www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

A GESTÃO DE PROCESSOS DE NEGÓCIO COMO FERRAMENTA DE APOIO NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

BUSINESS PROCESSES MANAGEMENT AS SUPPORT TOOL IN THE INFORMATION SECURITY MANAGEMENT

Fernando Della Flora[1]; Cristiano Tolfo[2]
[1]Núcleo de tecnologia da Informação e Comunicação - NTIC
Universidade Federal do Pampa – UNIPAMPA – Alegrete/RS – Brasil
fernandoflora@unipampa.edu.br
[2]Laboratório de Engenharia de Software Aplicada - LESA
Universidade Federal do Pampa – UNIPAMPA – Alegrete/RS – Brasil
cristianotolfo@unipampa.edu.br

Resumo

Os processos que envolvem a gestão da informação e do conhecimento nas organizações requerem a definição de processos relacionados à gestão da segurança da informação. Nesse sentido, a abordagem de gestão de processos de negócio é uma importante ferramenta de apoio, tanto na visualização como no mapeamento e definição de seus processos. O objetivo desse trabalho é apresentar um relato de experiência com o uso da gestão de processo de negócio com foco nos processos do segurança da informação. Utilizando a técnica de estudo de caso, foi observada, em um núcleo de segurança da informação de uma instituição pública de ensino superior, uma iniciativa em que foram mapeados e melhorados processos. Neste artigo é descrito um dos processos que foram modelados utilizando a notação BPMN, trata-se do processo de liberação de endereço IP público. Neste processo, foram identificadas oportunidades de melhoria durante a análise e a modelagem do seu estado atual. Estas melhorias foram analisadas e representadas durante a modelagem do estado futuro do processo. Como resultado destas análises e representações, aponta-se a atividade de análise de vulnerabilidades e a de auditoria de conformidade são as principais melhorias que foram implantadas no processo de liberação de endereço IP público. No que se refere à iniciativa de gestão de processos de negócios observada no estudo de caso, foi verificado que a perspectiva de processos de negócios pode auxiliar na gestão da segurança da informação, pois permite revisar atividades e recursos utilizados, formalizar o modo de gerenciar e comunicar processos envolvidos.

Palavras-chave: Gestão da segurança da informação, Gestão de processos de negócio; modelagem de processos; BPMN.

Abstract

The processes that involve the information and knowledge management on organizations require the definition of processes related to information security management. In this sense, business process management approach is an important support tool, both in view as the mapping and definition of its processes. The aim of this paper is to present a report of experience with the use of business process management with a focus on processes of information security. Using the case study technique, was observed in an information security core of a public institution of higher education, an initiative in which the processes were mapped and improved. In this paper is described the process of releasing public IP address that was modeled using BPMN notation. In this process, opportunities for improvement were identified during the analysis and modeling of its current state. These improvements were represented during the modeling of the future status process. As a result indicates that the analysis of vulnerabilities and compliance audit activities are the main improvements that have been implemented in this case. With regard to business process management initiative observed in the case study, it was found that the perspective of business processes can assist in information security management as it allows review activities and resources used to plan and formalize how to manage and communicate processes involved.

Keywords: information security management; business processed management; process modeling; BPMN.

1. Introdução

A informação tem sido apontada como um importante ativo para os diferentes segmentos da sociedade. Em decorrência dos avanços nas tecnologias e sistemas da informação a disseminação de informações contribui para a geração de conhecimento e por outro lado, gera a necessidade de gerenciar a segurança e a disponibilidade destas informações.

As organizações cada vez mais tem a informação como um ativo estratégico gerador de diferencial competitivo para o negócio. De acordo com Potrich, Vieira e Nunes (2013, p.170) “o processo de gerenciamento da informação busca explicar o comportamento da organização, examinando os fluxos de informação em torno dela”. Em decorrência disso, se faz necessário à proteção destas informações o que remete a iniciativas de gestão da segurança da informação.

Neste contexto, Soomro; Shah e Ahmed (2016) ressaltam a necessidade de criar-se uma visão holística que acumula conhecimentos sobre as funções e atividades que envolvem a gestão de segurança da informação. Ao citar estudos, como os realizados por Phillips (2013), Singh et al. (2013) e Siponen, Mahmood, e Pahnila (2014), os referidos autores evidenciam que as questões de segurança da informação precisam ser consideradas no contexto da gestão.

A segurança da informação sob uma perspectiva holística de processos e de gestão pode ser implantada pelas organizações com o auxilio da uma abordagem de gestão de processos de negócios, também conhecido como BPM - *Business Process Management*. Pois segundo Turban e Volonino (2013, p. 394), “Um processo de negócio consiste em um conjunto de tarefas ou

atividades que são executadas de acordo com certas regras relacionadas a determinados objetivos". Nesta perspectiva, um processo que envolve a segurança da informação contém tarefas a serem executadas seguindo normas de segurança, que visa atender objetivos organizacionais e se enquadra em um projeto de gestão de processos de negócios.

Este artigo apresenta um estudo de caso em que foram modelados processos de negócios relacionados à segurança da informação de uma Instituição Federal de Ensino Superior. O objetivo do trabalho é apontar a modelagem e a gestão de processos de negócios como uma alterativa para identificar possibilidades de melhoria da gestão da segurança da informação.

2. Referencial teórico

Esta seção aborda os assuntos relacionados com o objetivo do trabalho. Inicialmente é apresentado o conceito de gestão de segurança da informação. Na sequência são abordados assuntos que envolvem a gestão de processos de negócios, a abordagem adotada para a modelagem de processos e a notação para a representação destes processos.

2.1 Gestão da segurança da informação

A gestão de segurança da informação envolve a definição e implantação de um sistema de gestão de segurança da informação que pode seguir normas baseadas em padrões definidos pela ISO/IEC 27001:2013 (ABNT, 2013a) e ISO/IEC 27002:2013 (ABNT, 2013b). Na norma ISO/IEC 27001:2013, conforme a ABNT (2013a), são estabelecidos requisitos que possibilitam a definição, a implantação e a melhoria contínua de um sistema de gestão de segurança da informação. Enquanto que na ISO/IEC 27002:2013 são definidas diretrizes que orientam a implantação destes requisitos.

De acordo com Nazareth e Choi (2015, p. 123) "a gestão eficaz da segurança da informação requer que recursos de segurança sejam implantados em várias frentes, incluindo a prevenção ataque, redução da vulnerabilidade e dissuasão de ameaças". Além disso, a gestão da segurança da informação implica em mudanças organizacionais que envolvem ações que a institucionalizam. Segundo Dhillon, Syed e Pedron (2016, p.68) "a gestão de segurança da informação é uma consequência de como os processos de negócios são redesenhados, levando em consideração aspectos informais, formais e técnicos". Trabalhos como os apresentados por Kwon (2007), Eminağaoğlu; Uçar; Eren (2009), Ozkan e karabacak (2010), Yildirim et al. (2011), Ahmad; Baskerville; Spagnoletti e Kim (2014), Maynard e Shanks (2015), são estudos de casos que indicam a pertinência da gestão de segurança da informação tanto no âmbito acadêmico de pesquisa como no campo de aplicação prática.

2.2 Gestão de processos de negócios

Para o entendimento sobre gestão de processos de negócios é necessário compreender inicialmente o conceito de processo de negócio. Laudon e Laudon (2011, p. 37) definem processos de negócios como "um conjunto de atividades logicamente relacionadas que define como as tarefas organizacionais específicas serão executadas", segundo os mesmos autores, a tecnologia da informação pode aprimorar processos de negócios e que os sistemas de informação geram valor ao automatizar tarefas manuais, alterando o fluxo da informação e gerando a possibilidade de inovação.

A gestão de processos de negócios, segundo Laudon e Laudon (2011), é uma abordagem de gestão constituída de etapas cujo objetivo é a melhoria contínua. As etapas mencionadas envolvem identificar os processos a serem modelados, analisar os processos existentes, planejar o novo processo, implantar o novo processo e avaliar continuamente o processo após a sua implantação.

A AQPC (2010) propõe um framework para a classificação dos processos de negócios, denominado de *Process Classification Framework* (PCF), o qual as organizações podem utilizá-lo como referência para estruturar seus processos. O PCF pode ser ajustado ao contexto de cada empresa, visando seu o desdobramento na gestão de processos de negócios. Conforme pode ser observado na Figura 1, o PFC classifica algumas das atividades que envolvem gestão de segurança de informação como processos de gerência e serviços de apoio.

FIGURA 1 – Exemplo níveis do Process Classification Framewok - PCF.

Serviços de gerenciamento e suporte	7.0 - Gerenciar tecnologias da informação	7.3 - Gerenciar recuperação e risco do negócio.	7.3.4 - Testar, avaliar e implementar controles de segurança da informação e privacidade e proteção de dados. 7.3.4.1 - Estabelecer estratégias e níveis de segurança da informação, privacidade e proteção de dados. 7.3.4.2 - Testar, avaliar e implementar controles de segurança da informação, privacidade e proteção de dados.

Fonte: adaptado de APQC (2010).

As atividades de gestão de segurança da informação, descritas na Figura 1, encontram-se em forma de processos e derivam da categoria de processo gerenciar recuperação e risco de negócios que por sua vez está classificada na categoria gerenciar tecnologias da informação.

2.2.1 – Abordagem e notação para modelagem de processos de negócio

A abordagem utilizada neste trabalho para a modelagem de processos de negócios envolve a elaboração das versões AS-IS e TO-BE de processos. Ela tem sido abordada normalmente com o propósito de analisar um determinado processo tal como ele se encontra, realizando a modelagem do seu estado atual, que é o AS-IS do processo. A partir disso, deve-se analisar o estado atual do processo com vista a melhorias, sendo que estas melhorias são apontadas em uma nova modelagem, que é o estado futuro do processo, ou seja, o TO-BE do processo.

As modelagens do estado atual e estado futuro dos processos estão presentes na gestão de processos de negócios por serem formas de verificar como que a empresa esta operando e quais os pontos suscetíveis de melhorias. Os trabalhos realizados por Jacoski, e Grzebieluchas (2011), Pereira et al (2011). Santos (2011), Ahmed (2012), Cardoso, Alencar e Oliveira (2012), Dias Jr, Oliveira e Meira (2012), Milan e Soso (2012), Kirama (2013), Muckenberger et al. (2013), Islam e Sena (2013), Silva e Zaidan (2013), Leyer e Hollmann (2014) são alguns dos estudos que apresentam a utilização da abordagem AS-IS e TO-BE em diferentes contextos.

Na modelagem do AS-IS, Baldan et al. (2010) recomenda inicialmente de preparação do projeto de modelagem para a definição da equipe, do escopo e do planejamento do projeto, além da consulta da documentação a respeito do processo que será estudado. Na sequência podem ser realizadas as entrevistas e coleta de dados com usuários do processo, gerando documentação que servirá de subsidio para a etapa de documentação do processo, quando será modelado o processo. Na sequência ocorre a etapa de validação do processo, sendo o mesmo testado em uma instância real, sendo que a validação gera a possibilidade de correções da documentação.

Já a modelagem do TO-BE deve ter como objetivo a melhoria em relação ao processo AS-IS e conduzir à criação de um novo processo. Este novo processo pode ser uma melhoria onde tarefas consideradas desnecessárias são eliminadas ou um processo totalmente modificado com foco na inovação. De qualquer forma, qualquer mudança deve estar focada na agregação de valor.

As etapas que envolvem especialmente a análise e o planejamento na gestão de processos de negócios, necessitam da representação destes processos. Uma forma de representação é por meio da BPMN - *Business Process Management Notation*, disponível em OMG/BPMN (2015), que é uma notação que vem sendo utilizada para a modelagem de processos de negócio.

A notação BPMN é composta por um conjunto de elementos que permitem comunicar desde a representação de atividades pelas próprias pessoas que trabalham em um dado processo, até a automatização destas mesmas atividades por responsáveis pelo desenvolvimento de sistemas de informação. Os processos apresentados neste trabalho foram modelados utilizando a ferramenta *BizAgi modeler* (BIZAGI, 2015) e seguindo a notação BPMN.

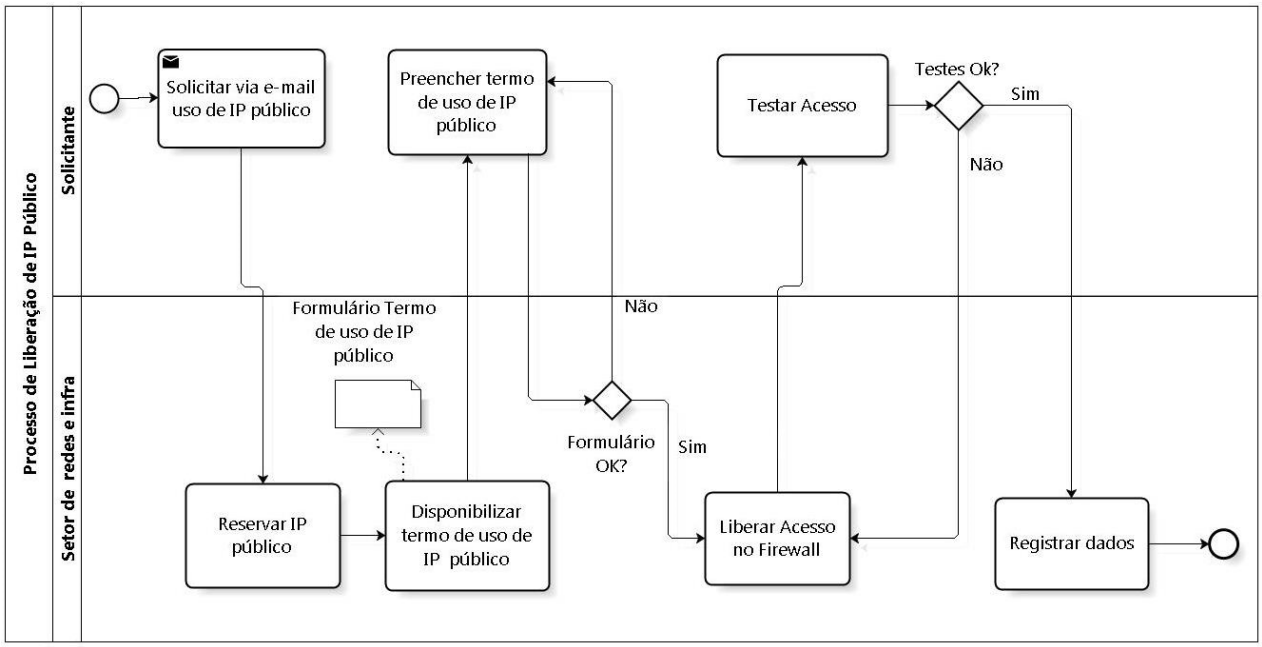
3. A pesquisa realizada

Seguindo a estrutura proposta por Bertucci (2011) para a elaboração da seção de metodologia, a pesquisa é exploratória, pois busca mostrar a aplicabilidade da modelagem de processos de negócios na gestão de segurança da informação. A técnica utilizada foi a de estudo de caso realizado na Coordenadoria de Segurança de Informação – CSI vinculada ao Núcleo de Segurança de Informação e Comunicação - NTIC da Universidade Federal do Pampa – UNIPAMPA. Como instrumento de coleta de dados neste estudo foi utilizado à análise documental baseada nos processos que foram modelados com vista na melhoria do processo de liberação de endereço IP público, complementado por entrevistas e observações diretas realizadas no CSI. Foi utilizada a abordagem AS-IS e TO-BE como forma de operacionalizar a busca por melhoria de processos e a notação BPMN como uma forma de representação destes processos.

3.1 Resultados obtidos

Tendo como foco o processo de liberação de endereço IP público, foi elaborada a modelagem AS-IS do atual processo, apresentado na Figura 2.

Figura 2 – Versão AS-IS do Processo de liberação de endereço IP público.



Fonte: Pesquisa de campo (2015).

A Figura 2 contém as atividades que são executadas no AS-IS. Este processo envolve duas partes, o solicitante, o qual é o interessado na liberação de um IP público para uso em um determinado serviço e a equipe da Coordenação de Infraestrutura Redes e Suporte - CORIS. O

processo inicia quando o solicitante envia e-mail para a CORIS, solicitando um IP Público para uso em um serviço a ser disponibilizado para a internet.

Ao receber a solicitação, a CORIS reserva um endereço IP para ser usado pelo solicitante e envia um formulário contendo um termo de uso para ser preenchido e assinado pelo solicitante. Após receber novamente o termo de uso assinado, a equipe da CORIS analisa se o termo está correto. Se houver algum problema de preenchimento ou na justificativa, o documento é devolvido ao solicitante para as devidas correções. Se o Termo de Uso estiver correto, a equipe da CORIS realiza a liberação do IP no firewall, de acordo com os dados que foram solicitados pelo solicitante. Após liberar o acesso, o solicitante é informado para que possa realizar os testes de validação. Se os testes não tiverem sucesso, a equipe da CORIS é informada para que possa fazer as devidas correções. O processo é encerrado quando os testes tiverem sucesso.

A modelagem AS-IS do processo de liberação de endereço IP público permitiu verificar a forma como o mesmo estava ocorrendo e auxiliou na análise de melhorias, que foram previstas na versão TO-BE. No Quadro 1 estão relacionadas as possibilidades de melhorias identificadas durante a modelagem AS-IS do processo e a sua implantação na versão TO-BE.

Quadro 1 – Melhorias no processo de liberação de endereço IP público

Possibilidades de melhorias no processo de liberação de endereço IP público	
AS-IS	**TO-BE**
Foi identificada a necessidade da definição de um instrumento contendo requisitos de segurança para a liberação de endereço IP público.	Foi criado um checklist contendo requisitos de segurança que precisam ser atendidos para realizar a liberação de endereço IP público. A aplicação do checklist com requisitos de segurança foi proposta para que a liberação de um serviço na internet atendesse a requisitos mínimos de segurança. A utilização do checklist foi modelada na versão TO-BE do processo de liberação de endereço IP público e está sendo seguida pelo CSI.
Identificado à necessidade de realizar auditoria ou algum tipo de checagem local do servidor que receberia o endereço IP público.	Foi definido um formulário de auditoria. A implementação do formulário de auditoria tem o propósito de assegurar que durante a auditoria, o analista responsável tenha identificado a conformidade dos requisitos de segurança. A utilização do formulário de auditoria foi modelada na versão TO-BE do processo de liberação de endereço IP público e está sendo seguida pelo CSI.

Fonte: Pesquisa de campo (2015).

O checklist de segurança contém recomendações que futuramente serão usados na auditoria e análise, por exemplo: aplicação deFirewall local; uso do SSH: na porta TCP definida como padrão pela equipe e acesso liberado apenas para usuários especificados no formulário de solicitação

3.2 Versão TO-BE do processo de liberação de endereço IP público

A modelagem e implementação da versão TO-BE do processo levou em consideração fatores técnicos e fatores organizacionais, entre eles estão, a configuração de um novo organograma na estrutura do NTIC, o aumento da demanda para uso de endereços IP Público e a possibilidade de um cenário de aumento da incidência de Incidentes de Segurança. O estudo que conduziu a elaboração da versão TO-BE do processo iniciou-se com a análise do AS-IS e das novas demandas. Como resultado dessa análise foi elaborado, no Quadro 2, um fluxo textual do processo de liberação de endereço IP público. Neste momento não foram previstos fluxos alternativos para o processo.

Quadro 2 – Fluxo textual da versão TO-BE do Processo de liberação de endereço IP público

Passo	Setor	Procedimento
1	Solicitante	Enviar e-mail solicitando reserva de IP Público
2	CSI	Enviar IP e procedimentos ao solicitante
3	Solicitante	Enviar e-mail com Termo de Responsabilidade (TR)
4	CSI	Analisar Preenchimento do TR
5	CSI	Analisar Justificativa
6	CSI	Enviar link do Checklist de Segurança
7	Solicitante	Responder Checklist
8	Solicitante	Implementar adequações do CheckList de Segurança
9	Solicitante	Confirmar adequações do CheckList de Segurança
10	Solicitante	Liberar acesso via SSH à equipe do CSI
11	Solicitante	Liberar acesso para a análise de vulnerabilidades
12	CSI	Fazer auditoria de acordo com o Checklist de Segurança
13	CSI	Proceder a Análise de Vulnerabilidades
14	CSI	Enviar relatório da Auditoria
15	CSI	Liberar portas e IP no Firewall
16	CSI	Solicitar testes ao solicitante
17	Solicitante	Comunicar resultados dos testes
18	CSI	Registrar Dados

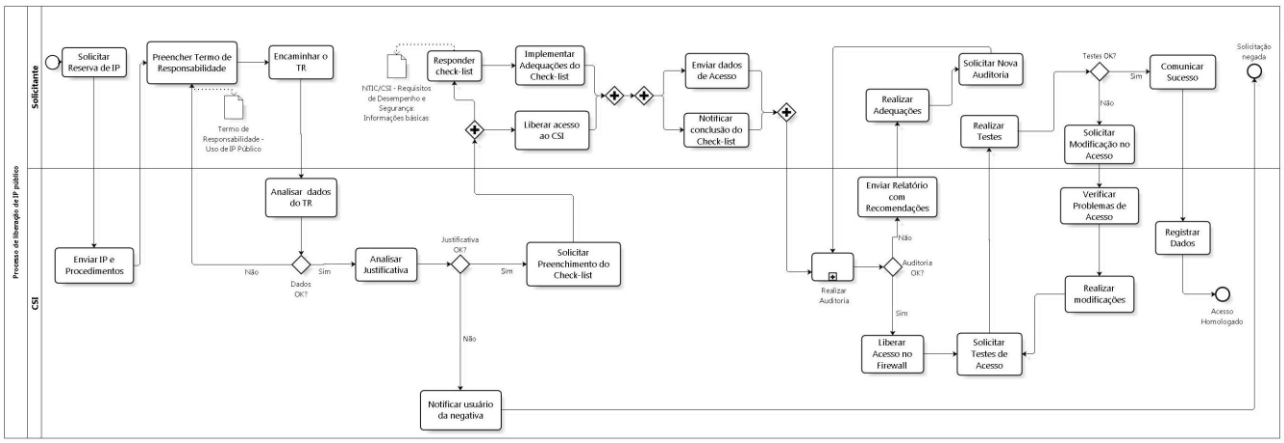
Fonte: Pesquisa de campo (2015).

O fluxo textual do processo serviu de subsídio para a etapa de modelagem do TO-BE do processo de liberação de endereço IP público. A versão TO-BE está representada na Figura 3 prevê as otimizações implantadas, por exemplo, na prevenção de incidentes de segurança da informação.

Na versão TO-BE do processo, como otimização foi previsto atividades referentes a um checklist de segurança da informação. Este checklist é um formulário, onde o solicitante insere as informações relativas ao serviço que será disponibilizado através do endereço IP solicitado, além de

informações de hardware e software do equipamento onde o serviço está hospedado. Este documento também contém orientações e requisitos de segurança, os quais deverão ser atendidos para a liberação final do IP.

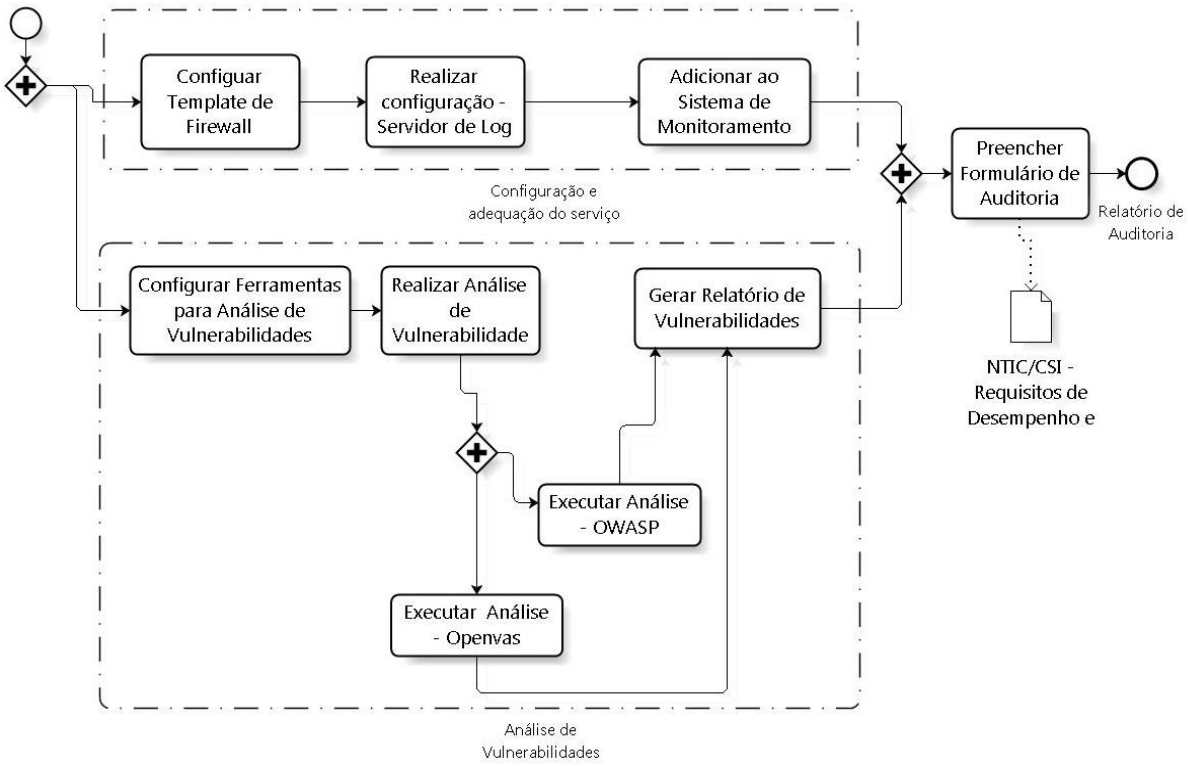
Figura 3 - Versão TO-BE do Processo de liberação de endereço IP público.



Fonte: Pesquisa de campo (2015).

No mesmo processo foi definida uma atividade a ser realizada concomitante com a resposta ao checklist, trata-se da atividade Implementar adequações do checklist. Nela o responsável pelo serviço pode adequar os requisitos de segurança de acordo com as recomendações contidas no checklist. Esses requisitos serão checados durante a auditoria. Assim que a CSI, receber os dados de acesso ao local onde o serviço está hospedado e a houver a conclusão do Checklist por parte do solicitante, será iniciada a auditoria. Na versão TO-BE do processo a tarefa de auditoria foi modelada como um subprocesso denominado de Realizar auditoria, conforme Figura 4.

Figura 4 - Subprocesso Realizar Auditoria



Fonte: Pesquisa de campo (2015).

O subprocesso realizar auditoria contém dois objetos de representação BPMN de grupos de atividades. O primeiro grupo está relacionado às atividades de configuração e adequação do serviço aos requisitos de segurança e o segundo, com atividades de análise de vulnerabilidades. Na fase final do processo caso os requisitos de segurança não tenham sido atendidos, o solicitante receberá um relatório com as recomendações que devem ser implementadas pelo responsável pelo serviço. Após realizar as adequações, o equipamento passará novamente pelo processo de auditoria.

Quando o processo de auditoria resultar de acordo com os requisitos de segurança, o processo segue para a liberação de acesso no firewall. Para que o serviço fique disponível através da internet e de acordo com a solicitação inicial. Nessa fase, são realizados testes de validação do acesso, até que o acesso esteja totalmente operacional. Por fim o processo é encerrado com o registro dos os dados contidos no Termo de responsabilidade – Uso de IP público em planilha de controle mantido pela CSI.

3.3 Discussões

No estudo de caso realizado verificou-se que a perspectiva de processos de negócios auxiliou na gestão da segurança da informação. Foram revisadas as atividades relacionadas ao processo de liberação de IP público e sendo que novas atividades precisaram ser adicionadas, tal como as que envolvem autoria e checagem. Houve a mudança dos setores envolvidos, pois

atribuições que antes eram de responsabilidade do CORIS passaram para o CSI. A modelagem formalizou o processo estudado, sendo que a partir disso as mudanças forma implementadas e o novo processo passou a ser seguido. Por consequência disso, considera-se que a perspectiva de processos permite melhorar, formalizar e comunicar os processos relacionados a gestão da segurança da informação.

Elaborar o AS-IS do processo de liberação de endereço IP público permitiu analisar como mesmo estava sendo executado e identificar possibilidades de melhorias na gestão de segurança da informação. O checklist de segurança da informação e as atividades de análise de vulnerabilidades são melhorias que foram identificadas no AS-IS e previstas na versão TO-BE do processo estudado.

O fato da versão TO-BE do processo de liberação de endereço IP público já ter sido incorporada nos processos de trabalho do CSI apontam para a importância da perspectiva de processos na operacionalização da gestão de segurança da informação. Além disso, de acordo com o CSI, as melhorias com o mapeamento desses processos e suas aplicações visam atender aos requisitos das seguintes normas: Instrução Normativa GSI nº 01, de 13 de Junho de 2008 (BRASIL, 2008); da Instrução Normativa GSI nº 02 de 5 de fevereiro de 2013 (BRASIL, 2013a) ; da Instrução Normativa GSI nº 03 de 6 de março de 2013 (BRASIL, 2013b); do Gabinete de Segurança Institucional da Presidência da República e suas normas complementares, assim como a implantação da Estrutura de Segurança da Informação e Comunicação (ESIC) na Universidade.

Em decorrrência do estudo realizado neste trabalho, já foram mapeados e modelados outros processos junto ao CSI, entre eles citam-se os processos de solicitação de acesso VPN, de solicitação de backup e de tratamento de incidentes de segurança da informação. Também se identificou potencial para melhorias em processos que ainda precisam ser modelados tal como o de manutenção em dispositivos de firewall e o de monitoramento de ativos. O estudo também aponta para as necessidades de:

- Definir um plano de segurança da informação e comunicação para a UNIPAMPA;

- Auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da instituição e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências;

- Planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com a análise de riscos e impactos relacionados a possíveis falhas de segurança;

- Registrar e tratar incidentes de segurança de informação e comunicação;

- Capacitar regularmente os membros da Estrutura da ESIC, com as especialidades das disciplinas relacionadas à segurança de informação e comunicação de acordo com suas funções.

Como trabalhos o CSI prevê melhorias tendo o objetivo de automatizar o manuseio de informação do Checklist em um sistema com armazenamento em banco de dados e a automatização de algumas atividades do processo de liberação de endereço IP público.

4. Considerações finais

Como consideração final afirmar-se que perspectiva de processos de negócios auxilia na gestão da segurança da informação. Gestores e equipes de segurança da informação podem utilizar esta perspectiva para, com o AS-IS do processo, revisar as atividades que são desenvolvidas e os recursos que estão sendo utilizados. Já com o estudo do TO-BE do processo, considera-se que o mesmo permite não apenas identificar as melhorias no processo atual, mas também planejar o gerenciamento da segurança da informação, assim como formalizar e comunicar este planejamento por meio da modelagem de processos.

A notação BPMN se mostrou adequada para a modelagem de processos relacionados à gestão da segurança da informação. Com diferentes níveis de complexidade a notação permite que processos sejam planejados por especialistas responsáveis por implantar a gestão de segurança da informação e comunicados para usuários dos serviços que requerem a segurança da informação.

O fato de ter realizado apenas um estudo de caso focando em um processo específico pode ser visto como uma limitação do trabalho. Como recomendação de trabalho futuro novos estudos de casos podem ser realizados em diferentes organizações que já pratiquem de gestão de segurança da informação implantado ou que pretendam implantar um sistema de gestão desta natureza.

Organizações que pretendam revisar os seus processos de gestão da segurança da informação podem verificar no o estudo realizado neste trabalho que utilizando a abordagem AS-IS e TO-BE é possível analisar os processos que estão sendo executados e identificar possíveis melhorias para mesmos. Já as organizações que precisam implantar um sistema de gestão da segurança da informação, podem ter na perspectiva de processos utilizando a notação BPMN uma visão de que atividades e papéis precisam ser desempenhados, bem como os demais recursos que estarão envolvidos nesta iniciativa.

Trabalhos futuros podem realizar estudos compartivos da aplicação de determinados processos em organizações que atuam na mesma área, a partir disso, pode-se propor um processo otimizado que contemple questões em comum de segurança da informação e de forma complementar definir indicadores de qualidade e de desempenho de processos relacionados com a gestão da segurança da informação para esta área.

5. Referências

AHMAD, A.; MAYNARD, S. B.; SHANKS, G. **A case analysis of information systems and security incident responses.** International Journal of Information Management, v. 35, n. 6, p. 717-723, 2015.

APQC. **American Productivity and Quality Control**. Disponível em: http://www.apqc.org/pcf. Acesso em: jun. 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001:** Tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2013a.

_____. **NBR ISO/IEC 27002:** Tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013b.

BALDAM, R. de L. et al. Gerenciamento de processos de negócios: **BPM–Business Process Management**. São Paulo: Érica, 2007.

BASKERVILLE, R.; SPAGNOLETTI, P.; KIM, J. **Incident-centered information security:** Managing a strategic balance between prevention and response. Information & Management, v. 51, n. 1, p. 138-151, 2014.

BERTUCCI, Janete Lara de Oliveira. **Metodologia básica para elaboração de trabalhos de conclusão de cursos (TCC):** ênfase na elaboração de TCC de pós-graduação Lato Sensu. São Paulo: Atlas, 2011.

BIZAGI – **BizAgi Modeler**. Disponível em: <http://www.bizagi.com/en/bpm-suite/bpm-products/modeler>. Acesso em Junho de 2014.

BRASIL. Tribunal de Contas da União - **Boas práticas em segurança da informação** - TCU - Brasília - DF 2008. Disponível em http: //portal2.tcu.gov.br/portal/pls/portal/docs/205916 0.PDF. Acesso em Mar. 2014.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Instrução Normativa GSI/PR nº 1**. Brasília, 13 de Jun. de 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em: 18 mar. 2015.

___. Gabinete de Segurança Institucional da Presidência da República. **Instrução Normativa GSI/PR nº 2**. Brasília, 05 de Fev. de 2013a. Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr2.pdf>. Acesso em: 18 mar. 2015.

___. Gabinete de Segurança Institucional da Presidência da República. **Instrução Normativa GSI/PR nº 3**. Brasília, 06 de Mar. de 2013b. Disponível em: <http://dsic.planalto.gov.br/documentos/instrucao_normativa_nr3.pdf>. Acesso em: 18 mar. 2015.

CARDOSO, J. H. de M.; OLIVEIRA, A. A. de; ALENCAR, F. **O Processo de Engenharia de Requisitos sob a Ótica da Gestão de Processos de Negócio**. In: WER - Workshop em Engenharia de Requisitos. 2012.

DHILLON, G.; SYED, R.; PEDRON, C. **Interpreting information security culture:** An organizational transformation case study. Computers & Security, v. 56, p. 63-69, 2016.

DIAS JR, J. J. L.; OLIVEIRA, J.; MEIRA, S. R de L. **Pontos Chaves para Adoção de Uma Arquitetura Orientada a Serviços:** Uma Análise Comparativa de Modelos de Maturidade SOA da Indústria. VIII Simpósio Brasileiro de Sistemas de Informação, SBSI. São Paulo, 2012.

EMINAĞAOĞLU, M.; UÇAR, E.; EREN, Ş. **The positive outcomes of information security awareness training in companies** – A case study. information security technical report, v. 14, n. 4, p. 223-229, 2009.

FONTES, E. Segurança da Informação: o usuário faz a diferença - São Paulo: Saraiva, 2006.

HIRAMA, K. **Social Requirements Elicitation for Socio-Technical Systems Development**. Latin America Transactions, IEEE (Revista IEEE America Latina), v. 11, n. 2, p. 870-877, 2013.

HOPE, P.; WALTHER, B. **Web segura guia de teste e soluções**: Técnicas sistemáticas para detectar problemas com rapidez - Alta Books - Rio de Janeiro, RJ - c2009

ISLAM, S.; AHMED, M. D. **Business process improvement of credit card department**: case study of a multinational bank. Business Process Management Journal, v. 18, n. 2, p. 284-303, 2012.

JACOSKI, C. A.; GRZEBIELUCHAS, T. **Modelagem da contratação de projetos utilizando os conceitos de BPM**-gerenciamento de processos de negócio. Produto & Produção, v. 12, n. 3, p. 29-37, 2011.

KENNETH, C. LAUDON; LAUDON, JANE P. **Sistemas de informação gerenciais**. Editora Person. São Paulo, 2011.

KWON, S. et al. **Common defects in information security management system of Korean companies.** Journal of Systems and Software, v. 80, n. 10, p. 1631-1638, 2007.

LEYER, M.; HOLLMANN, M. Introduction of electronic documents: **How business process simulation can help. Business Process Management Journal**, v. 20, n. 6, 2014.

LYRA, M. R. **Segurança e auditoria em sistemas de informação** - Ciência Moderna - Rio de Janeiro, RJ - 2008.

MILAN, G. S.; SOSO, F. A. **BPM–business process management como prática de gestão em uma empresa metalúrgica com estratégia de produção eto–engineer-to-order**. Revista Gestão Industrial, v. 8, n. 2, 2012.

MUCKENBERGER, E. et al . **Gestão de processos aplicada à realização de convênios internacionais bilaterais em uma instituição de ensino superior pública brasileira.** Prodution, São Paulo , v. 23, n. 3, Sept. 2013

NAKAMURA, E. T.; GEUS, P. L. **Segurança de redes em ambientes cooperativos** - Novatec - São paulo - SP - 2007

NAZARETH, D. L.; CHOI, J. **A system dynamics model for information security management.** Information & Management, v. 52, n. 1, p. 123-134, 2015.

OMG/BPMN. **Object Management Group** - Business Process Model and Notation. Disponível em: <http://www.bpmn.org/>. Acesso em: 18 mar. 2015.

OZKAN, S.; KARABACAK, B.. **Collaborative risk method for information security management practices:** A case context within Turkey. International Journal of Information Management, v. 30, n. 6, p. 567-572, 2010.

PEREIRA, M. F. et al. **Modelo de produção de material didático: o uso da notação bpmn em curso a distância DOI**: 10.5773/rai. v8i4. 898. RAI: Revista de Administração e Inovação, v. 8, n. 4, p. 45-66, 2011.

PHILLIPS, Brandis. **Information Technology Management Practice:** Impacts upon Effectiveness. Journal of Organizational and End User Computing (JOEUC), v. 25, n. 4, p. 50-74, 2013.

POTRICH, A. C. G.; VIEIRA, K. M.; NUNES, R. C. **Gestão da segurança da informação:** caracterização da incubadora tecnológica de Santa Maria. GEINTEC - Gestão, Inovação e Tecnologias, v. 3, n. 2, p. 167-185, 2013.

SANTOS, J. G. **Proposta de Melhoria do Processo de Contratação de Serviços de TI e da Gestão dos Contratos na Administração Pública Federal**. Revista Eixo, v. 2, n. 1, p. 17-38, 2013.

SENA, M. A. C. et al. **Soluções Digitais**: Oportunidades para a Melhoria dos Serviços Públicos Judicários. Anais do VIII Simpósio de Excelência em Gestão e Tecnologia. Rio de Janeiro: Resende, 2011.

SILVA, M. A.; ZAIDAN, F. H. **Gestão de Processos de Negócios Alinhada à Gestão de Mudanças com Ênfase na Melhoria Contínua se Processos**: processo folha de pagamento. Revista de Sistemas e Computação. v.3, n.1, pp.54-65. Salvador, 2013.

SINGH, A. N. et al. **Information security management (ism) practices:** Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management, v. 14, n. 4, p. 225-239, 2013.

SIPONEN, M.; MAHMOOD, M. A.; PAHNILA, S. **Employees' adherence to information security policies:** An exploratory field study. Information & Management, v. 51, n. 2, p. 217-224, 2014.

SIPONEN, Mikko; MAHMOOD, M. Adam; PAHNILA, Seppo. **Employees' adherence to information security policies:** An exploratory field study. Information & Management, v. 51, n. 2, p. 217-224, 2014.

SOOMRO, Z. A.; SHAH, M. H,; AHMED, J.. **Information security management needs more holistic approach:** A literature review. International Journal of Information Management, v. 36, n. 2, p. 215-225, 2016.

TURBAN, E.; VOLONINO, L. **Tecnologia da informação para gestão**: em busca do melhor desempenho estratégico e operacional. Porto Alegre: Bookman, 2013.

UNIVERSIDADE FEDERAL DO PAMPA – Conselho Universitário. **RESOLUÇÃO Nº 83** - Institui a Estrutura de Segurança da Informação e Comunicações (ESIC). Bagé, 30 de Out. 2014. Disponível em: <http://porteiras.r.unipampa.edu.br/portais/consuni/files/2010/06/Res.-83_2014-Instituir-a-Estrutura-de-Seguran%C3%A7a-da-Informa%C3%A7%C3%A3o-e-Comunica%C3%A7%C3%B5es-ESIC.pdf>. Acesso em: 18 mar. 2015.

___. Núcleo de tecnologia da Informação e Comunicação. **Plano Diretor de Tecnologia da Informação e Comunicação**. Bagé, Fev. de 2011. Disponível em: < http://ntic.unipampa.edu.br/files/2011/09/UNIPAMPA-NTIC-PDTIC-DOCUMENTO-PRINCIPAL-2011.pdf >. Acesso em: 18 mar. 2015.

YILDIRIM, E. Y. et al. **Factors influencing information security management in small-and medium-sized enterprises:** A case study from Turkey. International Journal of Information Management, v. 31, n. 4, p. 360-365, 2011.

Recebido: 10/04/2015

Aprovado: 16/01/2016