[2]

Aplicação Web é o termo utilizado para designar, de uma forma geral, sistemas de informação projetados para utilização através de um navegador, na internet ou em redes privadas - Intranet (Wikipédia, 2008a). Trata-se de um conjunto de programas que é executado em um servidor de HTTP[3] (Web Host). O desenvolvimento da tecnologia Web está relacionado, entre outros fatores, à necessidade de simplificar a atualização e a manutenção, mantendo a base de dados em um mesmo local, de onde é acessada pelos diferentes usuários.

O desenvolvimento de aplicações para Web modifica uma série de conceitos que estamos acostumados a lidar. Por exemplo, uma aplicação WEB executa em um ambiente distribuído, onde cada parte que compõe o programa pode ou não estar localizada em uma máquina diferente.

As aplicações Web são dispostas em camadas. Cada camada é autocontida o suficiente, de forma que a aplicação pode ser dividida em vários computadores em uma rede distribuída (Booch, 2001; Conallen, 1998). A forma mais comum da arquitetura é a aplicação em três camadas: interface com o usuário, lógica do negócio, e banco de dados. Este tipo de arquitetura envolve a separação das funcionalidades, com o objetivo de separar a lógica de apresentação, a lógica de negócio e a lógica de acesso a dados, como pode ser visto na Fig. 1.

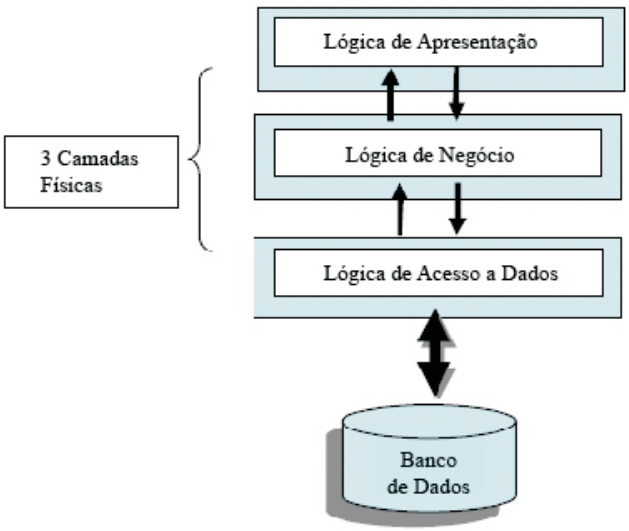

Fig. 1. Arquitetura em três camadas.

A separação em três camadas torna o sistema mais flexível, de modo que partes podem ser alteradas

[1] *Aluno do Curso Superior de Tecnologia em Informática da Unicamp, R. Paschoal Marmo, 1888, Jd. Nova Itália - 13484-332 - Limeira, SP. (e-mail: alexandrekop@gmail.com)*
[2] *Doutor em Ciencia da Computação, Pesquisador da Embrapa Informática Agropecuária, Caixa Postal 6041, Av. André Tosello, 209, Barão Geraldo - 13083-970 - Campinas, SP. (e-mail: stanley@cnptia.embrapa.br)*
[3] **HTTP** (acrônimo para ***Hypertext Transfer Protocol***, que significa ***Protocolo de Transferência de Hipertexto***) é um protocolo de comunicação (na camada de aplicação) utilizado para transferir dados por intranets e pela World Wide Web.

independentemente (Pressman, 2001). Com o emprego de arquitetura em três, qualquer alteração em uma determinada camada não influi nas demais, desde que o mecanismo de comunicação entre elas permaneça inalterado. Isto permite substituir uma camada inteira por outra, independente de que camada seja, como mostra a Fig. 2, ou que um projeto desenvolvido para Web, possa abranger também dispositivos móveis ou *standalone*, a partir da inclusão de uma nova camada de apresentação.

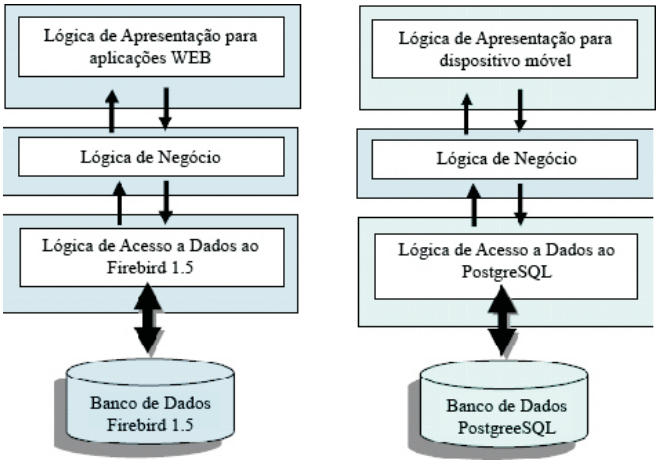

Fig. 2. Exemplo de substituição de camadas.

As principais características da arquitetura Web podem ser sumarizadas como segue: (i) baixos custos de disponibilização; (ii) baixos custos na mudança da base de dados; (iii) baixos custos na mudança da lógica de negócios; (iv) eficiente armazenamento e reutilização de recursos.

A popularidade de aplicações Web está cada dia maior e problemas com segurança estão seguindo o mesmo ritmo de crescimento. A segurança das aplicações, principalmente aquelas conectadas a uma rede aberta e perigosa como é a Internet, é bastante complexa. Esta complexidade advém do fato que as aplicações web, e-commerce, Internet bank, na realidade são agrupamentos bastante heterogêneos de plataformas, bancos de dados, servidores de aplicação, etc. Uma aplicação típica, geralmente, está distribuída em vários servidores, rodando diversos aplicativos e, para funcionar na velocidade adequada, a aplicação precisa que as interfaces entre os diversos sistemas sejam construídas com a premissa que os dados passados através da mesma são confiáveis e não hostis. Não há tempo hábil para duplas verificações.

Um dos mecanismos de segurança para aplicações Web é o controle de acesso (Date, 2004; Ramakrishnan & Gehrke, 2003). O controle de acesso, na segurança da informação, é composto dos processos de autenticação, autorização e auditoria (*accounting*). Neste contexto, o controle de acesso pode ser entendido como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo). A autenticação identifica quem acessa o sistema, a autorização determina o que um usuário autenticado pode fazer, e a auditoria diz o que o usuário fez.

O controle de acesso pode ser visto como a terceira camada de proteção em um sistema de segurança para aplicações Web. A primeira camada refere-se ao *firewall* que consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra. A segunda camada é a autenticação que faz parte de um processo que determina quem pode acessar determinado sistema. Durante a identificação o usuário diz ao sistema quem ele é (normalmente através de um nome de usuário). A identidade é verificada através de uma credencial (uma senha, por exemplo) fornecida pelo usuário. Finalmente, na terceira camada, entra em ação o controle de acesso. Este mecanismo é responsável por garantir que apenas usuários autorizados acessem os recursos protegidos de um sistema computacional. Os recursos incluem arquivos, programas de computador, dispositivos de *hardware* e funcionalidades disponibilizadas por aplicações instaladas em um sistema (Castano et al., 1995).

O objetivo deste trabalho é apresentar um modelo de controle de acesso para aplicações Web (Sistema de Informação sobre o mercado de software brasileiro) e mostrar como ele pode ser reutilizável para outras aplicações que utilizam o paradigma cliente-servidor. A ênfase do trabalho será, portanto, mostrar o modelo de controle de acesso e sua implementação usando software livre.

Modelos de controle de acesso

Vários avanços têm sido feitos na área de especificação e políticas de controle de acesso. Os modelos mais comuns existentes são: controle de acesso discricionário, controle de acesso obrigatório e controle de acesso baseado em papéis (Castano et al., 1995; Sandhu et al., 1996; Ferraiolo et al., 1995; Wikipédia, 2008b). Uma revisão geral de cada um desses modelos será apresentada a seguir.

a) Controle de acesso discricionário

O controle de acesso discricionário (*discretionary access control* ou DAC) é uma política de controle de acesso determinada pelo proprietário (*owner*) do recurso (um arquivo, por exemplo). O proprietário do recurso decide quem tem permissão de acesso em determinado recurso e qual privilégio ele tem. O DAC tem dois conceitos importantes:

I. *Todo objeto em um sistema deve ter um proprietário.* A política de acesso é determinada pelo proprietário do recurso. Teoricamente, um objeto sem um proprietário é considerado não

protegido.

II. *Direitos de acesso e permissões* são dados pelo proprietário do recurso a usuários individuais ou grupos de usuários.

O controle de acesso discricionário pode ser implementado através das seguintes técnicas:

I. *Listas de controle de acesso* (ACLs) definem os direitos e permissões que são dados a um sujeito sobre determinado objeto. As listas de controle de acesso disponibilizam um método flexível de adoção de controles de acesso discricionários.
II. *Controles de acesso baseados em papéis* (*roles*) definem os direitos e permissões baseados no papel que determinado usuário desempenha na organização. Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários.

Permissões de acesso e direitos sobre objetos são dados para qualquer grupo ou, em adição, indivíduos. Os indivíduos podem pertencer a um ou mais grupos. Os indivíduos podem adquirir permissões cumulativas ou ser desqualificados para qualquer permissão que não faz parte de todo grupo ao qual ele pertence. A vantagem óbvia desse modelo é ser extremamente flexível, porém não provê garantia real sobre o fluxo de informação em um sistema.

b) Controle de acesso obrigatório

No controle de acesso obrigatório (*mandatory access control* ou MAC) a política de acesso é determinada pelo sistema e não pelo proprietário do recurso. Este controle é utilizado em sistemas de múltiplos níveis cujos dados são altamente sensíveis, como algumas informações governamentais e militares. Um sistema de múltiplos níveis é constituído de um computador que manipula vários níveis de classificação entre usuários e objetos.

i. *Rótulos de sensibilidade.* Em sistemas de controle de acesso obrigatório, todos os usuários e objetos devem ter rótulos associados. Um rótulo de sensibilidade de um usuário define o seu nível de confiança. Um rótulo de sensibilidade de um objeto define o nível de confiança necessário para acessá-lo. Para acessar um determinado objeto, o usuário deve ter um rótulo de sensibilidade igual ou superior ao requisitado pelo objeto.
ii. *Importação e exportação de dados.* O controle de importação e exportação de dados para outros sistemas (incluindo impressoras) é uma função crítica de um sistema baseado em MAC. O sistema precisa garantir que os rótulos de sensibilidade são mantidos e implementados de maneira apropriada, de forma que a informação sensível seja protegida a qualquer momento.

Dois métodos são comumente utilizados na aplicação de MAC:

i. *Controles baseados em regras.* Todos os sistemas MAC implementam uma forma simples de controle de acesso baseado em regras que definem que o acesso deve ser dado ou negado com base no rótulo de sensibilidade do objeto e no rótulo de sensibilidade do usuário.
ii. *Controles de acesso baseados no modelo lattice*[1] (reticulado). Estes controles são muito usados em sistema de múltiplos níveis (ex.: aplicações militares), em que a permissão de um nível contém todas as permissões do nível inferior.

c) Controle de acesso baseado em papéis

Um controle de acesso baseado em papéis (Role-Based Access Control - RBAC) é uma abordagem para restringir o acesso a usuários autorizados. É uma abordagem nova e uma alternativa aos sistemas de controles de acesso do tipo MAC e DAC. A diferença fundamental entre DAC e RBAC é que, no primeiro, quem decide quem dá permissão de acesso a um determinado recurso é o proprietário desse recurso; ao passo que, no RBAC, somente o administrador do sistema define as permissões de um dado papel e cada usuário só acessa os recursos definidos no escopo de permissão desse papel.

O modelo RBAC é baseado no seguinte conjunto de entidades: usuários, papéis e permissões (também conhecidas como autorizações). Um usuário pode ser também representado por um grupo, ou mesmo um programa executando em nome de um usuário. Um usuário também pode assumir um ou mais papéis. Em aplicações Web, os perfis de usuários são mais complexos. Por exemplo, um mesmo usuário de uma empresa pode ser Diretor do Departamento de Recursos Humanos e Supervisor do Departamento de Finanças, além de ter permissão de usuário no Departamento de Informática. Neste caso, o mesmo usuário assume vários papéis.

A noção de papel segue o conceito da estrutura organizacional de uma empresa, isto é, papéis representam funções em uma organização e incorporam um conjunto específico de autorizações e responsabilidade para cada função. Da mesma forma, um papel pode ter várias permissões e as mesmas permissões podem ser associadas a muitos papéis. Portanto, um papel pode herdar permissões associadas a outros papéis, desde que a hierarquia de papéis seja o meio natural para representar as linhas de autoridade de uma organização.

Permissões são regras que descrevem como os objetos (e.g., tabelas, atributos, visões, etc) são

[4] Um reticulado é uma estrutura L = (L, R) tal que L é parcialmente ordenado por R e para cada dois elementos a, b de L existe supremo (menor limite superior) e ínfimo (maior limite inferior) de {a,b}.

acessados pelos usuários.

Os administradores de um sistema podem criar papéis, conceder permissões a esses papéis e então associar usuários aos papéis com base nas responsabilidades de suas funções. Isso simplifica grandemente o gerenciamento do direito de acesso aos objetos. Por essa razão, RBAC tem sido bem atrativo para diversos tipos de aplicações Web, tais como comerciais, governamentais, corporativas, além de outras. A grande vantagem é que os modelos RBAC são capazes de reduzir complexidade e custo na administração de segurança de informação. A razão é simples: somente o administrador do sistema define os papéis e suas permissões de uma aplicação. Portanto, quando um novo papel é criado, o administrador tem controle total das permissões concedidas aos seus usuários. Isso simplifica o gerenciamento de usuários e de suas permissões.

Um modelo de controle de acesso para aplicações Web

Nesta seção será apresentada a estrutura do modelo de controle de acesso para aplicações Web. O modelo adotado foi o RBAC (modelo baseado em papéis). Em particular, o modelo proposto foi concebido para um banco de dados com informações sobre o mapeamento da oferta de software para o setor agropecuário. Essas informações referem-se a produtos e serviços existentes no mercado, agentes que o integram, modelos de negócio utilizados, regimes de apropriabilidade e segmentos de atuação. No entanto, o foco aqui é no controle de acesso propriamente dito.

Convém ressaltar que, embora o modelo de controle de acesso proposto seja específico para o banco de dados mencionado acima, ele pode ser facilmente reutilizado para outras aplicações Web. Essa discussão será apresentada na conclusão deste trabalho.

De uma maneira geral, o modelo do controle de acesso é baseado no seguinte conjunto de entidades: usuários, módulos, papéis e permissões.

- **Usuários:** Os usuários do sistema são subdivididos em duas categorias: a) técnicos da Embrapa e de instituições parceiras no projeto sobre o mercado de software brasileiro; b) empresas externas: aquelas que desenvolvem software no âmbito do setor agropecuário.

- **Módulos:** Existem três módulos que compõem a estrutura do sistema: a) *formulários*: para manipulação de dados de empresas e de seus softwares produzidos; b) *consultas*: através do qual um usuário pode fazer buscas simples e avançadas sobre todo o conteúdo da base de dados; c) *preferências*: utilizado pelo administrador para gerenciamento de usuários, papéis e módulos do sistema.

- **Papéis:** Os papéis disponíveis no sistema são basicamente classificados em quatro categorias: a) *produtor de informação*: usuário que recebe permissão apenas para preencher um formulário eletrônico, em que os dados são armazenados na base de dados. Este é o papel associado ao tipo de usuário "empresa externa". Portanto, não tem a permissão para fazer consultas aos dados da base. Uma empresa externa apenas insere e edita seus próprios dados; b) *Gerente*: papel que fica geralmente atrelado a um técnico da Embrapa para manipulação de informação (inserção, edição e consulta) na base de dados do sistema. A única restrição é que este papel não possui autorização para excluir dados do sistema; c) *Consultor*: papel assumido por um técnico da Embrapa ou de uma instituição parceira no projeto. Um usuário com este papel apenas visualiza as informações do sistema, mas não pode alterá-las; d) *Administrador*: O papel de administrador tem todas as permissões possíveis, sem restrições. Este papel fica disponível apenas para um técnico da Embrapa.

- **Permissões:** são as autorizações que cada usuário recebe, de acordo com seu papel, para acessar o conteúdo de um módulo. As permissões disponíveis no sistema, para cada módulo, são: 1 – sem permissão; 2 – leitura; 4 – edição de dados, sem autorização para excluí-los; 8 – administração geral de dados do sistema e gerenciamento de usuários.

Convém ressaltar que as permissões acima são baseadas em potência de 2. Por exemplo, a permissão 8 (2 elevado a 3) é concedida somente para o administrador do sistema. Portanto, quando maior o valor da permissão, maior será a autorização concedida ao usuário. Note que a permissão 1 (2 elevado a 0), significa que um usuário não pode acessar um determinado módulo do sistema.

A Tabela 1 a seguir resume as permissões associadas aos papéis disponíveis no sistema.

Tabela 1. Papéis e tipos de permissão disponíveis no sistema.

Papel	Permisssão
Administrador	Administração de dados e usuários. Sem restrições.
Gerente	Manipulação geral de dados, sem a permissão de excluí-los.
Consultor	Acesso apenas ao módulo de consultas e relatórios.
Produtor de informação	Inserção e edição de dados de uma empresa externa, sem a permissão de ver os dados de outra empresa.

Note que, para cada módulo do sistema, um usuário pode ter permissões diferentes. Por exemplo, um usuário com o papel de Gerente recebe permissão 4 para qualquer módulo do sistema, com a exceção do módulo de administração de usuário em que a permissão para o papel de Gerente é 1. Por outro lado, uma empresa externa, com o papel de Produtor de Informação, só pode acessar o módulo de formulários. Portanto, a permissão neste caso é 4, isto é, a empresa externa só pode ler e editar seus próprios dados. Em outras palavras, ela pode inserir e atualizar todos os seus dados e seus respectivos softwares, mas não pode removê-los do sistema.

O modelo de dados do controle de acesso é composto por quatro tabelas e seus relacionamentos, como pode ser visto na Fig. 3. Esse é o modelo conhecido como modelo entidade-relacionamento (Date, 2004; Ramakrishnan & Gehrke, 2003).

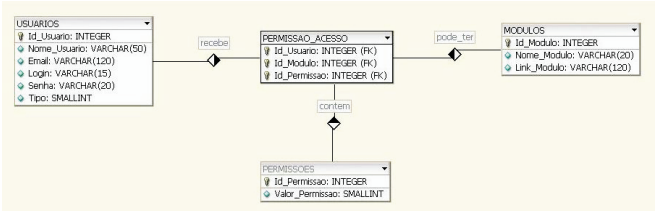

Fig. 3. Modelo de dados do controle de acesso para aplicação Web.

Como pode ser visto na tabela PERMISSÕES (Fig. 3), um usuário pode ter permissões diferentes para os módulos que ele acessa. Por exemplo, quando o tipo de usuário é empresa externa, somente o módulo de formulários (cadastro da empresa e de seus softwares) pode ser acessado, conforme ilustrado na Fig. 4. Note que no menu principal, o módulo de consultas não aparece para este usuário.

Fig. 4. Exemplo de acesso ao sistema por usuário externo, com o papel de produtor de informação.

Para um usuário (técnico da Embrapa) com o papel de gerente, a permissão concedida garante que ele pode manipular os dados do sistema, sem a permissão de excluí-los. Neste caso, todos os módulos do sistema estão habilitados no menu principal, como pode ser visto na Fig. 5.

Na Fig. 6, tem-se o exemplo do papel de administrador gerenciando usuários do sistema. O administrador tem autorização para definir todas as permissões associadas aos papéis dos usuários. Neste caso, em particular, o administrador está definindo as permissões para uma empresa externa que recebe o papel de produtor de informação.

Fig. 5. Exemplo de acesso ao sistema por usuário que é técnico da Embrapa e possui o papel de gerente.

Fig. 6. Exemplo de usuário com o papel de Administrador visualizando usuários do sistema e definindo permissões de uma empresa externa.

Conclusões

Neste trabalho, um modelo de controle de acesso baseado em papéis foi apresentado para uma aplicação Web: um sistema de informação sobre o mapeamento da oferta de software para o setor agropecuário.

Em particular, o controle de acesso foi implementado usando software livre para o ambiente Web. Para o modelo de dados, foi utilizada a ferramenta livre DBDesigner[5]. As tabelas do controle de acesso, juntamente com as tabelas do sistema de informação, são gerenciadas pelo MySQL[6], um sistema de gerenciamento de banco de dados (SGBD) que utiliza a linguagem de consulta estruturada SQL (Structured Query Language) como interface. sistema de informação. O acesso aos dados é feito por meio de páginas PHP[7]. Os usuários podem usar qualquer browser (Mozilla, Internet Explorer, Netscape) para manipular os dados, de acordo com as permissões concedidas para os papéis disponíveis no sistema de informação.

O projeto desse controle de acesso oferece alguns benefícios para outras aplicações Web que venham a ser desenvolvidas na Embrapa:

- *Flexibilidade:* eventuais mudanças no controle de acesso devem ser feitas rapidamente para atender novas necessidades de política de acesso à

[5] http://fabforce.net/dbdesigner4/
[6] http://www.mysql.com/
[7] PHP - Guia de Desenvolvimento Web. http://www.sobresites.com/desenvolvimentoweb/php.htm

informação do sistema. Por exemplo, se um novo módulo do sistema for implementado, basta acrescentar um registro na tabela de Módulos (Fig. 2). As demais tabelas não serão alteradas. Note que a manutenção será simplesmente nos dados e não no código fonte da interface do sistema.

- *Reusabilidade:* O modelo de dados do controle de acesso e código fonte da interface devem ser armazenadas e estar disponíveis para que outros desenvolvedores de aplicações Web os utilizem no projeto de novos sistemas de informação para o ambiente Web.

Referências Bibliográficas

BOOCH, G. The architecture of Web applications. 2001. Disponível em: <http://www-106.ibm.com/developerworks/library/it-booch_web/?dwzone=IBM>. Acesso em: 7 jan. 2008.

CASTANO, S.; FUGINI, M.; MARTELLA, G.; SAMARATI, P. Database security. Boston: Addison Wesley, 1995. 456 p.

CONALLEN, J. Modeling Web application design with UML. 1998. Disponível em: <http://www.rational.com/products/whitepapers/100462.jsp>. Acesso em: 7 jan. 2008.

DATE, C. J. Introdução a sistemas de bancos de dados. 8. ed. Rio de Janeiro: Campos, 2004.

FERRAIOLO, D. F.; CUGINI, J. A.; KUHN, D. R. Role-based access control: features and motivations. In: ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 11., 1995, New Orleans, LA. Proceedings… Los Alamitos, CA: IEEE Computer Society Press, 1995. p. 242-248.

PRESSMAN, R. S. Software engineering: a practioner's approach. 5th. ed. New York: McGraw-Hill, 2001. 860 p.

RAMAKRISHNAN, R.; GEHRKE, J. Database management systems. New York: McGraw-Hill, 2003. 1065 p.

SANDHU, R. S.; COYNE, E. J.; FEINSTEIN, H. L.;

Comunicado Técnico, 86

Ministério da Agricultura, Pecuária e Abastecimento

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Embrapa Informática Agropecuária
Área de Comunicação e Negócios (ACN)
Endereço: Caixa Postal 6041 - Barão Geraldo
13083-970 - Campinas, SP
Fone: (19) 3211-5743
Fax: (19) 3211-5754
URL: http://www.cnptia.embrapa.br
e-mail: sac@cnptia.embrapa.com.br

1ª edição on-line - 2008

Todos os direitos reservados.

Comitê de Publicações

Presidente: *Kleber Xavier Sampaio de Souza.*
Membros Efetivos: *Leandro Henrique Mendonça de Oliveira, Marcia Izabel Fugisawa Souza, Martha Delphino Bambini, Sílvia Maria Fonseca Silveira Massruhá, Stanley Robson de Medeiros Oliveira, Suzilei Carneiro (secretária).*

Suplentes: *Goran Neshich, Maria Goretti Gurgel Praxedes.*

Expediente

Supervisor editorial: *Suzilei Carneiro*
Normalização bibliográfica: *Marcia Izabel Fugisawa Souza*
Editoração eletrônica: *Área de Comunicação e Negócios*