Boletim do Tempo Presente - ISSN 1981-3384
Boletim do Tempo Presente, nº 12, de 2018, p. 87 - 105, | http://www.seer.ufs.br/index.php/tempopresente

DESCRIÇÃO E MODELAGEM PRÁTICA NA CONSTRUÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA SECRETARIA DE EDUCAÇÃO DO ESTADO DE PERNAMBUCO

Josué Fragoso da Silva, DADM, UFRPE- jfragosomail@gmail.com
Catarina Rosa e Silva de Albuquerque, DADM, UFRPE – catarina.albuquerque@ufrpe.br

Resumo-O presente artigo aborda a descrição da modelagem dos elementos essenciais na construção de uma política genérica de segurança da informação (PSI), a qual intenta uma maior proteção às informações consideradas sigilosas e críticas pela organização. A estratégia metodológica adotada foi qualitativa e foi operacionalizada por meio de um estudo de caso instrumental, cuja coleta de dados contou com a orientação de triangulação através de registros e documentos coletados na empresa, entrevistas e observações, onde foi possível identificar riscos às informações, devido a inexistência de diretrizes, normas e procedimentos que compusessem uma política de segurança formalizada, publicada, divulgada e revisada. Percebeu-se a necessidade da elaboração de um modelo participativo na construção de uma política de segurança da informação que envolveu os gestores e corpo executivo, de forma que fosse possível a disseminação da PSI, sensibilizando os colaboradores para uma cultura que minimizasse os riscos e assegurasse uma organização mais protegida na segurança de suas informações.

Palavras-chave: Política de Segurança da Informação; Cultura, Riscos.

DESCRIPTION AND PRACTICAL MODELING IN THE CONSTRUCTION OF AN INFORMATION SECURITY POLICY IN THE SECRETARIAT OF EDUCATION OF THE STATE OF PERNAMBUCO

Abstract - This article deals with the description of modeling the essential elements in the construction of a generic Information security policy (ISP), which tries to provide greater protection to information considered confidential and critical by the organization. The methodological strategy adopted was qualitative and was operationalized through an instrumental case study, whose data collection was guided by triangulation through records and documents collected in the company, interviews and observations, where it was possible to identify information risks due to the absence of guidelines, norms and procedures that make up a formalized, published, disclosed and revised security policy. It was realized the need to create a participatory model in the construction of an information security policy that involved the managers and executive staff, so that it was possible to disseminate the PSI, sensitizing employees to a culture that minimized risks and ensured more secure organization of your information.

Keywords: Politics, Security, Information, Culture, Risks.

1. INTRODUÇÃO

A informação é a estrutura do conhecimento (SALES; ALMEIDA, 2007), sendo fundamental nas organizações para o desenvolvimento de uma plataforma de trabalho que as habilitem a produzir com eficiência, inovar, gerir o capital e as pessoas.

Dentro do volume de informações que circulam e são armazenadas nas organizações em meio físico e digital, existem as que são públicas e podem ficar disponíveis ao acesso de todos, como também as que precisam ser protegidas e asseguradas para manterem seu sigilo, sua integridade ou sua disponibilidade, pois representam ativo valioso para a organização. Mesmo sendo intangível, difícil de identificar e quantificar, as empresas cada vez mais, utilizam as informações mediadas por recursos de tecnologia da informação, sendo assim, dependente destes, como defende Ikenaga (2008).

Em favor disso, Laureano e Moraes (2005) defendem que a informação deve ser diferenciada, protegida e gerenciada privadamente, pois é a essência da inteligência competitiva.

Para a proteção da informação é necessário um conjunto de fatores, composto por processos, ferramentas de *hardware* e *software* e pessoas (mão de obra qualificada e cultura organizacional), que usados isoladamente, podem comprometer o todo. Muitas organizações públicas ou privadas, investem em ferramentas e mão de obra qualificada, porém negligenciam os processos e a formação de uma cultura organizacional voltada para a segurança da informação, os quais são fundamentais na operacionalização e consolidação de todo o conjunto para a proteção da informação.

Neste contexto, considera-se a política de segurança da informação (PSI) como parte dos processos de proteção, para nortear, organizar e direcionar os esforços para a proteção da informação. Observa-se que a norma NBR ISO/IEC 27002:2005 -Tecnologia da Informação – Código de prática para gestão da segurança da informação, tem sido usada como referência para implantação de uma política de segurança da informação nas organizações, direcionando e ressaltando os itens que devem ser considerados na elaboração de uma política de segurança da informação, devido a sua criticidade e a importância e responsabilidade da alta gestão na implantação e conformidade com os objetivos da organização.

Por outro lado, a norma NBR ISO/IEC 27002:2005, por ser apenas uma referência, deve ser complementada, pois não detalha como a PSI deve ser implementada, as peculiaridades de

cada organização, a sequência de implementação, os aspectos relevantes, os impedimentos encontrados, entre outros.

Além disso, questões relevantes da organização como: setor, segmento, tamanho, tempo de vida, cultura, equipe técnica, infraestrutura disponível, etc., devem ser levados em consideração na implementação de uma PSI.

A Secretaria de Educação do Estado de Pernambuco (SEE-PE), instituição foco do estudo deste trabalho tem aproximadamente 120 anos, sendo pública e voltada à educação estadual, tanto no provimento de escolas públicas de ensino fundamental e médio, quanto pela autorização de funcionamento e monitoramento de unidades educacionais privadas do estado de Pernambuco.

Muitas das informações sob sua gestão são vitais e consideradas sigilosas, servindo de base para decisões que podem impactar a sociedade de forma positiva ou negativa. O vazamento, a distorção ou a indisponibilidade dessas informações podem gerar um transtorno incalculável e muitas vezes irreversível para a instituição e o público que atende.

Considerando os riscos envolvidos, a SEE-PE realizou investimentos em ferramentas tecnológicas de *hardware* e *software*, como controle de acesso, antivírus, filtros de conteúdo, *firewall*, sala cofre, entre outros, além de mão de obra qualificada, a qual se deu por meio da contratação de profissionais certificados e especializados em segurança da informação. Com estes investimentos, tornou-se possível realizar registros e controles automatizados por sistemas e tecnologias de informação, bem como o monitoramento das atividades realizadas por usuários autorizados e tentativas não autorizadas de acesso ao ambiente tecnológico.

Contudo, estes investimentos limitaram-se apenas à tecnologia, sendo necessária uma atenção às pessoas e processos, conforme orientações de Barman (2002), o qual considera que a segurança da informação deve ser mais abrangente e entendida no ambiente corporativo à luz da tríade pessoas, processos e tecnologias.

Essa falta de investimentos em processos e pessoas acarreta insegurança, pois levanta questionamentos como: Quais diretrizes seguir? Quais padrões e políticas de segurança deveriam ser estabelecidos para o uso das ferramentas disponíveis? Quais processos deveriam ser seguidos para cada tipo de incidente de segurança? Como os usuários poderiam proceder para minimizar os riscos e proteger as informações? Como estabelecer um processo de segurança da informação para manter as informações seguras? Como fazer para que as pessoas

apliquem e operacionalizem a segurança da informação, mantendo as informações críticas restritas?

Visando responder a esses questionamentos, em dezembro de 2015, a Secretaria de Educação de Pernambuco, publicou em seu Plano Diretor de Tecnologia da Informação (PDTI) para o triênio 2016-2018 (SEE-PE, 2015), dentre outras, a Necessidades do Negócio trinta e seis (NN 36), que versava sobre possibilitar a implantação de uma Política de Segurança da Informação. Dessa forma, mobilizou-se uma equipe de especialistas para o desenvolvimento deste projeto.

Neste contexto, em 2016, foi iniciada a construção, que culminou em uma política de segurança da informação (SEE-PE, Política de Segurança da Informação, 2017) composta por uma política principal, como diretriz e doze políticas complementares, como normas.

Em 2017, duas dessas políticas complementares (Acesso Remoto e Backup Corporativo) foram implementadas e neste mesmo ano foi realizada a divulgação para todos os gestores da organização, sendo estes, multiplicadores para os demais agentes públicos.

A divulgação abrangeu a sede da instituição, cinco anexos e dezesseis gerências regionais e suas respectivas escolas, totalizando mil e duzentas e formando, aproximadamente, mil e quinhentos agentes públicos.

Para o ano de 2018, ficaram as demais políticas complementares que serão implementadas, como também a revisão da documentação.

Diante disso, vislumbrou-se a possibilidade de investigar quais os elementos devem ser considerados na modelagem de uma política de segurança da informação genérica, considerando os critérios explicitados na norma NBR ISO/IEC 27002:2005, bem como aqueles encontrados nas constatações de especialistas. Para isso, utilizou-se, como referência, o processo de desenvolvimento e implementação da PSI executado na Secretaria de Educação de Estado de Pernambuco (SEE-PE).

2. REFERENCIAL TEÓRICO

2.1. Política de Segurança da Informação (PSI)

A política de segurança da informação define o conjunto de normas, métodos e procedimentos utilizados para manutenção da segurança da informação, devendo ser

formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação (FERREIRA; ARAÚJO, 2008). Tal compêndio serve para nortear, organizar e orientar, por meio de diretrizes, normas e procedimentos, ações que minimizem os riscos com perdas e violações dos bens da organização, auxiliando na proteção das informações consideradas como ativo crítico e importante na organização (NAKAMURA; GEUS, 2007).

Segundo Fontes (2012), o desenvolvimento de uma política de segurança de informação tem vários objetivos que, dentre os quais pode-se destacar a formalização das regras da organização em relação ao tratamento da informação, pois somente escrevendo e publicando o que se deseja no acesso e uso da informação é que a organização terá êxito no cumprimento das regras por ela estabelecidas.

Também, é fundamental a atribuição de responsabilidades e obrigações, que segundo aquele mesmo autor e Kovacich (2016), é o que vai determinar como a informação deve ser tratada e indicar quem será responsável por ela, evidenciando as obrigações, responsabilidades e poder de autorização.

Considera-se uma questão estrutural que a organização tenha uma política de segurança da informação para que o processo de proteção da informação possa ser elaborado, implantado e mantido (FONTES, 2012). Esta política definirá as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implantados na proteção da sua informação.

É importante ressaltar a importância e os objetivos relacionados à política de segurança da informação, as responsabilidades e atribuições que ela impõe, mas é fundamental que todas as fases do desenvolvimento do processo de implantação de uma política de segurança da informação sejam realizadas. Em muitas empresas, a construção se limita à escrita, em outras até publica-se, mas poucas realizam a implementação, divulgação e revisão.

Destaca-se, assim, a importância da aplicação de uma metodologia, que não só tenha a política por escrito, mas que esta seja implementada, divulgada e revisada e que seja participativa, contemplando e envolvendo todos os usuários da organização, refletindo a realidade correspondente e dando conhecimento do que pode ou não ser realizado (ALBERTIN; PINOCHET, 2010).

A política de segurança da informação deve ter características que a deixem legítima, sendo verdadeira e válida por todos, simples, patrocinada pela alta gestão e com disponibilidade de recursos (FERREIRA; ARAUJO, 2008).

Além disso, deve não só estar escrita e publicada com acesso de todos, mas conter o que a organização deseja de fato, com controles possíveis de serem implementados, para evitar que se escrevam regulamentos que nunca serão realizados, mesmo que estas implementações e controles sejam efetivadas após a definição e publicação das regras, como indica Fontes (2012).

Percebe-se que a política de segurança da informação, deve ser gerenciada e monitorada, visando atender as necessidades da empresa, garantindo continuidade ao processo conforme evolução, desenvolvimento e inovação de cada uma. Assim, cada política é individualizada e atende à necessidade de forma particular, sendo praticamente exclusiva, refletindo as peculiaridades que lhe é atribuída, conforme objetivos e realidade de cada empresa.

A NBR ISO/IEC 27002 (2005) destaca que a organização deve garantir que todos os usuários estejam cientes das ameaças e preocupações com a segurança da informação e estejam equipados para apoiar essa política no desenvolvimento normal de seu trabalho.

Assim, segundo Ferreira e Araújo (2008), todos da organização devem ser treinados e informados em relação a política de segurança da informação da organização, para o uso correto dos recursos de tecnologia e uso da informação, pois o elemento humano é fundamental para que o processo de implantação de uma política de segurança da informação seja eficaz.

Fontes (2008) reitera o exposto, citando que para desenvolver pessoas em segurança da informação é necessário conscientizar e treinar os usuários sob medida para cada organização.

Contudo, cabe à alta gestão a responsabilidade pela clara de proporcionar orientação a respeito da política de segurança da informação, alinhada com os objetivos de negócio expressando apoio e cumprimento por meio da publicação e manutenção de uma política de segurança da informação para toda a organização (ABNT, 2005).

O processo de gestão de segurança da informação deve ser encorajado de forma que os usuários enfatizem a importância e a melhoria contínua baseada em medições objetivas, neste sentido, ressalta-se a necessidade da política ser mantida atualizada.

Assim, fica claro que é um documento dinâmico e deve ser reavaliado e revisado periodicamente, tendo um responsável ou área que conste na própria política para isso, conforme descreve Campos (2007).

3. ESTRATÉGIA METODOLÓGICA

O presente trabalho se originou de uma pesquisa aplicada utilizando uma metodologia qualitativa de estudo de caso instrumental na Secretaria de Educação do Estado de Pernambuco

(SEE-PE), através de uma análise interpretativa de registros e documentos coletados na organização, entrevistas e observações, onde foi possível identificar o processo de desenvolvimento e implementação de uma política de segurança da informação.

No estudo de caso instrumental, o interesse no caso reside na crença de que ele tem potencial de facilitar a compreensão de algo mais amplo, possibilitando a elaboração *insights* sobre um determinado assunto (STAKE, 1995). Assim, a escolha da SEE-PE como objeto de estudo se deu pelo fato de que, além da facilidade de acesso aos registros do processo de desenvolvimento e implementação da PSI, a organização dirigiu todo o projeto seguindo metodologia indicada pela ABNT (ABNT, 2005) bem como pelos ensinamentos de especialistas considerados na investigação bibliográfica.

3.2. COLETA DE DADOS

A coleta de dados foi desenhada com base na utilização de várias fontes de evidências e de acordo com a estratégia de triangulação de dados proposta por Yin (2010). Assim, foram considerados dados resultantes de entrevistas semiestruturadas, de registros e documentação do projeto de PSI e da posição de especialistas em PSI a partir do relato de suas experiências em projetos similares.

Inicialmente, para obtenção dos dados necessários para a pesquisa, foram realizadas entrevistas semiestruturadas com os gestores das áreas: de tecnologia, de infraestrutura tecnológica, de educação, corregedoria, jurídico e da assessoria de imprensa, buscando obter informações necessárias a respeito dos impactos relativos aos incidentes relacionados à segurança da informação.

Além das entrevistas, foram coletados registros e documentos da organização, que viabilizaram a identificação de vulnerabilidades e consequentes riscos relativos a ausência de uma política de segurança formalizada, publicada, implementada e divulgada.

Como complemento dos dados levantados, o pesquisador contou com a participação de especialistas que foram consultados, bem como especialistas que publicaram registros de experiências em projetos de PSI em meios públicos. Nessa perspectiva, os dados coletados contemplaram a análise de riscos na organização, o comportamento das pessoas e a cultura da organização.

Por fim, o pesquisador também emprestou a sua percepção a respeito dos elementos constituintes do projeto da PSI da Secretaria de Educação, pois participou do processo de desenvolvimento e implementação na época em que ocorreu.

As entrevistas com os gestores foram gravadas mediante autorização e, posteriormente, transcritas, assim como as entrevistas e registros de especialistas, formando uma base de dados de texto para a análise interpretativa. Os registros e documentos do projeto foram analisados e organizados de acordo com as fases e com os temas componentes de uma PSI. Assim, foi composto um banco de dados para a análise dos dados.

3.3. ANÁLISE DE DADOS

Os dados coletados foram compilados e organizados em um banco de dados e, a partir daí, cumpriu-se um plano de trabalho sistematizado que orientou as tarefas analíticas, conforme orientado por Sampieri, Collado e Lucio (2006), contemplando: revisão dos dados coletados, criação de sistema de codificação, definição de metodologia de análise de dados e a análise dos dados.

Criaram-se códigos para o tipo de fonte do dado (entrevista, documento, memorandos de campo) e, em seguida, as categorias de análise para relacionar os dados coletados de acordo, quais sejam: (1) conhecimento/apropriação/aceitação da tecnologia; (2) burocratização/circulação de documentos em meio físico (papel); (4) camadas hierárquicas/departamentalização; (5) Procedimentos para criação de PSI.

Assim, após a organização dos dados, foi possível iniciar a análise, a qual foi realizada de forma interpretativa comparando-se os dados coletados na SEC-PE com a posição de especialistas, procedendo-se com a sistematização da modelagem de uma PSI genérica.

4. RESULTADOS DO ESTUDO

4.4. MODELAGEM NA IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Albertin e Pinochet (2010) sugerem um fluxo composto por 10 (dez) etapas para o desenvolvimento das políticas de segurança da informação, sendo primordial a designação de um responsável para esta implantação, conhecido como gestor de segurança.

Já Ferreira e Araújo (2008) dividem o desenvolvimento e a implementação das políticas de segurança da informação em 4 (quatro) fases, sendo a primeira o levantamento das informações, a segunda o desenvolvimento do conteúdo, a terceira a elaboração dos procedimentos e a quarta a revisão, aprovação, implantação e palestras.

O conjunto da política e dos demais regulamentos, deve facilitar a estruturação documentacional, sendo sugerido por Fontes (2012), a segregação entre política de segurança e seus regulamentos complementares, seguindo as seguintes etapas: 1) inicialização, desenvolvimento e entrega; 2) comunicação e treinamento do produto final; e 3) definição dos processos de revisão e atualização.

Campos (2007) sugere a separação da política em diretrizes, normas e procedimentos, utilizando uma agenda de trabalho em 5 (cinco) etapas: 1) método de trabalho; 2) avaliação das questões do negócio, legais e contratuais; 3) contexto estratégico e de risco; 4) construção e aprovação e 5) divulgação da política.

O processo utilizado na Secretaria de Educação do Estado de Pernambuco, adaptou as melhores práticas, dentre as pesquisadas, sendo elaborado em 4 (quatro) fases: 1) elaboração, 2) implementação, 3) divulgação e 4) revisão. O documento foi dividido em: política principal (diretrizes) e políticas complementares (normas), sendo complementado na fase de implementação com os procedimentos.

4.5. PROCESSO DE ELABORAÇÃO, IMPLEMENTAÇÃO, DIVULGAÇÃO E REVISÃO

4.5.1. ELABORAÇÃO

Esta fase teve por objetivo escrever as regras da política, sendo iniciada com uma reunião, tecnicamente chamada de *kick-off*, com todos os executivos da alta gestão para indicação dos gestores integrantes de equipe de elaboração da política de segurança da informação. Nessa reunião, foi apresentada a metodologia de construção com as 4 (quatro) fases, o macro cronograma e a formatação proposta para o documento.

A política de segurança da informação da Secretaria de Educação, foi elaborada com uma política principal, como diretriz, e doze políticas complementares, como as normas, estabelecendo as regras necessárias para cada controle identificado no levantamento de dados.

Segundo Fontes (2012), ao iniciar o processo de escrita, deve ser reunido todo o material necessário e criar um comitê de revisão, composto de pessoas das diversas áreas como: RH, jurídico, etc.. Em complemento, Ferreira e Araújo (2008) sugerem a criação de um comitê composto por integrantes indicados e nomeados pela alta gestão.

Deste modo, foi criado um comitê de elaboração, nomeado e publicado no Diário Oficial. Esta equipe foi composta por gestores de diversos setores da SEC-PE. Em seguida, juntamente

com o comitê, foi definida a agenda de reuniões da equipe, os prazos acordados com a alta gestão e a metodologia de trabalho para elaboração da política.

Para obtenção de sucesso na conclusão do trabalho, foi estabelecido que o especialista, faria uma escrita inicial para cada política e nos encontros quinzenais, estas seriam discutidas pelo grupo, chegando a um texto definitivo, o que ocorreu.

Após a conclusão do descritivo pela equipe de elaboração, a documentação foi encaminhada ao setor jurídico, para ratificação e verificação da existência de inconsistências com as leis vigentes. Em seguida, foi encaminhada para a assinatura do Secretário de Educação do Estado de Pernambuco e publicação no Diário Oficial do estado. Encerrando-se, assim, a primeira fase da construção da política.

Além da Política Principal, foram criadas as seguintes políticas complementares:

- Política de Uso de Senhas, com objetivo de estabelecer critérios para a criação de senhas fortes, proteção dessas senhas, bem como a frequência de suas atualizações;
- Política de Uso do Correio Eletrônico, com objetivo de estabelecer critérios que determinem as exigências mínimas de segurança para uma comunicação através do correio eletrônico institucional;
- Política de Resposta a Incidentes de Segurança da Informação, com objetivo de estabelecer medidas a serem tomadas nos tratamentos de incidentes envolvendo a segurança das informações em eventos que podem resultar em perda, dano ou acesso não-autorizado às informações;
- Política de Classificação da Informação, com objetivo de estabelecer padrões na determinação de quais informações podem ser divulgadas fora da SEE-PE, bem como a sensibilidade relativa de informações que não devem ser divulgadas sem a devida autorização;
- Política de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações, com objetivo de estabelecer as exigências mínimas que devem ser atendidas no desenvolvimento e aquisição e suporte das aplicações sistêmicas;
- Política de Uso da Internet, com objetivo de estabelecer as exigências mínimas de segurança da informação para o uso seguro da Internet;

- Política de Acesso Remoto, com objetivo de estabelecer regras e requisitos para acesso externo à rede da SEE-PE e minimizar o risco potencial para danos que possam resultar do uso não autorizado;
- Política de Gestão de Ativos, com objetivo de estabelecer a formalização da gestão de ativos da SEE-PE;
- Política de Controle de Acesso, com objetivo de estabelecer as exigências mínimas na criação de identidades em conformidade com as atividades funcionais e no controle de acesso dos usuários;
- Política de Dispositivos Móveis, com objetivo de estabelecer regras relativos aos controles dos dispositivos móveis;
- Política de *Backup* Corporativo, com o objetivo de estabelecer padrões para a cópia e restauração, com a finalidade da continuidade e disponibilidade das informações, observando a relevância e criticidade destas;
- Política de Combate a *Softwares* Maliciosos, com o objetivo de estabelecer as exigências mínimas de segurança para a proteção contra *softwares* maliciosos (vírus, trojan, entre outros).

4.5.2. IMPLEMENTAÇÃO

A fase de implementação compreende a adequação dos processos, procedimentos, infraestrutura e recursos necessários para que a política de segurança esteja de acordo com o que está descrito, sendo fundamental que cada tópico seja mapeado para verificação da compatibilidade com a prática ou se precisa de ajustes para tornar-se compatível.

Na Secretaria de Educação, foram implementadas inicialmente as políticas complementares de Acesso Remoto e de Backup Corporativo, seguindo a estratégia de iniciar a implementação por políticas que estivessem sob a gestão e controle do setor de tecnologia, para haver um mapeamento melhor e monitoramento das ações necessárias.

Neste contexto, foram mapeadas todas as regras relativas às respectivas políticas complementares, identificando o que seria necessário para implementação. A partir deste levantamento, um plano foi estruturado juntamente com a equipe técnica responsável, atribuindo responsabilidades e prazos combinados com a gestão do setor, visando que as ações realizadas e a implementação fossem concluídas conforme o planejado.

Dentre as atividades do plano de ação, constavam: o mapeamento dos processos, a elaboração dos procedimentos necessários para execução das atividades relativas à política, treinamento dos envolvidos no processo e a implementação propriamente dita.

Além dessas etapas de implementação, foram estabelecidas métricas comparativas para acompanhamento e medição da eficácia das ações realizadas, como por exemplo: a quantidade de solicitações de acesso remoto versus concessões realizadas, percentual mensal de falhas (definido a partir de histórico para ter um valor aceitável) versus total de backups realizados, entre outros. Foram formalizados termos de ciência das áreas técnicas, objetivando que os envolvidos fossem informados do novo processo, para ser colocado em operação. Foi colocado em produção e efetivado no início do segundo semestre de 2017, com os devidos monitoramentos.

4.5.3. DIVULGAÇÃO

A fase de divulgação da Política de Segurança da Informação, tem por objetivo apresentar, expor, informar e responsabilizar todos os envolvidos, em relação à mesma. Ressaltando as regras que devem ser seguidas e as proteções necessárias que os usuários devem estar atentos no manuseio, guarda e transferência das informações.

Yanus e Shin (2007) destacam que os programas de conscientização em Segurança da Informação envolvem educação, treinamento e comunicação e são criados a partir da política de segurança da informação. Neste sentido, após a elaboração, publicação da mesma em fevereiro de 2017 e inserção no site da educação (SEE-PE, Política de Segurança da Informação, 2017), foi realizado um planejamento, para ações de divulgação no início do segundo semestre.

Assim, foram realizadas palestras presenciais para os gestores das GREs, escolas e integrantes dos anexos e sede. Durante as palestras, foram destacados conceitos de riscos, informação e segurança da informação; e ao final, os integrantes assinavam um termo de compromisso, assumindo a responsabilidade de cuidar da segurança das informações sob sua tutela, entendendo que “o comprometimento envolve a colaboração de todos, indistintamente, para com os controles definidos na política de segurança da informação, desde a alta gestão até os profissionais da base organizacional” (ELLWANGER, 2009).

As palestras abrangeram os gestores e representantes das 16 (dezesseis) Gerências Regionais (GREs), gestores ou representantes de 1.200 (mil e duzentas) escolas, integrantes dos

5 (cinco) anexos, inclusive Biblioteca Pública do Estado e Conservatório de Música e a sede da SEE-PE.

4.5.4. REVISÃO

A revisão de uma política se constitui em uma das fases mais importantes, pois é nesta fase, que se verifica os ajustes, a necessidade de acrescentar ou retirar alguma política complementar, atribuir ou retirar responsabilidades, incluir ou retirar conformidades com alguma nova legislação ou processo, entre outras. “A revisão periódica da política de segurança da informação deve considerar as mudanças e as circunstâncias do negócio” (ABNT, 2005).

Na Secretaria de Educação do Estado de Pernambuco, a política de segurança da informação foi publicada em fevereiro de 2017, com previsão de revisão anual. Contudo, este prazo não deverá ser cumprido, pois como as políticas complementares não foram implementadas em sua totalidade, isso inviabilizaria uma revisão em toda a política, sem que a implementação estivesse concluída. Diante da constatação identificada, um dos ajustes prioritários, deverá ser no próprio prazo de revisão descrito na política.

Outro evento constatado e que deve ser revisto, está em relação à alguma das responsabilidades atribuídas ao comitê de Tecnologia da Informação (TI), que deveria ser composto pelos secretários executivos e a gestora geral de tecnologia da informação, mas que durante os dois últimos anos não foi constituído.

4.6. ANÁLISE DO PROCESSO DE IMPLEMENTAÇÃO DA PSI

São pontos críticos e essenciais para o sucesso na implantação de um processo de política de segurança da informação: a formalização dos processos e instrução de trabalho; a utilização de tecnologias capazes de prover segurança; atribuição formal das responsabilidades e das respectivas penalidades; a classificação da informação e treinamento e conscientização constantes (FERREIRA; ARAÚJO, 2008).

O processo de segurança da informação somente terá sucesso se a sua implantação for conduzida como decisão estratégica da organização e seja patrocinada pela alta gestão, com o apoio explícito no desenvolvimento, implantação e manutenção deste processo conforme afirma Fontes (2012). O mesmo autor reforça a necessidade de independência, autonomia e autoridade que o responsável pela gestão da segurança da informação deve ter para o sucesso da proteção da informação.

Segundo Ferreira (2003), o desenvolvimento de um processo de implantação de uma política de segurança da informação não deve ser encarado como simplório ou sem a atenção devida, mas fundamental para a segurança das operações e atividades do negócio.

Ramos e Cavalcante (2005) destacam que existem vários fatores que devem ser atentados, para o sucesso de uma política de segurança da informação implementável, aplicável e com responsabilidade em todos os níveis. Os mesmos autores ressaltam que a comunicação é um fator crítico de sucesso para a correta disseminação das políticas corporativas.

Outro fator importante é a instalação de um comitê de segurança da informação, com forte representatividade da cúpula estratégica, para realizar a análise crítica e aprovação (ALBERTIN; PINOCHET, 2010).

De forma geral, a metodologia utilizada permitiria o envolvimento da alta gestão, o que facilitou o levantamento de informações e o mapeamento de riscos que foram conduzidos por um especialista contratado. No entanto, os gestores de alto escalão, que deveriam ter um envolvimento maior no processo, só participaram da reunião inicial (kickoff).

A divisão da PSI em etapas facilitou o processo, permitindo que tanto os desenvolvedores, quanto os participantes pudessem ter a percepção de concretude da política a cada fase concluída.

Durante a fase de elaboração, pode-se destacar como pontos positivos a formação de um comitê de elaboração da política, o que permitiu o envolvimento, a interação e a colaboração dos participantes, fortalecendo o planejamento e o engajamento com tarefas e prazos estabelecidos, que não devem ser muito longos para diminuir a ocorrência de ausências de participantes por conta de ingresso em outros projetos ou demandas.

Já na fase de implementação, a participação dos gestores no acompanhamento e monitoramento da operacionalização das ações planejadas foi determinante para dirimir resistências e promover a participação efetiva das áreas técnicas. Outro elemento que merece destaque foi a definição e o desenho dos processos, o que permitiu maior visibilidade das tarefas executadas facilitando a coordenação e o controle.

A fase de divulgação contou com didáticas inovadoras para a apresentação dos componentes da política e contribuiu para a assimilação da dimensão segurança da informação na cultura organizacional.

Destaca-se aqui a ausência da fase de revisão, que não chegou a ser implementada durante o período analisado nesta pesquisa. No entanto, esta fase é de relevância crucial para a continuidade do processo.

Por fim, considera-se como mandatório e determinante para o sucesso de todas as etapas destacadas, o apoio do alto escalão da organização que deve apoiar e fazer-se presente em todos os estágios do processo de desenvolvimento da PSI. Tal posicionamento aumenta consideravelmente as chances de sucesso da implementação de uma PSI em qualquer organização.

5. CONCLUSÃO

De forma geral, as organizações, em sua grande maioria, ou não possuem uma política de segurança da informação, ou possuem de forma incompleta. Isso decorre, por considerarem que ter ferramentas de hardware e software de segurança e mão de obra qualificada para operar e monitorar essas ferramentas é o suficiente para proteção das informações. No entanto, isso acarreta fragilidades, principalmente as decorrentes de processos inexistentes ou imprecisos, assim como, o desconhecimento das pessoas em relação às suas responsabilidades e cuidados que devem ter com as informações que circulam através delas e principalmente sob sua guarda.

O desenvolvimento do presente trabalho possibilitou a análise da construção da Política de Segurança da Informação (PSI) na Secretaria de Educação do Estado de Pernambuco (SSE-PE), por meio de uma metodologia que viabilizou, não apenas a elaboração escrita e sua publicação, como também, possibilitou o desenvolvimento de procedimentos, fortalecendo os processos existentes e criando novos, para aumentar a segurança da informação, conforme objetivo do Plano Diretor de Tecnologia da Informação (PDTI) da SEE-PE. Além disso, também permitiu que os gestores da organização, tivessem uma capacitação em segurança da informação, através de palestras presenciais, e entendessem suas responsabilidades em relação a proteção das informações sob sua gestão, colaborando com a formação de uma cultura organizacional em segurança da informação.

Também foi possível verificar que os processos de elaboração, implementação, divulgação e revisão foram constituídos na instituição e descritos neste documento, o detalhamento dos pontos positivos e de melhoria que foram identificados e apresentados. Com este modelo, houve uma conscientização e responsabilização institucionalizada com relação a proteção da informação, iniciando uma mudança de hábitos e costumes, que será reforçada com

a implementação das demais políticas complementares em 2018. Permitindo assim, que os objetivos propostos realmente foram alcançados.

As entrevistas semiestruturadas com os gestores das áreas, possibilitaram identificar muitas fragilidades relacionadas à proteção da informação, tanto nas áreas usuárias, como nas áreas técnicas. Em algumas situações, o especialista, no papel de entrevistador, usou de técnicas de engenharia social e observação direta para, durante as entrevistas, identificar e evidenciar as fragilidades. Verificou-se que, apesar de ter um ambiente tecnológico completo e atualizado e ter profissionais qualificados para manter os controles necessários, apresentava riscos, por não ter uma normatização do uso da tecnologia e do cuidado com as informações, assim como, não havia um conhecimento e comprometimento em relação à segurança da informação por parte dos seus agentes públicos.

Vários registros e documentos foram coletados e lidos, principalmente referente às legislações em vigor, por se tratar de órgão público. Esses registros foram muito importantes, pois auxiliou na complementação e citação da política, referenciando e homologando a necessidade da construção do documento.

A análise de riscos e a observação direta do comportamento das pessoas e da cultura da organização, auxiliou o direcionamento da alta gestão para decisão de quais políticas complementares seriam elaboradas e priorizadas, sendo ratificadas pelo comitê de elaboração.

Vários livros e normas, serviram de referência na construção da política, principalmente a norma NBR ISO/IEC 27002:2005, que serviu de base para elaboração. Além da norma, vários autores contribuíram, principalmente os que diretamente foram escritos sobre o tema.

Durante as palestras e reuniões, foram usadas técnicas de dinâmica de grupo, com o objetivo de integração, “quebra gelo” e facilitar o entendimento dos participantes. Como por exemplo, na primeira reunião com a equipe de elaboração, foram divididos grupos para que cada um criasse uma imagem feita com as peças do tangram, registrando cada etapa da criação, sem que os outros grupos pudessem ver a imagem construída. Em seguida, foram coletadas as imagens e os registros foram trocados nos grupos, para que fossem criadas imagens a partir dos relatos escritos. No final, foram comparadas as imagens e enfatizada a importância da escrita clara pelo emissor para que o receptor tenha entendimento do que foi escrito.

Outra técnica utilizada, correspondeu a utilização de fatos vividos pelos participantes em seus respectivas realizadas, comparando situações reais com situações imaginárias e ligadas ao assunto de segurança, de uma forma leve e bem-humorada, num formato de *stand-up*

comedy, sem tirar a seriedade do assunto. Isso, permitiu um entendimento claro do tema e uma interação do palestrante com os participantes.

Dada a importância do assunto, faz-se necessário um envolvimento maior da alta gestão, para que o desenvolvimento do processo de construção, tenha o aval e participação, conforme sua importância. Com este envolvimento, além dos processos serem mais rapidamente implantados, a participação dos demais níveis hierárquicos se torna mais efetivo.

A construção de uma política de segurança da informação com todas as suas fases, constitui uma mudança cultural na organização, protegendo informações consideradas confidenciais e resguardando o patrimônio e seus agentes de possíveis malfeitores. O método foi aplicado em uma organização pública e pode ser replicado para outros órgãos semelhantes, mas também pode atender às instituições privadas, contribuindo na proteção das informações onde for aplicado. O processo apenas foi iniciado, mas precisa ser consolidado, para que a mudança na cultura organizacional em relação à segurança da informação, seja tão significativa que sirva de modelo para outras organizações e possa refletir nos hábitos e costumes pessoais e familiares.

Referências

ABNT. **NBR ISO/IEC 27002**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

ABNT. **NBR ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para gestão da segurança da informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

ALBERTIN, A. L.; PINOCHET, L. H. C. **Políca de Segurança de Informações Uma Visão Organizacional para a sua Formulação**. São Paulo: Campus, 2010.

CAMPOS, A. **Sistema de Informação Controlando os Riscos 2ª Edição**. Florianópolis: Visual Books, 2007.

CERT.BR, N. D. I. E. C. D. Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2015. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**, 13 fev. 2017. Disponivel em: <https://www.cert.br/stats/incidentes/2015-jan-dec/total.html>.

CETIC, C. G. D. I. N. B.-. Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação nas Escolas Brasileiras. **Site Comitê Gestor da internet no Brasil**, Outubro 2017. Disponivel em: <http://www.cetic.br/media/docs/publicacoes/2/TIC_EDU_2016_LivroEletronico.pdf>.

COIMBATORE KRISHNARAO PRAHALAD; GARY HAMEL. **A Competência Essencial da Corporação**. [S.l.]: [s.n.], 1990.

ELLWANGER, C. Impacto da Utilização de Técnicas de Endomarketing na Efetividade das Políticas de Segurança da Informação, Santa Maria, RS, 2009.

ERNST&YOUNG. O caminho para a ciber-resiliência Percepção, resistência, reação. **19ª Pesquisa Global de Segurança da Informação da EY 2016-17**, 2017. Disponivel em: <file:///C:/Users/josue.fsilva/Documents/Google/UFRPE/2017.2/ESO/GISS_2016_Report_Final.pdf>.

FERREIRA, F. N. F.; ARAÚJO, M. T. D. **Política de Segurança da Informação Guia Prático para Elaboração e Implementação**. Rio de Janeiro: Ciência Moderna, 2008.

FONTES, E. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

FONTES, E. **Políticas e Normas para a Segurança da Informação**. Rio de Janeiro: Brasport, 2012.

FONTES, E. **Políticas e Normas para a Segurança da Informação**. Rio de Janeiro: Brasport, 2012. 5 p.

GGTI. Plano Diretor de Tecnologia. **Site da Secretaria de Educação do Estado de Pernambuco**, 11 dezembro 2015. Disponivel em: <http://www.educacao.pe.gov.br/portal/upload/galeria/12289/Plano%20Diretor%20de%20Tecnologia%20da%20Informa%C3%A7%C3%A3o%20-%20PDTI%20-%20Simplificado.pdf>.

GITI. Política de Segurança da Informação. **Site da Secretaria de Educação do Estado de Pernambuco**, fev. 2017. Disponivel em: <http://www.educacao.pe.gov.br/portal/?pag=1&men=176>.

HENRY MINTZBERG, BRUCE AHLSTRAND E JOSEPH LAMPEL. **Safári de Estratégia. Um Roteiro Pela Selva do Planejamento Estratégico**. [S.l.]: [s.n.], 2010.

IKENAGA, C. Y. **Gestão da terceirização dos serviços de TI**. [S.l.]: [s.n.], 2008.

ISTART, I. Ístart Ética Digital. **Família mais Segura**, 2014. Disponivel em: <http://www.familiamaissegura.com.br/wp-content/uploads/2014/05/ISTART_Pesquisa_PanoramaEducacaoDigital_Ano2_2013-14-1.pdf>.

KOVACICH, G. L. **Information Systems Security officer's guide: Establishing and Managing an Information Protection Program**. 3ª. ed. Woburn - Massachusetts: Butterworth-Heinemann, 2016.

LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. **Revista Economia & Tecnologia**, São Paulo, p. 38-44, 2005.

MARIA CAROLINA ANDION; RUBENS FAVA. **Gestão Empresarial**. Curitiba: Associação Franciscana de Ensino Bom Jesus, 2002.

MICHAEL A. HITT; DUANE IRELAND; MICHAEL A HOSKISSON. **Administração Estratégica**. [S.l.]: [s.n.], 2002.

NAKAMURA, E. T.; GEUS, P. L. D. **Segurança em Redes em Ambientes Cooperativos**. São Paulo: NOVATEC, 2007.

KOTLER, P.; KEVIN LANE KELLER. **Administração de Marketing**. [S.l.]: [s.n.], 2006.

RAMOS, A. S. M.; CAVALCANTE, S. D. M. **Prátcasde Conscientização e Treinamento em Segurança da Informação no Correio Eletrônico**. [S.l.]: FGV-EAESP. 2005.

SALES, R.; ALMEIDA, P. P. Avaliação de Fontes de Informação na Internet : avaliando o site NUPILL/UFSC. **Revista Digital de Biblioteconomia e Ciência da Informação**, p. 67-87, 2007.

SCOTT, B. **Writting Information Security Polices**. Indianapolis: New Riders, 2002.

SEE-PE, S. D. E. D. E. D. P.-. GREs e ESCOLAS. **SECRETARIA DE EDUCAÇÃO DO ESTADO DE PERNAMBUCO**. Disponivel em: <http://www.educacao.pe.gov.br/portal/?pag=1&men=77>. Acesso em: 23 Fevereiro 2018.

SAMPIERI, Roberto Hernández; COLLADO, Carlos Fernandez; LUCIO, Pilar Baptista. **Metodologia de pesquisa.** 3. ed. São Paulo: Mcgraw Hill, 2006.

STAKE, R. E. **The art of case study research.** London: Sage, 1995.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais:** a pesquisa qualitativa em educação. São Paulo: Atlas, 1987.

YANUS, R; SHIN, N. **Critical Sucess Factors for Managing an Information Security Awareness Program**. Las Vegas, 2007.

YIN, R. **Estudo de caso: planejamento e métodos**. Porto Alegre: Bookman, 2010