RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 8 Nro. 1 2017

Implantação de políticas de segurança da informação em uma pequena empresa

Thiago Rodrigues Oliveira[1]

Resumo

Este artigo apresenta a implantação de uma política de segurança da informação (PSI) em uma pequena empresa. A metodologia é baseada nos principais padrões e normas de segurança da informação, que serviram de guia para elaboração do estudo. A política de segurança da informação criada neste artigo foi aplicada em um estudo de caso envolvendo as Lojas Mib, uma empresa de comércio varejista situada no norte de Minas Gerais, a garantia da confidencialidade e integridade das informações de seus clientes é fundamental para o funcionamento do negócio. A forma detalhada com que o artigo é apresentado facilita a aplicação do método em outras empresas de mesmo porte.

Palavras-chave: Informação. Normas. Políticas de Segurança da Informação. Segurança da Informação.

1 Introdução

Ao longo do tempo os computadores tornaram-se comuns em ambientes organizacionais, e as informações outrora em papéis hoje também são representadas por bits em grandes bases de dados, a utilização de redes locais e remotas fazem parte do dia à dia da maioria dos colaboradores de uma empresa, dessa forma, como o acesso a informação passou a ser feito também de forma lógica, a garantia da confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação, que são as propriedades que compõe a segurança da informação, é vital

[1] Universidade Estácio de Sá. Graduado em Sistemas de informação, pós-graduado em Segurança da informação.

para o bom funcionamento dos negócios. Nesse contexto, a segurança da informação assumiu papel de destaque em ambientes corporativos.

A Política de segurança da informação (PSI) é uma importante aliada na prevenção e na recuperação de incidentes de segurança, definindo diretrizes, normas e procedimentos seguros para proteger os ativos de informação e garantir as propriedades básicas de segurança nos sistemas de informação. A política aqui apresentada foi aplicada em um estudo de caso envolvendo a empresa Lojas Mib – uma empresa de pequeno porte que atua no comércio varejista, à garantia da confidencialidade e da integridade dos dados de seus clientes é fundamental para o bom funcionamento do negócio.

O objetivo geral foi: implantar uma política de segurança da informação em uma pequena empresa, atendendo suas necessidades e em acordo com suas limitações. Os objetivos específicos foram: definir os controles que serão utilizados; escrever o texto da política; conscientizar e treinar os colaboradores da empresa.

Pequenas empresas demonstram pouco interesse em segurança da informação, por falta de conhecimento ou investimento na área, o intuito desse artigo é apresentar para pequenas empresas, como à pesquisada, a importância da segurança da informação para as próprias, e que um pequeno esforço em segurança da informação pode torna-se uma vantagem competitiva no futuro. A implantação de políticas de segurança da informação é um passo importante para um futuro sistema de gestão de segurança da informação (SGSI), e tende a ser um projeto viável para empresas de pequeno porte, visto que a PSI se ajusta a realidade organizacional.

Este estudo foi realizado através de pesquisa aplicada de abordagem qualitativa, com caráter exploratório, a partir do procedimento técnico de estudo de caso para o desenvolvimento do trabalho.

2 Bibliografia e normas

Para realização desse trabalho, foi relevante o estudo de normas, bibliografias, conceitos e definições para guiar o seu desenvolvimento.

2.1 Segurança da informação

A informação pode existir em diversos formatos: impressa, armazenada eletronicamente, falada e etc. Em qualquer forma ou fase (manuseio, armazenamento, transporte e descarte) a informação deve ser protegida adequadamente. Assim sendo, a segurança da informação tem a responsabilidade de preserva-la de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar os riscos e maximizar os retornos. De acordo com a (ABNT NBR ISO/IEC:27002, 2013), uma segurança da informação eficaz reduz riscos, protegendo a organização das ameaças e vulnerabilidades e, assim, reduzindo o impacto aos seus ativos.

Aplicar controles é um dos aspectos para se atingir a segurança da informação, assim diz a (ABNT NBR ISO/IEC:27002, 2013, item 0.1), " a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, cultura organizacional e funções de software e hardware". A norma também destaca nesse mesmo item a importância de manter, monitorar e melhorar controles. "Estes controles precisam ser estabelecidos, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação sejam atendidos" (ABNT NBR ISO/IEC:27002, 2013, item 0.1).

A grande maioria das informações vitais e estratégicas de uma empresa está em seus sistemas de informática, acessos não autorizados, indisponibilidade e alterações feitas de forma indevida podem causar grandes danos as organizações ou até mesmo sua extinção, segundo (NETTO; SILVEIRA, 2007, p. 377) "[...] por isso as organizações dependem da confiabilidade de seus sistemas baseados em TI; se a confiança nesses dados for destruída, o impacto pode ser comparável à própria destruição do sistema".

Araújo, Bezerra e Coelho (2014) definem a segurança da informação como um fator determinante para condução de negócios bem sucedidos, tanto no setor público quanto no privado, além disso é um componente que viabiliza negócios, tais como e-Gov (governo eletrônico) ou e-commerce (comércio eletrônico).

Por fim, Araújo, Bezerra e Coelho (2014), completa que a segurança da informação abrange todos os ativos de informação, preservando-os contra desastres e erros (intencionais ou não), tentando reduzir a probabilidade ou os impactos causados por incidentes de segurança.

2.2 Políticas de segurança da informação

Criar um SGSI pode ser inviável para pequenas empresas, mas um considerável passo pode ser tomado para o tratamento seguro das informações, políticas de segurança da informação são as bases para uma efetiva segurança dos ativos de informação. Segundo (OLIVEIRA, 2015), a implantação de políticas de segurança da informação é essencial para a criação de um Sistema de Gestão de Segurança da Informação.

A norma ABNT NBR ISO/IEC 27002, que dispões dos controles para implementação de um SGSI baseado na ABNT NBR ISO/IEC 27001 recomenda a existência de políticas de segurança da informação, "convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas interessadas" (ABNT NBR ISO/IEC 27002, 2013, item 5.1.1).

A PSI deve alinhar-se aos objetivos de negócio da empresa, propiciar controles para proteger as informações de acordo com sua classificação e necessidade, contribuindo para um efetivo processo de segurança da informação. Como diz (FONTES, 2015, p. 20), “desenvolver, implantar e manter os regulamentos necessários para que a empresa possua um efetivo processo de segurança da informação. Esses regulamentos definem como a organização deseja que a informação seja utilizada, controlada e tenha seu uso responsabilizado”.

A elaboração de uma PSI requer comprometimento da alta direção da empresa, também é recomendado a criação de um comitê de segurança da informação com intuito de elaborar e manter a PSI atualizada e continuamente melhorada. Segundo Monteiro (2009), para que uma política de segurança da informação seja eficiente, deve-se garantir a disponibilidade, integridade, confidencialidade, legalidade e autenticidade das informações, deixando explícito o comprometimento da alta direção. Ainda de acordo com Monteiro (2009, p. 21) "É recomendado para sua elaboração, ter profissionais de diversos departamentos ou setores da organização, formando um Comitê de Segurança da Informação [...] com a finalidade de compor o documento da política".

A política de segurança da informação pode ser composta por um ou por vários documentos, não existe uma definição de quantidade ou estrutura do conjunto desses documentos, o importante é que eles estejam atrelados, assim diz o Manual de Boas Práticas em Segurança da Informação do Tribunal de Contas da União, que se expressa da seguinte forma: “A Política de Segurança da Informação pode ser composta por várias políticas inter-relacionadas. Ademais, quando a instituição achar conveniente e necessário, sugere-se a criação de outros documentos que especifiquem práticas e procedimentos e que descrevam com mais detalhes as regras de uso da tecnologia da informação" (TCU, 2012, p. 12).

2.3 Norma complementar 03 do gabinete de segurança institucional

O Gabinete de Segurança Institucional da Presidência da República (GSIPR), indica que o Departamento de Segurança da Informação e Comunicações (DSIC), deve elaborar normas com o objetivo de proteger a confidencialidade, integridade, disponibilidade e autenticidade dos seus ativos de informação, provendo tratamento seguro desses ativos nos órgãos da Administração Pública Federal. Conforme exposto na (INSTRUÇÃO NORMATIVA 01, 2008, art. 3), “Compete ao DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta”.

Dentre as várias normas estabelecidas pelo DSIC relativa a segurança da informação e comunicações, está a Norma Complementar 03, que trata especificamente da implantação de políticas de segurança da informação, e tem por objetivo: "estabelecer diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da política de segurança da informação nos órgãos e entidades da Administração Pública Federal" (NORMA COMPLEMENTAR 03, 2009, item 1).

Por ser um documento metodológico, com diretrizes, conceitos e definições a respeito da elaboração e implantação de políticas de segurança da informação em órgãos federais, essa norma foi incluída no contexto desse trabalho aliando-se à outras, dentre as quais destacamos a ABNT NBR ISO/IEC 27002.

2.4 ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002

O objetivo destas normas é fornecer um método para implantação e manutenção de um sistema de gestão de segurança da informação, para uso por aqueles que são responsáveis pela segurança da informação em suas empresas. Também se destina a recomendar requisitos e controles que garantam uma efetiva segurança da informação.

A origem da ISO/IEC 27001 e ISO/IEC 27002 aconteceu no final da década de 80. Em 1987, na Inglaterra, o *Department of Trade and Industry's* (DTI) criou o *Comercial Computer Security Centre* (CCSC) com o objetivo de auxiliar empresas britânicas que comercializavam produtos de segurança da informação através da criação de indicadores para avaliação da segurança. O documento evoluiu até torna-se um padrão britânico para gestão de segurança da informação, o mesmo se tornou a norma *British Standard* BS7799:1995.

Em 1999, foi lançada uma segunda parte da BS7799 a BS7799:1999-2 intitulada Sistemas de Gerenciamento de Segurança da Informação - Especificação com orientação de uso. A BS7799-2 focava em como implementar um sistema de gerenciamento de segurança da informação, referindo-se à estrutura e controles de gerenciamento de segurança da informação. Em 2005 foi publicada à terceira parte dessa norma versando sobre gerenciamento e análise de riscos. Antes disso em 2000 a *International Organization for Standardization* (ISO) homologou a norma, publicada como ISO/IEC 17799:2000.

Após a criação da família de normas ISO 27000 as normas acima mencionadas foram utilizadas como base para elaboração das normas ISO/IEC 27001 e ISO/IEC 27002.

A norma ABNT NBR ISO/IEC 27001 tem por objetivo "prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação" (ABNT NBR ISO/IEC 27001, 2013, item 0.1). Para cumprir com seu objetivo a ABNT NBR ISO/IEC 27001 utiliza o modelo PDCA (*Plan-Do-Check-Act*), esse modelo tende a garantir melhoria contínua do Sistema de Gestão de Segurança da Informação, para melhor entendimento desse

modelo a imagem abaixo ilustra o ciclo PDCA. Assim, a Figura 01 mostra todos os passos do ciclo PDCA com uma breve explicação.

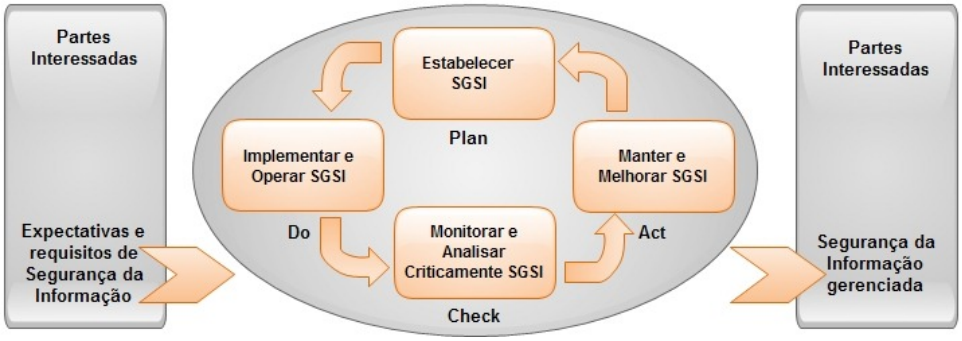

Figura 01 – Ciclo PDCA aplicado aos processos de um Sistema de Gestão de Segurança da Informação.
Fonte: https://www.profissionaisti.com.br/2010/10/conhecendo-a-abnt-nbr-isoiec-27001-parte-1/

A norma ABNT NBR ISO/IEC 27002, tem por objetivo sugerir boas práticas de gestão de segurança da informação para as organizações, através da seleção, implementação e gerenciamento de controles baseados nos ambientes organizacionais (ABNT NBR ISO/IEC 27002, 2013).

A ABNT NBR ISO/IEC 27002, possui 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles. Porém, isso não significa que sua organização somente estará segura se todos os controles expostos na norma forem implantados. Cada organização possui suas particularidades, leis e regulamentações que devem seguir, o que revela diferentes riscos de organização para organização, levando a utilização de controles distintos de uma empresa para a outra. A norma também permite que a organização crie seus próprios controles adequando-se as suas necessidades, ou utilize controles de outro conjunto.

Sobre a seleção dos controles a ABNT NBR ISO/IEC 27002, deixa a critério da organização com algumas ressalvas, assim como diz a norma. “A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco e nas opções para tratamento do risco aplicado à organização” (ABNT NBR ISO/IEC 27002, 2013, item 0.3). Outro ponto abordado pela norma são as regulamentações, “convém que também esteja sujeito a todas as legislações e regulamentações nacionais e internacionais, relevantes” (ABNT NBR

ISO/IEC 27002, 2013, item 0.3). Para finalizar a norma ressalta a importância da interação dos controles para se alcançar uma efetiva segurança da informação. “A seleção de controles também depende da maneira pela qual os controles interagem para prover uma proteção segura” (ABNT NBR ISO/IEC 27002, 2013, item 0.3).

2.5 ABNT NBR ISO/IEC 27005

A família de normas 27000 da *International Organization for Standardization* (ISO) convergem para o estabelecimento de um SGSI, abrangendo todos os aspectos relacionados a isso. Cada norma tem sua respectiva função, podendo ou não estarem relacionadas. A Figura 02 ilustra de forma sucinta o relacionamento das normas.

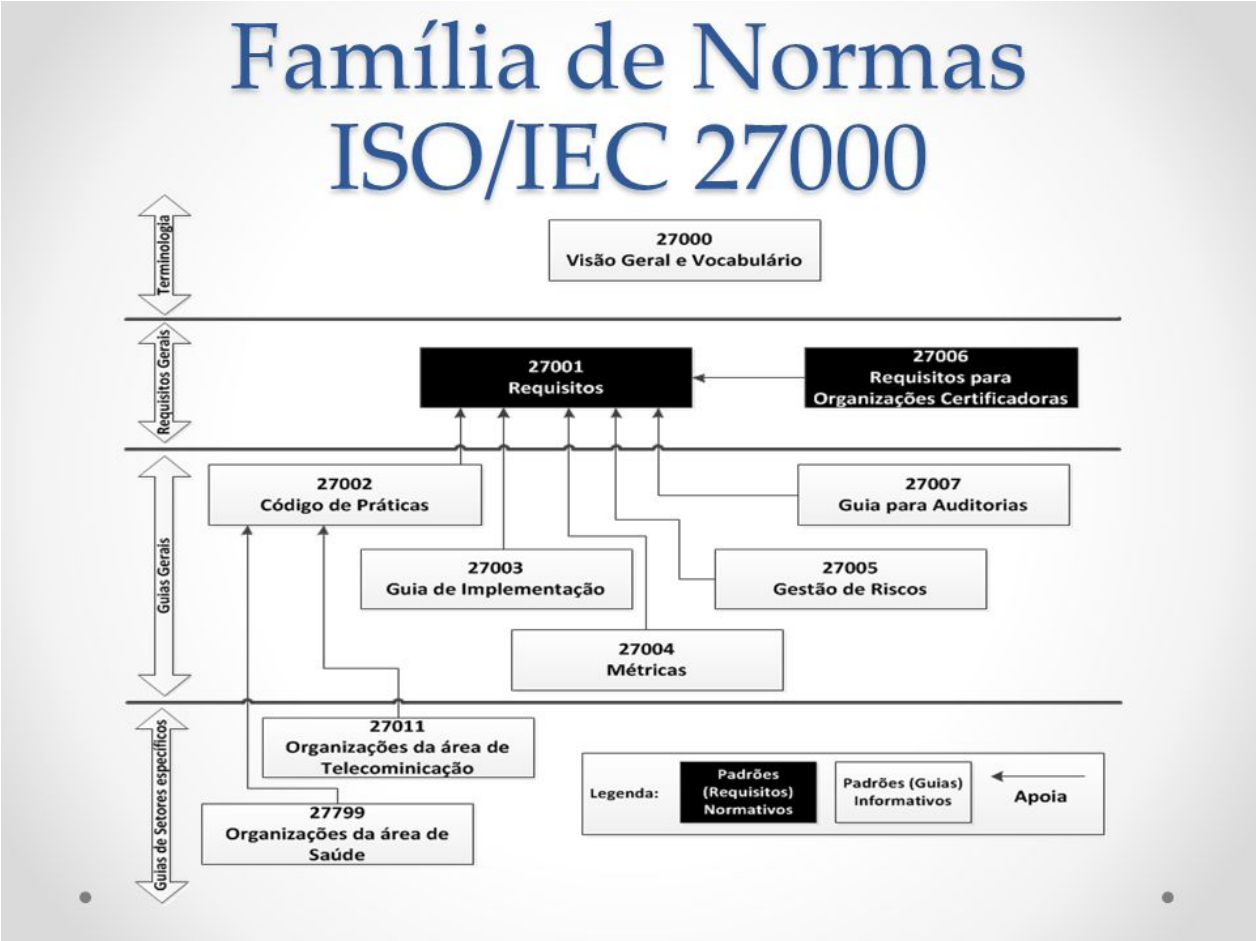

Figura 02 – Relacionamento da família de normas 27000.

Fonte: http://slideplayer.com.br/slide/2450398/

Tratando-se especificamente da ABNT NBR ISO/IEC 27005 o objetivo é montar uma gestão de riscos de segurança da informação atendendo os requisitos da norma ABNT NBR ISO/IEC 27001.

A ABNT NBR ISO/IEC 27005, "fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da informação" (ABNT NBR ISO/IEC 27005, 2011, p. 5).

Não faz parte do escopo desse trabalho a implantação de uma gestão de riscos, no entanto, fez-se necessário o estudo dessa norma, já que para implantação de uma política de segurança da informação recomenda-se uma prévia análise de riscos.

3 Desenvolvimento da política de segurança da informação

A análise da bibliografia e normas anteriormente citadas guiou o trabalho através dos seguintes passos, que estão dispostos na ordem em que foram executados:

1. Escopo
2. Classificação da informação;
3. Análise de riscos;
4. Definição dos controles;
5. Criação da Política de Segurança da Informação;
6. Elaboração de documentos auxiliares;
7. Treinamento dos usuários.

3.1 Escopo

O trabalho aconteceu nas Lojas Mib uma empresa de comércio varejista criada em 1998, com sede na Bahia, que também possui lojas no sudeste do país. Esse trabalho se deu nas lojas situadas em Montes Claros - Minas Gerais.

A empresa possui mais de 9 funcionários e menos de 50, classificada como empresa de pequeno porte, de acordo com critério adotado pelo Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE)[2].

[2]http://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/Anuario%20do%20Trabalho%20Na%20Micro%20e%20Pequena%20Empresa_2013.pdf

O trabalho foi realizado no ambiente administrativo da empresa, ou seja, em seus escritórios. Ali se encontra grande parte do parque tecnológico da organização, incluindo servidores, estações de trabalho e periféricos. Também é o local onde a informação recebe seu tratamento.

Segundo nomenclatura utilizada na empresa as áreas onde o trabalho foi aplicado são: Atendimento, Vendas, Administrativo, Financeiro, Cobrança, Diretoria e TI.

Os sujeitos da pesquisa foram todos os colaboradores que participam do fluxo de informação na empresa, além da sua diretoria.

3.2 Classificação da informação

Antes de elaborar a PSI, era importante saber que informação tinha mais relevância para a empresa, dessa forma, a PSI buscaria tratar essa informação de maneira segura, com intuito de que a informação não fosse modificada, divulgada de forma não autorizada ou torna-se indisponível quando solicitada. O primeiro passo então foi classificar a informação.

Como não há níveis padrões de classificação da informação estabelecidos, foi definido em reunião com a diretoria da empresa, que seriam utilizados três níveis de classificação, são eles:

- Confidencial - rótulo vermelho, informações que devem ser protegidas contra acesso externo. Somente pessoas autorizadas podem acessá-las, sua violação pode comprometer o funcionamento da organização, causar perdas financeiras, quebrar a imagem da empresa e possível perda de clientes para a concorrência;
- Interna - rótulo amarelo, são informações que não devem sair do âmbito organizacional. Todos os colaboradores da empresa têm acesso a esse tipo de informação, a divulgação externa dessa informação não causará danos consideráveis a organização;
- Pública - rótulo verde, informações que podem ser divulgadas ao público em geral, essa informação não tem valor interno para empresa.

Toda informação recebeu um rótulo em acordo com sua classificação, conforme descrito acima, nos formatos lógico e físico. Para facilitar a identificação da informação, ficou definido que a etiqueta utilizada para rotular a informação estaria sempre visível na frente dos dispositivos, independente de qual fosse, isso para o meio físico. No meio lógico os arquivos receberiam a rotulação no nome do arquivo e também em sua primeira página, caso fosse possível. Assim, o nível de classificação da informação seria identificado logo no primeiro momento de contato com a mesma.

Para classificar a informação foram feitas diversas reuniões com os proprietários da informação, no caso da empresa estudada os gerentes de cada área, até que eles conseguissem definir com clareza a classificação para cada tipo de informação.

3.3 Análise de risco

Após classificar a informação foi preciso saber a que ameaças essas informações estavam sujeitas, dessa forma, foi feita uma análise de riscos sobre as informações.

Por ser um método simples e de fácil entendimento foi escolhido o método qualitativo para a análise de riscos.

Com a lista dos ativos de informação, foram localizadas suas ameaças, as ameaças encontradas foram colocadas em uma tabela com 5 colunas (ameaças, valor da consequência, probabilidade de ocorrência, medida do risco, ordem da ameaça).

Para o preenchimento da tabela, a primeira etapa consiste em avaliar o valor da consequência, ou seja, o impacto caso a ameaça seja concretizada. Foi definido um valor de 1 a 5, onde 1 é o risco mais baixo e 5 o risco mais alto, para cada ameaça. Na segunda etapa o mesmo foi feito, agora para a coluna probabilidade de ocorrência, que indica com que frequência a ameaça ocorre.

Na terceira etapa foi feito o cálculo da medida do risco multiplicando (valor da consequência X probabilidade de ocorrência), esse valor indica o grau de risco da ameaça. Por último, na coluna ordem da ameaça, foram ordenadas as ameaças de acordo com a medida do risco calculado anteriormente. Para ilustrar melhor a análise acima descrita segue a tabela utilizada no desenvolvimento desse trabalho. Para preservar a empresa estudada, a tabela abaixo contém dados fictícios.

Ameaças	Valor da consequência	Probabilidade de ocorrência	Medida do risco	Ordem da ameaça
Ameaça A	5	2	10	2
Ameaça B	2	4	8	3
Ameaça C	3	5	15	1
Ameaça D	1	3	3	5
Ameaça E	4	1	4	4

Tabela 01 - Análise de riscos

Foi feita uma reunião com a diretoria e todos os proprietários de informação da empresa para definir os critérios de avaliação dos riscos. Ficando definido que, toda medida do risco igual ou superior a 4 seria tratada, o risco que tivesse medida 1 seria aceito, e riscos medindo 2 e 3 seriam analisados e avaliados para estipular ou não o seu tratamento. Essa análise e avaliação fica a cargo do comitê de segurança da informação.

A tabela acima exposta segue modelo sugerido pela ABNT NBR ISO/IEC 27005, essa tabela foi suficiente para o desenvolvimento desse trabalho, entretanto, a norma também apresenta outras tabelas indicando situações apropriadas para o uso de cada uma. Ainda assim, a norma inclui a possibilidade da criação de uma tabela personalizada, de acordo com as necessidades organizacionais.

3.4 Definição dos controles

A definição dos controles foi uma das fases mais desgastantes do projeto, foram necessárias diversas reuniões com a diretoria e gerência das áreas, os colaboradores da empresa viam os controles como burocracia, em alguns casos pensavam estarem sendo questionados seu caráter, foi necessário o início de um trabalho de conscientização explicando bem os controles e os benefícios de sua utilização. Assim foram definidos os controles um a um.

Os controles foram extraídos da norma ABNT NBR ISO/IEC 27002, baseando-se nas diretrizes fornecidas pela norma complementar 03 do DSIC e nos requisitos da

norma ABNT NBR ISO/IEC 27001. Outros fatores, com mesmo grau de importância, também foram levados em conta durante a escolha dos controles, como classificação da informação, análise de riscos, custo para implantação dos controles, necessidades da empresa e futuras demandas.

Feito isso, tudo estava pronto para a elaboração do texto da política de segurança da informação.

3.5 Criação da política de segurança da informação

Elaborar textos nem sempre é fácil, o escritor deve-se ater aos por menores, cuidar para que não haja má interpretação, ambiguidade ou brechas na sua escritura. O texto deve ser claro, para que qualquer pessoa possa entender o que o autor quer passar, além disso não deve conter erros ortográficos ou gramaticais. E com a política de segurança da informação não é diferente. Diante disso, foram feitas diversas revisões do texto, tentando não deixar nenhuma aresta aberta na PSI.

O desenvolvimento do texto ocorreu levando em conta todo o material estudado até aqui, bibliografia, normas, classificação da informação, análise de riscos e definição dos controles. A diretoria sugeriu alguns pontos importantes para empresa que também foram incluídos no texto.

Nessa fase foi definido os colaboradores que integrariam o comitê de segurança da informação, grupo responsável por operar, manter, monitorar, analisar criticamente e melhorar a PSI. Para cumprir seu objetivo o comitê utilizaria o ciclo PDCA com intuito de garantir a melhoria contínua da PSI. Abaixo é descrito a aplicação do PDCA as políticas de segurança da informação.

- *Plan* (planejar): Como o ciclo PDCA é aplicado à uma PSI já estabelecida, nessa fase serão levantados os riscos e controles de segurança que serão tratados, modificados ou incorporados;
- *Do* (fazer): Nessa fase serão executadas as atividades oriundas da etapa de planejamento. Também serão realizadas ações de treinamento e conscientização referente as mudanças estabelecidas na PSI;

- *Check* (checar): Aqui acontece o monitoramento e análise crítica dos controles implementados pela PSI, os resultados são avaliados pelo comitê e suas decisões alimentam o próximo passo;
- *Act* (agir): A última fase do ciclo irá busca a melhoria contínua da PSI, através da implementação de ações corretivas, preventivas e melhorias, a partir dos resultados da fase anterior.

Para a implantação da política de segurança da informação não foi necessário nenhum investimento direto, todo trabalho foi feito a partir do que a empresa já possuía, o que demonstra a viabilidade do projeto em pequenas organizações.

Após todas as tarefas desempenhadas, o texto final foi apresentado a diretoria, que autorizou a divulgação da PSI, a mesma foi apresentada no auditório da empresa na presença de todos os colaboradores e da diretoria.

A PSI, produto desse trabalho, não será apresentada aqui, visando preservar a segurança da informação da empresa Lojas Mib, contudo, todos os passos para a criação da PSI foram apresentados de forma detalhada, possibilitando a aplicação desse mesmo método em outras empresas, com o benefício da não influência da PSI desenvolvida por esse estudo, forçando a criação de uma nova PSI totalmente personalizada de acordo com a necessidade.

3.6 Elaboração de documentos auxiliares

Para dar suporte a PSI foram elaborados documentos auxiliares, o primeiro deles foi a "Declaração de Comprometimento", um documento que atesta a aprovação da PSI e o comprometimento da diretoria da empresa quanto ao cumprimento da mesma. A diretoria, ainda com o propósito de fortalecer o engajamento dos colaboradores com a PSI, criou um e-mail padrão intitulado "E-mail de boas-vindas", esse e-mail declarava a felicidade da empresa em receber um novo funcionário e reforçava o dever do colaborador em cumprir com a PSI.

Em seguida foi criado o documento "Comitê de Segurança da Informação" a fim de estabelecer formalmente o comitê, esse documento possui as responsabilidades atribuídas e a discriminação dos integrantes do comitê de segurança da informação.

Também foi criado o "Formulário de Registro de Incidentes de Segurança" com a ideia de registrar incidentes para posteriores análises, investigações e ações corretivas.

Foi necessário um "Termo de Responsabilidade" comprovando o conhecimento da PSI pelo funcionário, a fim de subsidiar a empresa em possíveis disputas judiciais. Criou-se também uma "Política de Backup", esclarecendo os procedimentos técnicos que seriam adotados para realização dos backups da organização.

Por fim, criou-se o documento "Plano de Continuidade de Negócio", que continha um plano para continuidade dos recursos e serviços mais críticos da empresa.

3.7 Treinamento dos usuários

Mesmo que haja uma estrutura segura e tolerante a falhas é nas pessoas que começa e termina a segurança, por isso, o treinamento e conscientização dos colaboradores é essencial, entender o porquê da utilização dos controles e a consequência de não usá-los é fundamental para o sucesso de uma política de segurança da informação. Pensando nisso, o treinamento elaborado para empresa foi dividido em duas partes.

Na primeira parte a empresa promoveu uma confraternização para que fosse feito o treinamento, onde, reuniu-se todos os colaboradores da empresa, fora do horário de expediente e em local externo. Nessa etapa foi passado os conceitos gerais de segurança da informação, as ameaças, os riscos e os impactos. Também foi explicado de forma clara (não técnica), alguns ataques comumente encontrados, enfatizando os ataques de engenharia social. Foram exibidos vários casos de ataques ocorridos no mundo, com uma breve análise explicando os motivos, os impactos, o tratamento e as soluções encontradas para os incidentes. Ainda nessa etapa foi mostrado casos de negligência por parte dos funcionários e como isso afetou consideravelmente a segurança de empresas. Essa etapa foi finalizada com a mensagem de que, a segurança de uma empresa é tão forte quanto o seu elo mais fraco.

Na segunda etapa, grupos específicos da empresa foram reunidos, nesse treinamento abordou-se os controles específicos utilizados por cada grupo. Nessa etapa a política de segurança da informação foi lida, relacionando os controles utilizados ao texto da PSI, abordou-se também, o ciclo de vida da informação

manipulada pelo grupo e como mantê-la segura em cada passo. Por fim, dicas de como manter uma conduta e um ambiente organizacional seguro foram passadas ao grupo.

Com a finalidade de manter os colaboradores da empresa em alerta, foram adicionados cartazes em lugares estratégicos contendo dicas, controles ou informações relativas à segurança da informação, o comitê de segurança da informação ficou responsável por passar um e-mail mensal, com abordagem humorística, contendo controles que devem ser seguidos pela empresa, fazendo sempre relação com a PSI.

4 Conclusão

Conforme exposto, esse trabalho vem atender pequenas empresas que não possuem nenhum ou poucos controles de segurança, também é destinado a empresas que possuem controles, mas não possuem uma PSI escrita e efetiva. O método usado, foi desenvolvido a partir das normas ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27005 e a DSIC/GSIPR NORMA COMPLEMENTAR n 03, devido ao sucesso da implantação de políticas de segurança da informação na empresa de pequeno porte Lojas Mib, utilizando o método apresentado nesse trabalho, o mesmo pode servir como guia para implantação em outras empresas de mesmo porte.

A implantação da PSI na empresa estudada, não gerou investimentos diretos para a empresa, o que não garante que outras organizações também implantaram a PSI sem custos, mas garante que, com o estudo de normas e padrões conhecidos e sua devida adaptação a realidade da empresa, o investimento pode ser pequeno e absorvido pela organização.

A oportunidade de utilizar um ambiente de produção como da empresa Lojas Mib neste estudo, mostrou as dificuldades encontradas por pequenas empresas na implantação de uma PSI, mostrou que para atingir um patamar de segurança desejável nem sempre é necessário dispor de altos investimentos, mas sim uma seleção criteriosa dos controles a partir da realização de uma classificação da informação e análise de risco. Como a PSI é parte integrante de um Sistema de Gestão de Segurança da Informação, pode-se considerar, que a implantação de Políticas de Segurança da Informação é um importante passo para criação de um SGSI.

Para posteriores estudos, sugere-se aplicar o método aqui utilizado em empresa de médio porte, a fim de constatar sua eficiência. Implantar um SGSI em uma pequena empresa pode ser um grande desafio. Seria possível?

Referências

ARAÚJO, L. G. S; BEZERRA, E. K; COELHO, F. E. S. **Gestão da Segurança da Informação**. Rio de Janeiro: RNP/ESR, 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da Informação: Técnicas de Segurança: Sistema de gestão da segurança da Informação: Requisitos. 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da Informação: Técnicasde Segurança: Código de prática para controles de segurança de informação. 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005**: Tecnologia da Informação: Técnicas de Segurança: Gestão de riscos de segurança de informação. 2011.

BRASIL. GSIPR. **INSTRUÇÃO NORMATIVA N 01**, DE 13 DE JUNHO DE 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acesso em: 08 mar. 2017, 10:28:45.

BRASIL. GSIPR/DSIC. **NORMA COMPLEMENTAR N 03**, DE 30 DE JUNHO DE 2009. Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf>. Acesso em: 08 mar. 2017, 10:35:10.

BRASIL. TCU. **Manual de Boas Práticas em Segurança da Informação.** 4. ed. Brasília. 2012. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 28 abr. 2017, 09:39:15.

FONTES, E. L. G. **Políticas de Segurança da Informação**. Rio de Janeiro: RNP/ESR, 2015.

MONTEIRO, I. L. C. O. **Proposta De Um Guia Para Elaboração De Políticas De Segurança Da Informação E Comunicações Em Órgãos Da Administração Pública Federal**. Universidade de Brasília. 2009. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/ina_lucia.pdf>. Acesso em: 19 abr. 2017, 15:46:46.

NETTO, A. S; SILVEIRA, M. A. P. Gestão da Segurança da Informação: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação.** Vol. 4, No. 3, p. 375-397, 2007.

OLIVEIRA, M. S. et al. Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica.** Vol. 06, Nr. 02, p. 37-49, 2015.