risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 07/07/2016
Aceitação/Acceptance: 15/11/2016

Mecanismo de controlo para a frente orientado ao risco como garantia da conformidade da execução de processos de negócio

Rui Pedro Marques[1, 2], Sérgio Guerreiro[3,4]

ruimarques@ua.pt, sergio.guerreiro@ulusofona.pt.

[1] Instituto Superior de Contabilidade e Administração, Universidade de Aveiro, 3810-500, Aveiro, Portugal

[2] Algoritmi, Universidade do Minho, Campus Azurém, 4800-058 Guimarães, Portugal

[3] Lusófona University, Campo Grande 376, 1749-024 Lisboa, Portugal

[4] Formetis, Hemelrijk 12c, 5281 PS Boxtel, Netherlands

DOI: 10.17013/risti.20.34–47

Resumo: Os modelos de processos de negócio desenhados para uma organização permitem representar e partilhar um entendimento comum entre os diversos intervenientes que recorrentemente têm interpretações divergentes. Contudo, quando os modelos de processos de negócio são instanciados, diversos riscos podem ser manifestados conduzindo à ocorrência de não conformidades com a sua prescrição inicial. Assim, é necessária a definição, implementação e operacionalização de soluções que permitam controlar a execução dos processos de negócio, observando o que está a ser feito e atuando em caso de não conformidade. Este artigo tem inicio com a proposta e a construção de uma conceptualização para o domínio deste problema. De seguida, os conceitos definidos são instanciados demonstrando a capacidade do controlo para a frente na avaliação do risco em tempo de execução. Se o risco é negativo, ele deve ser evitado sendo os utilizadores finais alertados para esse facto. Se o risco é positivo, poderá ter potencial para ser acomodado como novo modelo de processo de negócio ou como padrão de risco conhecido. Os resultados obtidos de um estudo de caso demonstraram eficiência na resposta do controlador e eficácia na separação entre riscos positivos e negativos. Contribuindo, desta forma, para uma melhoria operacional na execução de processos de negócio comerciais implementados por um ERP.

Palavras-chave: Controlo, Mapa conceptual, Operação, Processo de negócio, Risco.

Risk-oriented feedforward control mechanism on business processes compliance

Abstract: The business processes models are designed to share a common understanding between the various actors who have recurrently disparate interpretations of how to represent the organization. However, when the business processes models are instantiated, many risks can be manifested leading to

the occurrence of non-compliance situations when compared with its original prescription. Therefore, the definition, implementation and operation of solutions to control the execution of business processes instances is needed: observing what is being done and acting in the events of non-compliance. This article begins with a proposal for the construction of a conceptualization to the domain of this problem. Then, the defined concepts are instantiated demonstrating the forward control in the evaluation of runtime risks. If the risk is negative, then it should be avoided and the end users alerted to that fact. If the risk is positive, then it may have the potential to be accommodated as a new business process model or as a known risk. The results of a study case demonstrate the efficiency of the controller response and the effectiveness in the separation of positive and negative risks. Therefore, contributing to improvement in an operating commercial implementation of business processes implemented by an ERP.

***Keywords**:* Business process, Conceptual map, Control, Operation, Risk.

1. Introdução

São múltiplos os fatores endógenos e exógenos a uma organização que promovem a necessidade de mudança nos processos de negócio (Laudon & Laudon, 2015), por exemplo, alterações de requisitos, alterações legais ou tentativas de fraude. Ainda mais se verifica essa necessidade quando se consideram organizações com operação em suporte digital. Em resposta a estas múltiplas mudanças, é necessário que as organizações tenham capacidades nativas de encontrar continuamente soluções inovadoras que adaptem os seus processos de negócio para assim serem mais eficientes e eficazes. Neste contexto, a existência de mecanismos que habilitem a tomada de decisões informadas (Weber, 1987; Rocha & Freixo, 2015), ou o mais informadas possível, são uma competência chave para o sucesso da gestão da organização.

Os processos de negócio assumem um papel duplo de *(i)* prescrição das restrições de desenho para uma determinada realidade organizacional, sendo válida num determinado período de tempo (Hoogervorst, 2009), e *(ii)* suporte para implementação de sistemas que operam as ações executadas pelos atores organizacionais. Porém, os atores têm um papel ativo e autónomo na execução dos processos de negócio, existindo por esta razão um risco que as prescrições dos processos de negócio não sejam cumpridas em conformidade com as iniciais. Por exemplo, mesmo existindo uma recomendação da empresa para obter sempre um registo escrito quando são feitos contactos com os seus clientes, nada limita a capacidade de um ator em contactar diretamente um cliente, por telefone, sem deixar qualquer rastro da comunicação efetuada aos restantes atores da organização. O mesmo exemplo se pode aplicar a execuções de processos de negócio de compra e venda de produtos, em mercados financeiros, que fiquem desconhecidos para os restantes atores. Neste segundo exemplo, com potencial para impacto nefasto à organização e à sua envolvente. Alter (2014) descreve este fenómeno por soluções alternativas encontradas pelos atores (traduzido originalmente da literatura anglo saxónica como *workarounds*).

Assim, este artigo identifica como motivação de investigação, a necessidade de conceber mecanismos de controlo que permitam observar a execução dos processos de negócio, avaliar a sua adequação de acordo com as prescrições disponíveis e atuar quando necessário para mitigar os efeitos da não conformidade. Pretende-se que estes mecanismos de controlo funcionem nos principais componentes de um sistema de informação.

Para demonstração, apresenta-se um estudo de um caso referente à implementação de um protótipo com funcionalidade de controlo para a frente, no âmbito de uma solução de monitorização e auditoria contínua de processos de negócio executados exclusivamente em formato digital, num módulo comercial de um *Enterprise Resource Planning* (ERP).

Em específico, a questão de investigação colocada por este artigo é a seguinte: como desenhar e implementar um mecanismo de controlo das situações de não conformidade em execução de processos de negócio, baseado no conceito de perfil de risco?

Como hipótese este artigo considera o seguinte: é possível identificar e classificar a ocorrência de riscos em negativos e positivos a partir de um confronto com uma definição prévia de perfis de risco conhecidos.

A inovação oferecida por este artigo identifica-se pelos seguinte pontos: *(i)* um mapa conceptual que sintetiza todos os conceitos e relacionamentos envolvidos no mecanismo de conformidade da execução de processos de negócio, permitindo que outros investigadores possam usá-lo como forma de avaliação das suas próprias implementações, e *(ii)* demonstração das qualidades, limitações e desafios impostos pelo mecanismo de controlo para a frente, permitindo a sua implementação otimizada e prescrevendo controlo por retro alimentação nas situações em que se pretende uma abordagem de melhoria contínua.

O presente artigo organiza-se da seguinte forma. Na seção 2 apresenta-se o trabalho relacionado na área de interesse desta investigação. De seguida, a seção 3, introduz os conceitos de controlo de processos de negócio referenciados ao longo do artigo, terminando com uma síntese em forma de mapa conceptual para o controlo dinâmico da operação dos processos de negócio. A seção 4 apresenta o estudo de caso que será usado para discutir a aplicabilidade do controlo de processos de negócio. De seguida a seção 5, refere os resultados obtidos pelo esforço de validação e discute a hipótese levantada pelo artigo. No final, a seção 6 conclui o artigo e identifica trabalho futuro a ser executado como próximos esforços de investigação nesta área.

2. Trabalho relacionado

Esta seção apresenta o trabalho relacionado com o interesse de investigação deste artigo. Em primeiro lugar, são introduzidas as propostas para controlo de processos de negócio usualmente usadas no âmbito da auditoria de sistemas de informação. Em segundo lugar, os conceitos teóricos associados à gestão do risco.

2.1. Controlo de Processos de Negócio

Diversos sistemas de controlo existem numa organização e muitas perspetivas científicas e profissionais estão ao dispor de um gestor, como por exemplo, a teoria geral dos sistemas (Bertalanffy, 1969), o modelo do sistema viável (Beer, 1981), os sistemas baseados em inteligência artificial (Ling, 2015) e as recentes propostas da governação empresarial (Hoogervorst, 2009; Hoogervorst & Dietz, 2008). Um exemplo clássico de sistema de controlo organizacional é o controlo de acessos (Ferraiolo *et al.*, 2001) que tem a responsabilidade de conceder ou revogar o acesso dos utilizadores aos diferentes artefactos existentes numa organização. Outro exemplo são as regras de negócio responsáveis por

manter o funcionamento organizacional dentro dos objetivos pré-definidos (OMG, 2016). Em terceiro lugar, num âmbito mais amplo, a governação empresarial é um exemplo de controlo onde se especifica as restrições de desenho e as orientações de conceção para obter os modelos organizacionais desejados (Hoogervorst, 2009).

No contexto industrial mais lato das tecnologias da informação (TI), os esforços apresentados pelo ITIL (OGC, 2011) consistem num conjunto de boas práticas a aplicar nas infraestruturas, operação e manutenção de serviços de TI, apresentando uma solução que prescreve e orienta a operação contínua dos processos de gestão de mudança. Ainda nesta linha, o COBIT (2007) prescreve um quadro para reforçar a TI com mecanismos de controlo, utilizando as boas práticas, políticas, procedimentos, práticas e estruturas organizacionais. O COBIT preenche a lacuna entre os riscos do negócio, as necessidades de controlo e os aspetos técnicos e tem como objetivo principal identificar e corrigir os eventos indesejados.

De uma forma mais lata, Guerreiro *et al.* (2012) definem que a condução da organização (da literatura anglo-saxónica: *organizational steering*) está relacionada com a capacidade de controlar, dentro de um esforço limitado, a operação da empresa no sentido de cumprir os objetivos desejados sempre que ocorrerem qualquer tipo de alterações ou perturbações. Mais recentemente, Guerreiro & Tribolet (2013) recorrem à teoria e metodologia DEMO (Dietz, 2006), para desenhar uma solução ontológica de controlo da operação dos atores, verificando os modelos prescritos e as observações obtidas.

No contexto específico das instituições financeiras, Delgado & Velthuis (2015) apresentam uma *framework* que continuamente alinha a governação empresarial com as tecnologias de informação. Os autores propõem um ciclo composto por *(i)* identificação das iniciativas (*Plan*), *(ii)* implementação da melhoria (*Do*), *(iii)* monitorizar o processo implementado (*Check*) e *(iv)* melhoria por intermédio de implementações e refinamento sucessivo de ações (*Act*). Assim, demonstra-se a aplicabilidade às iniciativas do contexto financeiro. Contudo, é ainda referido que a solução é não aplicável a outros domínios que envolvam processos de negócio complexos.

2.2. Gestão do Risco

No âmbito da gestão do risco, é importante a identificação e a avaliação do risco, porque é a partir da identificação e avaliação que é possível controlar os processos de negócio com o objetivo de mitigar as suas vulnerabilidades ao risco e reduzir o impacto de eventuais incidentes.

Perfil de risco é conceito importante na identificação e avaliação do risco. Este é um conceito introduzido por Denning (1987) no contexto de investigações sobre deteção de intrusão. Posteriormente, este conceito foi utilizado em contextos organizacionais, nomeadamente na conceção de soluções de auditoria contínua (Santos, 2009) e mais recentemente em soluções de identificação, previsão e avaliação de riscos associados à execução de processos de negócio (Marques *et al.*, 2013b). Nestes últimos estudos, o conceito de perfil de risco está relacionado com a classificação de diferentes comportamentos que podem ocorrer na execução de processos de negócio e podem ser definidos como negativos ou positivos. Os perfis de risco negativos podem ser, por exemplo, operações incompletas, falha de procedimentos cruciais, inconformidades,

atrasos, inconsistências ou fraudes. Por outro lado, os perfis de risco positivos referem-se a todos os comportamentos de execução considerados válidos e apropriados.

Marques *et al.* (2013a) desenvolveram e implementaram uma base de dados, com o objetivo de ser um repositório de perfis de risco, para que possa ser usado como um conjunto de referências ou modelos de execução de processos de negócio. Este repositório de perfis de risco foi concebido de forma a que os perfis de risco sejam modelados e concebidos recorrendo à metodologia DEMO (Dietz, 2006). Este repositório foi utilizado como módulo de suporte a um sistema de informação de monitorização e auditoria contínua de processos de negócio, provando ser um elemento essencial para a averiguação da conformidade da execução de processos de negócio, porque permite que algoritmos de comparação consigam mapear as operações que estão a ser executadas no domínio organizacional com as operações que fazem parte dos perfis de risco definidos no repositório de perfis de risco, e identificar, em tempo de execução, qual o perfil de risco está a ser seguido pelo processo de negócio, antevendo o desfecho da sua execução (Marques *et al.*, 2015).

3. Conceptualização do controlo de processos de negócio

Nesta secção apresenta-se uma descrição textual dos conceitos que compõe a solução para o controlo dinâmico da operação dos processos de negócio, baseando-se em levantamento de trabalho relacionado. Sempre que necessário recorre-se à exemplificação com o intuito de clarificar as definições. De seguida, os conceitos são sintetizados por intermédio de um mapa conceptual e argumentados.

3.1. Actor

Os atores de uma organização são a parte fundamental de uma empresa e estão organizados em sistemas sociais (Winograd, 1986). Um ator é normalmente associado a uma pessoa, mas pode também ser uma máquina. Numa empresa podem coexistir visões individuais e coletivas da mesma realidade (Dietz *et al.*, 2013). Os atores têm liberdade de ação e agem de acordo com seus propósitos e orquestrações. São, portanto, autónomos na decisão sobre o que devem fazer de seguida. Algumas partes das tarefas da empresa pode ser automatizadas por sistemas de *software*, enquanto outras partes são realizadas por humanos. Para além disso, um ator executa diversas atividades ao longo do tempo. Para a realização de uma atividade, um ator cumpre, tacitamente ou explicitamente, um determinado papel. Realça-se ainda o facto do conceito de utilizador diferir do conceito de ator porque representa o acesso de um determinado ator a um determinado sistema de *software*.

3.2. Modelo e instância de um processo de negócio

Neste artigo estudam-se as organizações orientadas a processos de negócio. Para atingir este fim, introduzimos o conceito de transação de negócio DEMO (Dietz, 2006) que é considerado um conceito equivalente. Assim, um modelo de processo de negócio é uma representação abstrata que permite restringir a liberdade de desenho subsequente de uma organização num determinado período de tempo (Op't Land *et al.*, 2009). Por sua vez também é uma representação relevante para partilhar um entendimento comum

entre diferentes atores organizacionais que tal como referido pelo conceito de ator: têm diferentes interpretações da mesma realidade. Contudo, um modelo de processo de negócio não serve para ser operado diretamente pelos atores. É necessário que os modelos previamente desenhados sejam implementados em sistemas (manuais, semiautomáticos ou automáticos) e sejam contidos na organização, para que de seguida possam ser instanciados. Essa instanciação ocorre quando os atores executam as suas atividades ao longo do dia. Para além disso, as instâncias de processos de negócio vão revelar a existência real da organização no dia-a-dia. Múltiplas instâncias de processos de negócio ocorrem concomitantemente numa organização. Exemplificando os conceitos de modelo e instância de processo de negócio, um modelo de processo de negócio define quais os papéis de atores que estão envolvidos em cada transição de estado, mas são posteriormente os atores que especificamente instanciam as transições de estado dos processos de negócio. Para sistematização desta problemática, Dietz (2006) propõe um modelo de representação de processos de negócio envolvendo os seguintes três aspetos: *(i)* a definição dos papéis dos atores, de forma a especificar quem é responsável por cada parte do processo de negócio, *(ii)* a definição de um espaço de transição de estados e *(iii)* a definição de um espaço de estados. Do mesmo modo como se pode representar os modelos de processo de negócio, podem também ser representadas as instâncias de processos de negócio. Usando uma representação única habilita-se a capacidade de verificar se alguma das instâncias de um processo de negócio não está a respeitar a prescrição pelo modelo. Caso ocorra uma não observância do modelo, então as funções de controlo organizacionais deverão ser invocadas.

3.3. Observação

No contexto do controlo de sistemas dinâmicos, Franklin et al. (2009) referem que *"... um sistema é completamente observável se cada variável de estado do sistema afeta algumas das saídas. Muitas vezes, é desejável obter informações sobre as variáveis de estado das medições das saídas e das entradas. Se qualquer um dos estados não pode ser observado a partir das medições das saídas, o estado é dito não observável e o sistema não é completamente observável ou simplesmente não observável..."*. Assim, numa organização complexa, uma parte dos estados da operação dos seus processos de negócio são observáveis enquanto outra parte denomina-se de não observável. Logo, pode não ser possível obter observações sobre todos os estados da operação dos processos de negócio. Para além disso, usualmente, os estados do ambiente envolvente também não são totalmente observáveis. Quando um estado é não observável então as funções de controlo organizacionais não podem ser executadas de forma totalmente informada. Contudo, conforme demonstrado por Guerreiro (2014) a observação parcial combinada com processos de cálculo estocásticos podem potenciar a avaliação do impacto das decisões de controlo na operação da organização.

3.4. Ação de controlo

Dois tipos de variáveis de controlo existem num sistema: as que são controláveis e as que não são controláveis. De forma semelhante ao anterior conceito da observação apresenta-se a definição proposta no contexto do controlo de sistemas dinâmicos, Franklin *et al.* (2009): *"... um processo denomina-se totalmente controlável se cada variável de estado*

do processo fôr controlada para atingir um certo objetivo em tempo finito por um controlo u(t) sem restrições. Se qualquer uma das variáveis de estado for independente do controlo u(t) isto significa que não há nenhuma maneira de atuar, em tempo finito, essa variável de estado para o estado desejado. Portanto, esse estado em particular é denominado de incontrolável. Se houver pelo menos um estado incontrolável, então o sistema é denominado não totalmente controlável ou simplesmente incontrolável". No contexto de estudo dos processos de negócio, uma ação de controlo pode resultar em uma de duas diferentes possibilidades:

- Ação de controlo sobre as instâncias dos processos de negócio para evitar que as situações de desvio propositado não comprometam a operação da organização (também considerado de **controlo negativo**). Por exemplo, um ator que vê revogado o seu acesso a um determinado sistema;
- Ação de controlo sobre os modelos dos processos de negócio se for reconhecida que a situação de desvio representa inovação (também considerado de **controlo positivo**). Por exemplo, executar as mesmas atividades, mas de forma otimizada. Neste caso, uma nova prescrição é incorporada nos modelos da organização.

3.5. Tempo

Um ciclo de controlo de um sistema é essencialmente composto pela sequência clássica PDCA proposta por Shewhart (1980): *(i)* a inteligência para observar um problema organizacional, *(ii)* o desenho das potenciais soluções, *(iii)* a escolha da melhor solução e *(iv)* implementação da solução e verificação se satisfaz o cumprimento dos objetivos pretendidos. Entre as diferentes atividades de controlo ocorrem atrasos no tempo, ou seja, quando um controlador decide por uma ação de controlo *u(t)* esta é baseada na observações do passado *y(t-1), y(t-2),... ,y(t-n)*. Isto significa que quando o controlo *u(t)* é acionado pode já não ser válido na realidade operacional do sistema a controlar. Em termos conceptuais, tudo o que acontece antes da operação dos processos de negócio, denomina-se *ex-ante*, e relaciona-se por exemplo, com a prescrição dos modelos dos processos de negócio. Nesta fase, é necessário fazer estimativas acerca das situações desconhecidas. Por outro lado, tudo o que sucede depois da operação dos processos de negócio, denomina-se *ex-post*, e relaciona-se por exemplo, com a reação necessária quando algo ocorre de forma inesperada. Por omissão, os processos de decisão sobre a ação u(t) mais correta a ser tomada considera os modelos *ex-ante* dos processos de negócio como referência de controlo a ser seguida.

3.6. Padrão de controlo

O objetivo do controlo é permitir que a operação da(s) instância(s) dos processos de negócio sejam conduzidas, usando um esforço limitado, para um estado estável previamente definido pela organização, sendo capaz de reagir às alterações e perturbações exógenas e endógenas que vão ocorrendo. Conceptualmente, a estabilidade de um sistema é definida por Kuo (1995) como: *"...considerando a resposta de um sistema a entradas ou perturbações: um sistema que permaneça em estado constante, exceto quando é afetado por uma ação externa, mas que seja capaz de voltar ao estado constante inicial logo após essa ação externa ser removida então pode ser considerado estável..."*.

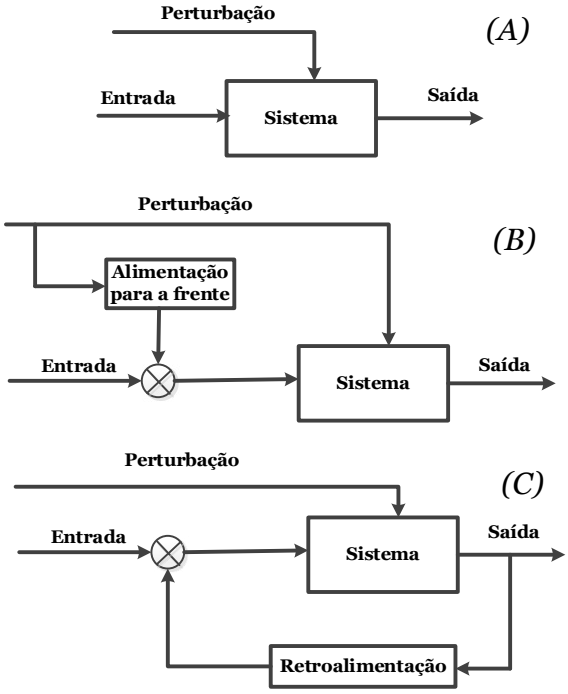

Figura 1 – Padrões de desenho de um sistema de controlo. (A) sem controlo, (B) controlo por alimentação para a frente e (C) controlo por retroalimentação.

Na Figura 1 apresentam-se os padrões clássicos para um sistema de controlo. Na parte superior, (A), é apresentado um sistema que não é controlado. A perturbação afeta sempre a saída entregue pelo sistema. Neste modelo, não é possível garantir o comportamento do sistema de saída. No meio da Figura 1, (B), um padrão de alimentação para a frente, que mostra que a entrada do sistema muda de acordo com a perturbação. Assim, a dinâmica específica do sistema não está incluída na ação de controlo. Na parte inferior da Figura 1, (C), um padrão de controlo de retroalimentação calcula a entrada do sistema de acordo com o desalinhamento real obtido entre a saída e entrada. Neste padrão, o cálculo de controlo de atuação toma em consideração a perturbação a dinâmica do sistema. A saída do sistema depende da perturbação aplicada no sistema e sobre a própria dinâmica do sistema.

Com estas definições dos padrões de controlo, torna-se agora explícito, que para obter um sistema de controlo que produza os resultados expectáveis, seja necessária a disponibilização das capacidades de observação *y(t)* e de atuação *u(t)* no sistema a controlar.

3.7. Mapa conceptual dos conceitos anteriores

Um modelo de processo de negócio é composto por papéis de atores, definição de estados e transições entre esses mesmos estados. A definição é feita *ex-ante*. Os modelos de processos de negócio têm o propósito de representar uma realidade organizacional

e são implementados pelas instâncias de processos de negócio. Os atores são os responsáveis por executar as instâncias de processos de negócio de acordo com os seus papéis. Por sua vez, a operação das instâncias é observável permitindo que os sistemas de controlo organizacionais consumam essa informação e assim possam decidir, de forma informada, sobre quais são as ações de controlo corretas a tomar em função dos desalinhamentos identificados. Os sistemas de controlo são desenhados segundo padrões pré-definidos: alimentação para a frente ou retroalimentação. Por último, as ações de controlo incidem sobre os modelos de processos de negócio (controlo positivo) ou sobre as instâncias de processos de negócio (controlo negativo). A ação de controlo *u(t)* é executada *ex-post* e baseia-se nas observações anteriores *y(t-1), y(t-2),.., y(t-n).* Quando o desalinhamento identificado é reconhecido como sendo inovador então é acomodado em novos modelos de processos de negócio que as futuras instâncias irão implementar. Quando o desalinhamento é reconhecido como prejudicial então as atuais instâncias de processos de negócio são intervencionadas para correção.

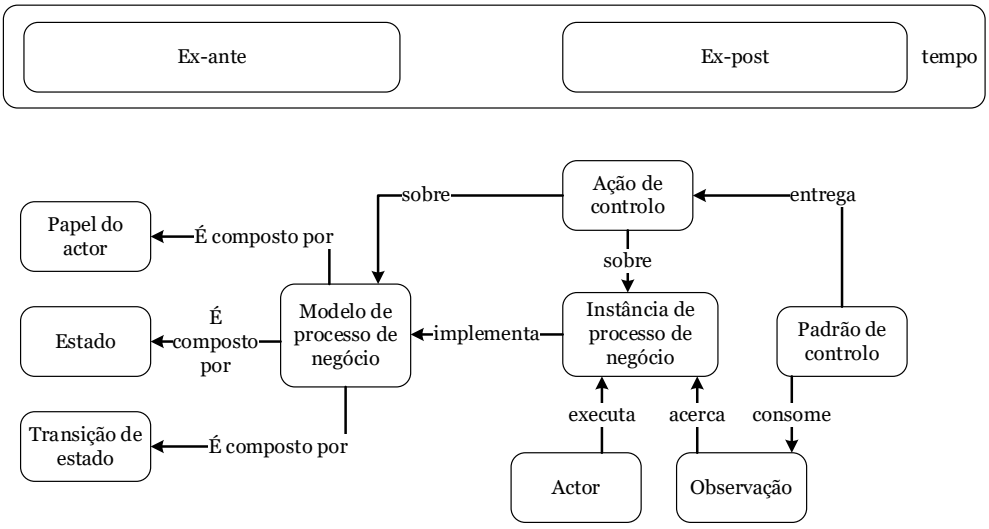

Figura 2 – Mapa conceptual para o controlo dinâmico da operação dos processos de negócio.

4. Apresentação do estudo de caso

Esta secção apresenta um estudo de caso em que se utilizou um protótipo que foi desenvolvido com o objetivo de oferecer controlo para a frente na execução de processos de negócio. A abordagem de conceção e desenvolvimento do protótipo foi validada (Marques, 2014), demonstrando a sua eficácia na monitorização e controlo de processos de negócio, numa perspetiva de auditoria contínua.

Este protótipo apresenta-se como um módulo independente de qualquer outro sistema de informação nos quais os processos de negócio possam ser executados (exemplo: ERP). A única ligação que existe entre o módulo e o contexto organizacional, é a existência de um conjunto alargado de mecanismos de controlo interno que tem como objetivo a

observação das operações executadas, passíveis de ser observadas. Estes mecanismos de controlo interno foram concebidos de forma a serem observadas as operações, de mais baixo nível, que constituem o processo de negócio a ser monitorizado e auditado. Exemplo destes mecanismos são *triggers* que observam os dados das bases de dados, com o objetivo de controlar a inserção de novos dados, assim como a sua atualização e eliminação.

Para além deste conjunto alargado de mecanismos de controlo interno, o protótipo é constituído por um repositório que gere os modelos de execução conhecidos, associados aos processos que se pretendem auditar. Para conceber os modelos de execução é utilizada a metodologia DEMO, para que de uma forma objetiva e sem ambiguidade se definam quais as sequências de operações esperadas, quais os intervalos de tempo mínimos e máximos entre operações, os perfis de utilizadores autorizados a executar as operações e outras condições de execução. Neste caso, referimo-nos aos modelos esperados, ou seja, os perfis de risco positivos. Mas este repositório gere também os perfis de risco negativos conhecidos pela organização, ou seja, as sequências de operações não desejadas, utilizadores não autorizados, e outras condições não permitidas na execução dos processos de negócio.

Além disso, um algoritmo compara, em tempo de execução, a informação proveniente dos mecanismos de controlo interno com os modelos de execução definidos no repositório de perfis de risco. Desta comparação, resultam os outputs do sistema, nomeadamente, o grau de conformidade da execução do processo e situações que requeiram atenção por parte dos utilizadores (por exemplo, verificação de que determinado processo de negócio está a seguir um perfil de execução negativo ou desconhecido), pois podem significar um risco potencial para a organização. Estes outputs permitem acompanhar o estado atual e histórico dos processos de negócio executados ou em execução, e são, essencialmente: relatórios, interface gráfica e *e-mails* de alerta.

Este estudo de caso refere-se a uma implementação do protótipo em ambiente organizacional simulado que envolveu três empresas de setores diferentes durante cerca de três meses. A implementação decorreu no âmbito da unidade curricular "Simulação Empresarial" da Licenciatura em Contabilidade da Universidade de Aveiro, na qual os estudantes criam as suas empresas e simulam um ano de atividade, cumprindo com todas as obrigações legais a que uma empresa do mesmo setor está realmente obrigada (Marques, 2014). Este estudo envolveu a observação e monitorização de processos de negócio exclusivamente executados em formato digital no ERP comercial utilizado em "Simulação Empresarial". Os processos de negócio selecionados para o estudo referem-se a transações comerciais, designadamente, operações relacionadas com a emissão de documentos e a respetiva autorização, porque são processos de negócio que estão objetivamente regulados. Portanto, a avaliação de risco, neste estudo, incidiu essencialmente, na avaliação do incumprimento dessa mesma regulação, nomeadamente, sequência, validade e alteração de documentos.

5. Validação

Durante o período de estudo, mais de 280 processos de negócio foram monitorizados, o que equivale à observação de cerca de 1130 operações. Dos resultados obtidos

verifica-se que o sistema concebido é eficaz no controlo para a frente, porque (Marques *et al.*, 2015):

1. 100% das operações executadas foram observadas;
2. para cada processo de negócio executado, ou ainda em execução, foram identificados quais os respetivos perfis de execução (positivos ou negativos) estão a ser observados; no caso da execução do processo de negócio estar a seguir um perfil de risco não definido, o sistema assinalou o processo como seguindo um perfil de risco desconhecido;
3. a grande parte dos processos de negócio que seguem perfis de risco positivos são corretamente identificados (a percentagem de não ser emitido um alerta é superior ou igual a 99,7% com um nível de significância de 1%);
4. praticamente todas os processos de negócio que seguem perfis de risco desconhecidos são corretamente identificados (a percentagem de ser emitido um alerta é superior ou igual a 99,9% com um nível de significância de 1%);
5. 100% dos processos de negócio que seguem perfis de risco negativos foram corretamente identificados e emitido um alerta.

Referenciando a hipótese inicialmente declarada: "*é possível identificar e classificar a ocorrência de riscos em negativos e positivos a partir de um confronto com uma definição prévia de perfis de risco conhecidos*", podemos então verificar que o sistema é capaz de estimar qualitativamente o risco com que um processo foi executado ou está a ser executado, devido à sua capacidade de identificar, em tempo de execução, os perfis de risco associados a execução que está a decorrer com base nos perfis de risco definidos e nos dados recolhidos pelos mecanismos de controlo interno, que permanentemente observam a base de dados do ERP onde estão a ser executados os processos de negócio. Além disso, é possível identificar a capacidade de verificar a conformidade de execução com as regras e políticas definidas para a execução e definidas no repositório de perfis de risco, e identificar as operações causadoras de irregularidades.

6. Conclusões e Trabalho Futuro

O presente artigo apresenta um mecanismo inovador que permite garantir a conformidade da execução de instâncias de processos de negócio usando um mecanismo de controlo para a frente baseado no conceito de perfil de risco. Os resultados obtidos de um estudo de caso demonstram, por intermédio de cinco indicadores, que a eficiência na resposta do controlador e a eficácia na separação entre riscos positivos e negativos é obtida. Contribuindo, desta forma, para uma melhoria operacional na execução de processos de negócio comerciais implementados por um ERP, na medida em que o sistema permite avaliar, em *run-time*, eventuais desvios de execução, alertando o utilizador para essa situação. Assim, ações fraudulentas podem ser mais facilmente identificadas, e os erros humanos mais rapidamente corrigidos, evitando a propagação do erro.

A inovação oferecida por este artigo identifica-se por um mapa conceptual que sintetiza todos os conceitos e relacionamentos envolvidos no mecanismo de conformidade da execução de processos de negócio, e pela demonstração das qualidades, limitações e desafios impostos pelo mecanismo de controlo para a frente.

Comparando esta solução com soluções existentes no domínio da mineração de processos (traduzido da literatura anglo-saxónica: *process mining*), Aalst (2011) enriquece a classificação de situações de risco positivas e negativas com situações que são consideradas verdadeiras e outras que são falsas. É segundo esta classificação aberto um espaço de solução maior do que o apresentado por este artigo. A nossa proposta de controlo para frente de instâncias de processos de negócio permite identificar as situações positivas e negativas a partir do conhecimento existente sobre perfis de risco, assumindo que o que é conhecido é verdadeiro e todo o restante é falso. Consideramos que esta abordagem, usada em exclusivo, pode implicar erros, e assim, como trabalho futuro é identificada a necessidade de classificar a veracidade ou falsidade de cada um dos riscos considerados positivos ou negativos. A teoria de Markov aplicada a sistemas parcialmente observáveis poderá ser uma possível solução para este problema.

Para além deste aspeto, é também identificada a necessidade de investigar mecanismos de controlo por retroalimentação que permitam incorporar novos riscos na base de conhecimento de perfis de risco. Ou seja, de acordo com as observações extraídas da execução das instâncias dos processos de negócio, o controlador compara o risco observado com a sua base de conhecimento e classifica como potencial novo risco. Desta forma, os perfis de risco podem evoluir de acordo com a dinâmica imposta pelos atores organizacionais, por exemplo, formas inovadoras de comunicar com o cliente ou otimização de tarefas nas prescrições dos modelos dos processos de negócio. Para classificação de novos riscos a equipa de investigação antevê o desenvolvimento de um módulo de *software* denominado de "*incubadora de riscos*" que permitirá o alojamento restrito do novo risco até que um ator o classifique manualmente acerca do seu perfil: positivo ou negativo.

Referências

Aalst, W. M. P. van der (2011). *Discovery, Conformance and Enhancement of Business Processes*, ser. Database Management & Information Retrieval. Springer, DOI: 10.1007/978-3-642-19345-3.

Alter, S. (2014). Theory of Workarounds, *Communications of the Association for Information Systems*, 34 (55) 1041–1066.

Beer, S. (1981). *Brain of the Firm: The Managerial Cybernetics of Organization*. New York: John Wiley & Sons, Inc.

Bertalanffy, L. (1969). *General Systems Theory*. George Braziller, New York.

COBIT. (2007). Control objectives for information and related technology (cobit). Edition 4.1. Rolling Meadows, IL: IT Governance Institute. Retrieved November 20, 2013, from http://www.isaca.org/cobit.htm

Delgado, A. P., & Velthuis, M. P. (2015). Propuesta de marco de mejora continua de gobierno TI en entidades financieras. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (15), 51–67, DOI: 10.17013/risti.15.51-67.

Denning, D. E. (1987). An intrusion-detection model, *IEEE Transactions on Software Engineering*, 2, 222–232, DOI: 10.1109/TSE.1987.232894.

Dietz, J. (2006). *Enterprise Ontology – Theory and Methodology*. Springer-Verlag. DOI:10.1007/3-540-33149-2.

Dietz, J., Hoogervorst, J., Albani, A., Aveiro, D., Babkin, E., & Barjis, J. et al. (2013). The discipline of enterprise engineering. *International Journal of Organisational Design and Engineering*, 3(1), 86–114. DOI:10.1504/IJODE.2013.053669.

Ferraiolo, F., Sandhu, R., Gavrila, S., Kuhn, D., & Chandramouli, R. (2001). Proposed nist standard for role-based access control. *ACM Trans. Inf. Syst. Secur.*, 4(3): 224–274, DOI:10.1145/501978.501980.

Franklin, F., Powell, D., & Emami-Naeini, A. (2009). *Feedback control of dynamic systems* (6th ed.). Addison-Wesley Publishing Company.

Guerreiro, S., Vasconcelos, A., & Tribolet, J. (2012). Enterprise dynamic systems control enforcement of run-time business transactions (EEWC 2012) (Vol. 110, pp. 46-60). Springer-Verlag. DOI: 10.1007/978-3-642-29903-2.

Guerreiro, S., & Tribolet, J. (2013). Conceptualizing Enterprise Dynamic Systems Control for Run-Time Business Transactions. Paper presented at the 21st ECIS 2013, Utrecht, Netherlands, June.

Guerreiro, S. (2014). Decision-making in partially observable environments, *16th IEEE Conference on Business Informatics* (IEEE CBI 2014), DOI: 10.1109/CBI.2014.15, Geneva, Switzerland, July, DOI: 10.1109/CBI.2014.15.

Hoogervorst, J. (2009). *Enterprise governance and enterprise engineering*. Berlin, Heidelberg: Springer-Verlag.

Hoogervorst, J., & Dietz, J. (2008). Enterprise architecture in enterprise engineering. *Enterprise Modelling and Information Systems Architecture*, 3, 3–11, DOI:10.18417/emisa.3.1.1.

Kuo, B. (1995). *Automatic control systems*, 7th edition, Prentice Hall International Editions.

Laudon, K., Laudon, J. (2015). *Management Information Systems: Managing the digital firm*, 15th ed. Pearson.

Ling, L. (2015). Research on Enterprise Internal Control Financial Assessment System Based on Artificial Intelligence, RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (16B), 224–234.

Marques, R. P., Santos, H., & Santos, C. (2013a). An enterprise ontology-based database for continuous monitoring application, in Business Informatics (CBI), 2013 IEEE 15th Conference on. IEEE, pp. 7–12, DOI: 10.1109/CBI.2013.10.

Marques, R. P., Santos, H., & Santos, C. (2013b). Organizational transactions with real time monitoring and auditing, *The Learning Organization*, 20(6), 390–405, DOI: 10.1108/TLO-09-2013-0048.

Marques, R. P. (2014). Organisational transactions with embedded control, PhD thesis, Universidade do Minho, Portugal.

Marques, R. P., Santos, H., & Santos, C. (2015). Monitoring organizational transactions in enterprise information systems with continuous assurance requirements, *International Journal of Enterprise Information Systems*, 11 (1), 13–32, DOI: 10.4018/ijeis.2015010102.

OGC. (2011). Office for Government Commerce, ITIL v3. Information Technology Infrastructure Library.

OMG (2016). Object management group. Semantics of business vocabulary and business rules. Retrieved September 2, 2016, from http://www.omg.org/spec/SBVR/1.0/PDF.

Op't Land, M., Proper, E., Waage, M., Cloo, J., & Steghuis, C. (2009). *Enterprise architecture: Creating value by informed governance*. Springer-Verlag.

Rocha, Á., & Freixo, J. (2015). Information Architecture for Quality Management Support in Hospitals. *Journal of Medical Systems*, 39(10), 1–11. DOI: 10.1007/s10916-015-0326-z

Santos, C. (2009). *Modelo Conceptual para Auditoria Organizacional Contínua com Análise em Tempo Real*, 1st ed. Penafiel: Editorial Novembro.

Shewhart, W. (1980). *Economic Control of Quality of Manufactured Product* / 50th Anniversary Commemorative Issue. American Society for Quality, ISBN 0-87389-076-0.

Weber, M. (1987). Decision making with incomplete information, *European Journal of Operation Research*, 28, 44–57, DOI: 10.1016/0377-2217(87)90168-8.

Winograd, T. (1986). A language/action perspective on the design of cooperative work. In Proceedings of the *ACM conference on Computer-supported cooperative work*, pp. 203-220. New York: ACM, DOI: 10.1207/s15327051hci0301_2.