colloquium exactarum

PROPOSTA DE PROCESSO SEGURO EM GESTÃO DE PESSOAL.

A PROPOSAL FOR SECURE PROCESS IN PERSONNEL MANAGEMENT.

Walter Lorençon[1]; Adilson Eduardo Guelfi[1], Claudio Luiz Sitolino[1], Eduardo Henrique Rizo[1].

[1]Faculdade de Informática – FIPP, Universidade do Oeste Paulista – UNOESTE.
e-mail: walterlorencon@gmail.com

RESUMO – Em segurança da informação, uma das áreas importantes é a gestão de pessoal que hoje é responsável por atuar no recrutamento, na seleção de candidatos, no treinamento e na capacitação dos funcionários, incluindo o desligamento. Esta atuação precisa também controlar os riscos organizacionais, sendo necessária a padronização de procedimentos e aplicação de métricas relacionadas ao Sistema de Gestão de Segurança da Informação. Este artigo propõe a definição de um processo seguro, baseado na norma NBR ISO/IEC 27002:2013, atuando em 3 momentos dentro do ciclo da gestão de pessoal, ou seja, antes, durante e no encerramento do vínculo profissional. As principais contribuições deste trabalho visam: a) identificar, corrigir e sugerir soluções para desconformidades encontradas quanto à segurança informação; b) assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades; c) reduzir os riscos de incidentes que podem prejudicar os ativos da organização.

Palavras-chave: segurança da informação; processo seguro; gestão de pessoal.

ABSTRACT – Currently, in information security, personnel management is an important area that is responsible for recruiting, selecting candidates, training and dismissal of employees. These actions also help to control organizational risks, and both the procedure standardization and the application of metrics related to the Information Security Management System are necessary. Thus, the aim of this paper is to propose the definition of a secure process, based on NBR ISO/IEC 27002: 2013 standard, which operates in 3 different moments within the personnel management cycle, i.e., before, during and at the end of the professional relationship. The main contributions of this work are: a) to identify, correct and suggest solutions for non-conformities found regarding security information; b) ensure that employees, suppliers and third parties understand their responsibilities; and c) reduce the risks of incidents that may affect the assets of the organization.

Keywords: information security; secure process; personnel management.

Recebido em: 19/01/2017
Revisado em: 04/09/2017
Aprovado em: 19/10/2017

1. INTRODUÇÃO

Atualmente, a informação é um recurso ou ativo de vital importância nas organizações. A Segurança da Informação (SI) tem por finalidade principal assegurar a continuidade dos negócios, fazendo com que os ativos de informação estejam protegidos de ameaças e tenham os seus riscos controlados (PHOENIX, 2008).

Uma boa Politica de Segurança da Informação (PSI) define regras claras, praticáveis e alinhadas com a cultura organizacional, condições de orçamento e ambiente tecnológico da empresa. Em suma, a PSI visa à aplicação simples e objetiva de controles por meio de processos, formalizando atividades e condutas que os funcionários devem ter em relação aos ativos de informação da empresa.

É importante destacar que a PSI possui algumas características entre elas: a) reforçar a SI; b) ter foco em pessoas e tecnologias; e c) auxiliar na validade jurídica para controles aplicáveis dentro as organização (DIAS, 2000, p.25).

Diante das ameaças e vulnerabilidades que os ativos de informação estão sujeitos, um Sistema de Gestão de Segurança da Informação (SGSI) torna-se fundamental em ambientes corporativos, uma vez que executa a PSI, permite aplicar controles de segurança e atua na prevenção perante todos os usuários (NBR ISO/IEC-27002:2013).

O conceito de Gestão de Pessoas (GP) depende para seu funcionamento de fatores como cultura e estrutura organizacional adotada, os tipos de negócios, os processos internos etc. (Chiavenato, 2006). Desta forma, tratar GP e SGSI requer uma abordagem para a elaboração de um processo seguro que pode estar baseado na seção "A.7- Segurança em Recursos Humanos" da Norma NBR ISO/IEC 27002:2013.

A importância de se ter um processo seguro em GP reside no fato de se poderem aplicar controles de segurança contra falhas ou atos ilícitos provenientes da atuação profissional de funcionários dentro da empresa, como por exemplo, roubos, indisponibilidade de ativos, serviços ou sistemas, engenheira social, dentre muitas outras.

Neste contexto, o objetivo deste trabalho é definir um processo seguro, baseado na norma NBR ISO/IEC 27002:2013, que atua no ciclo completo de gestão de pessoal (antes, durante e no encerramento do vínculo com a organização).

Este trabalho esta organizado da seguinte forma: a seção 2 faz uma breve interpretação das Normas NBR ISO/IEC 27001:2012 e 27002:2013 com relação à

Seção A.7-Segurança em Recursos Humanos; a seção 3 exibe os principais trabalhos relacionados; a seção 4 aborda a proposta do trabalho; por último, a seção 5 trata das contribuições e conclusões do trabalho, indicando propostas de trabalhos futuros.

2. REFERENCIAL TEÓRICO

2.1. NORMAS NBR ISO/IEC 27001 E 27002:

A Norma ISO/IEC 27001 especifica os requisitos para estabelecer, manter e melhorar continuamente um SGSI dentro da organização. Esta norma também inclui requisitos para avaliação e tratamento de riscos de segurança da informação voltados para as necessidades organizacionais.

Diante disso, a Norma ISO/IEC 27002:2013 serve de referência para organizações que necessitam gerenciar e controlar riscos de segurança da informação principalmente em ambientes de TI.

2.2. SEGURANÇA EM RECURSOS HUMANOS:

A seção A.7 da norma NBR ISO/IEC 27002:2013 descreve regras que visam assegurar que empregados, estagiários, aprendizes e prestadores de serviços, estejam cientes da estrutura normativa e procedimental do SGSI, sendo desta forma um meio para mitigar riscos, ameaças e vulnerabilidades. Considerando a GP, é de extrema importância os termos e as condições de contratação (como por exemplo, os acordos de confidencialidade), os controles, os processos disciplinares, o encerramento ou mesmo a mudança interna baseando-se na PSI.

Na fase anterior a formalização da contratação, a seção A.7 estabelece que seja necessário assegurar que partes externas entendam suas responsabilidades e seus papéis para os quais podem ser selecionados. Desta forma, na seleção, a verificação de um histórico do candidato pode ser relevante, como também expor os termos, as condições e as obrigações de contratação com que as partes externas declararão reponsabilidade perante a organização.

Na contratação deve-se assegurar que os candidatos formalizem as próprias responsabilidades quanto a SI para auxiliar na mitigação e controle das ameaças e das vulnerabilidades em ativos de informação. Compete ainda à organização detectar as necessidades de conscientização e treinamento que podem ocorrer antes do contratado assumir efetivamente seu cargo, periodicamente conforme definido pelas regras da PSI, ou então sempre que ocorrerem incidentes ou atualizações regulares das normas e procedimentos organizacionais.

O processo disciplinar deve existir formalmente, com meios adequados de divulgação e conhecimento para que ações

possam ser efetivamente tomadas perante funcionários que tenham cometido uma violação da PSI, evitando a percepção de impunidade quando procedimentos e normas internas venham a ser desrespeitadas.

O encerramento do vínculo visa proteger a organização quando houver mudança interna ou então quando o contrato de trabalho e/ou serviço for encerrado. No primeiro caso, pode ocorrer que as responsabilidades e as obrigações anteriores pela SI permaneçam válidas após a mudança interna. No segundo caso, procedimentos específicos devem assegurar que a informação organizacional esteja segura nos casos de dispensa, evitando comportamentos inadequados que podem surgir por descontentamento do funcionário.

3. TRABALHOS RELACIONADOS

Em Freitas (2011), o objetivo foi desenvolver e elaborar o Método MESI (Método Estruturado de Segurança da Informação), que em conjunto com a utilização de mapeamentos de processos, contempla a especificação de um SGSI com métricas adotadas, auditoria de sistemas e avaliação de controles. Em Freitas (2011), a validação do MESI proporcionou uma redução substancial do nível de riscos em aproximadamente 40 %. Freitas (2011) ainda comenta sobre limitações no entendimento por parte dos responsáveis com relação ao teor, abrangência ou até mesmo procedimentos de PSI a serem adotados.

Para Dias (2000), uma PSI é fundamental para garantir o funcionamento adequado de toda estrutura tecnológica da empresa, considerando atributos básicos de segurança da informação, como por exemplo, confidencialidade, integridade e a disponibilidade. Ainda, Dias (2000) mostra as principais técnicas para adoção de um plano tático bem organizado da PSI. Porém, em Dias (2000) critérios para adoção de controles SI em gestão de pessoas são comentados de forma genérica.

Nos trabalhos Freitas (2011) e Dias (2000), foram abordados tópicos referentes à elaboração de uma PSI completa e implantação de um SGSI.

A partir deste contexto, este trabalho se posiciona especificamente quanto ao Processo Seguro em Gestão de Pessoal, com aplicação de controles da Seção A.7 da Norma ISO IEC27002:2013, tendo como contribuição principal, dentro de um SGSI, considerar controles de SI que atuem no ciclo completo de GP, ou seja, antes, durante e no encerramento do vinculo funcional com a organização.

4. PROPOSTA

Conforme definido na seção 1, o objetivo deste trabalho é definir um processo seguro, baseado na norma NBR ISO/IEC

27002:2013, que atua no ciclo completo de gestão pessoal.

Ao permitir a padronização de controles internos seguros nas fases de seleção, contratação, vigência de vínculo e desligamento de colaboradores, a proposta serve para proteger os ativos de informação. Hoje existem leis e regulamentações que tornam as organizações responsáveis por manter seus adequados controles de riscos em SI (CALDER; WATKINS, 2008, p.10].

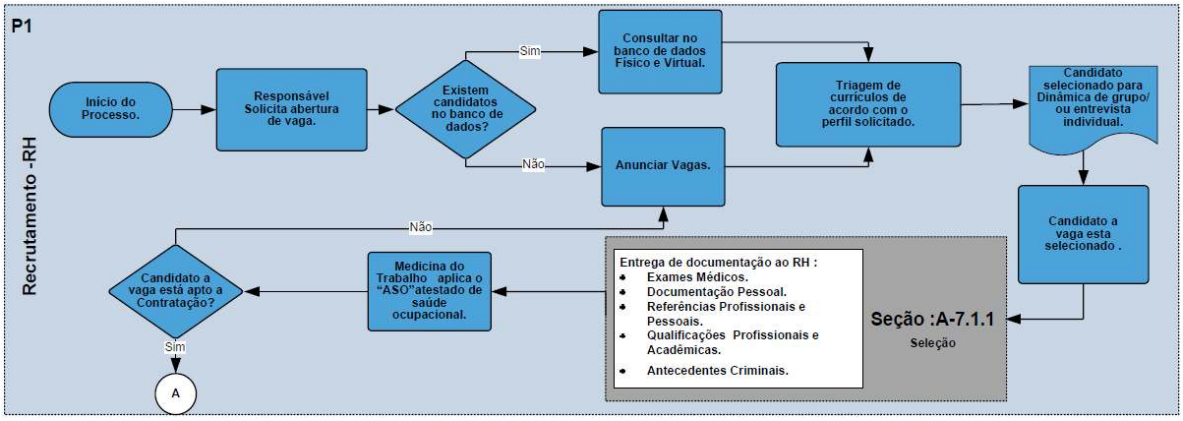
O Processo Seguro em Gestão de Pessoal (PSGP) proposto deve ser responsável por identificar, corrigir e controlar as desconformidades encontradas em setores que lidam com a GP, como também minimizar as situações que causam riscos e assim diminuir impactos e incidentes de SI (FREITAS, 2011).

Na proposta, o PSGP é composto por 4 subprocessos, a saber: a) Recrutamento-RH (P1); b) Admissão-DP (P2); c) Política de Sistemas–SGSI (P3); e d) Desligamento (P4). Estes 4 subprocessos podem então ser aplicados nos 3 momentos principais dentro do ciclo de GP da seguinte forma, ou seja, antes (P1 e P2), durante (P3) e no encerramento da contratação (P4).

O PSGP deve permitir sua aplicabilidade em setores envolvidos com atividades de GP, com autonomia para aplicar suas devidas penalidades e sanções quanto ao descumprimento das regras do SGSI.

O subprocesso P1 “Recrutamento-RH” esta definido na Figura 1 e tem como objetivo localizar e facilitar a escolha de profissionais (externos e internos) com potencial para cumprir as exigências da função e os valores da empresa.

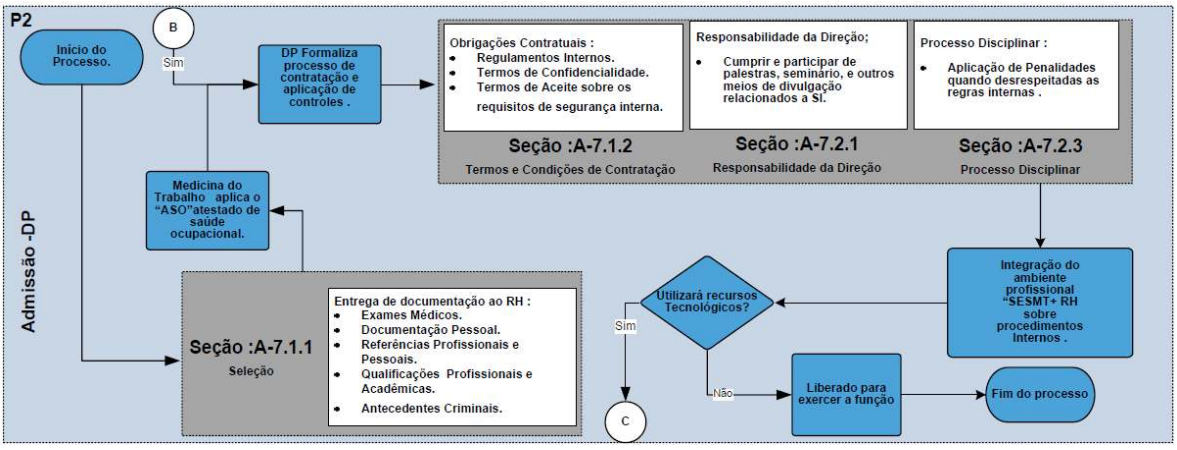
Figura 1. Subprocesso P1 - Recrutamento–RH



O subprocesso P1 deve iniciar por um conjunto de atividades normalmente relacionadas á atuação técnica do setor de GP, como por exemplo, a abertura de vaga, a coleta (interna e/ou externa) de potenciais candidatos, a triagem dos candidatos mais compatíveis com o perfil de vaga, a realização de entrevistas e dinâmicas, e por fim, a escolha do candidato mais apto para assumir o posto. Após esta escolha, aplica-se então, dentro do ciclo de GP, o primeiro controle de segurança recomendado pela NBR ISO/IEC 27002:2013 definido na seção A-7. 1.1 (seleção). Este controle define que devem ser requeridas do candidato selecionado a apresentação e comprovação de todas as documentações relativas á contratação, tais como, os exames médicos, as documentações pessoais, as referências profissionais e pessoais, os comprovantes das qualificações profissionais e acadêmicas e até os antecedentes criminais (quando for o caso).

É importante observar neste ponto que, as documentações mencionadas relativas à contratação podem variar dependendo do nível de exigência de cada vaga. Portanto, convém ao departamento de GP definir na atividade de abertura de vaga, o conjunto mínimo de documentos de contratação que devem ser apresentados e comprovados pelo candidato após ter sido selecionado. Por fim, o subprocesso P1 termina com a emissão do atestado de saúde ocupacional por um departamento organizacional responsável pela medicina do trabalho, e o candidato apto deve então ser encaminhado para a contratação seguindo para o subprocesso P2 "(Admissão-DP)" conforme mostra a figura 2.

Figura 2. Subprocesso P2 - Processo de Admissão-DP.



Quanto ao subprocesso P2 “Admissão-DP” existem duas entradas possíveis:

1. Entrega direta de todas as documentações relativas à contratação conforme descrito na NBR ISO/IEC 27002:2013, seção A-7. 1.1. Esta entrada pressupõe tratar os casos de contratação direta de funcionários por autonomia dos setores organizacionais, sem a necessidade de passar por fases de recrutamento e seleção; ou
2. A entrada é uma continuação dos resultados gerados pelo subprocesso P1.

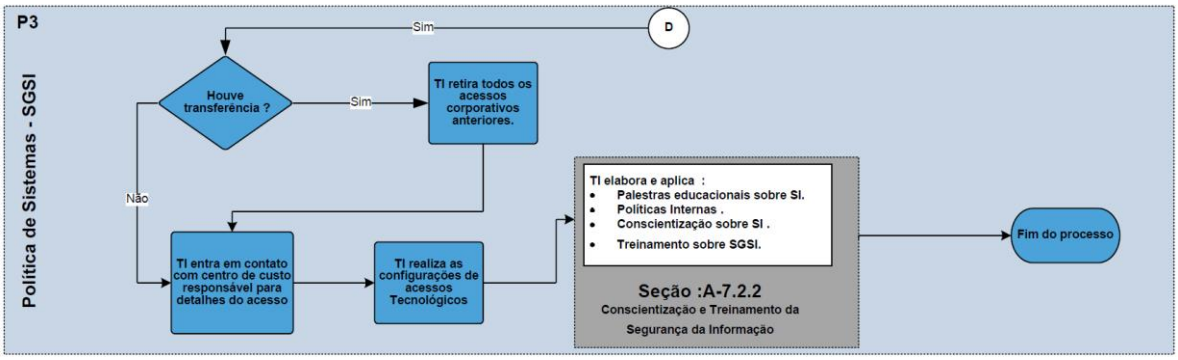
Diante disso, uma vez que a contratação tenha sido então formalizada, deve-se aplicar os controles das seções A-7.1.2, A-7.2.1 e A-7.2.3 definidos pela norma NBR ISO/IEC 27002:2013.

Na seção A-7.1.2 (Termos e Condições de Contratação) o funcionário deve tomar conhecimento e aceitar suas obrigações contratuais expressas nas formas de regulamento interno, termos de confidencialidade e termos específicos de aceite sobre os requisitos de segurança interna. Na seção A-7.2.1, o funcionário deve estar ciente e também concordar sobre o cumprimento e participação à treinamentos, palestras e literaturas especificas sobre políticas relacionadas à SI.

Na seção A-7.2.3 (Processo Disciplinar) todos os funcionários devem estar cientes de que existe um processo disciplinar ativo dentro da organização, responsável por averiguar descumprimentos e aplicar penalidades caso as regras internas de segurança determinadas pelo SGSI forem desrespeitadas, ou algum tipo violação na segurança for cometida, quanto a mau uso de ativos ou recursos tecnológicos. Este controle pode permitir lidar com incidentes de SI de forma mais apropriada, sendo possível coletar evidencias após qualquer tipo de ocorrência indesejada.

Com todas as diretrizes de segurança aplicadas no subprocesso P2, caso o funcionário necessite utilizar recursos tecnológicos em suas atividades diárias, então inicia-se o subprocesso P3 (Politicas de Sistemas-SGSI) conforme mostra a figura 3. Caso seja desnecessário o uso de recursos tecnológicos pelo funcionário no desempenho de suas atividades diárias, então será liberado normalmente para exercer sua função trabalhista sem os controles do subprocesso P3 e do subprocesso P4.

Figura 3. Subprocesso P3 - Politica de Sistemas-SGSI.

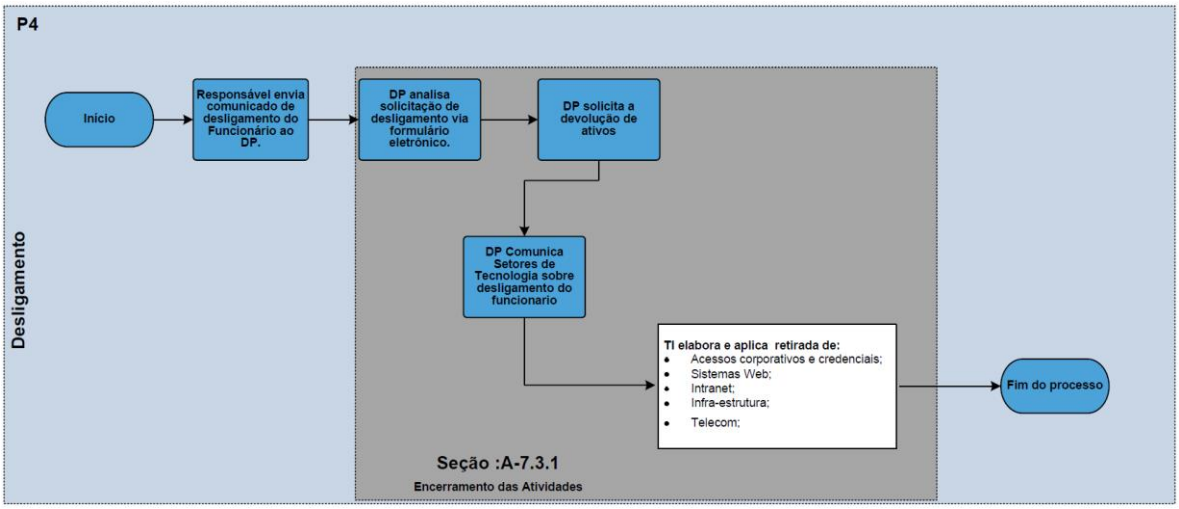


O subprocesso P3 “Politica de Sistemas-SGSI” tem por objetivo assegurar que, quer seja por transferência interna ou novo funcionário, as políticas de acesso aos sistemas de informação, no que diz respeito às restrições e às liberações de uso, sejam devidamente definidas para os serviços tecnológicos necessários ao desenvolvimento das funções do cargo, tais como e-mail, internet, intranet, formulários online, biometria, telecomunicações, banco de dados e outros. No caso de uma transferência interna, como mostra a figura 3, é mandatório ao departamento de TI antes retirar as permissões anteriores para depois conceder as novas permissões de acesso.

Para que haja uma melhor aplicação de segurança, o departamento de TI deve verificar o nível de acesso a ser aplicado com a autorização do responsável pelo departamento solicitante. Por fim, conforme controle definido em norma NBR ISO/IEC 27002:2013 seção A-7.2.2 (Conscientização e Treinamento da Segurança da Informação), a organização deve ter um programa interno de treinamento, palestras, campanhas educacionais e conscientização de seus funcionários sobre as melhores praticas em SI, auxiliando o empregado desde a entrada na nova função a evitar e mitigar problemas como fraudes, engenharia social, invasões, mal uso de ativos tecnológicos, dentre outros. Adicionalmente, campanhas ou programas internos de treinamento e conscientização sobre as melhores práticas em SI devem ocorrer periodicamente para proporcionar, em médio prazo, melhores níveis de entendimento sobre as responsabilidades de segurança dentro da organização. A conscientização é importante para que o funcionário tenha foco sobre como proceder de forma segura, mas também entender as razões que o levam a agir preservando a informação organizacional. Após o subprocesso p3, o funcionário estará apto inicialmente a desempenhar suas funções profissionais. O subprocesso P4 (ver figura 4) será adicionado ou executado somente nos casos

de desligamento, quer seja por iniciativa própria da organização ou do empregado.

Figura 4.Subprocesso P4 - Desligamento.



O subprocesso P4 “Desligamento” tem como objetivo proteger os interesses da organização aplicando controles no processo de mudança ou encerramento da contratação. As duas primeiras atividades se iniciam por meio de comunicado formal e análise pelo departamento de GP sobre a solicitação de desligamento do funcionário.

Na sequência, aplica-se os controles definidos na seção A-7.3.1 (Encerramento das Atividades) da norma NBR ISO/IEC 27002:2013, requisitando primeiro que todos os recursos tecnológicos em posse do funcionário que contenham ativos de informação sejam prontamente devolvidos, e depois emitir comunicado ao departamento de TI sobre o desligamento do funcionário. O departamento de TI, ao estar ciente do desligamento, deve então proceder com a retirada ou cancelamento imediato das permissões de acesso aos serviços e sistemas de informação organizacionais.

O subprocesso P4 então se encerra com o desligamento do funcionário sendo legalmente formalizado junto ao departamento de GP da organização.

5. CONSIDERAÇOES FINAIS

A metodologia utilizada neste trabalho considerou uma abordagem qualitativa, e foi desenvolvida por meio de estudo de caso dentro do SGSI organizacional. O objetivo do trabalho foi definir um processo seguro, baseado na norma NBR ISO/IEC 27002:2013, para tratar o ciclo completo de gestão de pessoal (antes, durante e no encerramento do vínculo coma organização). Portanto, os

resultados qualitativos deste trabalho podem ser aplicados diretamente em setores organizacionais como Recursos Humanos e/ou Gestão de Pessoas.

O PSGP foi proposto com 4 subprocessos: Recrutamento-RH (P1), Admissão-DP (P2), Política de Sistemas-SGSI (P3) e Desligamento (P4). O PSGP, guardando as devidas especificidades de cada organização, pode servir como referência básica para adequação aos principais controles de segurança definidos na norma NBR ISO/IEC 27002:2013 quanto à GP.

Analisando um dos possíveis resultados qualitativos do PGSP, é possível verificar sua adequação quanto às necessidades organizacionais de controlar a seleção de novos colaboradores, a manutenção do vínculo empregatício e também o desligamento quando se envolve a proteção de ativos de informação.

Como trabalhos futuros, sugere-se que o PSGP proposto possa ser replicado em outras organizações (ou outros estudos de caso semelhantes), possibilitando assim a verificação de sua maior efetividade, bem como o seu aprimoramento. De forma complementar, novos estudos de casos, juntamente com a definição de métricas de SI, poderiam trazer um volume de dados suficiente que venha a auxiliar na validação quantitativa do PSGP, para que se torne cada vez mais confiável e consistente.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Requisitos de Sistema de gestão de segurança da informação. ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2013.

CALDER, A.; WATKINS, S. Gestão de pessoas. O novo papel de recursos humanos nas organizações 3. ed. Rio de Janeiro, 2008.

CHIAVENATO, I. International IT governance: an executive guide to ISO/1799. EUA: Kogan Page, 2006. 366 p.

DIAS, C. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Axcel Books, 2000.

FREITAS, F. Método de Implementação de um SGSI. 2011. Dissertação (Mestrado) – IPT, São Paulo-SP, 2011.

PHOENIX, B. Boas praticas de segurança. 2008. Dissertação (Mestrado) – Universidade do Porto, Porto-PT, 2008.