Análise da Aplicabilidade do Uso de Ontologias e Regras Semânticas para Apoiar a Verificação de Conformidade no Contexto de Arquiteturas Orientadas a Serviço

Haroldo Maria Teixeira Filho[1,2], Leonardo Guerreiro Azevedo[1], Sean Siqueira[1]

[1]Programa de Pós-Graduação em Informática – Universidade Federal do Estado do Rio de Janeiro (UNIRIO)
Avenida Pasteur, 458 - Urca - Rio de Janeiro / RJ - CEP: 22290-240

[2]Administração de Serviços e Informações – Petróleo Brasileiro S/A
General Canabarro 500, 4º Andar – Maracanã – Rio de Janeiro / RJ – CEP: 20271-900

{haroldo.filho,Azevedo, sean}@uniriotec.br

Abstract. *Several organizations have used Service-Oriented Architecture to achieve cost and schedule gains. However, the success of this kind of strategy depends on the implementation of governance mechanisms that allows an architectural evolution aligned with the organization's objectives. To reach this goal, compliance with corporate policies must be ensured. This work proposes an approach for using ontologies and semantic rules to support the compliance evaluation in the SOA context. A proof of concept in a real scenario was executed demonstrating the proposal applicability.*

Resumo. *Muitas organizações tem utilizado a arquitetura orientada a serviços (SOA) para conseguir ganhos em custos e prazos. Porém o sucesso desta abordagem depende da implantação de mecanismos de governança que permitam a evolução da arquitetura alinhada com os objetivos do negócio. Dessa forma, é fundamental garantir conformidade com políticas corporativas. Este trabalho propõe abordagem de uso de ontologias e regras semânticas para apoiar a verificação de conformidade no contexto SOA. Uma prova de conceito considerando um cenário real foi conduzida comprovando a aplicabilidade da proposta.*

1. Introdução

Arquitetura orientada a Serviço (SOA) é um paradigma para construção de aplicações baseado em unidades reutilizáveis de software denominadas serviços, invocadas remotamente através de interfaces padronizadas (Josuttis, 2007). Os detalhes referentes à construção do serviço são abstraídos, inclusive a tecnologia utilizada, cabendo ao consumidor do serviço conhecer apenas uma descrição da interface para seu uso (Erl, 2005; Papazoglou, 2003). Nesta descrição são informadas as operações disponíveis, dados a serem trocados, a localização física do serviço e eventuais políticas que devem ser consideradas durante o seu uso, como, por exemplo, diretivas de segurança.

Dentre os benefícios identificados na literatura, podemos citar menores custos de desenvolvimento e manutenção, menores ciclos de desenvolvimento e maior flexibilidade e estabilidade das soluções de TI (Erl, 2005; Papazoglou, 2003). Porém, de acordo com o Open Group (The Open Group, 2009), existe dificuldade de estender estes ganhos para uma escala corporativa. São desafios da implantação de SOA (Niemann *et al.*, 2010; Schepers, Iacob e Van Eck, 2008):

- Garantir conformidade com regulamentações internas, externas e legais;
- Tratar questões referentes às múltiplas partes interessadas (*stakeholders*) e seus papéis e responsabilidades;
- Promover uma cultura de reuso e compartilhamento;
- Tratar modelos financeiros que contemplem compartilhamento de recursos;
- Controlar o impacto de mudanças em cenários heterogêneos, com múltiplos envolvidos.

Diversos trabalhos (Dias Jr, *et al.* 2012; Hojaji e Shirazi, 2010; Janiesch, *et al.*, 2009; Niemann *et al.*, 2010) apontam a implantação de governança SOA como solução para estes desafios. Janiesch *et al.* (2009) definem governança SOA como o estabelecimento de estruturas, processos, políticas e métricas apropriados para garantir a adoção, implementação, operação e evolução de uma arquitetura orientada a serviços alinhada com os objetivos de negócio e conforme com leis, regulamentações e boas práticas. Existem diversas abordagens para governança de serviços na academia (Hojaji e Shirazi, 2010; Niemann *et al.*, 2010; Papazoglou, 2003) e no mercado (Bennett, 2012).

Existe um conjunto elevado de processos e políticas para governança envolvendo contextos variados, indo desde questões técnicas, como acordos de níveis de serviço e mecanismos de autenticação (The Open Group, 2009), até questões relativas ao negócio, como a responsabilidade e limite de competência de cada nível da organização (Janiesch *et al.*, 2009). As características das principais propostas para governança SOA foram analisadas por Teixeira Filho e Azevedo (2012), os quais explicitaram diferenças e semelhanças entre elas e identificaram a necessidade de 51 processos para governança SOA. Niemann *et al.* (2010) identificaram nove domínios de políticas necessárias para apoiar estas atividades. Considerando este volume de elementos a serem validados e a diversidade de domínios de conhecimento envolvidos, a verificação de conformidade destes elementos se torna uma atividade complexa e onerosa. Dessa forma, métodos e ferramentas para simplificar esta validação precisam ser propostos.

Este trabalho apresenta uma aplicação prática do uso de ontologias e de regras para apoio a atividade de verificação de conformidade de arquiteturas orientadas a serviço. Ontologia é uma especificação explícita de uma conceituação (Gruber, 1993). Seu grande ganho é a possibilidade de interpretação por agentes computacionais, viabilizando o desenvolvimento de ferramentas que operem sobre o seu modelo.

A proposta deste trabalho apresenta uma evolução da ontologia para governança SOA proposta pelo Open Group (2010) e define mecanismos para garantir conformidade da implantação de uma abordagem SOA com políticas corporativas definidas a partir de conceitos definidos na ontologia.

Este trabalho é dividido da seguinte forma. A Seção 2 trata das propostas existentes na literatura a respeito do uso de ontologias e regras no contexto de governança. A Seção 3 apresenta uma proposta de ontologia e regras. A Seção 4 descreve os resultados de uma prova de conceito para verificar seu uso para identificação de conformidade. A Seção 5 apresenta as conclusões e trabalhos futuros.

2. Trabalhos relacionados

Nesta seção é apresentada uma análise dos trabalhos relacionados ao uso de ontologias para descrever o contexto SOA e para apoiar tarefas de governança.

2.1. Ontologias para SOA e Governança

Diversos trabalhos foram desenvolvidos a respeito do uso de ontologias para SOA e para governança como apresentado a seguir.

O Open Group (The Open Group, 2010) propôs uma ontologia para representar os conceitos envolvidos em uma arquitetura orientada a serviços. O trabalho considera como principais conceitos: (i) elementos, que representam quaisquer itens existentes em um contexto SOA; (ii) sistemas, que representam conjuntos de elementos; (iii) atores humanos, que representam unidades organizacionais, papéis ou pessoas que executam tarefas em um determinado negócio; (iv) serviços, que representam atividades de negócio executadas por algum elemento (sistema ou ator humano); (v) contratos de serviços e interfaces de serviços que especificam o que o serviço realiza; (vi) composições, que simbolizam grupos de elementos que executam funções de acordo com um padrão de composição (orquestração, coreografia ou colaboração); e (vii) políticas, que representam diretrizes a serem seguidas por elementos de acordo com a intenção de uma ou mais organizações. Uma visão resumida desta proposta é apresentada na Figura 1, considerando as linhas contínuas como relações de especialização e as linhas tracejadas como propriedades de objetos. Esta proposta foca em componentes que constituem soluções orientadas a serviço, porém não representa elementos necessários para governança, como processos, métricas e objetivos.

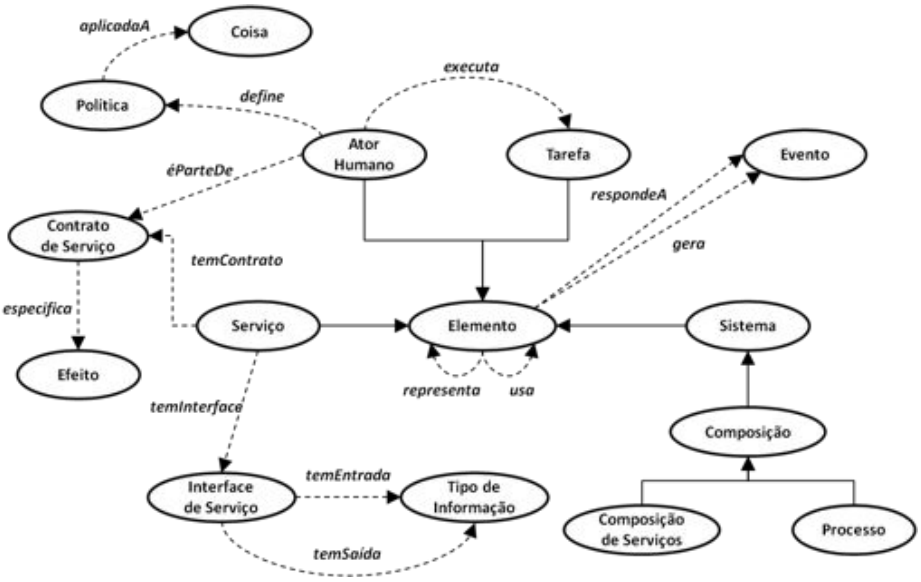

Figura 1. Ontologia para SOA (adaptada de (The Open Group, 2010))

Janiesch *et al. (2009)* propõem um conjunto de conceitos para governança SOA derivados de outros modelos de governança de TI, em especial COBiT (Cobit 4.1, 2007) e ITiL (Adams, 2009). Para tal, são considerados três domínios (Figura 2). O domínio Processos e Papéis, no qual são representados processo, artefato, papel, ferramenta, métrica e habilidade. Este domínio representa a estrutura necessária para constituir uma arquitetura. O domínio Visão e Indicadores, no qual são representados conceitos de modelo de maturidade, modelo de governança e fase. Este domínio permite criar visões da evolução da arquitetura de acordo com sua maturidade ou mapeando-a para outros frameworks de governança de TI. Por fim, o domínio Detalhes da Organização contempla conceitos que permitem descrever uma estrutura organizacional, desde uma organização até um indivíduo. Este modelo permite incluir relações entre artefatos gerados na arquitetura e seus respectivos processos. No entanto, ele não representa os objetivos SOA e não há uma relação com os elementos que constituem a arquitetura orientada a serviços. Além disso, ele não possui construtos para representar políticas organizacionais.

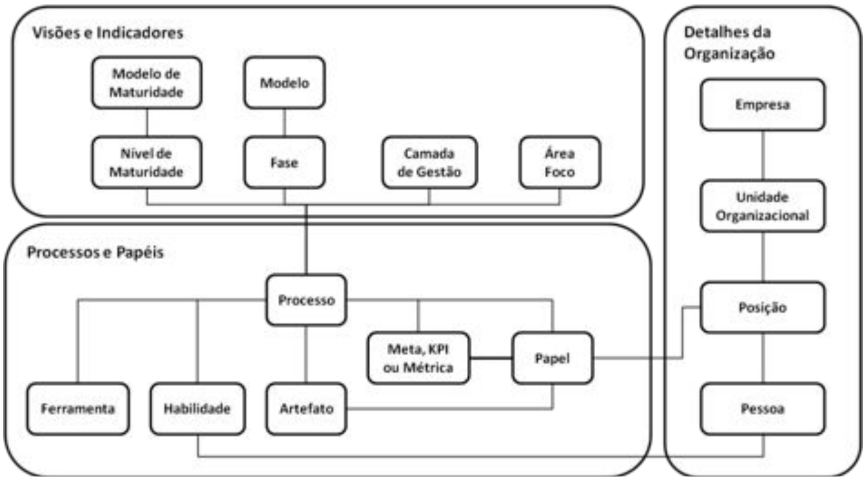

Figura 2. Conceitos para governança SOA de acordo com Janiesch *et al.* (2009)

Um exemplo específico de representação de políticas é proposto por Hu *et al.* (2011) através de uma ontologia para descrever políticas de segurança, considerando os conceitos: (i) sujeito: é avaliado quanto à política; (ii) recurso: objeto a ser manipulado pelo sujeito; (iv) ação: operação que o sujeito deseja realizar; (v) condição: eventuais restrições para a política; e (vi) efeito: resultado esperado para a situação (permitido ou não permitido). Utilizando esta representação, os autores propõem um framework para identificação de anomalias em políticas através da realização de inferências sobre a ontologia. Este trabalho apresenta o uso de ontologias e algoritmos para otimizar a validação da integridade de conjuntos de políticas, mostrando como tecnologias semânticas podem apoiar governança, porém seu contexto é de políticas de controle de acesso, sem referência a uma aplicação no contexto SOA.

Por fim Parejo, Fernandez e Ruiz-Cortés (2011) propõem definir descrições de políticas e processos para governança através de documentos de governança, que listam os recursos envolvidos (pessoas, serviços, sistemas), vocabulário a ser empregado, e as políticas sob a forma de regras. Para cada contexto, como por exemplo, uma organização ou departamento, é definido um documento de governança distinto, permitindo assim que múltiplos modelos coexistam. Neste trabalho, as ontologias são utilizadas somente para formalizar o vocabulário empregado, sem serem utilizadas para implementar melhorias nas atividades de governança SOA.

2.2. Uso de regras para validação de conformidade

Nesta seção são listados trabalhos que tratam mecanismos de verificação de conformidade baseados em regras.

Spies (2012) propõe o uso de regras descritas em Semantic Web Rule Language (SWRL)[1] para viabilizar a verificação de conformidade de maneira contínua. A validação do seu trabalho corresponde a criação de uma ontologia baseada no modelo COBiT combinada com modelos de verificação de segurança, descrita em OWL[2]. Foi aplicado um conjunto de regras para identificar não conformidades. Apesar de interessante, a abordagem é limitada ao contexto do framework COBiT, sem cobrir aspectos específicos de SOA.

Li *et al.* (2011) propõem criar uma camada de regras utilizando o framework Jena[3], de forma que agentes realizem a mediação de transações, utilizando as regras para verificar se estas se encontram em conformidade com os requisitos de segurança corporativos. Eles também propõem uma arquitetura que modifica o conteúdo das mensagens para incluir informação de contexto que é utilizada para alimentar as regras. Esta abordagem foca mais na implementação dos agentes para controlar o acesso do que na validação de conformidade propriamente dita e se aplica somente ao contexto de segurança, não tratando os aspectos de SOA.

Baiôco *et al.* (2009) propõem uma ontologia que utiliza ontologias de fundamentação (UFO-A, UFO-B e UFO-C) (Guizzardi, 2005) para descrever o domínio de gerência de configuração do ITiL. Para descrever as políticas a serem seguidas, são propostos diversos axiomas que complementam a ontologia. Este trabalho descreve detalhadamente como aplicar ontologias para descrever um domínio de governança, porém foca em apenas um processo do modelo ITiL (gerência de configuração), sem tratar questões específicas de SOA e utiliza a ontologia e regras para descrição do domínio, sem apresentar uma aplicação que apoie o contexto de governança.

3. Abordagem apoio à Governança SOA com Uso de Ontologias e Regras

Nesta seção é apresentada a proposta deste trabalho. A Seção 3.1 descreve a organização da proposta. A Seção 3.2 apresenta a construção da ontologia. A Seção 3.3 descreve exemplos de como políticas são transcritas em regras.

3.1 Descrição da Proposta

A hipótese considerada neste trabalho é que o uso de regras para descrever políticas de governança, aliado a uma ontologia que represente os conceitos de governança SOA e regras definidas empregando estes conceitos, reduz o trabalho de diagnóstico de conformidades em uma arquitetura orientada a serviços.

---

[1] Uma linguagem de regras para a Web Semântica proposta pelo W3C, combinando OWL-DL e OWL Lite com RuleML. http://www.w3.org/Submission/SWRL/

[2] OWL, ou Web Ontology language, é a linguagem para descrição de ontologias na Web proposta pela W3C. http://www.w3.org/2004/OWL/

[3] Jena é um framework Java da Apache para construir aplicações na Web Semântica. http://jena.apache.org/

Para verificar esta hipótese, foi criada uma ontologia baseada no modelo proposto pelo Open Group (The Open Group, 2010), com adição de elementos para apoiar a governança. Como o objetivo é tratar conformidade, foram selecionados conceitos que conseguissem, de maneira simplificada, representar os elementos que compõe uma arquitetura orientada a serviços.

Para desenvolver a ontologia foi considerado um processo simplificado, semelhante à metodologia 101 (Noy e McGuinness, 2001). Como a necessidade deste trabalho envolvia a geração de uma ontologia simples, com foco na verificação da hipótese proposta, e considerava o uso de uma ontologia existente, foi utilizada uma simplificação desta metodologia, de acordo com os seguintes passos:

1. Definição das políticas a serem validadas;
2. Listagem de questões de competência para delimitar o escopo da ontologia;
3. Projeto conceitual da ontologia em ferramenta UML;
4. Implementação da ontologia no Protégé[4];
5. Transcrição manual das regras para o Protégé;
6. Testes no próprio Protégé para validar o funcionamento.

3.2. Construção da Ontologia

O primeiro passo da construção da ontologia foi listar um conjunto de políticas para servir de base para a validação da aplicabilidade da proposta. Para fins deste trabalho, foram consideradas duas políticas:

- Política 1: Todo serviço pertence a uma área de uma organização, sendo esta responsável por sua correta operação;
- Política 2: Todo consumo de um serviço deve ser estabelecido através de um contrato emitido pelo responsável pelo serviço liberando o uso do serviço pela área responsável pelo sistema que irá consumi-lo.

A ontologia capaz de atender à validação de conformidade destas políticas deve responder as seguintes questões:

- Q1: Qual a área que administra um determinado serviço?
- Q2: Quem autorizou o acesso a um determinado serviço?
- Q3: Quais são as partes envolvidas em um contrato de serviço?
- Q4: Quais os contratos estabelecidos para um determinado serviço?
- Q5: Qual a área que administra uma determinada aplicação?
- Q6: Quais os serviços cujos acessos são liberados por um contrato?

[4] Protégé é um editor de ontologias, de código aberto e livre desenvolvido pela universidade de Stanford. http://protege.stanford.edu/

Com base nestas questões, foi montada uma ontologia com o Protégé, tomando como base a ontologia proposta pelo Open Group e complementando-a com novos elementos visando atender aos requisitos deste trabalho. Em especial:

- Foi criada uma nova propriedade de objeto, denominada *manages*, cujo domínio é *HumanActor* e o âmbito é de *Elements*. Esta propriedade representa o papel que uma determinada área pode ter como gestora de um elemento. Ela foi adicionada ao modelo porque a ontologia do OpenGroup considera apenas partes relacionadas, sem considerar papéis específicos. Também foi considerada uma propriedade inversa denominada *managedBy* e esta propriedade foi considerada transitiva, para conseguir representar hierarquias nas organizações;
- O conceito *Service Contract* da ontologia do Open Group se tornou domínio de uma propriedade de objeto *grantsAccessTo* que permite identificar que sistemas podem utilizar o serviço quando do estabelecimento do contrato. Também foi definida a sua inversa, *accessGrantedBy*.

Uma visão da estrutura da ontologia é apresentada na Figura 3. Esta ontologia foi desenvolvida utilizando o Protégé e armazenada em formato OWL. A barra após o nome de uma propriedade de objeto denota uma propriedade inversa.

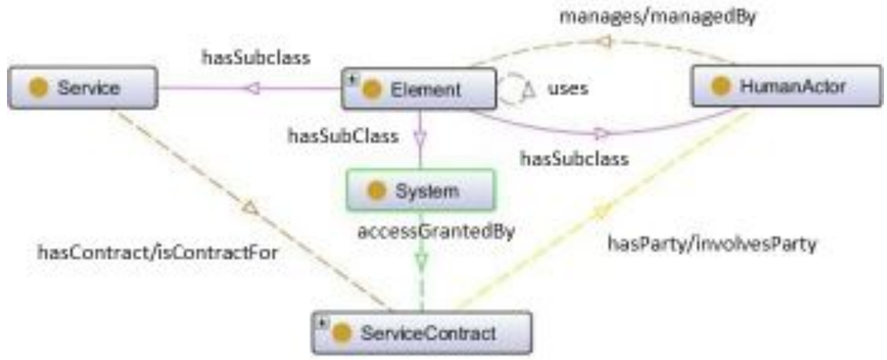

Figura 3. Conceitos da ontologia proposta modelada no Protégé

3.3. Implementação de políticas como regras

As políticas 1 e 2 foram então convertidas para o formato de descrições de regras da ferramenta Protégé, nos levando as seguintes expressões:

- Se um serviço *s* está em conformidade com a política 1, então este serviço será gerenciado por um ator humano *m* (pessoa ou área da organização). Tal condição pode ser expressa pela regra a seguir:

HumanActor(?m), Service(?s), managedBy(?s, ?m) -> CompliantThingWithPolicy1(?s)

- Se um determinado sistema *sy* está em conformidade com a política 2, então o sistema *sy*, cuja área responsável por sua gestão é a área *ay* e o serviço *sv* cuja área responsável por sua gestão é a área *av* são tais que *sy* usa o serviço *sv* e há um contrato *sc* criado para o serviço *sv* que habilita o acesso a *sy* e envolve as partes, comprovando que o sistema *sy* possui autorização para utilizar o serviço *sv*. Tal condição pode ser expressa pela regra a seguir:

System(?sy), HumanActor(?ay), managedBy (?sy, ?ay),
Service(?sv), HumanActor(?av), managedBy(?sv, ?av),
uses(?sy, ?sv),
ServiceContract(?sc), hasContract(?sv, ?sc), accessGrantedBy (?sy, ?sc),
involvesParty(?sc, ?ay), involvesParty (?sc, ?av), -> CompliantWithPolicy2(?sy)

4. Aplicação da Proposta em um Cenário Real

Para demonstrar o funcionamento da proposta, esta foi aplicada em uma amostra dos serviços utilizados por uma empresa brasileira do ramo de energia. O objetivo era comparar o tempo e a qualidade da verificação de conformidade realizada por um analista manualmente e com o apoio da ontologia e regras.

Para tal, foram carregadas na ontologia informações a respeito de quatro serviços utilizados para consulta de dados de colaboradores, dois serviços para consulta de estrutura organizacional e um serviço para consulta de dados de empresas subsidiárias da organização. A seleção destes serviços se baseou nos seguintes critérios: (i) os serviços relativos a colaboradores possuem gestores formalmente definidos, enquanto que os outros serviços não dispõem desta designação, permitindo uma avaliação da política 1; e (ii) os sete serviços em questão são os serviços mais reutilizados na organização, atendendo a quinze sistemas distintos, possibilitando quinze verificações da política 2. As informações carregadas contemplavam os serviços, sistemas, contratos e atores humanos envolvidos.

Uma vez carregados os dados, foi executada a verificação de conformidade utilizando a ontologia através do Protégé, solicitando que este classificasse serviços e sistemas respectivamente em categorias *CompliantWithPolicy1* e *CompliantWithPolicy2*. Este procedimento levou 5 segundos para executar, obtendo os resultados apresentados na Tabela 1.

Tabela 1. Resultados obtidos através do uso da solução proposta

Item	Quantidade	Não conformidades detectadas
Serviço	7	3 referentes a política 1
Sistema	15	10 referentes a política 2
Atores Humanos	19	Não se aplica na verificação de conformidade

Em seguida, foi solicitado a um analista da empresa, com experiência de 3 anos na auditoria de políticas de SOA e com 8 anos de experiência em TI, para realizar a mesma validação sobre o mesmo conjunto de elementos, sem o uso da ontologia, dispondo apenas de documentos e acesso ao barramento e repositório de serviços da organização. Neste caso, a tarefa teve duração de quatro horas e foram identificados os resultados apresentados na Tabela 2.

Tabela 2. Resultados obtidos através de análise manual dos dados

Item	Quantidade	Não conformidades identificadas
Serviço	7	3 referentes a política 1
Sistema	15	12 referentes a política 2
Atores Humanos	19	Não se aplica na verificação de conformidade

É possível verificar que ambas as abordagens levaram a identificação da mesma quantidade de não conformidades relativas à política 1, porém ocorreu divergência quanto ao número de não conformidades identificadas para a política 2. Para entender a causa desta diferença, foi realizada uma análise considerando a massa de dados utilizada para as instâncias de serviço, contratos de serviços e atores humanos, como ilustrado na tela capturada do Protégé (Figura 4) e descritas a seguir.

Figura 4. Instâncias dos contratos existentes na ontologia (tela do Protégé)

Na primeira coluna (*Individual*) são apresentadas cada uma das instâncias de contratos de serviço existentes na ontologia (por exemplo, contrato WF21_ASGD). Como temos quinze sistemas usuários de serviços e apenas sete contratos e a política demanda a existência de um contrato para acesso ao serviço, tal fato já nos gera oito não conformidades. Na segunda coluna (*involvesParty*) são expressos os atores humanos envolvidos no consumo do serviço, sendo um obrigatoriamente o gestor do serviço e o outro o gestor do sistema, respectivamente. A terceira coluna (*grantsAccessTo*) representa o sistema cujo acesso é concedido através do contrato, representado através de seu código de identificação na área de TI da empresa. A quarta coluna *(isContractFor)* representa o serviço cujo acesso é liberado. Como exemplo de informação armazenada temos que o serviço WORKFORCE_2.1 é gerido pelo gestor RH/PA e tem acesso liberado ao sistema ASGD cujo gestor é UO-BA/EXP/GDS pelo contrato WF21_ASGD.

Para analisar a causa das outras não conformidades, é necessário visualizar os gestores dos sistemas e dos serviços envolvidos, descritos na Tabela 3 e verificar a linha de raciocínio empregada pelo analista ao avaliar a política.

Tabela 3. Áreas gestoras dos serviços e sistemas indicados nos contratos

Serviço/Sistema	Gestor
WORKFORCE_2.1	RH/PA
WORKFORCE_2.3	RH/PA
ASGD	UO-BA/EXP/GDS
SATH	AB-RE/SOP/INF
7G6R	AB-PQ/PAPQ/ASGP
P294	UO-RIO/CBS/CNTS
GD01	COMPARTILHADO/SERV
6NQR	COMPARTILHADO/SERV
SGP0	COMPARTILHADO/RNNE/SMS/SSO

Considerando a política 2, é necessário que exista um contrato para uso do serviço, tendo como partes envolvidas o gestor do serviço e o gestor do sistema.

Tomando como exemplo o sistema ASGD, é possível ver que este tem acesso ao serviço WorkForce_2.1, autorizado por um contrato (WF21_ASGD), cujas partes são os gestores do serviço (RH/PA) e o gestor do sistema (UO-BA/EXP/GDS). Estas informações são apresentadas na Figura 4. Deste modo, este sistema se encontra conforme com a política e, por condições semelhantes, o mesmo é válido para os sistemas SATH e P294 (vide Figura 4). Estes três casos foram indicados como conformes tanto pelos analistas, quanto pela ontologia.

Para o sistema 7G6R, podemos verificar na Figura 4 que o contrato (WF21_7G6R) considera RH/PA como a parte responsável pelo serviço e AB/PQ/SPP como a parte responsável por gerir o sistema. No entanto, observando a configuração apresentada na Tabela 3, a parte gestora do sistema 7G6R é a área AB-PQ/PAPQ/ASGP e não AB/PQ/SPP. Isto torna o sistema não conforme com a política. O mesmo raciocínio é válido para o sistema SGP0. Ambos os casos foram classificados corretamente tanto pelo analista, quanto pela ontologia.

Já os sistemas GD01 e 6NQR foram classificados como conformes pela ontologia e não conformes pelo analista. Para compreender a causa desta diferença, foi solicitado ao analista que descrevesse como ele realizou a avaliação da política. A lógica utilizada é apresentada na Figura 5, itens (a) e (b), considerando o sistema 6NQR e descrita a seguir. O mesmo cenário se aplica ao sistema GD01.

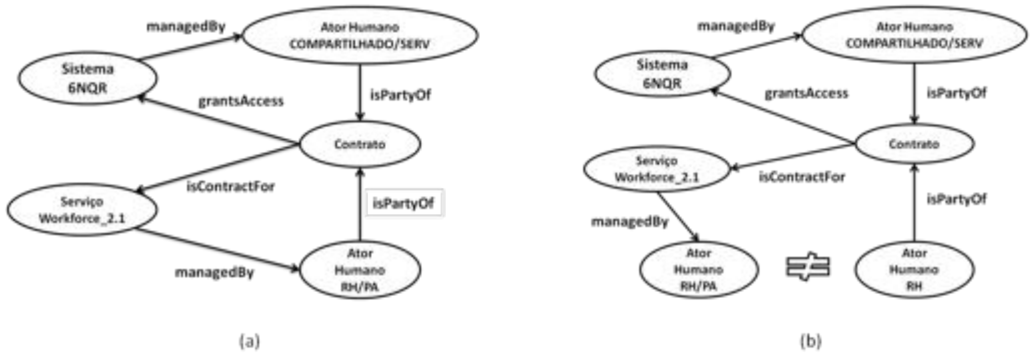

Figura 5. Avaliação realizada pelo analista

A situação esperada pelo analista é expressa na Figura 5.a. onde o gestor do sistema 6NQR é o ator humano COMPARTILHADO/SERV e o gestor do serviço em questão é o ator humano RH/PA. Esta figura representa as informações presentes na Tabela 3. Porém, ao verificar os contratos existentes (Figura 4), o analista identificou que as partes envolvidas eram COMPARTILHADO/SERV e RH, diferente do esperado (como destacado na Figura 5.b).

A causa da identificação de violação de forma incorreta pelo analista se deveu ao fato do analista desconhecer que o ator humano RH/PA é subordinado ao ator humano RH, representado na ontologia através de uma relação *managedBy*, conforme a Figura 6 apresenta. Conforme citado na Seção 3.2, esta propriedade foi adicionada ao modelo e considerada como transitiva exatamente para possibilitar a implementação de hierarquias nas organizações. Por conta desta transitividade, a ontologia classificou ambos os sistemas corretamente como conformes, enquanto que o analista ignorou esta relação por desconhecimento e os classificou como não conformes.

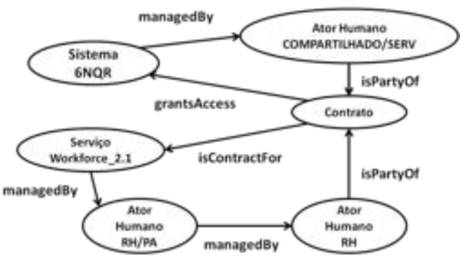

Figura 6. Cenário considerado pela ontologia

Com base neste cenário, podemos verificar que, além de ganho de desempenho, também foi identificado um ganho de qualidade do resultado.

5. Conclusões

Neste trabalho foi apresentada uma proposta de uso de ontologias e regras para verificação de conformidade de políticas de governança SOA. Foi possível identificar que o mecanismo permite ganhos de desempenho, devido a uma redução de tempo de execução de uma verificação em relação à execução manual sem a ontologia. Além disso, há ganhos na qualidade, devido a um maior número de situações de conformidade classificadas corretamente dado que é utilizada uma representação mais completa do conhecimento do domínio através da ontologia e a possibilidade de inferência sobre a semântica das relações envolvidas. Embora outras abordagens para automatização da solução de detecção de conformidade pudessem ser adotadas, possivelmente com o mesmo desempenho e qualidade, observa-se que o uso de ontologias e regras baseadas em padrões web tende a permitir o reuso e intercâmbio de informações e funcionalidades, bem como o processamento automatizado por diferentes agentes web.

Como trabalho futuro é proposta a execução de um estudo de caso mais amplo do que o exemplo apresentado neste trabalho a fim de caracterizar melhor os ganhos da proposta. Outra proposta é aprimorar a abrangência da ontologia utilizada tornando-a mais rica, uma vez que a ontologia do Open Group não contempla todos os elementos necessários para governança SOA. Também propomos utilizar uma ontologia de fundamentação para minimizar falhas no processo de modelagem.

6. Referências Bibliográficas

Adams, S. (2009). ITIL V3 Foundation handbook. The Stationery Office. 2a edição.

Baiôco, G., Costa, A., Calvi, C. e Garcia, A. (2009) "IT Service management and governance: Modeling an ITSM configuration process: A foundational ontology approach". In IEEE International Symposium on Integrated Network Management.

Bennet, S.G. (2012) "Oracle Practitioner Guide - A Framework for SOA Governance". Disponível em: <http://www.oracle.com/technetwork/topics/entarch/oracle-pg-soa-governance-fmwrk-r3-2-1561703.pdf>. Acesso em Julho de 2012.

Dias Jr, J., de Oliveira, J. e Meira, S (2012). “Pontos Chaves para Adoção de Uma Arquitetura Orientada a Serviços: Uma Análise Comparativa de Modelos de Maturidade SOA da Indústria”. In: VIII Simpósio Brasileiro de Sistemas de Informação, SBSI. São Paulo.

Erl, T. (2005), Service-Oriented Architecture: Concepts, Technology and Design, Prentice Hall, 1ª edição.

Gruber, T.R. (1993). "Towards Principles for the Design of Ontologies Used for Knowledge Sharing". In: Knowledge acquisition, pages 199-220.

Guizzardi, G. (2005). Ontological foundations for structural conceptual models, Tese de Doutorado, Universidade of Twente, Holanda.

Hojaji, F., Shirazi, M.R. (2010). "A comprehensive SOA Governance Framework based on CobiT". In: SERVICES-1, 6th Wold Congress on Services, Miami, EUA.

Hu, H., Ahn, G., Kulkanarni, K. (2011). "Ontology-based policy anomaly management for autonomic computing". In: Proceedings of the 7th International Conference on Collaborative Computing

IT Governance Institute (2007), CobiT 4.1, IT Governance Institute, 1ª edição.

Janiesch, C., Korthaus, A., Rosemann, M. (2009). "Conceptualisation and facilitation of SOA governance". In: Proceedings of 20th Australasian Conference on Information Systems, Melbourne, Australia.

Josuttis, N. (2007). SOA in practice. O'Reilly. 1ª edição.

Li, B., Zhao, L., Zhu, J., Wu, J. (2011). "A policy-based adaptive web services security framework". In: Journal of Software, v.6, n.12, p.2456-2463.

Niemann, M., Miede, A., Johannsen, W., Repp, N., Steinmetz, R. (2010). "Structuring SOA Governance". In: International Journal of IT/Business Alignment and Governance, v.1, n.1, p.58-75.

Noy, N., Mcguiness, D. (2001). "Ontology development 101: A guide to creating your first ontology". Stanford knowledge systems laboratory technical report KSL-01-05.

Papazoglou, M.P. (2003). "Service-oriented computing: concepts, characteristics and directions". In: Proceedings of the 4th International Conference on Web Information Systems Engineering.

Parejo, J.A., Fernandez, P., Ruiz-Cortés, A. (2011). "WS-Governance: A Policy Language for SOA Governance". In: Service-Oriented Computing, Lecture notes on computer science, v.7084, p.280-296.

Spies, M. (2012). "Continuous Monitoring for IT Governance with Domain Ontologies". In: Proceedings of the 23rd International Workshop on Database and Expert Systems Applications.

Teixeira Filho, H. M., Azevedo, L. G. (2012). "CommonGOV: A consolidate approach for governance of service-oriented architectures". In: 8th International Conference on Next Generation of Web Services Practices, São Carlos, Brasil.

The Open Group (2009). "SOA Governance Framework". Disponível em: <https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?catalogno=c093>. Acesso em Abril de 2012.

The Open Group (2010). "Service-Oriented Architecture Ontology". Disponível em: <https://www2.opengroup.org/ogsys/protected/publications/viewDocument.html?publicationid=12245&documentid=11637>. Acesso em Novembro de 2012.