Análise e Simulação do Mecanismo de Alocação de Recursos Humanos em Sistemas de Workflow Combinado com Algoritmos de Controle de Acesso Baseado em Papéis

Elaine Aires de Oliveira[1], Liliane do Nascimento Vale[1]

[1]Departamento de Ciência da Computação – Campus Catalão
Universidade Federal de Goiás (UFG) – Catalão – GO – Brasil

elaine.aires@gmail.com, lili_malman@yahoo.com.br

Abstract. *Workflow Management Systems are employed in coordinating and streamlining business processes and are used in critical applications in organizational and strategic. Then, security has become a major factor in workflows, viewed it involves the implementation of security mechanisms designed to guarantee access control tasks to be performed only by authorized users. In this paper, we propose the use of the security model Role-Based Access Control on the criterion of partitioning of roles in Workflow Systems, in order to progress in the administration of users access these systems, contributing to the achievement of the required level of safety in the corporate environment.*

Resumo. *Sistemas de Gerência de Workflow são empregados na coordenação e dinamização de processos de negócio, sendo utilizados em aplicações críticas e estratégicas no âmbito organizacional. Assim, a segurança tem se tornado um fator primordial em Workflows, visto que envolve a execução de mecanismos de segurança de controle de acesso objetivando garantir que as tarefas sejam executadas exclusivamente por usuários autorizados. Neste trabalho, é proposto a utilização do modelo de segurança Role-Based Access Control no critério de particionamento de papéis em Sistemas de Workflow, visando progressos na administração do acesso de usuários nestes sistemas, contribuindo para o alcance do nível de segurança exigido no ambiente corporativo.*

1. Introdução

O impacto do dinamismo decorrente do surgimento de novas tecnologias resulta em constantes variações no ambiente de negócios, em consequência exige-se uma maior capacidade de gerência das atividades nas organizações. Frente a este cenário, o desenvolvimento de pacotes de softwares genéricos para gerenciamento de processos de negócios - denominados Sistemas de Gerenciamento de *Workflows (SGWs)* - são particularmente importantes, pois provém suporte computadorizado às automações procedimentais das organizações garantindo maiores índices de qualidade e eficiência no gerenciamento de seus processos de negócio.

Sistemas de *Workflow* ou de gerenciamento de fluxo de trabalho correspondem a um conjunto de ferramentas que tem como finalidade a automação e gestão de processos, visando à minimização do problema da coordenação das tarefas nos processos de negócios e, fornecendo auxílio no alcance das metas empresariais com alta eficiência em termos da organização das atividades.

O formalismo das redes de Petri (RdP) é empregado neste trabalho para modelagem do SGW. As redes de Petri são consideradas ferramentas gráficas e matemáticas de representação formal que possibilitam a modelagem, a análise e o controle de sistemas de processamento de informação. [Aalst e Hee 2002] identificam três razões principais para aplicação de redes de Petri na modelagem de *Workflow*: (1) as redes de Petri possuem

semântica formal além da sua natureza gráfica; (2) permitem modelar explicitamente os estados do sistema e (3) existência de variedade e disponibilidade de técnicas de análise. Segundo [Merz *et al*. 1995], a principal vantagem de empregar RdP na modelagem de *Workflow* é a combinação de fundamentação matemática, representação gráfica compreensiva e possibilidade de simulações e verificações.

A segurança tem se tornado um fator essencial em *Workflows*. O serviço de segurança de autorização (controle de acesso) é de relevância primordial no contexto destes sistemas, pois objetiva assegurar que a tarefa seja executada exclusivamente por usuários autorizados. Um modelo de autorização deve ser capaz de impedir a modificação desautorizada dos dados e também fornecer meios de reforçar o padrão legítimo das operações nos dados acessados para a execução de uma tarefa. Em sistemas de *Workflow* são verificadas algumas deficiências referentes a ferramentas que promovam a segurança destes sistemas e dessa forma, neste artigo, o modelo de segurança utilizado como referência é o modelo *Role-Based Access Control* (RBAC), no critério de particionamento de papéis proposto em [Nyanchama and Osborn 1994]. Assim, o modelo de autorização é aplicado em sistemas de *Workflow*.

2. Trabalhos Relacionados

A segurança é um componente crítico e essencial em sistemas de *Workflows*. Na literatura são propostos diferentes métodos para a modelagem dessas propriedades de segurança, sobretudo em aplicações industriais para o controle da autorização e de acessos.

[Atluri *et al.* 1997] propõem em seu trabalho um poderoso modelo de segurança fundamentado na Lógica de Predicados. [Karlapalem and Hung 1997] também descrevem as características da segurança do *Workflow* e discute o *trade-off* entre a segurança e o risco de um sistema, apresentando uma métrica para avaliar tal *trade-off*. Os demais estudos relacionados abordam a segurança em Inter-*Workflows.*

Em [Jeske 2006] foi proposto um modelo de rede de Petri p-temporal com recursos híbridos fuzzy como solução para o problema de alocação de recursos humanos em Sistemas de Gerência de *Workflow*.

Propomos, neste trabalho, uma abordagem baseada em um modelo de rede de Petri para a modelagem de um SGW, como uma solução para o problema de alocação de recursos humanos e distribuição adequada de papéis aos recursos disponíveis. E também, o acoplamento dos mecanismos de RBAC disponíveis a este critério com a finalidade de incluir a capacidade de expressar e impor uma política de segurança específica e simplificar o oneroso processo de gerenciamento de segurança.

Portanto, este trabalho foca o estudo no conceito RBAC utilizando o modelo de grafo de papéis no contexto de particionamento de papéis, com o objetivo de mostrar a aplicabilidade e eficiência deste conceito em sistemas de *Workflows.*

3. Sistemas de Gerenciamento de *Workflow*

Sistemas de *Workflow* correspondem a um conjunto de ferramentas que permitem o projeto e a definição de fluxos de trabalho. Assim, é visado à eficiência do gerenciamento e do controle do trabalho e minimização do problema da coordenação das tarefas nos processos de negócios. Consequentemente, o ganho de competitividade das organizações é considerável.

Conforme a [WfMC 2006], *Workflow* é a automação de um processo de negócio, por inteiro ou por partes, durante o qual documentos, informações e atividades são passadas de um participante para outro para que estes desenvolvam ações respeitando um conjunto de regras procedimentais.

Nesse contexto, apresentam-se os Sistemas de Gerência de *Workflow*s (*Workflow Management System* – SGWs) que são, em geral, ferramentas colaborativas que provêem a automação procedimental do gerenciamento de processos de negócios [Aalst e Hee 2002], [Hollingsworth 1985].

Em modelos de SGWs consideram-se, entre outros, mecanismos de alocação de recursos cumulativos e restrições temporais (intervalos de datas de execução das atividades). Os recursos eventualmente precisam ser alocados a duas ou mais tarefas de casos diferentes em um mesmo instante de tempo para que se possa cumprir com o cronograma estabelecido. Considerando a inconsistência entre restrições de tempo e entre os períodos disponíveis dos recursos, a má alocação de recursos apropriados a determinadas atividades apresentam-se como um problema em SGWs.

A definição completa de Sistemas de *Workflows* pode ser vista em [Hollingsworth 1985] e [WfMC 2006].

4. Redes de Petri

O conceito de rede de Petri foi inicialmente postulada por Carl Adam Petri em sua tese de doutorado, *Kommunikation mit Automaten* (Comunicação entre autômatos). Segundo [Murata 1989], as redes de Petri são consideradas ferramentas gráficas e matemáticas de representação formal que possibilitam a modelagem, a análise e o controle de sistemas e eventos discretos, suportando atividades que se caracterizam como concorrentes, assíncronas e paralelas. A definição completa das redes de Petri podem ser vistas em [Cardoso *et al*. 1999], [David e Alla 2004], [Murata 1989] e [Peterson 1981].

De maneira simplificada, uma rede de Petri é apresentada como um grafo orientado e bipartido, conforme Figura 1, composto por dois elementos: transição e lugar. A transição (t) é o componente ativo correspondente a alguma ação desempenhada dentro do sistema, e o lugar (P1 e P2), é passivo e equivale a alguma variável de estado do sistema. Lugares podem apresentar um número inteiro de fichas que podem movimentar-se ao longo dos arcos, segundo a ação executada.

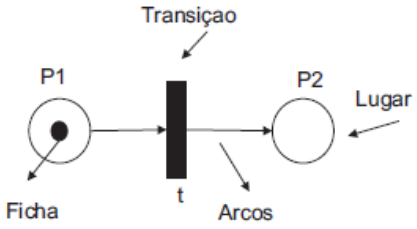

Figura 1. Rede de Petri

Definição 1: *Formalmente, a rede de Petri é dada por uma quíntupla, N = (P, T, Pre, Pos, M_0)* [Murata 1989], *onde:*

- *P é um conjunto finito de lugares,*
- *T é um conjunto finito de transições,*
- *Pre é uma aplicação de entrada tal que Pre: (P × T) → N,*
- *Pos é uma aplicação de saída tal que Pos: (T × P) → N e*
- *M_0 é a marcação inicial.*

Modelos fundamentados em redes de Petri foram definidos exclusivamente para a representação de *Workflow*: as *Workflow-nets (WF-nets)* [Aalst e Hee 2002]. Uma *WF-net* apresenta apenas um lugar de entrada (*Start*) e um lugar de saída (*End*) sinalizando o início e o fim do processo de negócio modelado. A representação de uma *WF-net* é mostrada na Figura 4. Verifica-se que essas redes são apropriadas para representação, validação e verificação de *Workflow*.

Uma *Workflow-net* é considerada logicamente correta *(Sound)* através do critério de verificação da correção *Soundness*, quando satisfaz as seguintes condições [Aalst e Hee 2002]:

- Para cada *ficha* colocada no lugar *Start*, exatamente uma única ficha alcança o lugar *End*;
- Quando uma ficha é colocada no lugar *End*, os demais lugares estão vazios;
- Para toda tarefa, é possível sair do estado inicial para um estado em que esta tarefa possa ser executada.

5. Controle de acesso

O controle de acesso é um dos itens de segurança ligado à confidencialidade das informações e acesso a operações. Conforme [Sandhu *et al*. 1996], o controle de acesso objetiva limitar as operações que podem ser realizadas por uma entidade sobre um determinado recurso, alcançando objetivos da segurança da informação, como sigilo e integridade, e prevenindo a exposição e a modificação não autorizada da informação.

O controle de acesso baseado em papel (RBAC) descreve mecanismos de segurança que controlam o acesso de usuários a recursos computacionais. Assim, permite que privilégios sejam atribuídos aos papéis arbitrários, os quais podem então ser distribuídos aos usuários reais [Koch and Parrisi-Presicce 2002], [Nyanchama and Osborn 1994], [Sandhu *et al*. 1996]. O controle de acesso baseado em papel provê um modo de controlar autorizações e executar tarefas em sistemas complexos com muitos usuários e recursos [Sandhu *et al*. 1996]. Na próxima seção é apresentada uma breve descrição do modelo de segurança RBAC.

6. Modelo de Segurança RBAC

O conceito básico do modelo de segurança RBAC é associar as permissões de acesso a papéis e estes por sua vez, são associados a usuários. Papéis são designados conforme os diferentes cargos ou funções em uma organização, e os usuários são associados a papéis segundo as suas responsabilidades e qualificações [Sandhu *et al*. 1996], [Wainer *et al*. 2003].

A política de controle de acesso baseada em papéis baseia-se na análise dos requisitos e das regras de negócio para determinar: os papéis necessários e suficientes para cobrir o domínio da informação; as permissões atribuídas a cada papel; os usuários aos quais serão atribuídos os papéis; a relação hierárquica entre papéis; as restrições de uso do mecanismo RBAC a fim de mantê-lo no escopo da política de segurança da organização [Koch and Parrisi-Presicce, 2002], [Nyanchama and Osborn 1994].

Conforme [Ferraiolo and Kuhn 1995] as principais motivações do RBAC são, em primeiro lugar, a capacidade para expressar e impor uma política de segurança específica para uma organização e, em segundo lugar, simplificar o processo de gerenciamento de segurança. Assim, o modelo RBAC reduz a complexidade de gerenciamento e o custo administrativo em ambientes com grande freqüência de mudanças.

O modelo de referência RBAC do tipo Hierárquico será utilizado neste trabalho por categorizar os papéis associados aos recursos de maneira hierárquica, objetivando uma menor concentração de privilégios dos papéis associados aos recursos.

No contexto organizacional e em aplicações de *Workflow*, o conceito de pessoas/papéis é prevalecente. Assim, é comum, por exemplo, que em um processo de negócio que reimplanta um pedido feito por um empregado necessita ser aprovado pelo chefe da unidade em que o empregado está estaticamente atribuído [Koch and Parrisi-Presicce 2002], [Nyanchama and Osborn 1999].

No modelo RBAC podem suceder situações em que algumas operações genéricas podem ser executadas por todos os empregados. Nesse contexto, especificar repetidamente estas operações gerais para cada papel se torna pouco eficiente. Assim, as hierarquias de papéis podem ser estabelecidas para fornecer a estrutura natural de uma organização.

A hierarquia é uma ordem parcial que define uma relação de precedência de papéis, por meio da qual, papéis de categoria superior adquirem as permissões dos seus subordinados. A hierarquia estrutura papéis permitindo a reflexão das linhas de autoridade e responsabilidade em uma organização [Sandhu *et al*. 1996].

A Figura 2(a) apresenta o grafo de papéis hierárquico associado ao modelo de RdP da Figura 4, para o processo de tratamento de reclamações.

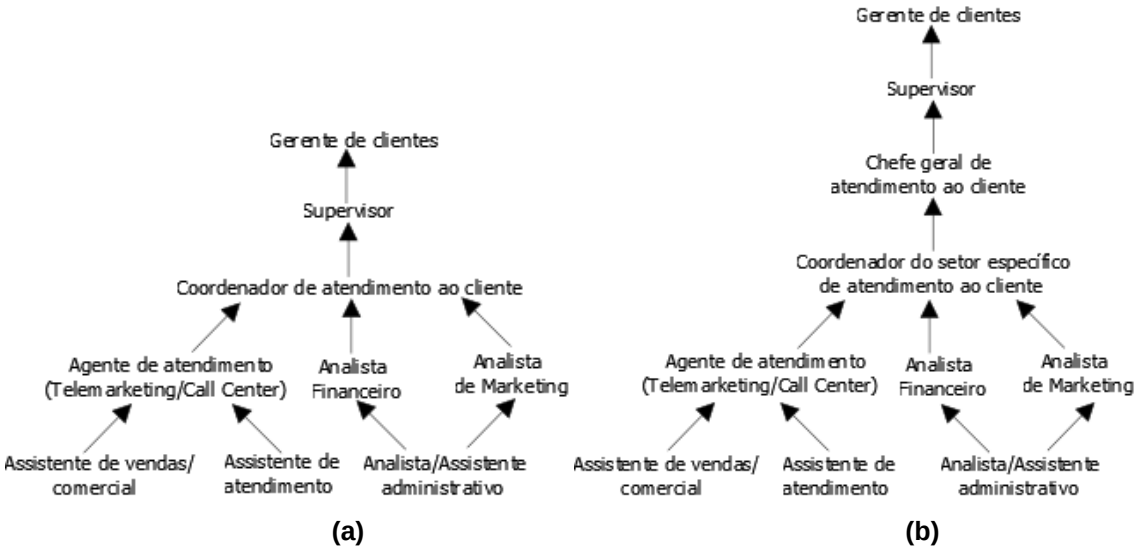

Figura 2. (a) Grafo de Papéis Hierárquico para o processo de tratamento de reclamações. (b) Grafo de papéis após o particionamento do papel 'Coordenador de atendimento ao cliente'.

7. Partições de Papéis no Grafo de Papéis Hierárquico

No contexto do modelo RBAC Hierárquico em [Nyanchama and Osborn 1994] foi proposto à implementação do modelo incluindo a partição de papéis. Verifica-se que um papel pode ser particionado em dois ou mais papéis. As operações básicas de particionamento podem ser desempenhadas de dois modos: verticais ou horizontais e podem naturalmente ser combinadas [Nyanchama and Osborn 1994].

A principal vantagem desta aplicação consiste na redução significativa dos privilégios que até então permaneciam concentrados em posse de apenas um usuário, o que favorecia o aumento da ocorrência de fraudes e demais erros na execução de tarefas. Neste artigo, por conveniência, foi abordado o modelo de particionamento vertical de papéis em sistemas de *Workflow*.

O particionamento vertical permite a quebra do papel em dois ou mais papéis e uma ordem é imposta ao relacionamento papel subordinado. Neste modelo, um papel é selecionado para ser quebrado, posteriormente ao particionamento são gerados novos papéis que passam a adquirir os privilégios do papel alvo. Considere por exemplo o papel X, este será particionado em X_1,..., X_n. Estes novos papéis serão criados de forma ordenada, de tal forma que em X_1 deve existir um caminho que leve a X_2 assim por diante, ou seja, (X_1,..., X_n). Assim que novos papéis forem gerados e após a distribuição dos privilégios, o papel alvo se tornará extinto. A Figura 3 ilustra o particionamento vertical de papéis abordado no estudo de caso.

Na Figura 3 é apresentado o resultado do particionamento vertical do papel alvo "Coordenador de atendimento ao cliente" presente no grafo de papéis hierárquico para o processo de tratamento de reclamações em dois papéis distintos: "Chefe geral de atendimento ao cliente" e "Coordenador do setor específico de atendimento ao cliente".

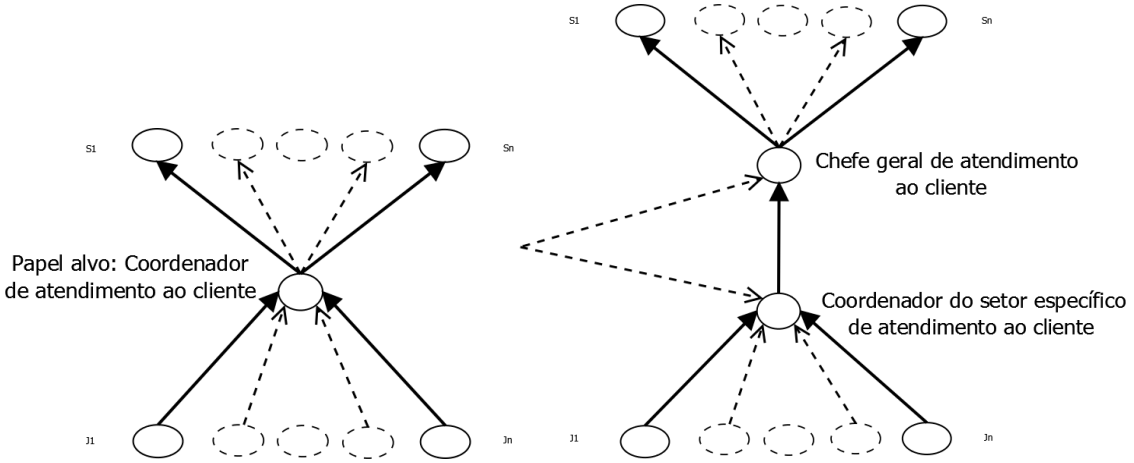

Figura 3. Representação do particionamento vertical do papel "Coordenador de atendimento ao cliente" em dois papéis distintos.

8. Estudo de caso

A Figura 4 apresenta a especificação de um processo de tratamento de reclamação com alocação de papéis, representados por chaves, associados às transições. Primeiramente, a reclamação é registrada pelo agente de atendimento. O cliente que registrou a reclamação e o departamento afetado pela reclamação são contatados pelo assistente de vendas/comercial e pelo assistente de atendimento, respectivamente. Estas duas situações (tarefas) podem ser executadas em paralelo. Posteriormente, os dados são recolhidos pelo assistente de atendimento para que uma decisão seja tomada pelo coordenador de atendimento ao cliente. Assim que a decisão é tomada, duas situações podem ocorrer: um pagamento de compensação é feito pelo analista financeiro ou uma carta é enviada pelo analista de marketing. Por último, a reclamação é arquivada pelo auxiliar/assistente administrativo.

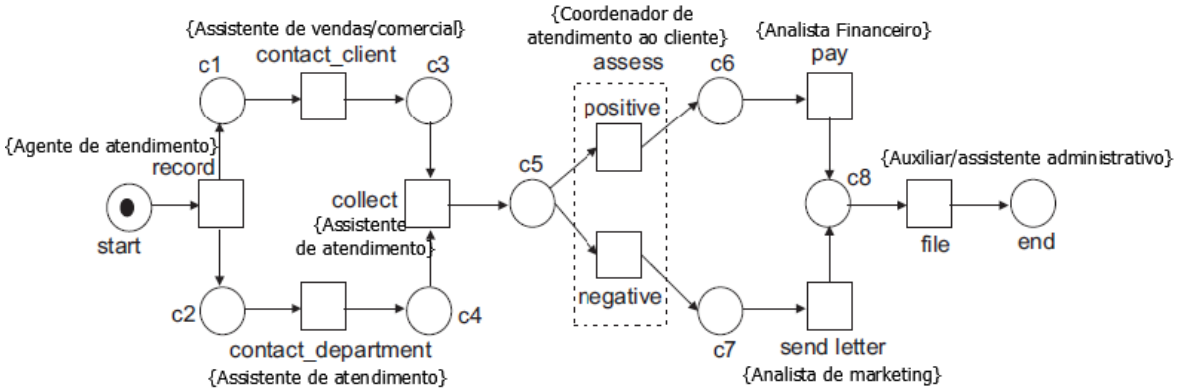

Figura 4. Modelo de uma *WF-net* para o processo de tratamento de reclamações e seus acionamentos.

Cada tarefa *record, contact_client, contact_departament, assess, pay, send letter e file* é representada por uma transição na RdP. A avaliação de uma reclamação corresponde às transições *positive* e *negative*, as quais representam uma decisão, positiva ou negativa, respectivamente.

Os casos são representados pelas fichas presentes nas redes. No lugar *start* da Figura 4, existe uma ficha indicando a presença de um caso. Se a transição *record* é disparada, duas fichas (uma em c1 e outra em c2) representam o mesmo caso. Quando um caso é tratado, o número de fichas pode variar. A quantidade de fichas que representa um caso particular é sempre igual ao número de suas condições que devem ser satisfeitas. No lugar *end* deverá haver uma ficha, quando o caso for concluído.

Cada processo deve cumprir dois requisitos: poder alcançar um estado em qualquer momento por meio da execução de tarefas; e, quando existir uma ficha em *end*, verificar se as demais desapareceram no restante dos processos. Dessa forma, é possível garantir que todo caso que se iniciou no lugar *start* será completado corretamente e finalizado no lugar *end*.

No processo de tratamento de reclamações, os papéis com mais permissões, ocupam posições mais altas, os quais por sua vez, herdam as permissões dos papéis localizados abaixo deles no grafo. Esta hierarquia permite a agregação de permissões de diferentes papéis em outro. A Figura 2(b) mostra o grafo de papéis particionado para o modelo de RdP apresentado na Figura 4.

O papel "Coordenador de atendimento ao cliente" da Figura 4 é o responsável por avaliar a reclamação, sinalizando-a como positiva ou negativa, além de suas atribuições específicas. Assim, verifica-se uma centralização de privilégios no processo decisório, o que favorece o retardamento nas decisões, sobrecarga de atividades, aumento da possibilidade de fraudes e avaliações pessoais errôneas.

Assim sendo, o papel "Coordenador de atendimento ao cliente" foi particionamento verticalmente em dois novos papéis: "Chefe geral de atendimento ao cliente" e "Coordenador do setor específico de atendimento ao cliente", como mostra a Figura 3, a fim de tornar mais dinâmica à operação da organização, descentralizando o poder decisorial e promovendo melhorias no processo de deliberação e na segurança. Dessa forma, a avaliação das transições *positive* e *negative* devem agora ser analisados pelos dois novos papéis.

Verifica-se que as decisões delegadas a dois novos papéis promovem a resolução correta e rápida do processo, provendo um retorno mais rápido aos clientes e avanços na segurança do processo. Assim, essa abordagem atende ao alinhamento das organizações em torno das estratégias para alcançar as metas estabelecidas e mantê-las competitivas no mercado. Além disso, é importante ressaltar que o particionamento vertical de papéis resolve o problema da alocação de recursos, uma vez que as atividades podem ser melhor distribuídas.

9. Conclusão e trabalhos futuros

Este trabalho está centrado no estudo das questões relativas à segurança em sistemas de *Workflow*. Assim, foi empregado um modelo matemático formal de controle de acesso baseado em papéis visando progressos na administração do acesso de usuários nestes sistemas.

O modelo de controle de acesso baseado em papel (RBAC) descreve mecanismos de segurança que controlam o acesso de usuários a recursos computacionais, fornecendo um modo de controle de autorizações e execução de tarefas em sistemas complexos. O RBAC do tipo Hierárquico foi utilizado por estruturar papéis permitindo a reflexão das linhas de autoridade e responsabilidade em uma organização. Foi realizado o particionamento vertical de papéis no Grafo de Papéis Hierárquico baseado no modelo de rede de Petri para o tratamento de reclamações.

Foi verificado que o modelo de particionamento vertical de papéis proposto em [Nyanchama and Osborn 1994] pode ser aplicado eficientemente em sistemas de

gerenciamento de *Workflow*, contribuindo para maior segurança ao acesso a dados e consequentemente a descentralização de poderes atribuídos a um papel, constituindo-se como solução do problema de alocação de recursos humanos nestes sistemas.

A principal contribuição deste trabalho é apresentar uma abordagem de segurança para sistemas de *Workflow* incluindo a capacidade de expressar e impor uma política de segurança e simplificar o oneroso processo de gerenciamento de segurança nestes sistemas.

Como proposta de trabalho futuro é sugerido à implementação do Modelo de rede de Petri analisado nesse trabalho.

10. Referências

Aalst, W., e Hee, K. (2002). "Workflow Management: Models, Methods, and Systems", The MIT Press Cambridge, Massachusetts. London, England.

Atluri V. and Bertino, E. (1997). "An execution model for multilevel secure *Workflows", Working Conference on Database Security.*

Cardoso, J., Valette, R., Dubois, D. (1999). "Possibilistic Petri Nets*", IEEE Trans. on Systems, Man, and Cybernetics* - Part B. Vol. 29, No. 5.

David, R., Alla, H. (2004). "Discrete, Continuous, and Hybrid Petri Nets", Springer.

Ferraiolo, D. and Cugini, J. and Kuhn, D. (1995). "Role based access control: Features and motivations". *Computer Security Applications Conference.*

Ferraiolo D.and Sandhu, R.and Gravila, S. K. R. C. R. (2001). "Proposed nist standard for role-based". *ACM Transactions on Information and System Security*.

Hollingsworth, D. (1985). "The *Workflow* Reference Model", *Workflow* Management Coalition Document Number TC00-1003. Document Status – Issue 1.1.

Jeske, C.J. (2006). "Mecanismo de alocação de recurso fuzzy para sistemas de gerenciamento de *Workflow",* Dissertação de mestrado, Universidade Federal de Uberlândia.

Karlapalem I. and Hung, P. (1997). "Security enforcementin activity mamgement systems", *Workshop management systems and interoperability.*, 164:165 – 194.

Koch, M., Mancini, L. and Parrisi-Presicce, F. (2002). "A graph-based formalism for rbac", *ACM Transactions on Information and System Security (TISSEC).*

Merz, M. *et al*., (1995). "*Workflow* modeling and execution with coloured petri net", *Proceedings*

Murata, T., (1989). "Petri nets: Properties, analysis and applications", Proceedings of the IEEE, v. 77, n. 4.

Nyanchama, M. and Osborn, S. (1999). "The role graph model and conflict of interest", *ACM Transactions on Information and System Security.*

Peterson, J. L. (1981). "*Petri Net Theory and the Modeling of Systems"*, Prentice Hall.

Sandhu, R., *et al*., (1996). "Role-based access control models", *IEE Computer.*

WfMC (2006). "WFMC, *Workflow* Management Coalition", Disponível em: http://www.wfmc.org/standards/XPDL.htm, Abril.