Automatizando a Estimativa de Riscos em Sistemas de Gerenciamento de Mudanças em TI*

Juliano Araujo Wickboldt, Roben Castagna Lunardi
Guilherme Sperb Machado, Weverton Luis da Costa Cordeiro
Alan Diego dos Santos, Fabrício Girardi Andreis, Cristiano Bonato Both
Lisandro Zambenedetti Granville, Luciano Paschoal Gaspary

Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre, RS – Brasil
{jwickboldt, rclunardi, gsmachado, weverton.cordeiro
adsantos, fgandreis, cbboth, granville, paschoal}@inf.ufrgs.br

Abstract. *Modern organizations take advantage of complex IT infrastructures in order to support their daily operations. Since these environments require special care, whenever changes become necessary, risks associated to them should be investigated. Usually, risk assessment is made by humans based only on their empirical knowledge, which is a very prohibitive task to do, that might lead to inaccurate or incomplete conclusions about risks associated to changes. In this paper, we present a solution for automating the process of risk assessment, based on data collected from past changes in order to identify possible problems for subsequent ones. A prototypical system was developed to evaluate the solution on an emulated IT infrastructure. The results achieved show how the automated solution is capable of raising the quality of the change planning as well as the organization of the managed infrastructure, in this way reducing the chances of disrupting the services delivered by the organization.*

Resumo. *Organizações modernas utilizam infra-estruturas de TI complexas para apoiar suas operações diárias. Por se tratar de um ambiente sensível, sempre que surge a necessidade de se aplicar mudanças é importante estimar quais riscos podem estar associados a elas. Geralmente, estimativas de riscos realizadas por humanos são baseadas apenas em conhecimento empírico, o que, além de acarretar uma quantidade proibitiva de trabalho, muitas vezes, leva a conclusões imprecisas e incompletas sobre os riscos associadas às mudanças. Neste artigo, é apresentada uma solução para automatização do processo de estimativa de riscos, baseando-se em informações de mudanças executadas no passado a fim de identificar possíveis problemas em implantações subseqüentes. Foi implementado um protótipo de sistema para avaliação da solução em uma infra-estrutura de TI emulada. Os resultados obtidos indicam que a solução é capaz de elevar a qualidade do planejamento das mudanças bem como da organização da infra-estrutura gerenciada, dessa forma causando menos danos aos serviços prestados pela organização.*

1. Introdução

Nas organizações modernas, a heterogeneidade das infra-estruturas de TI, associada à grande quantidade de dispositivos e aplicações presentes, torna a tarefa de gerenciamento

*Este trabalho foi desenvolvido em colaboração com a HP Brasil P&D.

de TI cada vez mais complexa. Uma infra-estrutura de TI é formada por um conjunto de *itens de configuração* (*Configuration Items* - CIs) que vão desde elementos concretos como servidores, estações de trabalho e roteadores, a elementos lógicos como pacotes de *software* e serviços de rede. Empregar políticas racionais de gerenciamento de TI eleva a qualidade dos serviços oferecidos pelas organizações, além de reduzir os custos de operação. Para manter de forma consistente e segura esse tipo de infra-estrutura, a OGC (*Office Government Commerce*) definiu um conjunto de processos e boas práticas que organizam as atividades de gerenciamento. Tais processos e boas práticas são publicados na biblioteca ITIL (*Information Technology Infrastructure Library*) [ITIL 2008].

A disciplina de *gerenciamento de mudanças*, contemplada no livro *Service Transition 3.0* [ITIL 2007] da ITIL, determina como uma mudança deve ser conduzida sobre uma infra-estrutura de TI, desde a sua solicitação, planejamento e análise até sua implementação. Nesse livro, a ITIL recomenda que toda mudança a ser realizada deve ser descrita em uma *requisição de mudança* (*Request for Change* - RFC). Uma RFC deve definir, de forma declarativa, dentre outros parâmetros, os motivos da mudança requisitada, os CIs envolvidos e o que deve ser alterado. Não é função de uma RFC, porém, indicar quais atividades de mais baixo nível devem ser executadas para que uma mudança seja realizada; isso é de fato tratado, por exemplo, por sistemas de gerenciamento automatizados, ou até mesmo por operadores humanos. Adicionalmente, todas as RFCs devem ser submetidas à análise, aprovação e agendamento por parte de um comitê denominado *Change Advisory Board* (CAB). Esse comitê, presidido geralmente por um *gerente de mudanças*, deve ser formado por pessoas com conhecimento amplo sobre os processos da organização, provenientes de diversas áreas, e não necessariamente terem domínio sobre as tecnologias utilizadas na infra-estrutura de TI.

Sabendo que as infra-estruturas de TI suportam serviços fundamentais para a continuidade do negócio das organizações, sempre que a necessidade de se realizar uma mudança nessas infra-estruturas é iminente, os riscos associados à mudança requisitada precisam ser considerados. Segundo a ITIL, riscos devem ser investigados e mensurados antes que uma mudança seja aprovada. Além disso, contramedidas devem ser estabelecidas para minimizar a possibilidade dos riscos se materializarem em problemas reais, causando deste modo danos para a continuidade do negócio. Alguns exemplos de eventos que caracterizam riscos aos quais uma infra-estrutura de TI fica exposta durante a implantação de mudanças são: falhas durante a instalação de *softwares*, configurações incorretas de equipamentos como *firewalls* ou roteadores e defeitos nos CIs manipulados. As ocorrências desses eventos podem fazer com que a infra-estrutura de TI evolua para um estado indesejável ou desconhecido.

Uma das recomendações apresentadas pela ITIL é que os riscos devem ser vistos como uma combinação da probabilidade da ocorrência de um evento possivelmente negativo e o impacto dessa ocorrência sobre os negócios da organização [ITIL 2007]. Porém, estimativas de risco são realizadas normalmente por operadores humanos, baseadas apenas no conhecimento empírico adquirido pelos mesmos ao longo de suas carreiras. No entanto, devido ao grande número de CIs envolvidos nas mudanças e a quantidade de variáveis que se deve considerar (*e.g.*, histórico de falhas e impacto dos CIs afetados), esse tipo de análise pode acabar sendo superficial ou imprecisa demais para que se possa usar como base para tomada de decisões.

Apesar das boas práticas introduzidas pela ITIL, essa biblioteca não define um método claro de análise de riscos no processo de mudança. Recentemente, alguns autores propuseram soluções para a automação do gerenciamento de mudança em suas diversas etapas [Cordeiro *et al.* 2008] [Machado *et al.* 2008] [Rebouças *et al.* 2007] [Sauvé *et al.* 2007]. Porém, tais trabalhos não propõem uma metodologia automatizada para investigação de riscos no planejamento de mudanças. Um método padronizado de análise de riscos pode fornecer ao operador subsídios para rapidamente identificar ameaças na mudança requisitada, antes de submetê-la para implantação. Com base nas informações da análise de riscos, o operador poderia fazer alterações na mudança original ou até mesmo promover modificações na infra-estrutura de TI, objetivando reduzir as possibilidades da mudança em questão causar danos às operações normais da organização.

A fim de atacar o problema previamente exposto, este trabalho propõe um método de análise automatizada de riscos em processos de gerenciamento de mudanças. A solução proposta baseia-se no histórico de execuções de mudanças sobre uma infra-estrutura de TI, analisando a ocorrência de falhas em implantações passadas para identificar possíveis problemas para as próximas execuções. Dessa forma, é possível munir um sistema de gerenciamento de mudanças com informações para tratamento de incidentes de forma proativa. Isso significa fornecer ao operador humano a oportunidade de minimizar a possibilidade de falhas ajustando as mudanças solicitadas e, conseqüentemente, elevar a qualidade dos serviços suportados pela infra-estrutura de TI.

No seguimento deste trabalho serão discutidos, na Seção 2, alguns dos principais trabalhos relacionados ao gerenciamento de riscos e gerenciamento de mudanças. Um detalhamento da solução de análise de riscos proposta é apresentado na Seção 3, enquanto que detalhes da implementação do protótipo desenvolvido para validação são descritos na Seção 4. Na Seção 5 é exibida uma avaliação experimental utilizada para mensurar os resultados da solução e, por fim, na Seção 6 são discutidos conclusões e trabalhos futuros.

2. Trabalhos Relacionados

Gerenciamento de riscos é uma disciplina transversal, ou seja, que se aplica a diferentes áreas do conhecimento. De uma forma genérica, pode-se dizer que o gerenciamento de riscos é o processo pelo qual as organizações avaliam os riscos associados as suas atividades, com objetivo de identificar e tratar ameaças obtendo um nível máximo sustentável de benefício [IRM 2002]. Os riscos em si, podem ser vistos como potenciais eventos com conseqüências que podem constituir oportunidades ou ameaças ao sucesso. Apesar de o risco vir sendo considerado na literatura sob os dois aspectos (positivo e negativo), em áreas como a de segurança, por exemplo, dificilmente se encontrará um lado positivo para eles. Nos últimos anos alguns trabalhos foram publicados abordando tópicos relacionados ao gerenciamento de riscos e gerenciamento de mudanças. Porém, são raras as iniciativas que levam em conta os riscos ocasionados pela necessidade de mudança.

Marques e Neves-Silva [Marques e Neves-Silva 2007] propuseram um método de avaliação de riscos para ajudar na tomada de decisão em linhas de montagem de grande porte. Os autores propõem quantificar o risco considerando a probabilidade da ocorrência de incidentes e os impactos que esses eventos teriam caso acontecessem. No entanto, esse método é aplicável para um ambiente onde os parâmetros necessários para o cálculo (probabilidade e impacto) possuem valores conhecidos para um conjunto limitado de eventos

possíveis. Por exemplo, quando um alarme é acionado indicando que uma variável monitorada ultrapassou um determinado limite (*e.g.*, tempo médio entre falhas). A partir de valores de probabilidade e impacto predefinidos é feita a estimativa automática de riscos para cada um dos incidentes possíveis.

Fewster e Mendes [Fewster e Mendes 2001] introduziram um *framework* para análise de riscos em editoração e desenvolvimento de sistemas Web utilizando um Modelo de Generalização Linear (*Generalized Linear Model* - GLM). O GLM se mostrou bastante eficaz na previsão de riscos, tais como, ultrapassar orçamento ou prazo previsto de término de um projeto. Utilizando um modelo estatístico não se fornece apenas um ponto máximo ou mínimo para a variável analisada, mas sim, uma distribuição de probabilidade. De posse dessas informações um gerente de projeto poderia estimar a probabilidade de não terminar um projeto dentro de um determinado tempo (por exemplo, 30 dias). Apesar disso, apenas a probabilidade de ocorrência dos eventos negativos são estimadas pelo GLM, o impacto que esses eventos possam ter para o projeto não são considerados.

Sauvé *et al.* [Sauvé *et al.* 2007] e Rebouças *et al.* [Rebouças *et al.* 2007] apresentaram um processo de análise de riscos durante a fase de agendamento de mudanças com a intenção de determinar as prioridades de execução de RFCs potencialmente concorrentes. Os métodos propostos são fortemente baseados em estimativas de tempo para implantação de RFCs e na maneira como elas podem ser agendadas em momentos diferentes, alterando assim o impacto dessas implantações sobre os objetivos do negócio. Segundo os autores, o tempo que transcorre desde a submissão de uma RFC até a sua implementação causa danos aos serviços afetados pela mudança, que podem, por exemplo, sofrer por degradação de desempenho. Além disso, durante a fase de implantação de uma RFC, a interrupção dos serviços alterados e eventuais descumprimentos de prazos podem acarretar perdas financeiras ou penalizações contratuais. No entanto, a análise de riscos proposta nesses trabalhos possui aplicação para a fase de agendamento de mudanças, e não para o seu planejamento, como abordado neste artigo.

De acordo com o conhecimento dos autores deste artigo, não existe um método de estimativa de riscos padronizado para gerenciamento de mudanças na fase de planejamento de RFCs. A importância dessa estimativa reside no fato de que a infra-estrutura gerenciada suporta os serviços prestados pela organização. Sendo assim, problemas durante a implantação de mudanças podem ocasionar indisponibilidade desses serviços, afetando a continuidade do negócio. A ITIL reforça essa importância afirmando que mesmo mudanças aparentemente inofensivas do ponto de vista de sua complexidade, ainda que indiretamente, podem causar danos significativos a serviços relevantes para o negócio.

3. Estimativa de Riscos Automatizada

Para que uma estimativa de riscos no processo de mudança possa ser automatizada, essa estimativa deve ser baseada em informações sobre execuções de mudanças coletadas do próprio ambiente de TI. A partir dessas informações, uma metodologia padronizada seria capaz de quantificar os riscos aos quais a infra-estrutura de TI estará exposta durante a implantação de uma mudança e servir de guia para a especificação de mudanças mais prudentes. Apesar das diversas abordagens adotadas para gerenciamento de riscos nas mais variadas áreas do conhecimento, riscos são geralmente tratados como uma combinação de dois fatores: (i) a possibilidade da ocorrência de um evento potencial-

mente negativo e (ii) o prejuízo que esse evento é capaz de causar sobre o objeto de análise [Chicken e Posner 1998]. A ITIL adota uma visão similar para riscos no gerenciamento de mudanças em TI ressaltando que estes devem ser avaliados levando em consideração os objetivos do negócio da organização.

Neste trabalho assume-se que falhas durante a implantação de mudanças são recorrentes, isto é, ao se observar o histórico de execuções de uma RFC é possível analisar falhas ocorridas no passado e estimar probabilidades de novas ocorrências das mesmas. Assume-se também que os itens da infra-estrutura de TI possuem uma relevância para os objetivos do negócio, direta ou indiretamente, e que essa relevância é definida para cada CI. Sendo assim, falhas que afetem esses CIs têm um impacto sobre a continuidade do negócio da organização, portanto, tal impacto deve ser investigado pela análise de riscos.

Nesta seção será apresentada a solução para automatização da análise de riscos no processo de gerenciamento de mudanças, considerando dois fatores: (i) a probabilidade de falha na implantação de uma RFC e (ii) o impacto dessas falhas para a continuidade do negócio da organização. Em um primeiro momento será revisado o ciclo de vida regular de uma RFC, desde a sua emissão até a implantação da mudança requerida. Posteriormente, será apresentado o componente do sistema gerenciamento de mudanças responsável por realizar a análise de riscos.

3.1. Arquitetura do Sistema de Gerenciamento de Mudanças

Uma vez que uma RFC é submetida ao sistema de gerenciamento de mudanças, um operador humano fará a especificação de um plano de mudança (*Change Plan* - CP) preliminar. Basicamente, este plano consiste em um *workflow* de atividades de alto nível que descrevem os passos a serem seguidos para materializar a mudança solicitada na RFC. O CP preliminar passa então por um processo de refinamento, gerando assim um *workflow* de atividades de baixo nível que podem ser efetivamente executadas sobre os CIs [Cordeiro *et al.* 2008]. Ao término da execução do CP refinado, a infra-estrutura de TI deve ter evoluído para um novo estado consistente. Como falhas podem ocorrer durante esse processo, devem ser previstos planos de remediação que serão executados para minimizar os danos causados por tais falhas. Planos de remediação podem tanto retornar a infra-estrutura de TI ao estado anterior à mudança (*rollback*) quanto executar atividades que compensem as falhas ocorridas [Machado *et al.* 2009].

Em um sistema sem suporte a análise de riscos, ao término das definições do plano de mudança e dos planos de remediação, uma RFC estaria pronta para ser aprovada e executada. Porém, sem uma avaliação apropriada de riscos, essa mudança poderia expor a infra-estrutura de TI a riscos desconhecidos. Falhas durante a execução do CP ocasionariam interrupções nos serviços por um tempo indeterminado, até que os planos de remediação fossem postos em prática. Por esse motivo, neste trabalho é introduzido o componente *Risk Analyzer* (Figura 1) que contempla a etapa de estimativa automatizada de riscos no planejamento da mudança. Esse componente recebe como entrada a RFC que se pretende executar, os registros de execuções anteriores da mesma e uma visão da infra-estrutura de TI. A partir dessas entradas, são feitas estimativas de forma automática sobre os riscos aos quais a infra-estrutura de TI estará exposta durante a execução da RFC e, ao final, um relatório de riscos será apresentado ao operador do sistema. Esse relatório pode ser utilizado como base para possíveis alterações na RFC original de forma a mitigar os riscos nela contidos, ou então, permitir que o operador promova modificações em

pontos críticos da infra-estrutura de TI a fim de minimizar o impacto da mudança sobre os CIs manipulados.

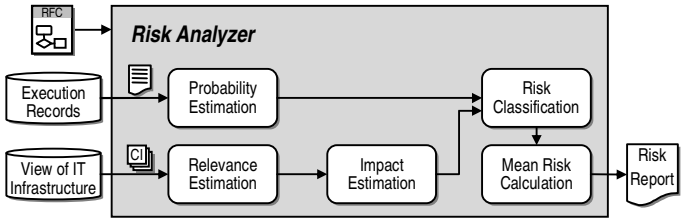

Figura 1. Disposição dos elementos do componente de análise de riscos

Os registros de execução (*Execution Records*) de uma RFC são definidos segundo um modelo proposto em um trabalho anterior [Wickboldt *et al.* 2009]. Esses registros representam os traços de execução do *workflow* da mudança respeitando a ordem em que as atividades foram realizadas. Além disso, são incluídas informações sobre o *status* da execução (sucesso ou falha) e, em caso de falha, tais registros compreendem ainda a classificação da falha e as medidas de remediação utilizadas. No modelo proposto, as falhas poderiam ser classificadas em seis categorias: *Activity Failure* (AF), *Resource Failure* (RF), *Human Failure* (HF), *Time Failure* (TF), *External Trigger* (ET) e *Constraint Violation* (CV). Porém, neste trabalho consideramos para fins de avaliação apenas duas classificações: AF, que representa as falhas intrínsecas às atividades do CP (*e.g.*, falhas em instalação de *software*) e RF, que representa falhas dos recursos manipulados durante a mudança (*e.g.*, defeitos em equipamentos alterados).

Para que se possa manter uma visão consistente da infra-estrutura de TI (*View of IT Infrastructure*) se faz necessário o uso de um modelo que represente, de maneira adequada, os CIs nela contidos. Neste trabalho, utilizou-se um subconjunto de classes do CIM (*Common Information Model*) [DMTF 2008], proposto pelo DMTF (*Distributed Management Task Force*). Esse modelo permite representar todos os tipos de CIs, sejam eles, elementos de *hardware*, *software*, serviços ou configurações, assim como as definições de relações e dependências entre esses elementos. A estimativa automatizada de riscos requer que, para cada CI representado, seja atribuído um valor de *relevância para o negócio* (*Business Relevance* - BsR). Esse parâmetro deve refletir a importância de um elemento (CI) da infra-estrutura de TI para a continuidade do negócio e deve ser expressado por um valor numérico qualquer, permitindo comparar relevâncias de diferentes elementos, independentemente da escala adotada. A BsR deve ser atribuída apenas aos elementos que possuem alguma relevância para o negócio e será útil para o cálculo de impacto dos CIs a ser apresentado no seguimento deste artigo.

3.2. Algoritmos para Análise de Riscos

Internamente, o *Risk Analyzer* procede a estimativa das probabilidades de falha através do módulo *Probability Estimation*. Esse módulo realiza o cálculo segundo uma função descrita no Algoritmo 1. Como entradas, são recebidos os registros de execução e o plano de mudança da RFC em questão. Para cada atividade do plano de mudança (Linha 2), a função encontra, entre os registros de execução, o número total de vezes que tais atividades foram realizadas (Linha 3). Em seguida, para cada tipo de falha (neste trabalho

são considerados AF e RF, Linha 4) a função procura nos registros de execução a quantidade de falhas de um determinado tipo para uma atividade (Linha 5). De posse dessas informações, a probabilidade de falha é calculada dividindo o número total de falhas encontradas pelo total de execuções da atividade (Linha 6). Cada probabilidade forma uma tupla, juntamente com a atividade e o tipo de falha, que será inserida em um conjunto (Linha 7), que ao final do cômputo será retornado pela função (Linha 8).

Algoritmo 1: *Função de Cálculo de Probabilidade*
Entrada: R: conjunto de registros de execução de uma RFC, CP: plano de mudança
Saída: conjunto de tuplas contendo atividade, probabilidade de falha e tipo de falha
1. $S \leftarrow$ conjunto vazio de tuplas (atividade, probabilidade de falha, tipo de falha)
2. **for each** $i \in$ conjunto de atividades do CP
3. **do** $T \leftarrow$ total de execuções de i **in** R
4. **for each** $j \in$ tipos possíveis de falha
5. **do** $F \leftarrow$ total de falhas da atividade i para o tipo de falha j **in** R
6. $\varphi \leftarrow F \div T$
7. $S \leftarrow S \cup \{i, \varphi, j\}$
8. **return** S

A segunda funcionalidade do *Risk Analyzer* é estimar o impacto de uma mudança sobre os elementos (CIs) da infra-estrutura de TI. Em um primeiro momento, o módulo *Relevance Estimation* calculará a *relevância absoluta* (*Absolute Relevance* - AR) dos elementos manipulados no plano de mudança através da função apresentada no Algoritmo 2. A AR é um fator que indica a relevância total de um elemento para a continuidade do negócio, incluindo sua BsR e a de todos os elementos que dependem dele, direta ou indiretamente. Nesse algoritmo, para cada CI (variável ci) envolvido no plano de mudança (Linha 2), o algoritmo inicia o valor de AR do elemento (variável γ) com a sua própria BsR (Linha 3). Logo após, é criada uma lista (D) contendo os elementos dependentes, direta ou indiretamente, de ci (*e.g.*, *softwares* que dependem dos computadores em que estão instalados ou serviços que dependem de outros serviços) (Linha 4). Essa lista é preenchida recursivamente, percorrendo as dependências definidas entre os CIs. No entanto, esse procedimento não é apresentado neste artigo por medida de simplificação. Feito isso, para cada elemento contido na lista D (Linha 5), é acumulada sua BsR na variável γ (Linha 6). Após percorrer todos os elementos de D, a tupla (CI, AR) é incluída no conjunto U (Linha 7), que ao final da função será retornado (Linha 8).

Algoritmo 2: *Função de Cálculo de Relevância Absoluta*
Entrada: V: visão da infra-estrutura de TI, CP: plano de mudança
Saída: conjunto de tuplas contendo CIs e suas relevâcias absolutas
1. $U \leftarrow$ conjunto vazio de tuplas (CI, relevância absoluta)
2. **for each** $ci \in$ conjunto de CIs manipulados pelo CP
3. **do** $\gamma \leftarrow$ BsR de ci
4. $D \leftarrow$ lista de todos os elementos dependentes diretos e indiretos de ci
5. **for each** $d \in D$
6. **do** $\gamma \leftarrow \gamma +$ BsR de d
7. $U \leftarrow U \cup \{ci, \gamma\}$
8. **return** U

Uma vez calculadas as ARs dos elementos, será função do módulo *Impact Estimation* fazer a normalização desses valores para uma escala de impacto. O *fator de impacto* (*Impact Factor* - IF) de um elemento representa a parcela da infra-estrutura de TI que é afetada pela falha de um determinado CI, no que diz respeito ao prejuízo causado para a continuidade do negócio. A função de cálculo do IF, detalhada no Algoritmo 3, recebe como entrada a saída da função de cálculo de AR realizado pelo Algoritmo 2. Para que seja possível calcular o impacto dos CIs em relação à infra-estrutura de TI, existe um elemento que representa a infra-estrutura gerenciada, do qual todos os outros CIs dependem. Esse elemento terá como AR a soma de todas as BsRs definidas e será manipulado em todas as RFCs. Inicialmente, o algoritmo instancia na, variável t, o elemento que representa a infra-estrutura de TI como um todo (Linha 2) e a seguir utiliza um procedimento que localiza e extrai tal CI do conjunto R (Linha 3). Para cada tupla do conjunto R (Linha 4), é dividida a AR do CI contido na tupla i pela AR total do sistema contido na tupla T (Linha 5). Um conjunto I receberá os resultados dessas divisões (Linha 6) e será retornado ao final da função (Linha 7).

Algoritmo 3: *Função de Cálculo de Fator de Impacto*
Entrada: R: conjunto de tuplas contendo CIs e suas relevâcias absolutas
Saída: conjunto de tuplas contendo CIs e seus fatores de impacto
1. $I \leftarrow$ conjunto vazio de tuplas (CI, fator de impacto)
2. $t \leftarrow$ CI que representa a infra-estrutura de TI
3. $T \leftarrow$ *extract_ci*(t, R)
4. **for each** $i \in$ conjunto tuplas R
5. **do** $\lambda \leftarrow$ AR de $i \div$ AR de T
6. $I \leftarrow I \cup \{ci, \lambda\}$
7. **return** I

Os resultados obtidos através dos cálculos das probabilidades de falha e dos impactos dos CIs servirão de base para a classificação dos riscos das atividades do plano de mudança a ser feita pelo módulo *Risk Classification*. O objetivo, ao se realizar estimativas de riscos automatizadas, é auxiliar o operador a compreender os riscos contidos em uma requisição de mudança. Por isso, os resultados precisam ser apresentados de forma clara e objetiva. O IRM [IRM 2002] recomenda que se quantifique a probabilidade e o impacto nas seguintes escalas: (i) alta (provável), média (possível) e baixa (improvável) para probabilidades e (ii) alto (significante), médio (moderado) e baixo (insignificante) para impacto. Os valores obtidos nos passos anteriores serão então mapeados nessas escalas, sendo que os índices de probabilidade e impacto (alto, médio e baixo) podem ser parâmetros do sistema e variar conforme a exigência do ambiente. Uma matriz de classificação de riscos, como a apresentada na Tabela 1, costuma ser utilizada pelas organizações modernas no gerenciamento de riscos. Finalmente, cada atividade do plano de mudança receberá uma classificação em uma das nove categorias da matriz para cada tipo de falha considerado. O algoritmo que classifica as atividades segundo as categorias de risco é trivial e não será apresentado neste artigo.

Na última etapa da análise de riscos será calculado o *risco médio* (*Mean Risk* - MR) de cada atividade do plano de mudança através do módulo *Mean Risk Calculator*. A entrada para esse módulo será o conjunto de atividades do CP classificadas segundo a matriz da Tabela 1 para cada tipo de falha considerado na análise. No entanto, apresentar

Tabela 1. Matriz de classificação de riscos

	Probabilidade de Falha		
Fator de Impacto	Impacto Alto Probabilidade Baixa Categoria 3	Impacto Alto Probabilidade Média Categoria 2	Impacto Alto Probabilidade Alta Categoria 1
	Impacto Médio Probabilidade Baixa Categoria 6	Impacto Médio Probabilidade Média Categoria 5	Impacto Médio Probabilidade Alta Categoria 4
	Impacto Baixo Probabilidade Baixa Categoria 9	Impacto Baixo Probabilidade Média Categoria 8	Impacto Baixo Probabilidade Alta Categoria 7

a um operador diversas classificações de risco para cada atividade do CP pode acabar gerando uma quantidade de dados impraticável para avaliação, dependendo do número de atividades e de tipos de falha considerados. Por esse motivo, o *Mean Risk Calculator* calcula uma média harmônica dos valores das categorias de risco obtidos para cada tipo de falha, resultando em um valor de MR (em uma escala de 1 a 9) por atividade. Por exemplo, supondo que uma atividade do CP seja de instalação de um *software* sw sobre um sistema computacional cs. Onde a probabilidade de AF é Média com impacto Baixo (Categoria 8) e a probabilidade de RF é Baixa com impacto Alto (Categoria 3). Sendo assim, o MR da atividade de instalação de *software* classificada nas categorias 3 e 8 teria um valor de 4,36. A utilização da média harmônica funciona como uma abordagem pessimista para a estimativa de riscos, uma vez que esse cálculo sempre aproxima o resultado final da menor parcela, tendendo assim a priorizar a categoria com maior risco. O relatório de riscos exibido ao final da análise apresenta as atividades do CP ordenadas pelos seus valores de MR de forma crescente, levando as atividades com maior fator de risco para o topo da lista.

4. Protótipo

A fim de comprovar a funcionalidade da solução proposta para automatização da análise de riscos, foi desenvolvido um protótipo e incorporado ao sistema de gerenciamento de mudanças CHANGELEDGE, concebido em um esforço conjunto entre a HP e a UFRGS. Nesse sistema é utilizado um subconjunto de classes do CIM para representação da infra-estrutura gerenciada e uma extensão do modelo de *workflow* proposto pelo WfMC (*Workflow Management Coalition*) [WfMC 2007] para expressar os planos de mudança. A seguir, serão descritos alguns detalhes técnicos do protótipo.

Conforme mencionado anteriormente neste artigo, os CIs da infra-estrutura de TI devem receber valores de BsR ajustados à sua importância frente ao negócio da organização. Para representar a BsR no protótipo foi definida uma métrica através da classe `BaseMatricDefinition` do CIM. Essa métrica define uma faixa de valores de relevância possíveis para serem aplicados aos elementos gerenciados, por exemplo: Alta (1,00), Média (0,50) e Baixa (0,25). Para os elementos relevantes devem ser associadas instâncias de `BaseMatricValue` contendo o valor de BsR atribuído ao CI. Caso não seja definida uma BsR a um CI, a função de cálculo de AR considerará o elemento irrelevante do ponto de vista do negócio (*i.e.*, BsR igual a zero).

Para representar dependências entre os CIs, o CIM define uma série de objetos que mapeiam relações entre itens de uma infra-estrutura de TI. Algumas dessas relações re-

presentam dependências explícitas como, por exemplo, `ServiceServiceDependency`, que indica quando um serviço depende de outro serviço para funcionar. Outras relações, apesar de não necessariamente representarem dependências, são consideradas como tal para a análise de riscos. Esse é o caso da relação `InstalledSoftwareElement`, que mapeia a dependência de um *software* para o sistema computacional onde ele está instalado. No protótipo, é utilizada uma lista de dependências, a qual é percorrida pelo algoritmo para calcular as ARs dos CIs.

A fim de aplicar as mudanças sobre a infra-estrutura de TI, o sistema CHANGELEDGE faz uso de um subsistema de implantação de mudanças (*deployment system*) que faz a tradução de um *workflow* de mudança em um documento BPEL (*Business Process Execution Language*) [Machado *et al.* 2008]. O documento BPEL gerado é então submetido para execução pelo sistema de orquestração de *Web services* ActiveBPEL [Active Endpoints 2008] que fará o controle da execução do *workflow* e tratamento de falhas. Cada CI da infra-estrutura de TI deve possuir uma interface de gerenciamento por *Web services* a ser invocada pelo ActiveBPEL para execução das atividades de mudança. Ao término de cada atividade o *Web service* de gerenciamento reporta a uma base de dados o *status* da execução, eventuais falhas ocorridas, tempo transcorrido, entre outros dados para popular os registros de execução da RFC.

Para fins de simulação, os *Web services* fornecidos pelos CIs introduzem falhas de forma pseudo-aleatória, segundo uma distribuição de probabilidades uniforme, durante a execução das atividades de mudança. Tais falhas, inseridas na forma de exceções, fazem com que o sistema de orquestração interrompa o fluxo normal do *workflow* e ative os planos de remediação associados. É possivel definir diferentes probabilidades de falha para os diferentes tipos de atividade ou para falhas na manipulação de CIs específicos.

5. Avaliação Experimental

Com o objetivo de comprovar a usabilidade da solução de estimativa de riscos proposta neste trabalho, foi criado um ambiente de TI emulado, sobre o qual foram realizados testes e medições com uso do sistema CHANGELEDGE. A RFC definida para avaliação possui o objetivo de manter atualizado um sistema de envio e recebimento de e-mails de um domínio corporativo, incluindo funções como fazer *backup* dos dados dos usuários e atualizar filtros de lixo eletrônico (*spam*). Esse sistema utiliza em conjunto quatro elementos de *software*: Postfix para os servidores POP e SMTP, SquirrelMail para o serviço de Webmail, Apache como servidor HTTP para hospedagem do Webmail e um SpamAssassin para filtragem de *spam*. No cenário estabelecido, o serviço que possui maior relevância é o de troca de mensagens via POP/SMTP, uma vez que a maioria dos colaboradores utilizará programas cliente de e-mail. Sendo assim, o serviço de Webmail serve como uma opção de acesso alternativo às mensagens. O plano de mudança descrito na Figura 2 foi desenvolvido para ser executado periodicamente e manter todos os *softwares* envolvidos no fornecimento do serviço de e-mail atualizados.

Na ocasião da instalação do serviço de e-mail, a infra-estrutura de TI já continha um sistema de *Enterprise Resource Planning* (ERP), o qual utiliza um servidor dedicado (*System Server*) e um banco de dados próprio (*MySQL*). Porém, com o passar do tempo novos serviços foram sendo incorporados, evoluindo a infra-estrutura gerenciada para um novo estado, conforme representado na Figura 3. A organização, que antes for-

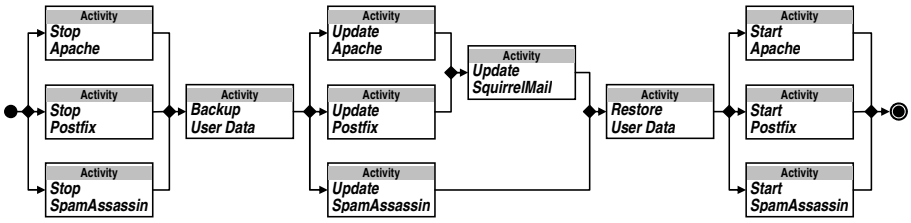

Figura 2. *Workflow* do plano de mudança

necia produtos através de venda direta ou televendas, passou a oferecê-los também por comércio eletrônico, assim como o suporte aos consumidores passou a ser prestado por uma aplicação de suporte *on-line*. As dependências entre os objetos mapeadas na Figura 3 são representadas pelas setas, indicando, por exemplo, que os novos serviços de vendas e suporte *on-line* dependem do serviço prestado pelo *software* Apache para funcionarem. A BsR dos elementos é representada pelos números posicionados na parte inferior-direita das caixas, sendo que a escala de relevâncias utilizada foi: Máxima (1,00), Alta (0,75), Média (0,50), Baixa (0,25) e Nenhuma (0,00).

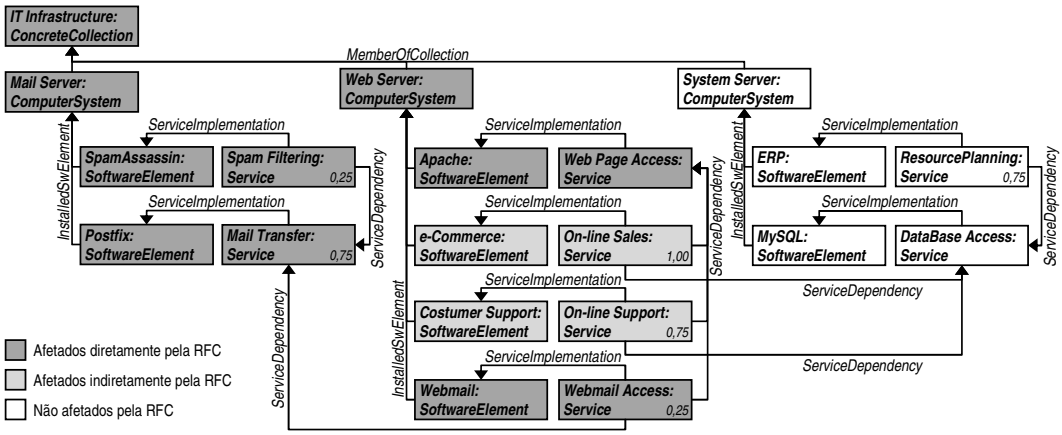

Figura 3. Representação atual da infra-estrutura de TI

No momento da criação do plano de mudança da RFC descrita, os índices de riscos eram baixos. Porém, com as mudanças na infra-estrutura, esse plano de mudança deve ser repensado, para que os riscos sejam reduzidos a níveis aceitáveis. O resultado da análise de riscos realizada sobre esse CP, considerando a infra-estrutura de TI da Figura 3, é mostrado na Tabela 2-(a). Observando esse resultado, fica claro que as quatro atividades que possuem maior risco são executadas sobre o mesmo servidor (*Web Server*). Isso acontece devido aos efeitos indiretos que a mudança tem sobre elementos que não fazem parte da RFC, mas que dependem dos serviços alterados por ela. Por exemplo, das atividades com maior risco no plano de mudança, três manipulam o *Apache*, que ainda provê serviço para outras três aplicações, enquanto uma atualiza o *SquirrelMail*, o qual dentro do serviço de e-mail possui um papel secundário.

Frente a esse cenário, uma alteração sobre a infra-estrutura de TI foi promovida, a fim de minimizar o impacto das atividades de maior risco. Essa alteração contemplou a migração do *SquirrelMail* para o *Mail Server*, combinada com a instalação de um servidor HTTP exclusivo para o serviço de Webmail nessa mesma máquina. Ajustando o plano de

mudança à nova realidade, a análise de riscos apresenta novos resultados conforme a Tabela 2-(b). É notório que houve uma redução dos índices de risco das atividades que manipulam o *Apache* e o *SquirrelMail*, logo, a modificação feita na infra-estrutura obteve êxito em reduzir os impactos do plano de mudança sobre o negócio da organização.

Tabela 2. Resultados da análise de riscos antes e depois da mudança promovida

(a) Resultado no cenário atual		(b) Resultado após a mudança	
Atividade	Mean Risk	Atividade	Mean Risk
Update Apache	2,40	Update Postfix	5,45
Start Apache	3,00	Stop Postfix	6,00
Stop Apache	3,00	Backup User Data	6,00
Update SquirrelMail	4,50	Restore User Data	6,00
Update Postfix	5,45	Start Postfix	6,00
Restore User Data	6,00	Update SpamAssassin	6,86
Backup User Data	6,00	Update Apache	6,86
Stop Postfix	6,00	Update SquirrelMail	7,20
Start Postfix	6,00	Stop Apache	7,20
Update SpamAssassin	6,86	Stop SpamAssassin	7,20
Stop SpamAssassin	7,20	Start SpamAssassin	7,20
Start SpamAssassin	7,20	Start Apache	7,20

A redução dos indicadores de riscos não comprova, por si só, uma efetiva melhora na qualidade do plano de mudança. A ITIL recomenda que sejam utilizadas medidas para analisar o desempenho das mudanças implementadas em uma infra-estrutura de TI. Uma dessas medidas é um fator de indisponibilidade dos serviços (*Service Disruption* - SD) originado por mudanças mal sucedidas. O SD depende do tempo que transcorre após uma falha em uma mudança até que o sistema seja capaz de recuperar a consistência da infra-estrutura gerenciada, como demonstrado na Figura 4. Além disso, o SD deve levar em consideração o impacto do serviço afetado. Neste trabalho, é utilizada a Equação 1 para o cálculo do SD para uma dada atividade i de um plano de mudança. O cálculo é feito multiplicando três parcelas: ($F_{x,i}$) total de falhas de um tipo x encontradas nos registros de execução da RFC para a atividade i, ($t_{x,i}$) tempo médio de recuperação do sistema para uma falha do tipo x em uma atividade i (pode ser obtido analisando os registros de execução das atividades de remediação) e ($IF_{x,i}$) fator de impacto do elemento afetado pela falha do tipo x da atividade i. Esses produtos são somados para cada tipo de atividade considerado (nesta simulação utilizou-se AF e RF).

$$SD_i = (F_{AF,i} * t_{AF,i} * IF_{AF,i}) + (F_{RF,i} * t_{RF,i} * IF_{RF,i}) \quad (1)$$

Para avaliar o fator de SD da RFC de atualização do serviço de e-mail, foi criado um ambiente de TI emulado onde foram reproduzidos os dois planos de mudança e a infra-estrutura de TI apresentados nesta seção. Os planos de mudança foram submetidos para implantação 30 vezes cada (representando uma execução semanal durante pouco mais de 6 meses) e falhas foram inseridas de forma pseudo-aleatória em suas atividades. Os percentuais de falha inseridos foram: 20% para AF de *update*, 5% para AF de *start*/*stop*, 1% para AF de *backup*/*restore* e 5% para RF de qualquer atividade. Considerando as falhas injetadas durante a emulação e os tempos de recuperação do sistema, o plano de mudança original executado sobre a infra-estrutura da Figura 3 obteve um valor total de SD (somando o SD_i de todas as atividades) de 19,43. Enquanto que a execução do plano modificado com base na análise de riscos atingiu um valor total de SD de 14,31,

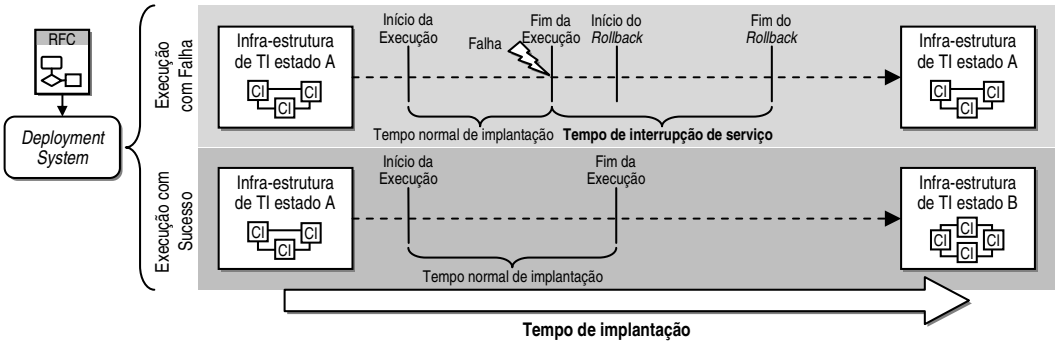

Figura 4. Tempo de interrupção de serviços devido a falhas em implantação de mudanças

o que representa uma redução de aproximadamente 26% na interrupção dos serviços e, conseqüentemente, uma melhora no desempenho do plano de mudança.

6. Conclusões e Trabalhos Futuros

Neste trabalho, foi discutida a necessidade das organizações em utilizar políticas racionais de gerenciamento de mudanças para suas infra-estruturas de TI. Foi visto que falhas durante a implantação dessas mudanças são uma realidade, e que as mesmas podem ter efeito direto na continuidade do negócio. Sendo assim, é fundamental que os riscos associados às mudanças sejam estimados e mitigados, porém, esse processo de avaliação de riscos geralmente fica sob responsabilidade de humanos. Por esse motivo, neste artigo foi proposta uma solução para automatização da estimativa de riscos em gerenciamento de mudanças, visando auxiliar os administradores a minimizar as possibilidades das mudanças causarem danos aos serviços suportados pela infra-estrutura de TI.

Os resultados obtidos demonstraram, em um primeiro momento, que a estimativa proposta neste trabalho é capaz de gerar indicadores de riscos para planos de mudança com base nas informações contidas no sistema de gerenciamento, analisando o histórico de execuções de uma RFC e a visão da infra-estrutura de TI. Essa estimativa se mostrou útil para identificar ameaças em um plano de mudança, servindo como base para criação de medidas de tratamento dos riscos e para tomada de decisões estratégicas durante o planejamento de mudanças. Além disso, uma medida de indisponibilidade de serviços foi utilizada para comparar os diferentes planos de mudança, que revelaram riscos distintos entre si. A redução dos índices de riscos, que ocasionou em uma melhora no fator SD, indica que os relatórios da estimativa de riscos automatizada refletem ameaças reais aos serviços prestados.

Na estimativa de riscos proposta neste artigo foram considerados apenas dois tipos de falha dentre os seis previstos pela classificação adotada. Porém, a solução se mostrou perfeitamente ajustável para contemplar outras classificações. Em trabalhos futuros podem ser analisadas, por exemplo, probabilidades de falhas de humanos alocados para as atividades manuais do plano de mudança. Essa análise poderia auxiliar na alocação de recursos humanos de forma mais adequada considerando as falhas ocorridas em execuções anteriores. Além disso, seria interessante considerar outras possibilidades de combinação dos valores de probabilidade de falha e impacto (além da classificação da Tabela 1), procurando entender as diferenças entre os resultados obtidos.

Referências

Active Endpoints (2008). ActiveBPEL Open Source Engine. http://www.activebpel.org.

Chicken, J. e Posner, T. (1998). *The Philosophy of Risk*. Thomas Telford.

Cordeiro, W. L. C., Machado, G. S., Daitx, F. F., *et al.* (2008). A Template-based Solution to Support Knowledge Reuse in IT Change Design. In *11th IEEE/IFIP Network Operations and Management Symposium (NOMS 2008)*, pages 355–362, Salvador, Brazil.

DMTF (2008). Common Information Model. http://www.dmtf.org/standards/cim.

Fewster, R. e Mendes, E. (2001). Measurement, prediction and risk analysis for Web applications. *7th International Software Metrics Symposium, 2001. METRICS 2001*, pages 338–348.

IRM (2002). *A Risk Management Standard*. The Institute of Risk Management, United Kingdom.

ITIL (2007). *ITIL - Information Technology Infrastructure Library: Service Transition Version 3.0*. Office of Government Commerce (OGC).

ITIL (2008). ITIL - Information Technology Infrastructure Library (ITIL). http://www.itil-officialsite.com/.

Machado, G. S., Cordeiro, W. L. C., Santos, A. D., *et al.* (2008). Algoritmo para Geração Automática de Ações de Rollback em Sistemas de Gerenciamento de Mudanças em TI. In *Brazilian Symposium on Computer Networks (SBRC 2008)*, Rio de Janeiro, Brazil.

Machado, G. S., Wickboldt, J., Cordeiro, W. L. C., *et al.* (2009). Refined failure remediation in it change management systems. In *Mini-conference of 11th IFIP/IEEE International Symposium on Integrated Network Management (IM 2009)*, New York, USA.

Marques, M. e Neves-Silva, R. (2007). Risk assessment to support decision on complex manufacturing and assembly lines. *5th IEEE International Conference on Industrial Informatics*, pages 1209–1214.

Rebouças, R., Sauvé, J., Moura, A., *et al.* (2007). A Decision Support Tool to Optimize Scheduling of IT Changes. In *10th IFIP/IEEE International Symposium on Integrated Network Management (IM 2007)*, pages 343–352, Munich, Germany.

Sauvé, J., Santos, R. A., Almeida, R. R., Moura, A., *et al.* (2007). On the Risk Exposure and Priority Determination of Changes in IT Service Management. In *18th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2007)*, pages 147–158, San Jose, CA, USA.

WfMC (2007). Workflow Process Definition Interface - XML Process Definition Language. http://www.wfmc.org/standards/docs/TC-1025_10_xpdl_102502.pdf.

Wickboldt, J. A., Machado, G. S., Cordeiro, W. L. C., *et al.* (2009). A Solution to Support Risk Analysis on IT Change Management. In *Mini-conference of 11th IFIP/IEEE International Symposium on Integrated Network Management (IM 2009)*, New York, NY, USA.