Avaliação de Ferramentas para Gestão e Execução de Regras de Autorização

Leonardo Azevedo, Diego Duarte, Fernanda Araujo Baião, Claudia Cappelli

NP2Tec – Núcleo de Pesquisa e Prática em Tecnologia
Universidade Federal do Estado do Rio de Janeiro (UNIRIO)
{azevedo, diego.duarte, fernanda.baiao,claudia.cappelli}@uniriotec.br

Resumo. *Segurança da informação é um tema essencial em organizações comerciais e governamentais, e sua operacionalização requer a existência de ferramentas de suporte, tanto em tempo de edição e manutenção das regras quanto em tempo de execução das aplicações que realizam acesso aos dados corporativos, quando se deve assegurar que as regras previamente definidas sejam respeitadas. Em cenários reais, este suporte computacional é tipicamente definido por atividades de prospecção da área de Arquitetura de TI. A avaliação de ferramentas de regras de autorização, no entanto, não é trivial. Este trabalho relata a avaliação de ferramentas de gestão e execução de regras de autorização, seguindo o framework composto por uma arquitetura genérica e um processo de avaliação propostos anteriormente. Além disso, são propostos uma taxonomia de critérios de avaliação e uma metodologia de cálculo das notas atribuídas aos critérios. A avaliação foi realizada em um cenário real de uma organização, e os resultados mostraram ser possível adotar um BRMS para suporte à gestão de regras de autorização, e às funcionalidades inerentes a SGBD como o Oracle tanto para armazenamento quanto para execução de regras de autorização.*

1. Introdução

A pesquisa em segurança da informação tem recebido cada vez mais atenção a fim de atender às necessidades de segurança de aplicações comerciais e governamentais. A integridade, disponibilidade e confidencialidade dos dados em sistemas de software, bancos de dados e redes de dados são as principais preocupações de todos os setores das organizações. O acesso não autorizado a recursos corporativos podem impactar fortemente as operações das organizações e levar a sérios problemas financeiros, legais, de segurança pessoal, privacidade e confidencialidade. As maiores questões de segurança e confidencialidade se encontram na integridade da informação, a qual é garantida por mecanismos de controle (ou autorização) de acesso [Sandhu *et al.*, 1996; Yang, 2009; Cali e Martinenghi, 2008; Murthy e Sedlar, 2007]. Estes mecanismos fazem com que regras de negócio do tipo assertiva de ação de autorização sejam garantidas. Segundo [BRG 2009], regra de negócio é uma declaração que define ou restringe algum aspecto de uma organização. Regras de negócio têm como objetivo definir a estrutura de um negócio ou controlar ou influenciar o seu comportamento. Em particular, uma categoria de regras de negócio é a assertiva de ação de autorização, ou **regra de autorização**, a qual restringe **quem** é permitido realizar uma **ação** na organização sobre quais **informações**.

Deitert e McCoy [2007] apontam que, com a percepção de que as regras de negócio não deveriam estar implícitas nas aplicações e sim externas a elas de maneira que se tornassem reutilizáveis, ferramentas foram sugeridas para gestão e execução de regras. Inicialmente denominadas de BRE (*Business Rule Engine* ou Motor de Regras de Negócio), tais ferramentas consistiam em um ambiente para desenvolvimento das regras e um motor de execução para controle da aplicação das regras. No entanto, com a evolução do uso destas ferramentas e criação e execução de regras complexas, novas funcionalidades foram adicionadas às ferramentas, as quais evoluíram para BRMS (*Business Rule Management System* ou Sistema de Gestão de Regras de negócio). Existem várias ferramentas no mercado para gestão de regras de negócio como, por exemplo, as ferramentas enumeradas em [Sinur 2005] e [Rymer e Gualtieri 2008], cujos trabalhos apresentam avaliações de ferramentas existentes no mercado.

O estudo e prospecção de ferramentas de apoio computacional às atividades em uma organização são de responsabilidade da área de Arquitetura de Tecnologia da Informação (TI) [Botto 2004]. Durante o processo de prospecção de ferramentas é realizada a avaliação e seleção de ferramentas necessárias para fornecer apoio aos processos organizacionais.

Para que a avaliação de uma ferramenta seja conduzida de forma imparcial, faz-se necessária a definição dos critérios que serão utilizados nesta avaliação, assim como a escala de pontuação e o grau de importância (peso) de cada um deles. As avaliações de ferramentas para gestão de regras de negócio conduzidas por [Sinur 2005] e [Rymer e Gualtieri 2008] auxiliam na fase inicial de busca por ferramentas desta área. No entanto, para a efetiva escolha da ferramenta que atenda aos requisitos específicos de uma organização, critérios mais detalhados e especializados são necessários.

Neste trabalho, o foco está na avaliação de ferramentas BRMS para tratar regras de autorização. A maioria das ferramentas BRMS existentes no mercado foca na gestão e execução de regras de negócio dos tipos termos de negócio, fatos relacionando termos entre si, derivações e sentenças de ação [BRG, 2009], mas não tratam de forma apropriada sentenças de ação de autorização (regras de autorização). Por outro lado, as implementações de funcionalidades para garantir regras de autorização em Sistemas Gerenciadores de Banco de Dados (SGBD) (por exemplo, Oracle, Sybase e Microsoft SQL-Server [Yang 2009]) focam na execução de regras de autorização, não tendo uma interface adequada para gestão de regras de autorização.

Este trabalho apresenta a avaliação de ferramentas para gestão e execução de regras de autorização para controle de autorização de acesso a bases de dados, e um conjunto de critérios para a avaliação de ferramentas BRMS com intuito de classificá-las e avaliar até que ponto elas atendem aos requisitos da organização.

Este trabalho está dividido da seguinte forma. A seção 1 é a presente introdução. Na seção 2 são caracterizados mecanismos específicos para execução de regras de autorização . A implementação destes mecanismos em ferramentas existentes e a avaliação do uso destas funcionalidades são apresentadas. As BRMS existentes no mercado são listadas e uma análise das mesmas é apresentada em relação a regras de autorização. Na seção 3, é apresentada a proposta de divisão das ferramentas em gestão e execução de regras de autorização, além de uma proposta de critérios para avaliação das ferramentas. Na seção 4 é apresentado um caso real de avaliação das ferramentas

BRMS segundo os critérios propostos. Finalmente, na seção 5 são apresentadas as conclusões obtidas e os trabalhos futuros.

2. Trabalhos Relacionados

Os mecanismos de controle de autorização de acesso a dados podem ser divididos em DAC (*Discricionary Access Control*), MAC (*Mandatory Access Control*), ambos propostos por [DoD 1983], e mais recentemente RBAC (*Role-Based Access Control*) [Ferraiolo e Khun, 1992].

O mecanismo DAC restringe acesso a objetos baseado na identidade de usuários e/ou grupos aos quais eles pertencem. [Yang 2009] aponta que políticas DAC não garantem controle sobre o fluxo de informações, pois torna possível que informações cheguem a usuários que não têm permissão de lê-las. As políticas MAC, também conhecidas como *label security*, são baseadas em regulamentações mandatórias determinadas por uma autoridade central [Yang 2009]. A forma mais comum de MAC é a política de segurança de múltiplos níveis usando classificação de sujeitos (usuários ou grupos) e objetos (dados) dos sistemas. MAC controla o fluxo de informações, embora não aborde as ações que podem ser executadas pelos sujeitos sobre os dados [Ferraiolo e Khun, 1992]. Além disso, como um rótulo é atribuído a cada instância de dados, o custo de gestão e de manutenção dos rótulos é alto, e pouco flexível, se existirem muitas políticas definidas. No caso de RBAC, o controle de acesso considera funções e informações, além das informações. Neste caso, o interesse principal é proteger a integridade da informação: **quem** pode realizar qual **ação** sobre qual **informação** [Ferraiolo e Khun, 1992]. Em [Ferraiolo *et al.* 2001] é proposto um padrão para RBAC a fim de unificar idéias existentes em diferentes modelos de referência de RBAC, produtos comerciais e protótipos de pesquisa.

Os mecanismos para controle de acesso encontram-se implementados em diferentes Sistemas Gerenciadores de Banco de Dados (SGBD), como Oracle, Sybase, Microsoft SQL-Server [Yang 2009]. Após análise destas ferramentas, observamos que estas implementações estão muito mais voltadas para tratar a execução das regras de autorização do que a gestão das regras. A especificação das regras requer conhecimento profundo de conceitos de banco de dados (linguagem SQL e *stored procedures*). Dessa forma, não é o foco destas ferramentas a criação, edição, alteração e manutenção de regras de autorização por usuários do negócio, mas sim por administradores de bancos de dados. Nestas ferramentas, a edição, composição, consultas e visualização das regras e suas dependências, versionamento, validação, simulação de execução, entre outras funcionalidades, não são simples de serem executadas ou mesmo não são suportadas. Isto torna inviável que tais funcionalidades sejam executadas pelos usuários do negócio, que seriam o perfil mais apropriado já que possuem conhecimento profundo sobre o negócio e das restrições de acesso à informação.

Por outro lado, ferramentas BRMS são construídas com o intuito de possibilitar que usuários do negócio criem, gerenciem e mantenham regras de negócio, permitindo também a execução de regras de negócio. Em [Sinur 2005], ferramentas BRMS são analisadas, e seus fornecedores são caracterizados como: líder, visionário, desafiante ou executores em nicho específico. Já [Rymer e Gualtieri 2008] apresentam uma análise das ferramentas de mercado utilizando uma série de critérios e entrevistas com os

fornecedores e clientes de cada plataforma. Para ajudar na escolha entre as plataformas, os autores apresentam ainda cinco visões do mercado de regras de negócio: plataformas para fins gerais, plataformas especializadas, plataformas para desenvolvedores de aplicações Java, plataformas para desenvolvedores de aplicações .NET e plataformas para analistas de negócio que desenvolvem e mantém aplicações. As ferramentas são avaliadas segundo o suporte a todos os tipos de regras de negócio definidos pela BRG [2009]. No entanto, não tratam as especificidades das regras de autorização de forma apropriada como, por exemplo, o controle das regras em tempo de execução do acesso aos dados armazenados nas bases de dados.

Existe um conjunto de ferramentas voltado para a execução de regras de autorização, enquanto outro conjunto se propõe à gestão e execução de regras de negócio em geral, ,mas não atendem as especificidades das regras de autorização. Desta forma, para o primeiro conjunto, é necessário um módulo (ou mesmo outra ferramenta) que facilite o cadastro, edição, alteração, versionamento, implantação etc. de regras de autorização. Por outro lado, o segundo conjunto de ferramentas deve ser analisado com cuidado a fim de avaliar o potencial de seu uso para regras de autorização.

Para a avaliação de ferramentas, um *framework* que considere os dois conjuntos de ferramentas deve ser empregado. Neste trabalho, está sendo considerado o *framework* proposto por Azevedo *et al.* [2010] que divide as regras de autorização em dois módulos: (i) Gestão de Regras de Autorização (GRA) e (ii) Execução de Regras de Autorização (ERA). O módulo GRA (Figura 1) é responsável pela criação, alteração, visualização, composição, teste e simulação de regras de autorização. O GRA permite definir regras de acesso aos termos/conceitos da organização incluindo as operações que podem ser executadas por cada perfil existente. Um exemplo de regra é "O **Gerente local** pode **consultar** apenas os **pedidos** com **valor inferior a R$ 1.000,00**". Todas as regras criadas neste módulo são armazenadas em um banco de dados de regras de autorização.

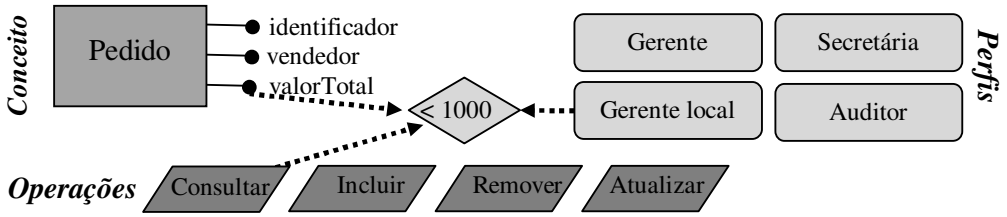

Figura 1 – Definição de regra de autorização na ferramenta de gestão

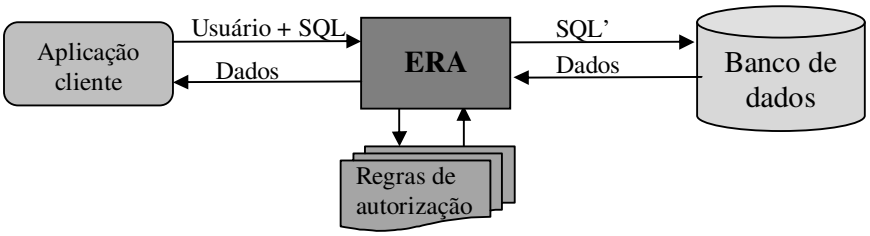

Figura 2 - Ferramenta de execução de regra de autorização

O módulo ERA (Figura 2) está de acordo com a definição de política RBAC descrita na seção 2, e é responsável por garantir que as regras de autorização definidas previamente e armazenadas na base de regras sejam garantidas. Todas as operações de manipulação (consulta, inserção, remoção e atualização) invocadas pelas aplicações do negócio sobre os dados corporativos são controladas em tempo de execução.

3. Propostas do Trabalho

Como as ferramentas BRMS existentes no mercado possuem vários componentes para gestão e para execução de regras de negócio, neste trabalho propomos um conjunto de critérios para avaliar, especificamente, o atendimento destas ferramentas para gestão e execução de regras de autorização segundo o *framework* proposto por Azevedo *et al.* [2010], apresentado na seção anterior.

Os critérios foram elaborados pela confecção de questionários, como proposto por [Tariq e Akhter 2005]. Estes questionários identificam as características mais importantes em uma ferramenta de acordo com as prioridades da organização. Os critérios foram elaborados a partir de critérios propostos em outros trabalhos de avaliação de ferramentas [Azevedo *et al.* 2008b], características das ferramentas enumeradas em comunidades de pesquisa na área [BRG 2009; BRCommunity 2009] e avaliações de ferramentas BRMS [Sinur 2005; Rymer e Gualtieri 2008]. Os critérios foram então avaliados e revisados com profissionais e pesquisadores da área. Para cada critério de avaliação foi definida uma escala de pontuação dentro do intervalo de 0 a 1, seguindo a abordagem de [Kitchenham 1996]. O extremo 0 (zero) significa uma total inadequação ou ausência do critério na ferramenta e o extremo 1 significa que a ferramenta satisfaz completamente o critério. Com o intuito de caracterizar como determinado valor deve ser atribuído em resposta a um critério, o raciocínio a ser aplicado para cada pontuação possível foi detalhado, de acordo com estudo de caso real realizado. Obviamente, a forma de pontuar pode variar de organização para organização. Ainda segundo [Kitchenham 1996], e de acordo com o observado na realidade das organizações atuais, foram definidos pesos para cada critério, na escala de 1 a 5, refletindo a importância do critério na avaliação final. Peso 1 indica uma funcionalidade insignificante, peso 2 para uma funcionalidade de baixa importância; peso 3 para uma funcionalidade útil, peso 4 para uma funcionalidade desejável mas não indispensável; e peso 5 para uma funcionalidade indispensável. Esta pontuação pode variar de organização para organização.

Nesta proposta, estendemos abordagem de [Kitchenham 1996] e, além da pontuação em escala e pesos atribuídos aos critérios, foram definidos pesos distintos para avaliação da documentação da ferramenta (peso 1) e para a avaliação dos critérios em laboratório (peso 2). Dessa forma, por exemplo, se a avaliação da documentação de acordo com um critério resultou em uma pontuação igual a 0,8 e a avaliação do mesmo critério em laboratório resultou em pontuação igual 0,6, então o resultado final seria igual a $(1 \times 0{,}8 + 2 \times 0{,}6) / (1 + 2) = 0{,}67$.

Os critérios definidos foram organizados segundo uma taxonomia de macro-critérios e foram classificados em genéricos e específicos. Macro-critérios genéricos correspondem a um conjunto de critérios que podem ser avaliados em qualquer ferramenta, independente da sua área de aplicação. Logo, podem ser utilizados tanto

para ferramenta de gestão como para ferramenta de execução. Macro-critérios específicos são aplicados especificamente às ferramentas da área em questão e foram divididos em critérios específicos para gestão e específicos para execução das regras de autorização.

Analisando cada macro-critério, pode-se observar que um macro-critério com muitos critérios terá um peso maior do que um macro-critério com poucos critérios. Por exemplo, o macro-critério "Segurança" possui 5 critérios com peso 5, o que produz um valor máximo igual a 25, enquanto que o macro-critério "Simulação de regras" tem valor máximo igual a 6. No entanto, de acordo com análises com especialistas em BRMS, observamos que "Segurança" não é 4 vezes mais importante do que "Simulação de regras". Para evitar estas distorções, foram definidos pesos também para cada macro-cirtério, após análise com pesquisadores e profissionais da área, segundo a tabela 4. Dessa forma, o cálculo da pontuação da ferramenta é realizado ponderado pelo peso atribuído a cada macro-critério.

Tabela 1 – Critérios genéricos agrupados em macro-critérios (MC)

M.	Critério
Distribuição	Como são entregues as novas versões da ferramenta?
	A empresa está em algum processo de venda ou junção?
	A empresa foi adquirida recentemente por outra empresa?
	Quantos clientes para o produto o fornecedor possui?
	Há quanto tempo a empresa está no mercado?
	Há quanto tempo a empresa disponibiliza o produto?
	A empresa vende o produto como um produto único?
	Novas versões são integráveis com a versão corrente?
Escalabilidade	Número máximo de regras que a ferramenta permite incluir/executar?
	Tempo para execução de consultas?
Flexibilidade	A ferramenta permite a adição de novas funcionalidades?
	Quais são os requisitos para realizar a programação/criação de novas funcionalidades (requisitos de linguagem de programação e software)?
	É possível customizar a ferramenta de acordo com as características específicas da empresa compradora?
Integração	Permite relacionar itens de regras de negócio com elementos de banco de dados (tabelas, relacionamentos, atributos etc)?
	Permite integração com SGDB?
Plataforma	Instalação no Linux?
	Instalação no Windows?
Qualidade da documentação	Documentação é clara quanto a objetivos e propostas da ferramenta?
	Documentação aborda instalação e configuração da ferramenta?
	Documentação aborda o uso das funcionalidades da ferramenta?
	Documentação contém tutoriais para aprendizagem da ferramenta?
	Documentação aborda questões como escalabilidade e resultados de testes com a ferramenta?
	Existe fórum de discussão da ferramenta e o fórum é utilizado intensamente?
Suporte	Existe suporte a novas versões da ferramenta? (código fechado/código aberto)
	Possui suporte por email?
	Possui suporte por telefone?
	Possui suporte *in loco*?
	Fornecedor possui parceiro no Brasil para venda e suporte?

Tabela 2 – Critérios específicos para ferramenta de gestão

M.	Critério
Edição	Permite uso por múltiplos usuários ao mesmo tempo?
	Possui um Ambiente Integrado de Desenvolvimento (IDE) de regras?
	Possui capacidades de inclusão, alteração e remoção de elementos de uma regra?
	Realiza verificação de conflito entre regras durante edição?
	Suporta a criação de vocabulários para as regras?
	Suporta linguagens para descrição de regras? Quais?
	Permite cadastrar/importar informações de usuários e associá-los às regras?
	Permite criação de elementos de regras de negócio utilizando diretamente o modo de edição gráfica?
	Tipos de regras de negócio suportadas (Segundo a classificação BRG)
	Oferece template para acelerar o processo de criação de regras?
	Possui wizards para auxiliar usuários do negócio na criação das regras?
	Permite criar wizards para auxiliar usuários do negócio na criação das regras?
	Permite realizar as operações de edição de regras através da API para integração?
Consulta	Permite realizar consultas nas linguagens de consultas para regras?
	Permite consultas restritas a domínios?
	Possui mecanismos de inferência?
	Permite utilização dos mecanismos de inferências durante a consulta?
	Permite criação de explicações em linguagem natural para as inferências realizadas pelo usuário?
	Permite a geração de relatórios derivados dos resultados de consultas?

M.	Critério
	Permite realizar as operações de consulta a regras através da API para integração?
	Permite gerar relatórios do dicionário de dados das regras.
Visualização	Possui mecanismos para visualização de regras?
	Possui formas de acesso às propriedades dos itens de regras durante sua visualização?
	É possível imprimir a visão exibida?
	Permite gerar relatórios das regras de acordo com o que se deseja visualizar?
	Permite utilizar os mecanismos de visualização de regras através da API para integração?
Exportação/ Importação	Possui conversores de formatos que apóiam a tradução da regra para outros formatos?
	Importa e exporta regras em diferentes formatos de representação?
	Possui ferramentas para derivação de regras (semi) automaticamente utilizando textos de linguagem natural?
Armazenamento	Permite armazenar diferentes versões da regra?
	Permite comparar e fazer merge entre diferentes versões da regra?
	É possível verificar conflitos e inconsistências entre versões?
	O controle de versões se dá em nível de regras e não somente em nível físico (arquivos)?
	Possui a funcionalidade de repositório distribuído?
	É possível estender o metamodelo do repositório?
	O repositório de regras é independente do componente de execução?
	É possível armazenar histórico das alterações ocorridas em cada versão da regra?

M.	Critério
Integ.	Permite realizar combinação entre regras?
	Permite definir regras de exceção?
Validação	Possui ferramentas para teste e depuração?
	Permite geração de relatórios para validação de regras?
	Permite execução de testes de consistência (ex: regras incompletas)?
Simulação	Possui um modelo de simulação de regras?
	Permite visualizar graficamente a sequência de execução da regra e suas dependências?
	Permite simular a execução da regra utilizando dados novos bem como dados antigos?
Segurança	Permite criação de contas de usuários?
	Possui controle de concorrência?
	Permite criação de perfis de acesso para usuários?
	É possível associar os perfis de acesso ao perfil do usuário da Petrobras (associando a chave)?
	É possível definir as permissões de acordo com os tipos de regras? (Ex.: Regras do Poço, Regras de bloco).
	Possui controle de acesso aos elementos das regras?
Qualidade	Permite a definição de padrões organizacionais para descrição de regras (por exemplo, regras de nomenclatura, etc.)?
	Permite a validação de padrões organizacionais pela ferramenta?
Adm	Provê ferramentas para publicação das regras de negócio nos ambientes alvo?
	Permite promover regras entre ambientes?

Tabela 3 - Critérios específicos para ferramenta de execução

M.	Critério
Execução	Nível de transparência em relação às aplicações clientes.
	Possui a opção de geração de código para linguagem de programação?
	Permite invocar as regras via web services?
	Executa a regra de negócio para um usuário/perfil específico?
	Permite diferentes modos de execução de regras (dinâmica/estática)?
Administração	Permite monitorar e rastrear a execução das regras individualmente dentro do motor de execução?
	Permite monitorar o desempenho do servidor? Por exemplo, se o servidor está sobrecarregado (por exemplo, o servidor executando em 90% da capacidade);

M.	Critério
	uso de memória etc.
Auditoria	Permite consulta ao log de execução?
	Permite visualização gráfica do log de execução?
	Provê wizards de relatórios de regras para gerar consultas customizadas às regras (por exemplo, relatórios de análise de impacto)?
	É possível verificar a associação de perfil x permissão que estão em produção?
	É possível verificar a associação de perfil x permissão que já não estão mais em produção?

Tabela 4 – Definição de pesos para cada macro-critério

Tipo	Macro-critério	Peso	Tipo	Macro-critério	Peso
Genérico	Escalabilidade	3	Gestão	Edição	5
	Flexibilidade	3		Consulta	4
	Integração com outros sistemas	3		Segurança	3
	Qualidade da documentação	3		Visualização	2
	Suporte	3		Repositório e Versionamento	2
	Plataforma tecnológica	2		Integração de regras	2
	Distribuição	1		Validação	2
Execução	Administração do ambiente de execução	2		Simulação	2
	Execução de regras	5		Exportação / Importação	2
	Auditoria	2		Qualidade das regras	1
				Administração	1

4. Avaliação de ferramentas para tratar regras de autorização

Nesta seção, apresentamos a avaliação de ferramentas BRMS executada na área de Gestão de Dados Integrada do E&P da PETROBRAS (TIC/TIC-E&P/GDIEP), com o objetivo de indicar uma ferramenta que desse suporte à gestão e execução de regras de

autorização. A PETROBRAS é a maior e mais importante empresa de óleo e gás do Brasil. O departamento de Gestão de Dados e Informações do E&P (GDIEP) é responsável pela gestão dos dados no domínio de óleo e gás da exploração e produção.

O processo utilizado para avaliação das ferramentas corresponde a uma adaptação do processo proposto pela SEI (Software Engineering Institute) apresentado em [COMELLA-DORA 2004]. O processo é ilustrado na Figura 3.

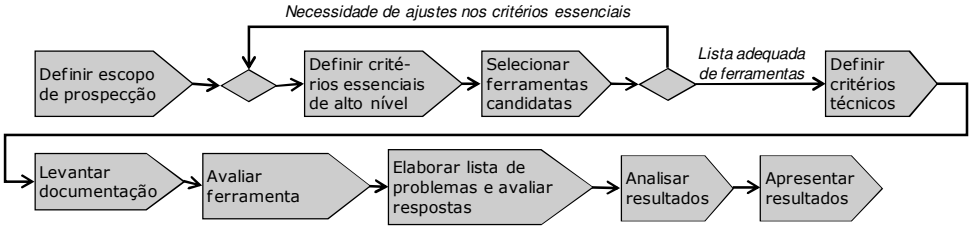

Figura 3 – Processo para avaliação de ferramentas [Azevedo *et al.*, 2008a]

1. **Definir escopo de prospecção:** O objetivo do trabalho de prospecção de ferramentas foi encontrar uma ferramenta que permitisse à GDIEP realizar a gestão de regras de autorização, bem como garantisse a execução de regras de autorização.

2. **Definir critérios essenciais de alto nível:** Os critérios essenciais foram definidos de acordo com o tipo de ferramenta. Para a ferramenta de gestão foram definidos os critérios: (i) possuir interface gráfica para manipulação da regra; (ii) permitir integração com a ferramenta de execução; (iii) possuir suporte. Para a ferramenta de execução foram definidos os critérios: (i) permitir a execução de regras de autorização sobre dados armazenados no SGBD Oracle com o menor impacto possível para as arquiteturas de acesso a dados; (ii) possuir suporte.

3. **Selecionar ferramentas candidatas:** A escolha das ferramentas para avaliação foi baseada nas referências às empresas que possuem ferramentas BRMS apresentadas por [BRG 2000] e [BRCommunity, 2009], além das ferramentas avaliadas por [Sinur 2005] e [Rymer e Gualtieri 2008] e pesquisas realizadas.

   As seguintes ferramentas foram escolhidas para avaliação: Corticon Business Rules Management System[1]; ESI Logist[2]; FICO Blaze Advisor[3]; ILOG BRMS[4]; JBoss Enterprise BRMS[5]; RuleXpress[6]; SAP NetWeaver BRM[7]; Sapiens eMerge[8]; Ness Usoft[9]; Visual Rules[10]; G2 Plataform[11]; Versata BRMS[12]; PegaRules[13]; InRule[14]; Oracle Business Rules[15], ARIS Business Rule Designer[16].

[1] (http://www.corticon.com/Products/Business-Rules-Management-System.php)
[2] http://www.esi-knowledge.com/products_logist.aspx
[3] http://www.fico.com/en/Products/DMTools/Pages/FICO-Blaze-Advisor-System.aspx
[4] http://www.ilog.com/products/businessrules/index.cfm
[5] http://www.jboss.com/products/platforms/brms/
[6] http://www.rulearts.com/RuleXpress
[7] http://www.sap.com/platform/netweaver/components/brm/index.epx
[8] http://www.sapiens.com/Dev2Go.Web?id=207028
[9] http://www.usoft.com
[10] http://www.visual-rules.com/business-rules-management-enterprise-decision-management.html
[11] http://www.gensym.com/index.php?option=com_content&view=article&id=47&Itemid=54

Com esse conjunto de ferramentas levantado, foi feita uma pesquisa sobre cada ferramenta para adquirir as informações necessárias para responder aos critérios essenciais definidos no passo 2.

Praticamente todas as ferramentas atenderam aos critérios essenciais para gestão de regras de autorização, enquanto algumas atendiam aos critérios essenciais para execução de regras de autorização. As restrições de prazo estabelecidas para a avaliação impuseram um ajuste nos critérios essenciais, de forma a reduzir o número de avaliações detalhadas. Foi incluído um critério essencial adicional: o bom posicionamento da ferramenta nas avaliações realizadas por [Sinur 2005] e [Rymer e Gualtieri 2008]. A partir deste ajuste, as seguintes ferramentas foram selecionadas para serem avaliadas detalhadamente: WebSphere Ilog BRMS; InRule; Corticon; FICO Blaze Advisor; Usoft; ESI Logist.

4. **Definir critérios técnicos:** Os critérios técnicos utilizados para realizar as avaliações foram os apresentados na seção 3.2. Foram utilizados 29 critérios genéricos, 55 critérios para avaliar ferramentas quanto à gestão de regras de autorização e 11 critérios para avaliação quanto à execução de regras de autorização.
5. **Levantar documentação com fornecedores:** A equipe de avaliação de ferramentas entrou em contato com os fornecedores, obtendo manuais, tutoriais, vídeos, *data sheets*, *white papers* e outros documentos para realizar a avaliação.
6. **Avaliar ferramentas**: Os critérios definidos no passo 4, e apresentados na seção 3.2 (Tabelas 1-3), foram respondidos por analistas de sistemas (chamados de Avaliadores) treinados em avaliação de ferramentas e na aplicação dos critérios definidos. As avaliações foram revisadas por um profissional experiente na avaliação de ferramentas e na aplicação dos critérios (chamado de Avaliador máster). Após a revisão pelo Avaliador máster, os Avaliadores fizeram ajustes nas avaliações realizadas.

   Os macro-critérios da Tabela 4 foram priorizados por profissionais da própria organização.

   Para cada ferramenta foram realizadas três avaliações: quanto aos critérios genéricos; quanto aos critérios específicos para gestão; quanto aos critérios específicos para execução. A partir daí, foram realizados dois tipos de avaliações: avaliação em relação à documentação, onde cada critério deveria ser respondido consultando apenas as documentações disponibilizadas pelo fornecedor; e, avaliação em laboratório, na qual cada critério foi testado em laboratório. Foi definido peso 1 para o resultado obtido a partir da avaliação em relação à documentação, e peso 2 para o resultado obtido na avaliação em laboratório.

   Depois que as ferramentas foram avaliadas, uma planilha foi gerada para cada ferramenta com a pontuação de cada critério. Os critérios que não obtiveram

[12] http://www.versata.com/index2.php?option=com_content&task=view&id=124
[13] http://www.pega.com/Products/RulesTechnology.asp
[14] http://www.inrule.com/products/InRule.aspx
[15] http://www.oracle.com/technology/products/ias/business_rules/index.html
[16] http://www.ids-scheer.com/en/ARIS/ARIS_Platform/ARIS_Business_Rules_Designer/3747.html

nota máxima foram comentados justificando a razão da perda de pontuação de cada critério.

7. **Elaborar lista de problemas e avaliar respostas:** As características que tiveram problemas durante a avaliação foram listadas e os fornecedores foram contatados para enviarem respostas para estes problemas. As respostas foram analisadas.

8. **Analisar resultados:** O quadro de pontuação de cada ferramenta resultante da execução da etapa 6 foi ajustado. As notas dos critérios em dúvida foram alteradas de acordo com as respostas dos problemas identificados e foi calculada a pontuação final de cada ferramenta, a qual é apresentada parcialmente na Tabela 5. Observe que algumas avaliações receberam "-" como pontuação. Este valor foi atribuído após analisarmos a ferramenta e identificarmos que as mesmas não tinham uma arquitetura adequada para o tipo de ferramenta. Esta análise, em muitos casos, ocorreu através de discussões por telefone e email com equipe técnica do fornecedor, como foi o caso das ferramentas ILOG e CORTICON. No caso da ILOG, inclusive, houve discussão pessoalmente com o técnico responsável pelo suporte da ferramenta no Brasil. As discussões com equipe técnica das outras ferramentas foram realizadas por telefone.

Tabela 5 - Pontuação final obtida por cada ferramenta

		ILOG	InRule	Corticon	Blaze Advisor
Genéricos		77%	32%	77%	65%
Gestão	Documentação	72%	47%	68%	54%
	Laboratório	71%	47%	-	39%
Total		73%	43%	-	49%
Execução	Documentação	-	59%	23%	-
	Laboratório	-	33%	-	-
Total		-	39%	-	-

9. **Apresentar resultados:** Os resultados obtidos com cada avaliação foram apresentados aos membros da equipe de funcionários do departamento de Gestão de Dados e Informações do E&P da PETROBRAS (TIC/TIC-E&P/GDIEP). Eles são as pessoas responsáveis pela tomada de decisão.

5. Conclusões

Segurança da informação é um tópico de pesquisa que tem recebido cada vez mais atenção, tanto em contextos comerciais quanto governamentais. Dessa forma, a autorização de acesso a informações em organizações é determinante. Autorização de acesso é um tipo de regra de negócio (regra de assertiva de ação de autorização) [BRG 2009], e restringe a **quem** é permitido realizar uma **ação** na organização sobre quais **informações**.

Existem várias ferramentas no mercado para tratar regras de negócio. Estas ferramentas são denominadas BRMS. Avaliações quanto às funcionalidades das mesmas são apresentadas por [Sinur 2005] e [Rymer e Gualtieri 2008]. No entanto, estes trabalhos avaliam estas ferramentas quanto à gestão e execução dos seguintes tipos de regras de negócio [BRG, 2009]: definição de termos de negócio, fatos relacionando termos entre si, derivações e sentenças de ação. Estas avaliações não tratam de forma apropriada regras de autorização e suas especificidades, como o controle em tempo de

execução de forma a não impactar o desempenho das aplicações no acesso às fontes de dados corporativas.

Este trabalho utilizou um framework para avaliação de ferramentas para gestão e execução de regras de autorização, composto por uma arquitetura genérica de ferramentas e propôs um processo, uma taxonomia de critérios de avaliação e um método de cálculo das notas atribuídas aos critérios. A arquitetura genérica é composta por dois módulos, dividindo as ferramentas analisadas em ferramentas para gestão de regras de autorização e ferramentas para execução de regras de autorização. O método de cálculo das notas adicionou pesos aos critérios e aos macro-critérios, além de escalas de pontuação definidas em conjunto entre especialistas de domínio e especialistas em avaliação de ferramentas em geral.

As ferramentas avaliadas foram selecionadas a partir de pesquisas, avaliações anteriormente realizadas e consultas aos sítios dos fornecedores de ferramentas mais importantes. As bem classificadas na avaliação essencial foram então avaliadas de forma detalhada. Como resultado, observamos que as ferramentas possuem muitas funcionalidades para gestão de regras de autorização, tais como: edição, consulta, visualização da regra e dependências entre regras, versionamento, controle de concorrência, permitem um nível de abstração mais elevado para descrever as regras etc. No entanto, as ferramentas não se mostraram adequadas para execução de regras de autorização. Além disso, estão mais voltadas para outros tipos de regras e não para regra de autorização. Portanto, as avaliações realizadas demonstraram ser possível adotar uma das ferramentas avaliadas para gestão de regras e as funcionalidades de um SGBD tanto para armazenamento das regras quanto para a execução de regras de autorização.

Como trabalho futuro, propomos considerar no método o fato do resultado final ter ferramentas com pontuações muito próximas. Neste caso, uma segunda etapa de avaliação, por exemplo, considerando apenas os critérios considerados mais relevantes pela organização, poderia ser executado. Outra informação que poderia ser incorporada ao método é a determinação de um limite mínimo de pontuação que uma ferramenta deve atingir. Neste caso, se uma ferramenta não alcançar este limite em uma avaliação (por exemplo, na avaliação segundo os critérios genéricos), ela deveria ser descartada do processo de avaliação.

Agradecimentos

Agradecemos à TIC/TIC-E&P/GDIEP (PETROBRAS) pelo apoio a este trabalho.

References

AZEVEDO, L. G., LOPES, M., SOUZA, J., SIQUEIRA, S., CAPPELLI, C., BAIAO, F.A., 2008a. “Uma metodologia de avaliação de ferramentas para gestão de ontologias”. In: Seminário de Pesquisa em Ontologia no Brasil, Niterói.

AZEVEDO, L. G., SOUZA, J., LOPES, M., SIQUEIRA, S., CAPPELLI, C., BAIAO, F.A., *et al.* 2008b. “Inspeção de Ferramentas de Ontologias”. Relatório Técnico 0003/2008, Departamento de Informática Aplicada da UNIRIO, Rio de Janeiro.

Azevedo, L. G., Puntar, S., Thiago, R., Baião, F., Cappelli, C., 2010. “A Flexible Framework for Applying Data Access Authorization Business Rules”. In: 12th

International Conference on Enterprise Information Systems (ICEIS 2010), Funchal, Madeira, Portugal.

BRCOMMUNITY (2009) "Business Rules Community". http://www.brcommunity.com.

BRG (2009) "The Business Rules Group". http://www.businessrulesgroup.org.

CALÌ, A. E MARTINENGHI, D. (2008). Querying data under access limitations. In Proc. of ICDE, Cancun.

CHEN, L. e CRAMPTOM, J. (2009) "Set Covering Problems in Role-Based Access Control". In: Proceedings of 14th European Symposium on Research in Computer Security, Saint-Malo, France.

COMELLA-DORA, S., DEAN, J., LEWIS, G., MORRIS, E., OBERNDORF, P., HARPER, E. (2004) "A Process for COTS Software". Technical Report CMU/SEI-2003-TR-017. Carnegie Mellon Software Engineering Institute.

DEITERT, E., MCCOY, D. (2007) "The Anatomy of a Business Rule Management System". Gartner Research.

DoD (1983) "Trusted Computer Security Evaluation Criteria". Department of Defense, DoD 5200.28-STD.

FERRAIOLO, D.F. e KHUN, D. R. (1992) "Role-Based Access Control". In: 15th National Computer Security Conference, pp. 554—563, Baltimore, MD.

FERRAIOLO, D.F., SANDHU, R., GAVRILA, S., KUHN, D.R., CHANDRAMOULI, R. (2001) "Proposed NIST standard for role-based access control". ACM Transactions on Information and System Security (TISSEC) 4 (3), pp. 224—274.

KITCHENHAM, B. (1996) "DESMET: A method for evaluating software engineering methods and tools". http://www.osel.co.uk/desmet.pdf.

MURTHY, R. E SEDLAR, E. (2007). Flexible and efficient access control in oracle. In *ACM SIGMOD 2007*, pp. 973-980, Beijing.

RYMER, J., GUALTIERI, M. (2008) "The Forrester Wave™: Business Rules Plataform, Q2". Forrester Research, http://www.forrester.com/go?docid=39088.

SANDHU, R.S., COYNE, E.J., FEINSTEIN, H.L., YOUMAN, C.E. (1996) "Role-based access control models". IEEE Computer, vol. 29, no. 2, pp 38-47.

SINUR, J. (2005) "Magic Quadrant for Business Rule Engines", Gartner Research.

TARIQ, N.A. e AKHTER, N. (2005) "Comparison of Model Driven Architecture (MDA) based tools". In: Proceedings of 13th Nordic Baltic Conference (NBC), v. 9.

YANG, L. (2009) "Teaching database security and auditing". ACM SIGCSE'09, v.1, issue 1, pp. 241—245.