CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Segurança da Informação

Bruna Sasse

UTILIZAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM EMPRESA DE MÉDIO PORTE

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Segurança da Informação

Bruna Sasse

UTILIZAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM EMPRESA DE MÉDIO PORTE

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação do (a) Prof. Esp. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação

Americana, SP

2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Sasse, Bruna
S264u Utilização de políticas de segurança da informação em empresa de médio porte. / Bruna Sasse. – Americana: 2015.
44f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Edson Roberto Gaseta

1. Segurança em sistemas de informação I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681,518,5

BRUNA SASSE

UTILIZAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO EM EMPRESA DE MÉDIO PORTE

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnóloga em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 27 de junho de 2015.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
Fatec Americana

Clerivaldo José Roccia (Membro)
Mestre
Fatec Americana

Alberto Martins Júnior (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus que permitiu que tudo isso acontecesse.

A instituição, seu corpo docente, direção e administração pela oportunidade proporcionada.

Ao orientador Edson R. Gaseta pelo suporte dado durante a elaboração do trabalho.

Aos meus familiares pelo amor, incentivo e apoio incondicional.

Aos meus amigos, companheiros de trabalho e a todos que direta ou indiretamente fizeram parte da minha formação.

DEDICATÓRIA

Aos meus pais que sempre me incentivaram para a realização dos meus ideais, encorajando-me a enfrentar todos os momentos difíceis da vida.

RESUMO

Este trabalho apresenta uma proposta para melhoria da política de segurança da informação de uma empresa de médio porte. Para atender a esta proposta foram apresentados conceitos sobre segurança da informação, políticas de segurança da informação e aspectos importantes associados à gestão destas políticas. Foi realizado um estudo de caso em uma empresa de médio porte, situada na Região Metropolitana de Campinas (RMC), considerando os principais aspectos de gestão de políticas de segurança da informação, em conformidade com a ISO 27002. Este estudo de caso foi descrito detalhadamente. Foram descritos e considerados todos os aspectos de política de segurança da informação existentes na empresa estudada, bem como a gestão desta política. Os resultados obtidos foram analisados, usando abordagem estatística. Em função destes resultados foram apresentadas diversas propostas de melhorias na política de gestão da empresa, sempre em conformidade com a norma ISO 27002, justificando-se cada uma delas. Sugestões para trabalhos futuros foram feitas, considerando-se a necessidade de um novo estudo de caso na mesma empresa, após a implementação das melhorias propostas, para verificar a evolução ocorrida na gestão da política de segurança adotada.

Palavras Chave: Gestão de Política de Segurança da Informação; ISO 27002; Segurança da Informação.

ABSTRACT

This essay presents a proposal for improvement of information security policy in a medium-sized company. To meet this proposal were presented concepts on information security, information security policies and important aspects associated with the management of these policies. It was conducted a case study in a medium-sized company, located in the Metropolitan Region of Campinas (RMC), considering the main aspects of information security policy management in accordance with ISO 27002. This case study was described in details. They were described and considered all the security policy aspects of the existing information in the studied company, and the management of this policy. The results were analyzed using statistical approach. Based on these results were presented several proposals for improvements in the company's management policy, always in accordance with the ISO 27002 standard, justifying each one of them. Suggestions for future work were made, considering the need for a new case study in the same company after implementation of the proposed improvements, to check the developments ocurred in the security management policy adopted.

Keywords: *Security Policy Information Management; ISO 27002; Information Security.*

SUMÁRIO

LISTA DE ILUSTRAÇÕES

1 INTRODUÇÃO

Atualmente cada vez mais a segurança da informação é um assunto importante nas organizações, e tem como base um conjunto de normas, referências, procedimentos e políticas. Tem como objetivo proteger uma informação fazendo com que uma organização tenha sua meta alcançada nos seus negócios.

Uma política de segurança da informação é uma ferramenta que faz com que diminua as ameaças do negócio, relacionadas à dependência no uso dos recursos de informação para o funcionamento total da organização (FONTES, 2006).

Este trabalho apresenta uma abordagem de como aumentar o nível de segurança baseado no negócio da empresa e nos requisitos de segurança de uma norma. A partir disso, sugere-se a implementação de uma gestão de política que possa realizar a segurança de uma organização, atingindo seus objetivos. Para que a informação esteja protegida é preciso garantir disponibilidade, integridade e confidencialidade da informação, entre outros aspectos (FONTES, 2006).

O **problema** proposto neste trabalho foi a determinação e gestão dos aspectos de segurança atendidos pela empresa, baseados na análise do que há na empresa e o que diz a norma de segurança da informação.

Em decorrência do problema apresentado, a **pergunta** pertinente a ele foi: Quais são as práticas de gestão de segurança da informação exercitadas por uma empresa em relação às normas adotadas?

Algumas hipóteses que foram levantadas, relacionadas ao problema apresentado foram:

a) A empresa pode não permitir exposição dos seus dados;

b) O plano de segurança da empresa contempla poucos aspectos da norma adotada ou não tem um bom gestor;

c) O grau de maturidade da empresa está próximo dos aspectos de segurança da empresa, e em consequência, tem um bom gestor.

O **objetivo geral** deste trabalho foi sugerir o uso da gestão de políticas para aumentar a segurança dos recursos tecnológicos da empresa.

Os **objetivos específicos** foram:

- Estudar aspectos de segurança da informação, melhorando a compreensão sobre o assunto;

- Estudar as políticas de segurança da informação, facilitando a compreensão sobre a necessidade da existência de uma política de segurança em empresas de maneira geral;

- Explicar suas possíveis implementações, mostrando algumas alternativas de solução;

- Estudar aspectos de uma boa gestão de políticas de segurança da informação, destacando as características de uma boa gestão;

- Aumentar a confidencialidade, disponibilidade e integridade usando políticas de segurança da informação, atendendo o tripé de segurança da informação;

- Realizar um estudo de caso em um ambiente pertinente, verificando em que estágio se encontra a política de segurança da empresa analisada;

- Exibir uma análise dos pontos favoráveis e de possíveis pontos desfavoráveis utilizando os resultados do estudo de caso, usando os dados obtidos no estudo de caso.

A **justificativa** para a escolha deste tema foi a necessidade de aquisição de novos conhecimentos sobre políticas de segurança, em função do trabalho executado pela autora, Sabe-se que uma política de segurança tem de ser criada antes do acontecimento de problemas que possam afetar a segurança da informação, visando a prevenir ou mitigar os efeitos destes problemas

(FERREIRA; ARAUJO, 2008). Vale lembrar que uma gestão de políticas de segurança da informação é uma tendência que veio para ficar (BARBIERI, 2013).

Os **procedimentos metodológicos** usados neste trabalho foram: pesquisa de abordagem hipotético dedutiva, além de ter utilizado o método de procedimentos. Foram utilizadas as quatro modalidades (comparativo, histórico, estudo de caso e estatístico), pois a pesquisa foi referente á gestão de políticas de segurança, baseada no comparativo do que é exercitado na empresa e o que diz a norma adotada pela mesma. Levantamento do histórico das normas que a empresa utiliza e um estudo de caso referente ao comparativo de quais as normas a empresa adota e o que diz as politicas de segurança da norma adotada pela empresa. A análise estatística dos resultados foi necessária para situar a posição da empresa no contexto do tema tratado no trabalho.

O tipo de pesquisa, quanto à natureza, foi pesquisa aplicada baseada nas politicas de segurança da informação existentes. Quanto ao objetivo geral, foi exploratória, pois foi realizado um estudo preliminar das politicas de segurança da empresa e da norma adotada pela mesma. A partir disso foi feito um levantamento bibliográfico sobre segurança da informação e sua gestão, a norma adotada e dos resultados obtidos relacionados ao que a empresa pode adotar.

A técnica para obtenção de dados foi coleta documental bibliográfica e dos resultados obtidos no estudo de caso realizado, a partir de relatórios de pesquisa e relatórios da empresa e através de observações feitas quanto aos aspectos de segurança da informação.

Este trabalho foi **organizado** da seguinte forma: no Capítulo 1 foram apresentados conceitos sobre segurança da informação. No Capítulo 2 foi feito um levantamento sobre políticas de segurança da informação. No Capítulo 3 apresentou-se a norma ISO 27002. No Capítulo 4 foram apresentados o estudo de caso feito e os resultados obtidos. O Capítulo 5 apresentou uma proposta de política de segurança da informação e o Capítulo 6 apresentou as Conclusões.

2 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação é a proteção da informação e seus ativos contra fraudes, modificações não autorizadas, erros e desastres. O objetivo é proteger seus dados em todos os meios de transmissão e assegurar a continuidade do negócio, reduzir os riscos e aumentar as oportunidades do mesmo (COELHO, ARAÚJO, BEZERRA, 2014).

A segurança da informação visa garantir três princípios fundamentais: Confidencialidade, Integridade e Disponibilidade.

Confidencialidade: Proteger informações de todos, exceto daqueles que tenham direto a elas. Incluem: dados particulares do indivíduo, propriedade intelectual das empresas e segurança nacional para países e governos. Garantir a confidencialidade possibilita que as pessoas não tenham conhecimento da informação de qualquer forma sem que tenham autorização.

Integridade: Lida com a validade e precisão dos dados. Os dados tem integridade se são dados não alterados, válidos e precisos. Visa à garantia de não violar os dados para expor, alterar ou excluir o mesmo.

Disponibilidade: A informação é acessível por usuários autorizados sempre que solicitados. A ausência da disponibilidade é quando há tentativa de acesso a uma informação e não se obtém o acesso (SÊMOLA, 2003). A Figura 1 ilustra os conceitos apresentados por Sêmola.

Figura 1 - Os Três Pilares da Segurança da Informação.

Fonte: Maia (2013).

2.1 DADOS X INFORMAÇÃO

Os dados são elementos que possuem formato bruto – texto, imagens, sons, nomes, código – usados em forma individual pode não assimilar determinada situação.

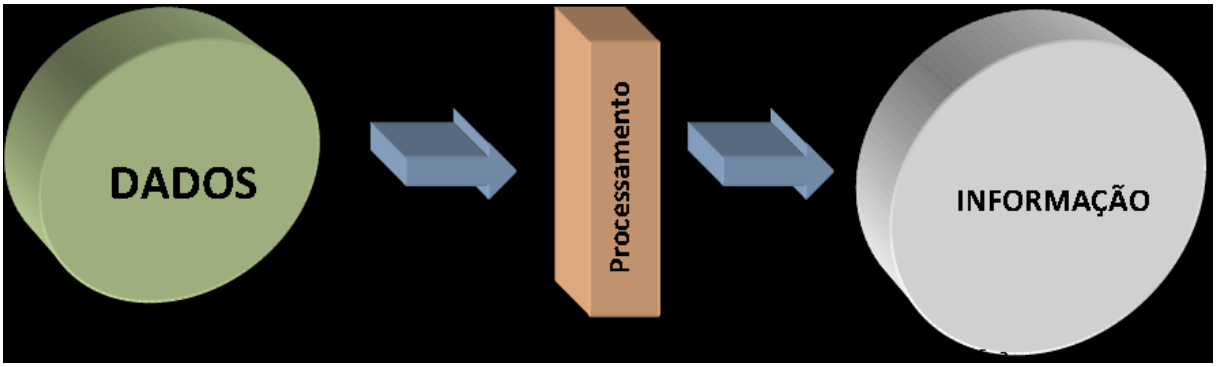
A informação é a organização dos dados concedendo significado em um contexto. O resultado do processamento dos dados é a informação (AUDY, ANDRADE, CIDRAL, 2005). A Tabela 1 mostra exemplos destes conceitos. A Figura 2 mostra os conceitos de dados X informação.

Tabela 1 - Exemplo de Dados e Informações

DADOS	INFORMAÇÕES DE UMA PESSOA
NOME DO FUNCIONÁRIO	MARIA
ENDEREÇO DO FUNCIONÁRIO	RUA CEM, Nº 2 – CENTRO
CIDADE DO FUNCIONÁRIO	AMERICANA

Fonte: Autoria Própria.

Figura 2 - Dados X Informação.



Fonte: Adaptado de Ataíde (2003).

2.2 CICLO DE VIDA DA INFORMAÇÃO

O ciclo de vida da informação divide-se em quatro fases, a saber, Manuseio, Armazenamento, Transporte e Descarte.

Manuseio: É o ponto em que a informação é elaborada e pode ser através da autenticação de uma senha de acesso.

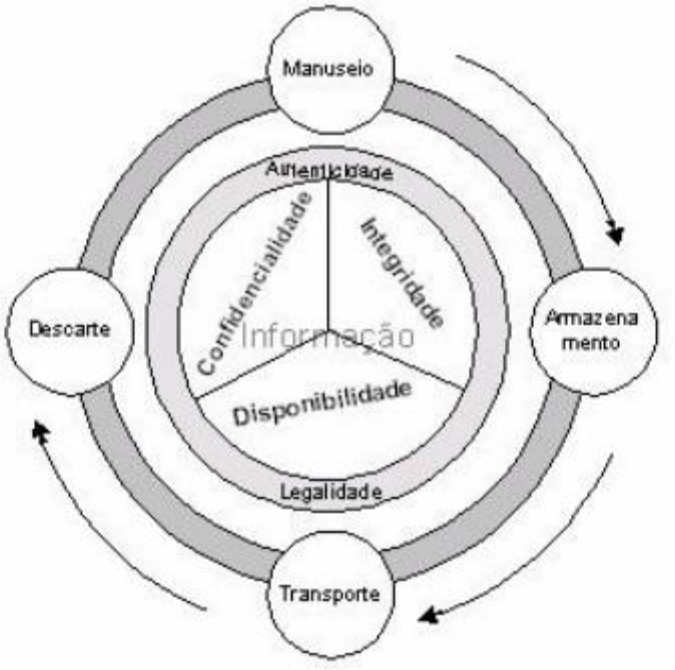
Armazenamento: É o ponto em que essa informação é guardada, podendo ser em mídias removíveis ou em banco de dados.

Transporte: Quando a informação é enviada, podendo ser via telefone ou em muitos casos via *e-mail*.

Descarte: Quando a informação é descartada, o que pode considerar sendo a mesma apagada do computador ou quando impressa sendo jogada no lixo da empresa.

O ciclo de vida da informação é formado a partir do momento em que as informações são colocadas em situação de risco, a partir daí os ativos entram em ação para fazer uso da informação. A violação acontece quando o controle falha ou há sinais de descuidos podendo afetar o trabalho realizado para retenção de riscos (SEMÔLA, 2001). A Figura 3 ilustra o ciclo de vida da informação.

Figura 3 - Ciclo de Vida da Informação.



Fonte: Laureano e Morais (2014).

2.3 RECURSOS UTILIZADOS PARA MITIGAR FALHAS DE SEGURANÇA DA INFORMAÇÃO

Atualmente muitos recursos de software e hardware são utilizados para mitigar falhas de segurança da informação. Podem ser citados (entre outros) os seguintes recursos: Sistemas de Detecção de Intrusões (IDS); Sistemas de Prevenção a Intrusões (IPS); uso de *Firewalls*, uso de antivírus, criptografia, normas e políticas de segurança da informação (que serão tratadas no próximo capítulo).

O IDS é um software que automatiza o processo de detecção de intrusos e identifica o ataque após o ocorrido. Através do formato em que foram desenvolvidas as tecnologias IDS, são classificadas em: *wireless*, baseada em rede, análise do comportamento da rede e baseada em *host*. Vale ressaltar que um IDS detecta a tentativa de ataque, mas não trata o ataque. Para isso recomenda-se o uso de sistemas IPS.

Um sistema IPS é um software que tem todas as capacidades de um sistema de detecção de intrusos e pode também tentar parar possíveis incidentes antes de ocorrem, impedindo a ação do atacante.

O uso de *Firewalls* serve para fiscalizar tudo que entra e sai do computador. Seu objetivo é bloquear todos os arquivos que apresentem algum tipo de risco ao sistema operacional. Após a definição de uma política de segurança local apenas o tráfego autorizado será permitido passar. O *firewall* utiliza quatro técnicas para controlar o acesso e estabelecer a política de segurança. Dentre elas o controle de serviço, o controle de direção, o controle de usuário e o controle de comportamento (STALLINGS, 2008).

O uso de antivírus serve para proteger o computador de ações de vírus. O objetivo do antivírus é exclusivamente para detectar ameaças que estão prestes a atingir ou já tenham atingido um computador. Eles proporcionam uma prevenção da entrada dos vírus, a detecção da contaminação e a remoção quando for detectado o vírus.

A criptografia serve para codificar mensagens garantindo a proteção das informações fazendo com que a privacidade dos indivíduos esteja reservada. Tem como objetivo fazer com que o algoritmo de criptografia seja complexo e atualizado o suficiente para cumprir suas funcionalidades. Há algoritmos de chave simétrica que fazem uso da mesma chave para codificação e descodificação. Há também algoritmos de chave assimétrica, que as chaves de codificação e decodificação são diferentes e em função disso a chave de decodificação não pode ser derivada da chave de codificação (TANENBAUM, 2011).

3 POLITÍCAS DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação compõe ativos de informação e estabelece a responsabilidade legal para todos os usuários. Deve ser comunicada, aplicada e cumprida por todos os departamentos de uma instituição. Visa garantir a viabilidade e seu uso deve ser somente por pessoas autorizadas que necessitem dela para cumprir sua atividade dentro da instituição buscando reduzir a probabilidade de fraudes de informações.

> A política de segurança é composta por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente, de modo a garantir a sua confidencialidade, integridade e disponibilidade (FERREIRA; ARAUJO, 2008, p. 36).

3.1 SOBRE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação de uma empresa determina normas e procedimentos que atendam a intenção de proteger a informação, podendo reduzir riscos para a operação do negócio da empresa.

Todos os bens e dados que uma empresa possui fazem parte de seu patrimônio. A política de segurança da informação é uma ferramenta importante que, ao ser implementada corretamente, diminui a probabilidade de ameaças que influenciam na perda de informação. A política de segurança não estabelece métodos e mecanismos que são específicos para a proteção da informação, mas concedem responsabilidades e certos direitos às pessoas que lidam com essa informação. Sua implementação é a partir da aplicação de regras que podem limitar o acesso de uma entidade às informações e bens.

Em uma empresa é importante implementar a política de segurança, uma vez que a informação é um bem de valor abstrato, e que não há apenas meios tecnológicos e informatizados para protegê-la contra danos e ataques internos e externos. Com isso, a empresa precisa de uma Política de Segurança da Informação

bem estruturada, com a capacidade de obter uma solução que faça com que as informações sejam íntegras e seguras.

3.2 ETAPAS PARA O DESENVOLVIMENTO DE UMA POLITICA DE SEGURANÇA DA INFORMAÇÃO

Antes de implantar a segurança, é preciso ter conhecimento de seu ambiente e o que ele pode proporcionar. Através disso devem ser priorizados os critérios mais instáveis e que possam precisar de uma maior cautela e que os mesmos sejam determinantes para o futuro da organização.

A Tabela 2 destaca as fases para o desenvolvimento de uma Política de Segurança da Informação:

Tabela 2 - Etapas para o desenvolvimento de uma Política de Segurança da Informação.

FASES	DESCRIÇÃO	FASES	DESCRIÇÃO
Fase I	**Levantamento de Informações**	**Fase II**	**Desenvolvimento de Conteúdo da Política e Normas da Segurança**
1.1	Obtenção dos padrões, normas e procedimentos de segurança já existentes para análise.	2.1	Gerenciamento da política de segurança: -Definição da segurança da informação; -Objetivo do gerenciamento; -Fatores críticos de sucesso; -Gerenciamento da versão e manutenção da política; -Referência para outras políticas, padrões e procedimentos.

1.2	Entendimento das necessidades e uso dos recursos da tecnologia da informação (sistemas, equipamentos e dados) nos processos de negócios.	2.2	Atribuição de regras e responsabilidades: -Comitê de segurança da informação; -Proprietário das informações; -Área de segurança da informação; -Usuários de informações; -Recursos humanos; -Auditoria Interna.
1.3	Obtenção de informações sobre os ambientes de negócio: -Processos de negócios; -Tendências de mercado; -Controles e áreas de risco.	2.3	Critérios para classificação das informações: -Introdução; -Classificando a informação; -Níveis de classificação; -Reclassificação; -Armazenamento e descarte; -Armazenamentos e saídas.

1.4	Obtenção de informações sobre o ambiente tecnológico: -*Workflow* entre ambientes; -Redes de aplicações; -Plataformas computacionais.	2.4	Procedimentos de segurança de informações: -Classificação e tratamento da informação; -Notificação e gerenciamento de incidentes de segurança da informação; -Processo disciplinar; -Aquisição e uso de hardware e software; -Proteção contra software malicioso; -Segurança e tratamento de mídias; -Uso de *Internet*; -Uso de correio eletrônico; -Utilização de recursos de TI; -Backup; -Manutenção de teste e equipamentos; -Coleta e registro de falhas; -Gerenciamento e controle da rede; -Monitoração do uso e acesso aos sistemas; -Uso de controles de criptografia e gerenciamento de chaves; -Controle de mudanças operacionais; -Inventário dos ativos de informação; -Controle de acesso físico às áreas sensíveis; -Segurança física; -Supervisão de visitantes e prestadores de serviço;

FASES	DESCRIÇÃO	FASES	DESCRIÇÃO
Fase III	**Elaboração dos Procedimentos de Segurança da Informação**	**Fase IV**	**Revisão, Aprovação e Implantação das Políticas, Normas e Procedimentos de Segurança da Informação.**
3.1	Pesquisas sobre as melhores práticas em segurança da informação utilizadas no mercado.	4.1	Revisão e aprovação das políticas, normas e procedimentos de segurança da informação.
3.2	Desenvolvimento de procedimentos e padrões, para discussão com a Alta Administração, de acordo com as melhores práticas de mercado e com as necessidades e metas da organização.	4.2	Efetiva implantação das políticas, normas e procedimentos de segurança da informação por meio das seguintes iniciativas: - Atuação junto à área responsável pela comunicação, ou área correspondente, na orientação para preparação do material promocional, de divulgação e de consulta; -Divulgação das responsabilidades dos colaboradores, bem como da importância das políticas, normas e procedimentos de segurança da informação; -Realização de palestras executivas referentes ás políticas, normas e procedimentos de segurança da informação desenvolvidas, tendo por público-alvo a Presidência, Diretorias e Gerências; -Realização de palestras referentes às políticas, normas e

			procedimentos de segurança, tendo por público-alvo outros colaboradores da organização.
3.3	Formalização dos procedimentos para integrá-los às políticas corporativas.		

Fonte: Ferreira, Araújo (2008).

A Tabela 2 também mostra as quatro principais fases para a implantação de uma política de segurança da informação. Na fase I (composta por quatro etapas), faz-se o levantamento das informações com a finalidade de se entender a missão da empresa. Na fase II (composta por quatro etapas), faz-se o anteprojeto do plano de política de segurança da informação. Após o aceite passa-se para a fase III (composta por três etapas), passa-se à elaboração dos procedimentos de segurança da informação. Na fase IV (composta por duas etapas) faz-se a revisão, aceite e posterior implementação das normas de política de segurança da informação. Vale lembrar que as etapas de treinamento, educação e revisão das normas propostas são de fundamental importância para o sucesso do plano de política de segurança da informação.

3.3 PRINCIPAIS CARACTERÍSTICAS DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As informações muitas vezes estão vulneráveis a fraudes e ameaças, revelando a grande importância da política de segurança da informação em uma empresa. Para que ela seja efetiva, deve seguir alguns aspectos:

Ser Verdadeira: apresentar a tomada de decisão da empresa e aceitar as ações da mesma.

Ser Complementada com a Disponibilidade de Recursos: Através de uma ação mostra que a política é aceita pela direção e possa ser executada ao longo do tempo.

Ser Válida para Todos: a política é válida para todos os que estão na empresa como diretores, presidentes, funcionários e estagiários.

Ser Simples: Deve ser de fácil entendimento para que todos possam interpretar de forma clara, vindo a entender o que está descrito.

Comprometimento da Alta Administração da Organização: Deve ter a aceitação da presidência para empenhar a aceitação da política por todos os outros funcionários (FERREIRA, ARAÚJO, 2008).

3.4 OBJETIVOS DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O objetivo de uma política de segurança da informação é a proteção de uma informação e que ela seja usada de maneira correta. O usuário deve estar consciente das regras de seu manuseio para garantir os três pilares de segurança da informação: confidencialidade, integridade e disponibilidade (ALEVATE, 2014).

A política de segurança da informação deve ser de fácil entendimento para que todos os usuários que venham fazer uso dela consigam interpretar de forma clara e entender os tópicos descritos. Também devem estar descritas normas de utilização e as operações que são proibidas na empresa.

Os objetivos da política são os recursos que gerenciam de forma correta a segurança da informação e que são distribuídos aos usuários como treinamentos, equipamentos e estudos (ALEVATE, 2014).

3.5 VISÃO DA EMPRESA EM RELAÇÃO A UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Após o levantamento das necessidades da instituição, o setor responsável pela criação e composição da política de segurança estabelece as questões fundamentais da política em questão. A partir disso é primordial ressaltar o que a instituição espera antes de começar um estudo para elaboração da política de segurança, sabendo que a mesma muda com o tipo de instituição em que será implantada. A elaboração da política é feita após o conhecimento do negócio

realizado pela empresa e as informações utilizadas por ela. A política tem que estar em conformidade com alguma norma, legislação e com algum regulamento interno estabelecido pela empresa (se existir). Após essas considerações para estabelecer a política, a empresa tem como base as etapas apresentadas na Tabela 2.

4 ISO 27002 – CÓDIGO DE PRÁTICA PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A segurança da Informação possui um conjunto de normas que são utilizadas nas organizações, com o objetivo de permitir uma padronização dos requisitos e procedimentos para a implementação de um SGSI – Sistema de Gestão de Segurança da Informação.

A norma NBR ISO/IEC 27002 é internacional e possui controles para garantir a segurança da informação. Ela propõe diretrizes e conceitos gerais para implementar e melhorar a gestão de segurança da informação. O objetivo da norma é assegurar as melhores práticas voltadas para controles de segurança, visando a proteção do ativo mais valioso da empresa que é a informação.

Já a NBR ISO/IEC 27001 é uma norma que possui certificações em seu sistema interno de gestão de segurança da informação.

As normas 27001 e 27002 devem ser usadas em conjunto, pois os controles existentes na norma 27002 ajudam as empresas a alcançarem as exigências da norma 27001. A parte importante da norma 27002 está dividida em 11 seções. São elas:

1- Políticas de Segurança da Informação: Deve ser criada uma política de segurança da informação da instituição, que deve abranger vários tópicos como os conceitos de segurança da informação, as políticas, os princípios, entre outros. Esta também deve ser informada a todos.

2- Organização da Segurança da Informação: Para a implementação da segurança da informação em uma instituição é preciso que seja elaborada uma estrutura para poder ser coordenada por uma pessoa ou um grupo de pessoas.

3- Gestão de Ativos: Para que os ativos da organização estejam seguros devem estar organizados e as informações classificadas através do nível de proteção.

4- Segurança em Recursos Humanos: A partir da contratação de um funcionário é preciso que o mesmo esteja informado das atividades que desempenhará principalmente no que diz respeito à segurança da informação. É importante que os

funcionários sejam treinados e preparados para colaborar com as políticas de segurança da empresa. É importante também que sejam avaliados especificamente no que diz respeito às informações sigilosas da empresa.

5- Segurança Física e do Ambiente: Os equipamentos e instalações devem estar em locais que não possuem riscos contra desastres que possam vir acontecer e também contra ameaças físicas e ambientais.

6- Gestão das Operações e Comunicações: É preciso ter a garantia do gerenciamento seguro da rede e que estejam determinados os cuidados pela gestão dos recursos de processamento das informações. Também é preciso ter um planejamento para que não haja risco de falhas e que os mesmos devem ser reduzidos.

7- Controle de Acessos: É de grande importância que as informações sigilosas estejam protegidas contra acessos não autorizados. Os usuários devem conhecer as normas e suas responsabilidades referentes ao uso de senhas e equipamentos que possuam informações de uso da empresa.

8- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação: Toda e qualquer informação da instituição deve ser protegida para garantir os três pilares de segurança da informação – disponibilidade, integridade e confidencialidade, através de meios criptográficos, entre outros.

9- Gestão de Incidentes de Segurança da Informação: Os funcionários da organização devem ser notificados quanto aos procedimentos de eventuais acontecimentos para que, se houver algum problema, a tomada de ação seja de forma rápida e precisa.

10- Gestão de Continuidade do Negócio: Deve-se sempre proteger os procedimentos contra falhas e fraudes e certificar de que se acontecer alguma coisa a tomada de ação também seja rápida e precisa. Certificando-se também que os procedimentos sejam ágeis em sua recuperação.

11- Conformidade: Visa evitar a quebra de qualquer lei criminal ou civil de qualquer quesito da segurança da informação. A partir disso é responsabilidade da instituição contratar ou não consultoria especializada para evitar a quebra da lei.

Essas seções têm, no total, 39 categorias e cada uma tem um objetivo de controle e um ou mais controles para serem aplicados (DANTAS, 2011). Vale lembrar que os objetivos de controle fornecem orientações sobre as metas a serem atingidas pela gestão da segurança da informação. São implementados para atender os requisitos identificados durante a fase de análise e avaliação de riscos (ALEVATE, 2014).

5 ESTUDO DE CASO

Este capítulo apresenta o estudo de caso realizado em uma empresa, bem como os resultados obtidos. A empresa em questão é de transporte, situada na Região Metropolitana de Campinas (RMC), com 300 funcionários. Foram analisados todos os setores da empresa, para coletar dados e verificar se estão em conformidade com a norma 27002, fazendo-se um mapeamento dos aspectos da norma, quanto à segurança da informação, atendidos pela empresa.

5.1 DESCRIÇÃO DO ESTUDO DE CASO

A empresa ABC, é uma sociedade que atua no ramo de transportes de produtos perigosos por todo o mundo visando sempre à geração de resultados e buscando a excelência através de investimentos em tecnologia, qualificação de seus colaboradores e melhoria contínua de todos seus processos. A empresa conta com 18 filiais espalhadas por todo o mundo, sendo a cidade de São Paulo, sua matriz. A empresa possui cerca de 2.500 funcionários distribuídos entre as filiais espalhadas por todo o mundo. Este estudo de caso foi feito na filial da RMC, que possui 300 funcionários.

A missão da empresa é transportar e fazer a gestão de cargas pelo modal rodoviário, agregando negócios na cadeia de suprimentos dos clientes, assegurando a satisfação de todas as partes envolvidas.

A filial 1 é onde se encontra o centro administrativo e comercial da empresa e onde foi realizado o presente estudo de caso. A empresa é classificada como de médio porte e é subdividida em departamentos de acordo com as características de cada setor. Toda parte de TI da empresa é de responsabilidade do departamento de Tecnologia da Informação e Processos.

A empresa ABC, não possui, atualmente, políticas de segurança da informação. Seus sistemas são todos abertos a qualquer usuário que for fazer uso do mesmo naquele momento. A partir disso todos que estão na empresa têm acesso ao sistema deixando-o vulnerável a fraudes. Além disso, sem a política de senha, caso aconteça alguma fraude, o departamento de TI que é responsável não consegue

identificar qual usuário cometeu o delito. Outro problema é quanto ao termo de responsabilidade da empresa. Assim que um funcionário novo é contratado não há nenhum documento do qual o mesmo fica responsável por zelar por senhas que são confidenciais a empresa, por revelar fora do âmbito profissional qualquer informação que tenha conhecimento e que possa vir a prejudicar a empresa e por acessar sistemas que não seja para necessidades de seu cargo.

5.2 ASPECTOS DE GESTÃO DA ISO 27002

Tabela 3 - Tabela ISO 27002

ITENS – ISO 27002		**ATENDE SIM / NÃO / NÃO SEI / PARCIALMENTE**			
1	Política de Segurança da Informação.		NÃO		
2	Organizando a Segurança da Informação.	SIM			
3	Gestão de Ativos.				PARCIALMENTE
4	Segurança em Recursos Humanos.		NÃO		
5	Segurança Física e do Ambiente.		NÃO		
6	Gestão das Operações e Comunicações.		NÃO		
7	Controle de Acessos.		NÃO		
8	Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.			NÃO SEI	
9	Gestão de Incidente de Segurança da Informação.		NÃO		
10	Gestão de Continuidade do Negócio.	SIM			

11	Conformidade.	SIM			

Fonte: Autoria Própria.

Vale destacar que no item 6 (Gestão das Operações e Comunicações) a empresa tem regulamento interno e que o grupo responsável por esta gestão está em conformidade com o regulamento, mas nada se sabe sobre o fato de estar em conformidade com a norma citada na tabela. O mesmo ocorre com o item 9 (Gestão de Incidentes de Segurança). O aspecto indicado no item 10 (Gestão de Continuidade de Negócios) está sob a responsabilidade de uma equipe que faz parte do planejamento estratégico da empresa, mas também não se sabe se essa equipe segue a norma ISO 27002. Em relação ao aspecto Conformidade (item 11), sabe-se que a empresa está em conformidade com a legislação, mas nada se pode afirmar quanto à conformidade com a norma ISO 27002.

Os resultados apresentados na Tabela 3 mostram o seguinte:

- 3 aspectos da norma são atendidos (cerca de 27 % do total);

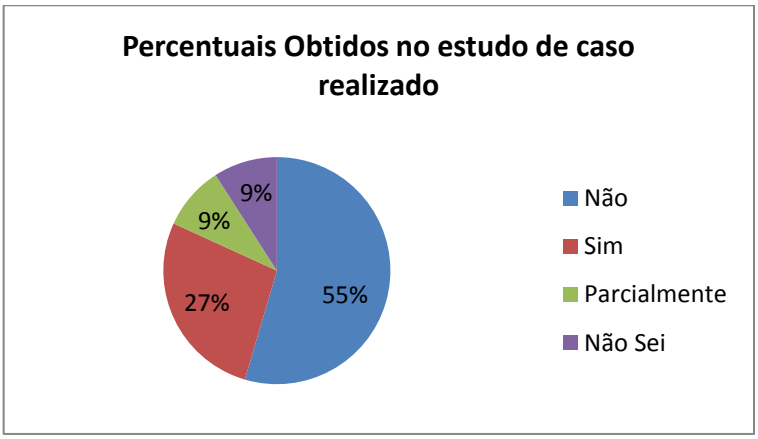
- 6 aspectos da norma não são atendidos (cerca de 54,5 % do total);

- 1 aspecto da norma é atendido parcialmente (cerca de 9 % do total);

- Não se tem informação sobre 1 aspecto da norma (se é atendido ou não) (cerca de 9% do total).

O Gráfico 1 apresenta os resultados já descritos, mostrando a situação atual da empresa estudada no que diz respeito à política de segurança da informação conforme a norma ISO 27002. Considerações sobre isso são feitas após a apresentação do gráfico.

Gráfico 1 – Resultados do Estudo de Caso realizado



Fonte: Autoria Própria.

O resultado final mostra que 27% dos aspectos da norma são atendidos pela empresa do estudo de caso feito. Portanto é recomendável que essa empresa adote medidas para agilizar o processo de conformidade com a norma ISO 27002. No próximo capítulo a autora apresenta um conjunto de sugestões para melhorar os aspectos de segurança desta empresa, no sentido de agilizar o processo de conformidade com a norma mostrada na Tabela 3.

6 ELABORAÇÃO DE POLITÍCAS PARA RESOLVER PROBLEMAS CITADOS NO ESTUDO DE CASO

Este capítulo apresenta propostas de melhoria na gestão da política de segurança da empresa estudada, na RMC. Estas propostas baseiam-se nos resultados obtidos pelo estudo de caso, descrito no Capítulo 4 deste trabalho e no conteúdo da norma ISO 27002, que trata de gestão de política de segurança da informação de instituições de maneira geral.

6.1 POLÍTICAS DE SENHA

As senhas são pontos importantes da segurança do computador. Uma senha mal escolhida ou uma senha fraca pode resultar em acessos não autorizados ou extração de recursos e informações da empresa. Todos que utilizam os acessos nos sistemas são responsáveis por tomar as medidas adequadas para proteger suas senhas. Seu objetivo é criar um padrão para a criação de senhas fortes, a proteção dessas senhas e também a frequência de mudança dessas senhas.

A criação de senha deve partir do princípio que todos os usuários e senhas de nível de sistema devem estar de acordo com as diretrizes de construção de senhas. Nenhum usuário deve usar a mesma senha de acesso para todas as contas.

Todas as senhas de nível de sistema devem ser alteradas pelo menos trimestralmente. Essas senhas devem ser substituídas pelo menos a cada seis meses. As senhas não devem ser compartilhadas com ninguém. Todas as senhas devem ser tratadas como informações confidenciais. As senhas não devem ser inseridas em mensagens de *e-mail*, ser reveladas por telefone para ninguém ou em questionários ou formulários de segurança.

6.2 DIRETRIZES DE CONSTRUÇÃO DE SENHAS

As senhas são um componente crítico de segurança da informação. Senhas servem para proteger usuário e contas; no entanto, uma senha mal construída pode

resultar na evasão de indivíduos, sistemas, dados ou rede Cisco. Esta diretriz fornece as melhores práticas para a criação de seguro de senhas.

O objetivo dessa diretriz é fornecer melhores práticas para a criação de senhas fortes. Aplica-se a todos que trabalham na empresa e que utilizam as senhas incluindo contas de nível de usuário, contas de nível de sistema, contas de web, *e-mail*, entre outros. Todas as senhas devem atender ou exceder as diretrizes a seguir:

As senhas fortes têm as seguintes características:

- Conter pelo menos 12 caracteres alfanuméricos.
- Conter letras maiúsculas e minúsculas.
- Conter pelo menos um número (por exemplo, 0-9).
- Conter pelo menos um caractere especial (por exemplo, $% ^ & * () _ + | =).

As senhas fracas têm as seguintes características:

- Conter menos de oito caracteres.
- Conter informações pessoais, como data de nascimento, endereços, números de telefone ou nomes de membros da família.
- Conter informações relacionadas com o trabalho, tais como nomes de construção, comandos do sistema, sites, empresas, *hardware* ou s*oftware*.
- Conter padrões numéricos.

O usuário nunca deve anotar uma senha. Em vez disso, tentar criar senhas que possam ser lembradas facilmente.

Frases de senha geralmente são usadas para autenticação de chave pública e privada. Um sistema de chave pública e privada define uma relação matemática entre a chave pública que é conhecida por todos, e a chave privada que é conhecida apenas pelo usuário. Sem a senha para desbloquear a chave privada, o usuário não tem permissão para obter acesso.

6.3 POLÍTICA DE *E-MAIL*

E-mail eletrônico é usado em quase todos os setores da empresa e muitas vezes é o método de comunicação primária dentro de uma organização. Ao mesmo tempo, o uso indevido de *e-mail* pode trazer muitos riscos, portanto, é importante

para os usuários a entender o uso adequado de comunicações eletrônicas. O objetivo desta política é garantir o uso adequado de sistema de *e-mail* e fazer com que os usuários estejam conscientes do que é aceitável e inaceitável do seu sistema de *e-mail*. Aplica-se a todos os funcionários da empresa.

Todo o uso do *e-mail* deve ser coerente com as políticas e procedimentos de conduta ética. A conta de *e-mail* deve ser utilizada principalmente para fins profissionais. Todos os dados contidos dentro de uma mensagem de *e-mail* ou um anexo devem ser assegurados de acordo com o Padrão de Proteção de Dados.

6.4 POLÍTICA DE COMUNICAÇÃO SEM FIO

Esta política especifica os requisitos técnicos que os dispositivos de infraestrutura sem fio devem satisfazer para se conectar a uma rede. Todos os funcionários da empresa devem cumprir esta norma. Aplicam-se aos dispositivos sem fio que fazem a conexão da rede e todos os dispositivos de infraestrutura sem fio que fornecem conectividade sem fio à rede.

6.5 POLÍTICA DE USO DE INTERNET

A Política de uso da Internet se aplica a todos os que utilizam a Internet por meio dos recursos de redes. O acesso à Internet será fornecido aos usuários para apoiar atividades e somente quando necessário para executar seus trabalhos. O objetivo desta política é definir os usos apropriados da Internet. O acesso à Internet deve ser usado apenas para fins profissionais. Como parte do processo de solicitação de acesso à Internet, o funcionário é obrigado a ler a Política de uso da Internet e o usuário deve, então, assinar as declarações que ele se compromete a cumprir as Políticas. Usuários que não cumpram essas Políticas poderiam estar sujeitos a medidas disciplinares, inclusive demissão.

Todos os IDs (identificação de acesso do usuário à rede) de usuários que sejam inativos por trinta dias serão revogados. Os privilégios concedidos aos usuários devem ser reavaliados pela administração anualmente.

O acesso à Internet será aprovado e fornecido apenas se as necessidades razoáveis de negócios são identificadas. Serviços de Internet serão concedidos com base nas responsabilidades do trabalho atual de um funcionário. Se um trabalhador se desloca para outra unidade de negócio ou altera funções de trabalho, um novo pedido de acesso à Internet deve ser apresentado no prazo de cinco dias. Requisitos de acesso à Internet do utilizador serão revistos periodicamente por departamentos da empresa para garantir que existem necessidades contínuas.

A utilização da Internet é concedida com o único propósito de apoiar as atividades empresariais necessárias para realizar funções de trabalho. Todos os usuários devem seguir os princípios corporativos em relação ao uso dos recursos e usar o bom senso na utilização da Internet.

A empresa proíbe a qualquer forma de coleta de informações a partir de nossas instalações, engajar-se em atividades fraudulentas, ou conscientemente divulgação de materiais falsos ou de outra forma difamatórias.

6.6 TERMO DE RESPONSABILIDADE

Este termo tem como objetivo formalizar e ressaltar o compromisso de todos os funcionários e prestadores de serviços, que devido as suas funções, têm com a proteção das informações que suportam perante a empresa.

São finalidades do Termo de Responsabilidade:

- Proteger as informações de propriedade ou sob custódia da empresa;
- Informar aos funcionários do termo as suas responsabilidades, para proteger, usar e divulgar a informação de maneira responsável e autorizada;
- Evitar que o funcionário se exima da responsabilidade imputada alegando desconhecimento das práticas de segurança da informação a que este deve respeitar;
- Manter sigilo das responsabilidades com a proteção das informações a que têm acesso.

6.7 POLÍTICA DE MONITORAMENTO E FILTRAGEM DE INTERNET

O objetivo desta política é definir normas para os sistemas que monitoram e limitar o uso de qualquer host dentro da rede. Estas normas foram concebidas para garantir que os funcionários utilizem a Internet de uma forma segura e responsável, e assegurar que seu uso pode ser monitorado. Esta política se aplica a todos os funcionários e empregados da empresa e todas as comunicações iniciadas no usuário final entre a rede e a Internet, incluindo a navegação na web, mensagens instantâneas, transferência de arquivos, compartilhamento de arquivos e outros protocolos padrão que serão monitorados. O Departamento de Tecnologia da Informação (TI) devem controlar o uso da Internet a partir de todos os computadores e dispositivos conectados à rede corporativa. Todo o tráfego do sistema de monitoramento deve gravar o endereço IP de origem, a data, a hora, o protocolo, e o site ou servidor de destino. O sistema deve gravar o ID de usuário ou a conta de origem do tráfego. Os registros devem ser preservados por pelo menos 180 dias. Os membros da equipe de respostas a incidentes de segurança da informação podem acessar todos os relatórios e dados, se necessário, para responder a um incidente de segurança. Os relatórios que identificam usuários específicos, locais, equipes, ou dispositivos, só serão disponíveis mediante solicitação por escrito ou e-mail. O departamento de TI deve bloquear o acesso a sites da Internet e protocolos que são consideradas impróprias para ambiente corporativo. A seguir protocolos e categorias de sites devem ser bloqueados:

- Conteúdo Adulto
- Anúncios & *Pop-Ups*
- Bate-papo e Mensagens Instantâneas
- Jogos
- Redes Sociais
- *Peer to Peer* e Compartilhamento de Arquivos
- Spam e Fraude
- Conteúdo Ofensivo
- Conteúdos Ligados a Violência

Se um empregado precisa ter acesso a um site que está bloqueado ele deve apresentar um pedido a seu representante de Recursos Humanos (RH). O RH vai apresentar a solicitação de exceção já aprovada ao departamento de TI, por escrito

ou por e-mail. O departamento de TI vai desbloquear esse site apenas para o associado, e irá monitorar essa exceção e relatá-las em cima do pedido do RH.

O Departamento de Tecnologia da Informação deve rever periodicamente e recomendar alterações nas regras de filtragem da web e protocolo. O departamento de Recursos Humanos (RH) examinará as recomendações e irão decidir se as alterações devem ser feitas.

Um funcionário ou empregado acusado de violar esta política pode estar sujeito à ação disciplinar, e até demissão.

6.8 POLÍTICA DE ANTIVÍRUS

A política deverá ter um processo definido para evitar problemas com vírus:

- Sempre executar o padrão empresarial, apoiado no software antivírus e sempre baixar atualizações de software antivírus assim que estiverem disponíveis.
- Nunca abrir quaisquer arquivos anexados a um e-mail de um desconhecido, suspeito ou fonte não confiável, excluir estes anexos imediatamente.
- Eliminar spam e outros e-mails indesejados.
- Nunca baixar arquivos de fontes desconhecidas ou suspeitas.
- Backups de dados do sistema devem ser armazenados em lugares seguros.
- Não execute quaisquer aplicativos que podem transferir um vírus, por exemplo, compartilhamento de arquivos.
- Novos vírus são descobertos quase todos os dias. Verifique periodicamente o antivírus.

6.9 POLÍTICA DE EQUIPAMENTOS DE COMUNICAÇÃO

Este documento descreve os requisitos para configurações de segurança de equipamentos de comunicação. Esta política se aplica a todos os equipamentos de comunicação que faz parte da rede de dados da empresa. As características de

segurança necessárias para minimizar os riscos para equipamentos de comunicação devem ser configurados nos equipamentos antes da sua colocação em serviço. Há duas maneiras para a equipe que gerencia o equipamento de comunicação: monitoramento e administrador. A função de monitorização tem apenas privilégios. A função de administrador é capaz de alterar os parâmetros de configuração. Todos os comandos emitidos por usuários serão gravados, como quaisquer outros eventos de segurança que possam constituir uma ameaça para o equipamento. Todas as informações transmitidas a partir do dispositivo devem ser criptografadas por um algoritmo de criptografia para minimizar os riscos de espionagem nas comunicações e ataques. Os eventos registados pelo equipamento de comunicação devem ser mantidos em mídia de armazenamento que são sujeitos a um processo de backup regular. O processo de manter esses backups deve garantir que a informação não seja alterada. A senha do usuário administrador do equipamento de comunicação não deve ser conhecida por qualquer pessoa na equipe que gerencia o equipamento. A Equipe irá verificar o cumprimento a esta política através de vários métodos, como, relatórios de ferramentas de negócios, interna e externa, auditorias, e *feedback* para o proprietário da política.

6.10 POLÍTICA DE MÍDIA REMOVÍVEL

Mídia removível é uma fonte bem conhecida de infecções por *malware* e foi diretamente ligada à perda de informações importantes em muitas organizações. O objetivo desta política é minimizar o risco de perda ou exposição de informações de grande importância para a empresa para reduzir o risco de adquirir infecções por *malware* em computadores operados diariamente. Esta política abrange todos os computadores e servidores que operam na empresa.

6.11 POLÍTICA DE AVALIAÇÃO DE RISCOS

A realização de avaliações de riscos de segurança da informação periódica tem a finalidade de interceptar as áreas que estão vulneráveis. As avaliações de risco podem ser realizadas em qualquer entidade dentro da empresa ou qualquer

entidade exterior que assinou um acordo de terceiros. Pode ser realizado em qualquer sistema de informação, incluindo aplicações, servidores e redes, e qualquer processo ou procedimento pelo que estes sistemas são administrados.

A execução, desenvolvimento e implementação de programas de remediação é a junção com o departamento responsável pela área de sistema que está sendo avaliada. Os funcionários devem cooperar plenamente com qualquer avaliação que esteja sendo conduzidas em sistemas para os quais eles são responsabilizados.

6.12 POLÍTICA DE REDE PRIVADA VIRTUAL

O objetivo desta política é fornecer diretrizes para acesso remoto ou virtual. Esta política se aplica a todos os funcionários, empregados, incluindo todo o pessoal afiliadas com terceiros utilizando o acesso à rede privada. Há alguns tópicos no qual devem ser cumpridos referentes à política de rede privada virtual.

- É da responsabilidade do funcionário com privilégios de acesso a rede privada virtual garantir que os usuários não autorizados não tenham permissão de acesso para redes internas.
- O uso da rede privada virtual deve ser controlado usando uma autenticação de senha de uma só vez, como um dispositivo de *token* ou um sistema de chave pública / privada com uma senha forte.
- É permitida apenas uma conexão de rede.
- *Gateways* de rede privada virtual serão criados e geridos por uma rede operacional.
- Todos os computadores conectados a redes internas via rede privada virtual deve usar o software mais o antivírus que é o padrão corporativo, isto inclui computadores pessoais.
- Usuários de rede privada virtual serão automaticamente desligados da rede depois trinta minutos de inatividade. O usuário deve, em seguida, fazer *logon* novamente para reconectar à rede.
- Os usuários devem configurar os equipamentos utilizados cumprindo as políticas de rede.

6.13 POLÍTICA DE ÉTICA

Essa política está empenhada em proteger funcionários, parceiros, fornecedores e também a empresa de ações ilegais ou prejudiciais por parte de indivíduos, sejam consciente ou inconscientemente. Quando aborda questões de forma proativa e usa o julgamento correto, ela vai ajudar a não tolerar qualquer irregularidade em qualquer momento e tomará as medidas adequadas, agindo rapidamente para corrigir o problema, caso o código de ética seja quebrado. O objetivo desta política é estabelecer uma cultura de abertura e confiança. Esta política serve para orientar o comportamento das empresas para assegurar a conduta ética. A ética eficaz é um esforço de equipe envolvendo a participação e o apoio de todos os empregados.

Os líderes e executivos dentro da empresa devem definir um excelente exemplo. Em qualquer prática de negócio, honestidade e integridade deve ser prioridade para os executivos. Eles devem ter uma política de porta aberta e aceitar sugestões e preocupações dos empregados, permitindo que os funcionários se sintam à vontade para discutir quaisquer questões e poderão alertar os executivos a preocupações dentro do ambiente de trabalho. Todos os funcionários e empregados devem tratar a todos de forma justa, ter respeito mútuo e promover um ambiente de trabalho em equipe. Cada funcionário precisa dedicar esforço e inteligência para manter o valor da ética. São eles que irão aumentar a satisfação dos clientes e fornecedores oferecendo produtos de qualidade. É importante certificar se o código de ética foi entregue a todos os funcionários e que as dúvidas em relação ao código podem ser abordadas. Os funcionários irão verificar a conformidade com esta política através de vários métodos, incluindo relatórios da ferramenta de negócio, auditorias internas e externas, e *feedback*.

6.14 POLÍTICA DE ACESSO REMOTO

O acesso remoto da rede corporativa é essencial para manter a produtividade da equipe, mas em muitos casos, este acesso remoto origina de redes que já podem ser comprometidos ou são em uma postura de segurança significativamente menor

do que a rede corporativa. O objetivo desta política é definir as regras e requisitos para se conectar a rede a partir de qualquer máquina. Estas regras e requisitos são projetados para minimizar o potencial de exposição de danos que possam resultar do uso não autorizado de recursos. Os danos incluem a perda de sensibilidade ou dados confidenciais da empresa, propriedade intelectual, danos à imagem pública, danos aos sistemas internos e multas como resultado dessas perdas. Esta política se aplica a conexões de acesso remoto, usados para fazer o trabalho em nome da empresa incluindo a leitura ou o envio de *e-mail* e visualização de recursos da *web*. Esta política abrange toda e qualquer implementação técnica de acesso remoto, usados para conectar-se a rede.

Ao acessar a rede a partir de um computador pessoal, os usuários autorizados são responsáveis por impedir o acesso a quaisquer recursos do computador ou dados por usuários não autorizados. O desempenho de atividades ilegais através da rede é proibido. O usuário autorizado é responsável pelas consequências da má utilização e deverão proteger seu *login* e senha enquanto estiver usando um computador para se conectar remotamente a rede corporativa eles devem garantir que o computador remoto não é ligado a qualquer outra rede ao mesmo tempo, com a exceção de redes pessoais que estão sob seu controle completo ou sob o controle total de um usuário autorizado ou de Terceiros. O acesso remoto seguro deve ser rigorosamente controlado com criptografia (www.sans.org).

7 CONSIDERAÇÕES FINAIS

Este trabalho propôs fazer um estudo de caso em uma empresa de médio porte objetivando determinar se a empresa possui uma gestão política de segurança da informação e, se possui, qual é a eficácia desta gestão. Esta proposta teve como objetivo geral propor melhorias na gestão de política de segurança existente, pois se trata da área de estudo da autora, que tem interesse em aplicar os conhecimentos adquiridos em suas atividades acadêmicas. Para atender este objetivo alguns conceitos sobre segurança da informação, normas, políticas e gestão de políticas de segurança da informação foram apresentados (Capítulos 1, 2 e 3 deste trabalho), alcançando os objetivos específicos explícitos na introdução deste trabalho. Algumas hipóteses foram consideradas, antes do estudo de caso. Após a obtenção dos resultados do estudo de caso, tem-se que as hipóteses a) e c) são falsas, pois a empresa disponibilizou informações para a realização do estudo (contrariando a hipótese a) e os resultados obtidos mostraram que o grau de maturidade da empresa, no que diz respeito às políticas de segurança da informação ainda pode evoluir (contrariando a hipótese c).

Os resultados obtidos no estudo de caso indicam que a empresa atende 27% dos aspectos de política de segurança e que cerca de 55% dos atributos relacionados à gestão de políticas de segurança não são atendidos (Capítulo 4).

Foi feita uma proposta para melhorar a gestão da política de segurança (Capítulo 5) e sugestões para trabalhos futuros incluem um novo estudo de caso na mesma empresa, após a implementação das sugestões propostas, visando a verificação do *status* de gestão da política adotada, comparando os resultados obtidos antes e após a adoção das medidas propostas.

Entende-se que a contribuição deste trabalho serve para empresas de perfil semelhante ao da empresa analisada, pois além de apresentar conceitos importantes sobre normas, políticas de segurança e sua gestão, apresenta um estudo que pode servir de exemplo a ser seguido, na contínua busca de melhoria da segurança, um dos aspectos fundamentais na área de gestão de políticas de segurança e de continuidade de negócios (ALEVATE, 2014).

REFERÊNCIAS BIBLIOGRÁFICAS

ALEVATE, William. **GESTÃO DE CONTINUIDADE DE NEGÓCIOS.** Rio de Janeiro: Elsevier, 2014.

AUDY, J. L. N.; ANDRADE, G. K.; CIDRAL, Alexandre. **FUNDAMENTOS DE SISTEMAS DE INFORMAÇÃO.** Belo Horizonte: Artmed. Rio Grande do Sul. 2005.

BARBIERI, C. **ANÁLISE DA PESQUISA:** o perfil das empresas brasileiras em gestão e governança de dados. Belo Horizonte: FumSoft. Minas Gerais, Brasil. 2013.

COELHO, F. E. S.; ARAÚJO, L. G. S.; BEZERRA, E. K. **GESTÃO DA SEGURANÇA DA INFORMAÇÃO:** NBR 27001 e NBR 27002. Rio de Janeiro: Escola Superior de Redes. Rio de Janeiro, Brasil. 2014.

DANTAS, M. L. **SEGURANÇA DA INFORMAÇÃO:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido. Pernambuco, Brasil. 2011.

FERREIRA, F. F. F.; ARAÚJO, M. T. **POLITÍCAS DE SEGURANÇA DA INFORMAÇÃO:** guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna. Rio de Janeiro, Brasil. 2008.

FONTES, E. **SEGURANÇA DA INFORMAÇÃO:** o usuário faz a diferença. São Paulo: Saraiva. São Paulo, Brasil. 2006.

SÊMOLA, M. **SEGURANÇA DA INFORMAÇÃO**: LENDAS E VERDADES. - IDGNow®. Junho de 2001.
<http://www.semola.com.br/disco/Coluna_IDGNow_33.pdf>. Acesso em 14. Mar. 2015.

SÊMOLA, M. **GESTÃO DA SEGURANÇA DA INFORMAÇÃO**: uma visão executiva. Rio de Janeiro: Elsevier. Rio de Janeiro, Brasil. 2003.

STALLINGS, W. **CRIPTOGRAFIA E SEGURANÇA DE REDES**: princípios e práticas. São Paulo: Pearson. São Paulo, Brasil. 2008.

SANS.ORG. **Políticas de Segurança da Informação.** Disponível em:
<http://www.sans.org/security-resources/policies/>. Acesso em: 23 de mai. 2015.

TANENBAUM, A. S. **COMPUTER NETWORKS.** São Paulo: Campus. São Paulo,Brasil, 4ª. Ed. 2011.