Da Elaboração a Implantação da Política de Segurança da Informação: uma proposta baseada no ciclo PDCA

Peter Prevedello[1], Diogo Otto Kunde[1]

[1]Eixo Informação e Comunicação - Instituto Federal de Educação, Ciência e Tecnologia Farroupilha

Postal 98130-000 – Júlio de Castilhos – RS - Brasil

peterprevedello@gmail.com, diogokunde@hotmail.com

Abstract. *Information security is an area of knowledge dedicated to information asset protection against unauthorized access, unauthorized changes or unavailability. From a broader way we can also consider it as risk management practice involving the commitment of the three main concepts of security: confidentiality, integrity and availability of information. In this work we present a proposal to develop and implement an Information Security Policy based on the PDCA cycle, which enables continuous process improvement and problem solving.*

Resumo. *Segurança da Informação é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. De uma forma mais ampla, podemos também considerá-la como prática de gestão de riscos que impliquem o comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. Neste trabalho apresentaremos uma proposta de elaboração e implantação de uma Política de Segurança da Informação baseada no ciclo PDCA, que possibilita a melhoria contínua de processos e solução de problemas.*

Introdução

Com o rápido aumento de dispositivos conectados a rede, a informação se tornou o ativo mais crítico dentro das instituições e a criação e implantação de uma Política de Segurança da Informação (PSI) se tornou de extrema importância para garantir sua confidencialidade, integridade e disponibilidade. A segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados [ISO/IEC 27001 2013]. Neste contexto, é inadmissível uma instituição de ensino não possuir no seu planejamento um processo de implantação de política de segurança da informação. Desta forma este trabalho tem como objetivo apresentar uma proposta de processo de elaboração e implantação de política de segurança da informação (PSI) com base no ciclo PDCA no Instituto Federal Farroupilha, campus Júlio de Castilhos-RS (IF-Farroupilha-JC).

A Norma Brasileira (NBR) ISO/IEC 27001:2013 adota o ciclo PDCA – Plan-Do-Check-Act (Planejar, Fazer, Checar e Agir) para estruturar todos os processos envolvidos em uma PSI, sendo que o PDCA é uma ferramenta gerencial que possibilita a melhoria contínua de processos e a solução de problemas [AGUIAR 2006].

O IF-Farroupilha-JC é uma instituição de educação superior, básica e profissional, especializada na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino [FARROUPILHA 2015]. Atualmente o campus possui um pouco mais de vinte setores e por esse motivo a proposta prevê a elaboração e implantação de PSI por setor, com o objetivo de envolver todos os funcionários da instituição. Neste sentido, a proposta do processo de elaboração e implantação da PSI teve como base a NBR ISO 27001:2013, e trás como objetivo especificar requisitos para o estabelecimento, implementação, operação, monitoração, análise crítica, manutenção e melhoria de uma PSI [ISO/IEC 27001:2013].

Elaboração e implantação da PSI

Tendo em vista o PDCA, todo processo deve ter uma ampla fase de planejamento, onde se busca conhecer o ambiente a qual será implantada uma PSI [SÊMOLA 2014]. Sendo assim a presente proposta prevê quatro fases para sua implantação em um setor do IF-Farroupilha-JC. A Figura 1 ilustra a proposta de elaboração e implantação da PSI com base no ciclo PDCA.

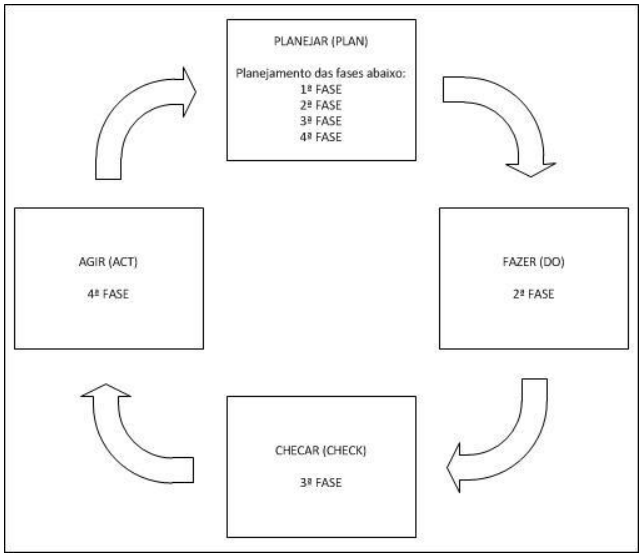

Figura 1 - Proposta de elaboração e implantação da PSI com base no ciclo PDCA.

A primeira fase propõe a criação do comitê gestor de segurança que será responsável pela implantação e execução das fases um e três, sendo necessária a participação efetiva da direção geral do campus, demonstrando liderança e comprometimento, garantindo assim que a PSI seja compatível com o plano de desenvolvimento institucional[1] (PDI) do campus. O comitê gestor de segurança da

[1] http://www.iffarroupilha.edu.br/site/conteudo.php?cat=168&sub=5377

informação deverá ser definido e composto pela direção geral e pelo coordenador de tecnologia da informação, da mesma forma um comitê operacional também deverá ser criado para a implantação e execução das fases dois e quatro. O comitê operacional deverá ser composto pelos funcionários do setor onde a PSI está sendo implantada e também pelos funcionários da coordenação de tecnologia da informação [BEZERRA 2011].

Na segunda fase será realizada a gestão de riscos utilizando como referência a NBR ISO/IEC 27005:2013, onde serão analisados e avaliados estes riscos através da identificação dos ativos e identificação dos processos de negócio [CAMPOS 2007]. Feito isso, será necessário determinar a relação ativo *versus* processo, a fim de identificar a sua necessidade de segurança, de acordo com as propriedades confidencialidade, integridade e disponibilidade utilizando as seguintes perguntas [BEZERRA 2011]:

- Pode ficar indisponível por algum período de tempo? (Disponibilidade);
- Pode ser acessado e divulgado por qualquer pessoa? (Confidencialidade);
- Pode ser modificado por qualquer pessoa? (Integridade).

A partir da analise dos resultados, caso a resposta seja "não" em alguma destas perguntas, o ativo em questão necessita de segurança que garanta aquela propriedade. Para iniciar a identificação dos riscos devem-se avaliar os ativos conforme sua importância, impacto e valor financeiro [ISO/IEC 27005 2013]. Da mesma forma, é necessário identificar e avaliar as ameaças classificando-as em naturais ou humanas, conforme o Anexo C da NBR ISO/IEC 27005:2013. Após identificação das ameaças, identificar e avaliar as suas vulnerabilidades utilizando como referência o Anexo 'D' da NBR ISO/IEC 27005:2013. Por fim, propõe-se a estimativa de riscos através da equação, conforme o Quadro 1 [ISO/IEC 27005 2013].

Quadro 1 - Equação para estimativa do risco.

Risco (A) = SOMA [Ameaça * Vulnerabilidade] (A) * Valor do ativo (A).

O resultado desse cálculo representa o RISCO FINAL DE CADA ATIVO e com base nestes resultados realizar-se-á o tratamento dos riscos, utilizando as seções de controle de segurança da NBR ISO/IEC 27002:2013, projetada para as instituições usarem como uma referência na seleção de controles dentro do processo de implementação de PSI baseada na NBR ISO/IEC 27001:2013.

Conforme Manuel (2014), "Não se pode gerenciar aquilo que não se pode medir; por esse motivo deve-se ter um painel de indicadores com o objetivo de controlar, medir e melhorar [...]", e nesse contexto, será realizada na terceira fase uma auditoria interna por parte do comitê gestor de segurança da informação, verificando o quanto o processo de PSI está implementado e mantido efetivamente. Para tal, este comitê realizará novamente as etapas contidas na segunda fase. O resultado dessa auditoria servirá como indicador de desempenho, a fim de apontar problemas existentes no processo, que na quarta e última fase serão tratados com o intuito de realizar correções e melhorias, utilizando as seções de controle de segurança da NBR ISO/IEC 27002:2013.

Resultados Preliminares e Trabalhos futuros

O processo descrito nesse trabalho foi aplicado parcialmente na Central de Processamento de Dados (CPD) do Setor de Tecnologia da Informação IF-Farroupilha-JC visando alguns resultados preliminares. O processo foi aplicado implantando parte da primeira fase e toda a segunda fase da proposta. Após aplicação do processo no CPD, verificou-se que os ativos que apresentam maior risco são a Internet e o servidor de arquivos, devido à existência de ameaças com alto grau de probabilidade de ocorrerem, entre elas estão à falha do equipamento de telecomunicação e as ameaças representadas por seres humanos como engenharia social[2], acesso não autorizado ao sistema e vazamento de informações, sendo que todas essas ameaças possuem vulnerabilidades que poderão comprometer todos os serviços dependentes da Internet se vierem ocorrer.

Como trabalhos futuros, pretende-se aplicar a proposta completa em todos os setores do IF-Farroupilha-JC com o objetivo de envolver os funcionários da instituição. Acredita-se que as pessoas são o principal agente de transformação neste processo de melhoria continua e o estabelecimento na prática da Política de segurança da Informação.

Referências

AGUIAR, Silvio. Integração das Ferramentas da Qualidade ao PDCA e ao Programa Seis Sigma. Nova Lima: INDG Tecnologia e Serviços Ltda., 2006.

BEZERRA, Edson Kowask. Gestão de riscos de TI: NBR 27005. Rio de Janeiro: RNP/ESR, 2011.

CAMPOS, André. Sistema de Segurança da informação: Controlando os Riscos. 2. ed. - Florianópolis: Visual Books, 2007.

MANUEL, Sergio da Silva. Governança de segurança da informação: como criar oportunidades para o seu negócio. Rio de Janeiro: Brasport, 2014.

NBR ISO/IEC 27001 - Tecnologia da Informação. Sistema de Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2013.

NBR ISO/IEC 27002 - Tecnologia da Informação. Código de prática para gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2013.

NBR ISO/IEC 27005 - Tecnologia da Informação. Gestão de riscos de Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2013.

PEIXOTO, Mário C. P. Engenharia Social e Segurança da Informação na Gestão Corporativa . Rio de Janeiro: Brasport, 2006.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. 2. ed. – Rio de Janeiro: Elsevier, 2014.

[2] Segundo Peixoto (2006), a Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser usado na persuasão de uma determinada pessoa, fazendo a agir conforme seu desejo.