REVISTA MIRANTE, Anápolis (GO), v. 11, n. 6 (edição especial), abr. 2018. ISSN 19814089

IMPLANTAÇÃO DE UM SGSI EM ORGANIZAÇÃO REALIZADORA DE PROCESSOS SELETIVOS E CONCURSOS

IMPLEMENTATION OF AN SGSI IN THE ORGANIZATION OF SELECTIVE PROCESSES AND COMPETITIONS

CRISTIANE DE FÁTIMA RIBEIRO ROCHA
Especialista em Gestão e Segurança em Redes de Computadores, Universidade Estadual de Goiás (UEG), Campus de Trindade
ribeirorocha.cristiane@gmail.com

ANTÔNIO CRUVINEL BORGES NETO
Mestre em Engenharia Agrícola e docente da Universidade Estadual de Goiás (UEG) - Campus de Ciências Exatas e Tecnológicas Henrique Santillo (Anápolis - GO) e diretor educacional da Universidade Estadual de Goiás (UEG), Campus de Trindade
antonio@cruvinel.com.br

Resumo: Este artigo propõe um modelo de implantação de um Sistema de Gestão de Segurança da Informação (SGSI) direcionado a organizações realizadoras de processos seletivos e/ou concursos. O modelo é composto por pontos de controle de segurança da informação comuns a este tipo de organização e processos que tratam estes pontos de controle previamente levantados. Um fluxo de implantação dos processos que compõe o SGSI é proposto, englobando a análise do ambiente organizacional, a adaptação dos pontos de controle e dos processos do SGSI, estabelecendo-se ainda uma priorização de implantação e tratativa destes processos com base nos riscos inerentes aos seus pontos de controle de segurança da informação. O modelo de SGSI proposto permite que organizações que atuem no mercado de elaboração e aplicação de avaliações de processos seletivos e/ou concursos implantem processos de segurança da informação que agreguem valor ao serviço que desempenham no mercado.
Palavras-chave: Segurança da informação. Políticas de segurança da informação. Sistema de Gestão de Segurança da Informação.

Abstract: This paper proposes a model for the implementation of an Information Security Management System (SGSI) directed to organizations conducting selective processes and/or competitive exams. The model is composed by information security control points common to this type of organization and processes that deal with these control points previously raised. A flow of implementation of the processes that make up the SGSI is proposed, involving the analysis of the organizational environment, the adaptation of the control points and SGSI processes, and prioritization of the implementation and treatment of these processes based on the risks inherent to their security information control points. The proposed SGSI model allows organizations that operate in the market for the preparation and application of evaluations of selective processes and competitive exams to implement information security processes that add value to the service they perform in the market.
Keywords: Information security. Information Security Policies. Information Security Management System.

INTRODUÇÃO

A informação é o ativo mais valioso de diversas organizações dos mais diversos segmentos de mercado. Entretanto, muitas dessas organizações se esquivam em valorizar e proteger suas informações, colocando em segundo plano a definição de regras e ações que devem ser aplicadas para garantir a segurança destas informações e, consequentemente, garantir a segurança dos processos de negócio. Os riscos relacionados aos ativos de informação devem ser devidamente identificados e analisados a fim de especificar medidas de segurança que mitiguem o impacto destes riscos no negócio.

Organizações realizadoras de processos seletivos e concursos têm como prioridade vital de negócio a segurança das informações que nelas trafegam. Esta prioridade é proveniente da existência de alguns princípios legais que estabelecem que uma seleção pública deva ocorrer de forma igualitária, excluindo-se as possibilidades de que alguns candidatos tenham acesso a informações em espaço temporal anterior aos demais. Faz-se assim crucial a proteção das informações referentes ao processo para que só no momento certo estas se tornem de conhecimento público e que esse processo ocorra de uma forma isonômica, sem privilegiar nenhum dos envolvidos.

O autor Rocha (2013), apresenta um modelo de políticas de segurança da informação direcionado a organizações realizadoras de processos seletivos e concursos. Embora o modelo seja interessante com objetivos sólidos, importante na mitigação dos riscos inerentes à segurança da informação dentro de uma organização, apenas o documento de políticas de segurança não é suficientemente detalhista para a inclusão na organização de procedimentos que zelem pela segurança das informações importantes para o negócio.

O documento de políticas de segurança deve fazer parte de algo maior dentro da organização, o Sistema de Gestão de Segurança da Informação (SGSI), o qual deve conter processos que tratem dos principais pontos de controle de segurança da informação, definindo diretrizes para a adoção de atividades e tarefas que deverão fazer parte da rotina organizacional, mitigando-se assim os riscos inerentes ao negócio.

Baseando-se no modelo organizacional e no modelo de documento de políticas de segurança previamente definidos em Rocha (2013), neste trabalho delineia-se um modelo de implantação de um SGSI direcionado para organizações realizadoras de

processos seletivos e concursos, contendo os processos básicos necessários para mitigação dos riscos considerados não aceitáveis no modelo organizacional utilizado.

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Um sistema de gestão de segurança da informação deve ser abordado em nível estratégico dentro de uma organização, sendo defendido pela alta administração responsável pela área de informação, fazendo parte do hall de prioridades para manutenção do negócio. Segundo a NBR ISO/IEC 27001, um SGSI é um conjunto de processos de gestão de riscos e objetiva preservar a confidencialidade, integridade e disponibilidade das informações da organização, fornecendo assim confiança para as partes interessadas, de que os riscos estão sendo gerenciados. A norma NBR ISO/IEC 27001 trás ainda um fluxo para um SGSI baseado no modelo PDCA (*Plan-Do-Check-Act* [Planejar-executar-checar-agir]) o qual, ao longo de seus estágios, baseia-se no planejamento das ações necessárias para o estabelecimento da segurança das informações, implantação das ações planejadas, avaliação e análise crítica dos resultados obtidos através desta implantação e o contínuo aperfeiçoamento e monitoramento destas ações de segurança, buscando sempre o estado de melhoria contínua dos processos de gestão de segurança.

Martins e Santos (2005) apresentam uma metodologia de implantação de um SGSI baseada nos principais padrões e normas de segurança, objetivando a uniformização e documentação dos procedimentos, empregando ferramentas e técnicas para o provimento da segurança das informações na organização. O foco da metodologia apresentada é ser uma referência para implantação e acompanhamento de Sistemas de Gestão de Segurança da Informação.

De acordo com a NBR ISO/IEC 27001 (2013), as primeiras ações que devem ser tomadas na implantação de um SGSI são: a declaração de comprometimento da alta administração com os procedimentos de segurança da informação e a definição de políticas de segurança aplicáveis ao ambiente organizacional. A administração da organização deve liderar o processo de implantação do SGSI, e deixar claro, a todas as demais equipes o seu comprometimento diante da elaboração, implantação e melhoria contínua dos processos de segurança da informação.

Em seguida o documento de políticas de segurança torna-se primordial na implantação de um SGSI, pois é a partir dele que se determinam os pontos de controle que devem ser atingidos nos processos a serem elaborados e implantados.

CENÁRIO DO MODELO ORGANIZACIONAL UTILIZADO COMO BASE PARA A DEFINIÇÃO DO MODELO DE SGSI

A missão da maioria das organizações, públicas e privadas, que realizam processos seletivos e/ou concursos é direcionada principalmente na seleção de recursos humanos para preencher vagas e cargos, nos mais variados segmentos do mercado e do ambiente acadêmico, de forma a recrutar pessoas habilitadas a tal função de forma eficiente e eficaz. Para que essa missão seja consolidada é necessário que as atividades envolvidas nesse tipo de prestação de serviço sejam atenciosamente acompanhadas e protegidas contra qualquer tipo de risco que possa surgir e comprometer o andamento do processo de seleção. Existem muitas pessoas envolvidas nestes processos de seleção, em sua maioria candidatos que, na condição de clientes indiretos destas organizações, empenham grande esforço monetário e psicológico no conhecimento destas atividades. A compensação por parte da organização busca-se a conclusão de um processo transparente, seguro e organizado, respeitando aspectos importantes relacionados à equidade de oportunidades, e a não diferenciação de pessoas quanto à raça, cor e sexo.

Para a constituição do modelo de SGSI proposto neste trabalho foi considerada uma organização fictícia neste segmento, onde alguns conceitos são adotados de forma geral a fim de explanar a condição considerada. A estrutura fictícia é a mesma utilizada para definição do modelo de políticas de segurança aproveitado como referência na definição dos processos modelo deste SGSI.

Abaixo seguem alguns conceitos relacionados à estrutura modelo e utilizados nos modelo de SGSI delineado:

- **Informações confidenciais e/ou sigilosas**: correspondem aos dados que não podem ser divulgados para elementos externos à organização do processo. São exemplos: a composição das bancas elaboradoras e corretoras das avaliações, a formulação das avaliações antes destas serem aplicadas, e demais informações de acesso restrito.
- **Informações públicas**: corresponde aos dados já disponíveis ao público externo em relação à organização. Nestes incluem os editais, provas e gabaritos

posterior a aplicação da avaliação, e demais elementos já disponíveis para acesso público.

- **Ambientes seguros:** Refere-se aos ambientes de elaboração das questões que comporão as avaliações, a área de impressão destas avaliações, a área onde são realizados os processamentos de dados, localização dos servidores e local onde as mídias de armazenamento de informações ou os impressos são armazenados.
- **Edital**: Todo concurso ou processos seletivo é regido por um edital, que se refere ao documento de acesso público no qual são definidas as regras de um determinado concurso ou processo seletivo.
- **Local de prova**: São os locais físicos nos quais as avaliações são aplicadas.

No modelo organizacional utilizado na definição deste modelo de SGSI é composto por seis departamentos divididos pelas atividades específicas que exercem, sendo todos eles subordinados à direção geral da organização. Todos estes departamentos possuem uma coordenação geral que é responsável pelas tarefas das equipes pertencentes àquele departamento. Cada coordenação relaciona-se diretamente com a direção, responsável pelo acompanhamento geral das atividades desenvolvidas pela organização.

Para melhor entendimento uma breve descrição dos departamentos é realizada a seguir:

- **Departamento de Tecnologia da Informação**: É o departamento responsável pela análise de risco dos ativos de TI da organização e pela análise dos pontos de controle na implantação da política de segurança. Também cuida da manutenção da estrutura de computadores e de rede da organização, conservação de sites e sistemas, processamento de dados e gestão da segurança da informação.
- **Departamento Técnico-pedagógico**: São pessoas divididas em equipes que são responsáveis pela: elaboração, correção, revisão das avaliações, elaboração dos editais dos processos e concursos e da conferência, dos resultados processados antes destes serem publicados, junto ao departamento de TI, ou seja, se os resultados estão de acordo com as regras do edital do processo.
- **Departamento de Recursos Humanos** A gestão de recursos humanos é realizada pelo departamento de recursos humanos, responsável pela seleção e treinamento de colaboradores para todos os demais departamentos. Neste trabalho em questão a gestão de recursos humanos é um fator de grande importância na manutenção da segurança das informações nelas trafegadas.

- **Departamento de Logística**: Este departamento atua nas atividades de definição dos locais de realização das provas, levantamento das funções e o número de colaboradores necessários para a aplicação das provas, definição e preparação dos materiais a serem utilizados, durante a aplicação das provas.
- **Secretaria**: É responsável pelos trâmites administrativos inerentes a toda a organização, pelo atendimento ao público e pelo controle do patrimônio da organização.
- **Financeiro**: É responsável pelos processos referentes às finanças da organização, como controle de folha de pagamento, aquisição de materiais e serviços e gestão de recursos financeiros.

De acordo com a estrutura organizacional fictícia ora descrita, os principais pontos de controle de segurança da informação foram definidos, direcionando maiores esforços no estabelecimento de procedimentos de segurança referentes a estes pontos previamente destacados. O apêndice A apresenta os pontos de controle elencados, assim como uma breve descrição de cada um deles.

MODELO DE SGSI PARA ORGANIZAÇÕES REALIZADORAS DE PROCESSOS SELETIVOS E/OU CONCURSOS

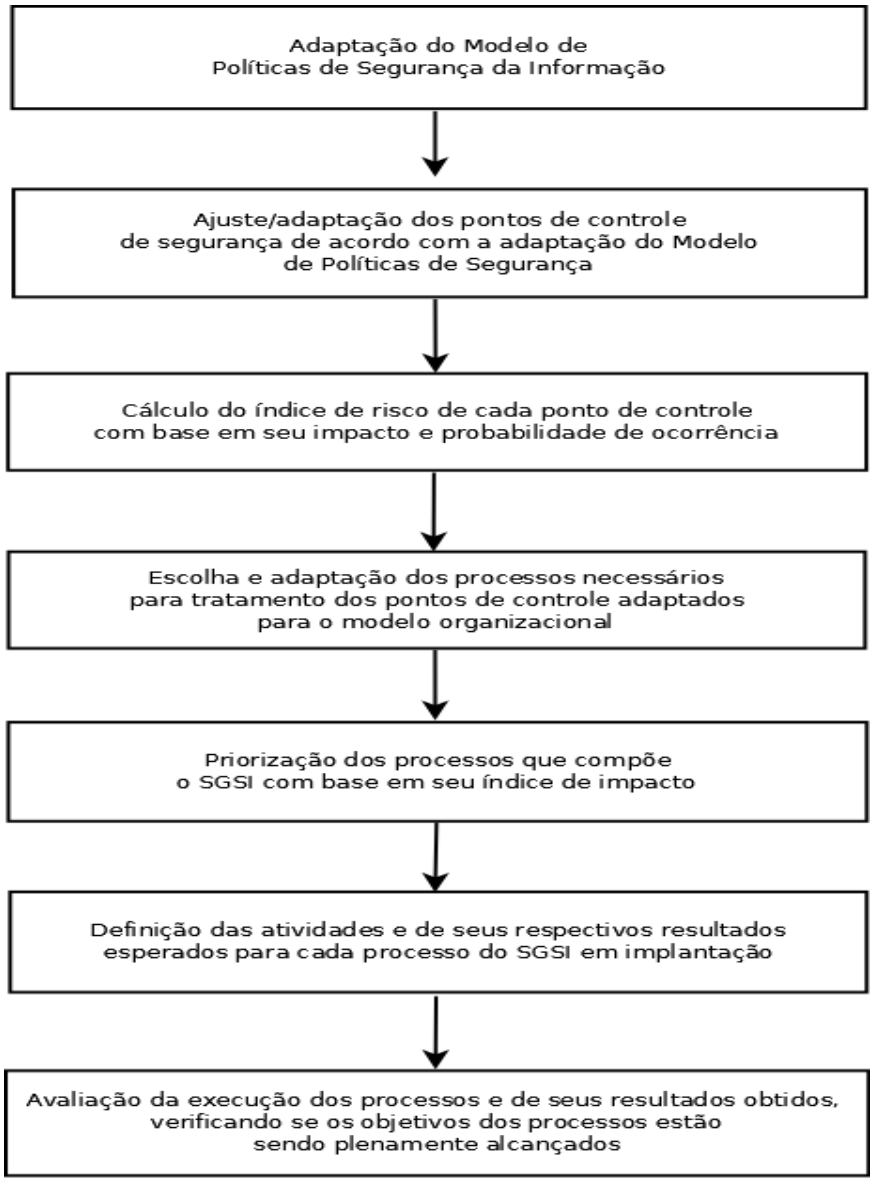
O modelo de SGSI desenvolvido neste trabalho é baseado nos requisitos apresentados na norma NBR ISO/IEC 27002, adaptados para o modelo organizacional apresentado na seção 3, partindo dos pontos de controle definidos no modelo de políticas de segurança apresentado por Rocha (2013). As etapas que compõe esse modelo são baseadas no fluxo de etapas contidas na metodologia de implantação de SGSI (MARTINS; SANTOS, 2005).

A metodologia de implantação de SGSI que foi adotada por Martins e Santos (2005) segue o fluxo definido pelo modelo PDCA utilizado na norma NBR ISSO/IEC 27002, o qual contém fases de planejamento, implementação, checagem e aperfeiçoamento dos processos, todas executadas em um ciclo de melhoria contínua. Segundo esta metodologia, a primeira etapa de implantação de um SGSI é a definição das políticas de segurança da informação. Esta etapa encontra-se detalhada por Rocha (2013) através do modelo de políticas de segurança da informação direcionado a organizações realizadoras de processos seletivos e/ou concursos, assim como suas respectivas instruções de implementação e adequação à realidade de cada organização. A adequação do modelo de políticas de segurança e sua efetiva implantação na

organização englobam a adaptação dos principais pontos de controle que devem ser levados em consideração na implementação de processos de segurança da informação neste modelo organizacional.

Na figura 1 encontra-se um fluxograma relacionando os pontos de controle apresentados no modelo de políticas de segurança, utilizado como base para definição do modelo de SGSI aqui trabalhado, às principais vulnerabilidades relacionadas à falta de tratativa destes pontos. Uma análise de impacto e probabilidade de ocorrência dessas vulnerabilidades deve ser realizada a fim de identificar o seu nível de risco.

Figura 1 - Fluxograma de modelo de SGSI



Fonte: Autores, 2017.

ANÁLISE DE RESULTADOS

Cada vulnerabilidade elencada deve receber uma classificação de impacto e de probabilidade. As escalas de classificação de impacto e de probabilidade variam entre 1, 2 e 3, sendo que impactos e probabilidades com índice 1 são menores que as vulnerabilidades com índice 2 e 3. Com base nessa valoração e de acordo com a matriz de risco presente no Apêndice A, estabelece-se o nível de risco de cada vulnerabilidade identificada, o qual pode ser alto, médio ou baixo. O nível de risco das vulnerabilidades de cada ponto de controle servirá de base para a priorização de implantação e acompanhamento dos processos do SGSI em implantação. Pontos de controle que tenham mais vulnerabilidades de alto risco devem ser priorizados diante de pontos de controle com maiores vulnerabilidades de risco médio e baixo, sendo que os processos que tratam os pontos de controle mais prioritários também devem ser priorizados no SGSI.

Depois de realizada a devida adequação dos pontos de controle e a priorização com base nos riscos de cada um, os processos que compõem o modelo de SGSI em questão devem ser adaptados e suas atividades definidas. No apêndice B são apresentados os processos genéricos que compõem este modelo de SGSI, baseados nos pontos de controle identificados para este modelo organizacional. Os processos que compõe o modelo contêm uma estrutura de documentação que inclui sua identificação, versão e data, nome do processo, sua descrição, seus responsáveis, quais os itens do documento de políticas de segurança atendidos por este processo e quais os pontos de controle a ele relacionados.

Os processos foram definidos obedecendo-se esta estrutura para manter sua rastreabilidade e fácil identificação de relacionamento com os demais documentos de segurança da informação da organização. Cada processo definido contempla uma descrição concisa do que deve ser abordado em suas atividades. Baseando-se nesta descrição, as organizações que vão implantar o modelo de SGSI aqui proposto devem definir as atividades e tarefas que vão garantir que os requisitos dos processos sejam devidamente atendidos, mitigando-se os principais riscos da organização.

Embora este modelo seja direcionado a um segmento de negócio específico, cada organização possui uma realidade diferente e pode ter estratégias, recursos e ativos que diferem de alguns controles e processos aqui definidos. Cabem a cada uma destas

organizações realizarem o seu próprio estudo de caso, estudando seus ativos, adequando os pontos de controle e, consequentemente, os processos contidos neste modelo.

É importante sempre lembrar que um SGSI só terá seu objetivo alcançado quando estiver completamente alinhado com a estratégia e o modelo de negócio da instituição em que for implantado. Sendo assim, o modelo proposto neste estudo serve como instrução e guia para a identificação de vulnerabilidades e seus pontos de controle e mapeamento de processos que suavizem os riscos de tecnologia da informação da organização, aumentando a segurança das atividades do negócio de organizações que possuem nenhuma ou pouca definição de processos de segurança.

CONCLUSÃO

A confidencialidade, integridade e disponibilidade das informações concernentes aos processos de seleção em organizações realizadoras de concursos e/ou processos seletivos é primordial para a manutenção do negócio, sendo indispensável para uma prestação de serviço confiável e de qualidade. Alguns dos grandes obstáculos na implantação da segurança das informações de uma organização é o comprometimento da direção e dos demais colaboradores com processos que mantenham os riscos relacionados às informações sob níveis aceitáveis, além da falta de processos estruturados e bem difundidos dentre os seus interessados que estabeleçam ações que contribuam para a segurança da informação.

Um SGSI implementa processos que direcionam esforços e padronizam atividades que auxiliem na mitigação dos principais riscos de segurança das informações de uma organização. Foi apresentado neste trabalho um modelo de SGSI com o objetivo de facilitar a implantação de processos de segurança nas organizações realizadoras de processos seletivos e/ou concursos, baseado em um modelo organizacional fictício e que utiliza um modelo de políticas de segurança da informação previamente apresentado em Rocha (2013), levando em consideração as características genéricas das atividades desenvolvidas por este segmento de negócio em organizações públicas ou privadas.

O modelo de SGSI apresentado neste trabalho provê diretrizes para estudo de cenário de segurança da informação organizacional e padronização de processos de segurança da informação em organizações realizadoras de processos seletivos e/ou concursos. Através dos pontos de controle definidos e dos processos abordados pelo

modelo proposto, as organizações deste segmento de mercado podem implantar processos padronizados e avaliá-los quanto à sua conformidade, tomando como ponto de partida a estrutura organizacional já utilizada na definição deste modelo.

Seguindo o fluxo de implantação proposto, na partir de um modelo previamente delineado as organizações podem estudar melhor seu cenário organizacional, adaptando as políticas de segurança, os pontos de controle previamente levantados e, consequentemente, os processos apresentados pelo modelo de SGSI implantado de acordo com sua realidade de operação.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: **Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos.** Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: **Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação - Requisitos**. Rio de Janeiro, 2013.

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel. **Uma Metodologia para Implantação de Um Sistema de Gestão de Segurança da Informação**. Revista de Gestão da Tecnologia e Sistemas de Informação. Journal of Information Systems and Technology Management. Vol. 2, No. 2, 2005, pp. 121-136. ISSN online: 1807-1775. Disponível em: <www.egov.ufsc.br/portal/conteudo/uma-metodologia-para-implantação-de-um-sistema-de-gestão-de-segurança-da-informação>. Acesso em 03/09/2016.

ROCHA, Cristiane de Fátima Ribeiro. **Um modelo de políticas de segurança direcionado a organizações realizadoras de processos seletivos e concursos.** 2013. 66 f. Monografia (Graduação em Sistemas de Informação) – Universidade Federal de Goiás, Goiânia, 2013.