UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
CURSO DE ESPECIALIZAÇÃO EM GESTÃO PÚBLICA (UNISERPRO)
Modalidade à Distância

ANTONIO CARLOS TIBONI

SOFTWARE LIVRE COMO POLÍTICA DE GOVERNO

PORTO ALEGRE
2014

ANTONIO CARLOS TIBONI

SOFTWARE LIVRE COMO POLÍTICA DE GOVERNO

Trabalho de Conclusão de Curso, apresentada ao Curso de Especialização em Gestão Pública (UNISERPRO) – modalidade a distância da Universidade Federal do Rio Grande do Sul como requisito para a obtenção do título de especialista.

Orientador: Prof. Dr. Rogério Faé

PORTO ALEGRE
2014

ANTONIO CARLOS TIBONI

SOFTWARE LIVRE COMO POLÍTICA DE GOVERNO

Trabalho de Conclusão de Curso, apresentada ao Curso de Especialização em Gestão Pública (UNISERPRO) – modalidade a distância da Universidade Federal do Rio Grande do Sul como requisito para a obtenção do título de especialista.

Orientador: Prof. Dr. Rogério Faé

Conceito Final: A

Aprovado em 12 de dezembro de 2014.

BANCA EXAMINADORA:

_____

Prof. Paulo Ricardo Zilio Abdala

DEDICATÓRIA

Dedico este trabalho de conclusão ao meu filho Pedro Henrique Tiboni, que apesar de querer brincar nas horas que eu estava trabalhando na pesquisa, quando dava um sorriso recarregava as minhas baterias.

AGRADECIMENTOS

A Universidade Federal do Rio Grande do Sul, seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior, eivado pela acendrada confiança no mérito e ética aqui presentes.

Ao meu orientador Professor Rogério Faé, pelo suporte, pelas suas correções e incentivos.

A minha tutora Rosária Lanziotti.

E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

RESUMO

O incentivo ao uso de Software Livre através das politicas públicas do Governo Federal está alinhado com a percepção da necessidade de inovação e domínio tecnológico nos sistemas de informação estratégicos. O presente estudo objetivou analisar o impacto das políticas de software livre no Serpro em relação com a segurança das informações dos seus clientes internos e externos. A fundamentação teórica foi construída a partir do estudo dos temas software livre e segurança da informação em relação com a utilização destes em demandas da administração pública. Neste trabalho foi realizada uma análise sobre a forma como a internalização de politicas públicas de software livre afetam a segurança da informação, a partir o estudo de caso das áreas responsáveis pela gestão da segurança da informação do Serviço Federal de Processamento de dados, (SERPRO), no atendimento das demandas dos seus clientes internos, que são seus funcionários, e externos, que são os órgãos da administração pública federal. Para atingir os objetivos do trabalho foram realizadas análise documental, aplicação de questionário para as áreas de segurança do Serpro e entrevistas com gestores. A análise dos dados dos questionários buscou verificar o nível de concordância ou discordância em relação à segurança das informações e, nas entrevistas, buscou-se analisar o quanto o domínio do código do software (software livre) afeta a segurança da informação dos clientes internos e externos do SERPRO. Conclui-se ao final que, no contexto de uma politica de segurança, a organização ter acesso ao código-fonte proporcionada pelo software livre poderá trazer maior segurança as informações através da proteção contra códigos maliciosos embutidos no seu código-fonte, e caso necessário poderá alterá-lo para deixá-lo de acordo com a politica de segurança corporativa.

ABSTRACT

Encouraging the use of Free Software through public policies of the Federal Government is aligned with the perceived need for innovation and technology in strategic information systems. This study aimed to analyze the impact of open source policies in Serpro in relation to information security of its internal and external customers. The theoretical framework was built from the study of the themes free software and information security in relation to the use of these demands in public administration . This work was performed an analysis on how the internalization of open source public policies affect information security , from the case study of the areas responsible for the management of information security of the Federal Service for Data Processing , (SERPRO) in meeting the demands of its internal customers, who are its employees, and external , which are the federal public administration. To achieve the objectives of the study were conducted document analysis, questionnaire for Serpro security areas and interviews with managers. The overall questionnaire data analysis aims to evaluate the level of agreement or disagreement with regard to information security and , in interviews , we sought to analyze how much the software code domain (free software) affects the security of the information from internal clients and external SERPRO . It was concluded at the end that in the context of a security policy , the organization have access to the source code provided by the free software will improve, the information security by protecting against malicious code embedded in your source code , and if needed, can change it to make it according to corporate security policy.

LISTA DE ILUSTRAÇÕES

Figura 1 - Mecanismo de seleção de licença.....24
Figura 2 - Ameças a segurança da informação das instituições.....32
Gráfico 1 - Respostas da questão 1.....45
Gráfico 2 - Respostas da questão 2.....46
Gráfico 3 - Respostas da questão 3.....47
Gráfico 4 - Respostas da questão 4.....48
Gráfico 5 - Respostas da questão 5.....49
Gráfico 6 - Respostas da questão 6.....49
Gráfico 7 - Respostas da questão 7.....50
Gráfico 8 - Respostas da questão 8.....51
Gráfico 9 - Respostas da questão 9.....52

LISTA DE TABELAS

Tabela 1 - Quanto as vendas de Linux movimentam no mundo.....26
Tabela 2 - Utilização de ferramentas e soluções desenvolvidas em Software Livre.....28

LISTA DE ABREVIATURAS E SIGLAS

SERPRO - Serviço Federal de Processamento de Dados
CISL - Comitê de Implementação de Software Livre
ePING - Padrões de Interoperabilidade de Governo Eletrônico
NSA - National Security Agency
DSCI - Departamento de Segurança da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO.....12
2 CONTEXTUALIZAÇÃO TEÓRICA EM SOFTWARE LIVRE E SEGURANÇA DA INFORMAÇÃO 16
2.1 RAZÕES QUE LEVARAM O GOVERNO BRASILEIRO A ADOTAR POLÍTICAS PÚBLICAS DE INCENTIVO AO SOFTWARE LIVRE 16
2.2 O SOFTWARE LIVRE E A SEGURANÇA DA INFORMAÇÃO 17
2.3 PROCESSO COLABORATIVO DE DESENVOLVIMENTO DE SOFTWARE.....18
2.4 SOFTWARE.....20
2.4.1 Software Livre 20
2.4.2 Panorama do Software Fora do Brasil 25
2.4.3 Panorama do Software Livre no Brasil 27
2.5 SEGURANÇA DA INFORMAÇÃO.....30
2.5.1 Politica de Segurança do Governo Federal 32
2.5.2 A Espionagem e a Segurança da Informação.....33
3 AS POLÍTICAS PÚBLICAS DE SOFTWARE LIVRE EM ESCALA NACIONAL E SUA INTERNALIZAÇÃO PELO SERPRO 37
4 O SERPRO COMO AGENTE DE FOMENTO DO SOFTWARE LIVRE 39
5 PROCEDIMENTOS METODOLÓGICOS.....42
5.1 MÉTODO ESCOLHIDO E JUSTIFICATIVA.....42
5.2 INSTRUMENTOS DE COLETA DE DADOS.....42
5.3 A AMOSTRA DOS RESPONDENTES DO INSTRUMENTO DE PESQUISA.....43
5.4 A APLICAÇÃO DO INSTRUMENTO DE PESQUISA.....44
5.5 ANÁLISE DOS DADOS.....44
6 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS 45
7 CONSIDERAÇÕES FINAIS 57
APÊNDICE A - QUESTIONÁRIO.....64
APÊNDICE B - ENTREVISTA.....67

1 INTRODUÇÃO

A informação é um dos maiores patrimônios dos governos e organizações, sendo um ativo muito importante na realização dos negócios. A expressão sociedade de informação transformou-se rapidamente em jargão na área da tecnologia da informação, sendo o software uma ferramenta primordial neste novo contexto. A informação representa a inteligência competitiva dos negócios e é reconhecido como ativo crítico para a continuidade operacional da empresa (SÊMOLA, 2003).

A evolução tecnológica traz a tona a preocupação com a segurança dos sistemas de informação por parte de empresas e governos, principalmente quando trabalham com dados sigilosos, como é o caso dos bancos e de algumas empresas públicas, como o Serviço Federal de Processamento de Dados (SERPRO). Os sistemas são constantemente postos à prova por vários tipos de ataques, incluindo ação de invasores e de diversas espécies de vírus. As ações de defesa contra esses ataques geralmente se concentram na prevenção de incidentes de segurança através de ferramentas tais como autenticação e controle de acesso, porém, com frequência sistemas supostamente seguros são comprometidos, devido a vulnerabilidades não detectadas no desenvolvimento e testes do software. Outro fator a ser considerado, é que a partir da década de 80 os fabricantes que antes entregavam os softwares junto com o hardware percebem que vender programas separadamente seria um meio de aumentar o lucro, por consequência passam a adotar modelos fechados, ou comumente chamados proprietários para o desenvolvimento dos softwares, definindo licenças com restrições do direito de uso. O surgimento do Software Livre na década de 80 criou as bases de um novo modelo de desenvolvimento e uso do software, por anos este modelo foi crescendo aos poucos até se consolidar como uma alternativa de fato ao modelo proprietário.

Durante muitos anos, a comunidade brasileira de Software Livre cobrou que o Governo Federal investisse em Software Livre, e compartilhasse, com todos, a sua inteligência na área de desenvolvimento e deixasse de ser apenas um mero usuário das soluções proprietárias, mas somente a partir de 2003 o governo começou a oficializar através de politicas públicas a opção preferencial pelo Software Livre, promovendo a adoção de padrões abertos, entendendo ser um recurso estratégico para a implementação do governo eletrônico. Processo que ganhou força com as denúncias do ex analista da NSA, Edward Snowden, sobre um esquema de espionagem, em que dados de empresas e pessoas de vários países estavam sendo monitorados pelo governo dos Estados Unidos. No caso do Brasil, as

denúncias são de interceptação das comunicações da Presidente Dilma Rousseff, e acesso a dados da Petrobras e do Ministério das Minas e Energia visando informações referentes às reservas energéticas do Brasil. Estas denúncias reforçaram o direcionamento estratégico do Governo Federal na adoção de políticas públicas de Software Livre. O objetivo é tentar reduzir ao máximo o espaço para espionagem. A nova informação, veiculada no Diário Oficial através do Decreto Federal nº. 8.135, de 4 de novembro de 2013 (BRASIL), é que computadores e softwares que não possibilitarem auditoria pelo poder público não serão mais comprados, o que deve abrir espaço para o software livre. Desta forma, a partir de 2015, sistemas proprietários não poderão ser mais ser utilizados, caso as empresas não permitam investigação, dando acesso ao código-fonte. Além de melhorar a segurança das informações governamentais, a medida também possibilitaria uma economia grande para os cofres públicos, já que estes programas não requerem o pagamento de licenças, como é o caso dos computadores proprietários. Nesse contexto, este estudo buscou responder a seguinte problemática de pesquisa: como a internalização das politicas públicas de software livre no Serpro impacta a segurança das informações dos clientes internos e externos?

Para responder ao problema de pesquisa apresentado foram traçados os seguintes objetivos:

Objetivo geral: analisar o impacto das políticas de software livre no Serpro em relação a segurança das informações dos seus clientes internos e externos.

Objetivos específicos:

1. identificar as razões que levaram o Governo Brasileiro à adoção de políticas públicas de incentivo ao Software Livre;
2. explorar a literatura sobre software livre e segurança da informação;
3. conhecer as politicas públicas de software livre do governo brasileiro;
4. entender as politicas de segurança, e respectivas normas complementares do governo internalizadas pelo SERPRO;
5. analisar o quanto o domínio do código do software (software livre) afeta a segurança da informação dos clientes internos e externos do SERPRO.

A escolha do tema para este estudo está diretamente relacionada a área de atuação do autor do trabalho, que é Gerente da Coordenação Estratégica de Tecnologia, CETEC, do

Serpro, área responsável pela coordenação do programa Serpro de Software Livre, PSSL, nos últimos três anos, e que parte do conhecimento teórico elaborada faz parte de sua experiência prática e profissional no assunto. O PSSL tem como objetivo prover a empresa de direcionamentos para o uso e o desenvolvimento de soluções em Software Livre, pela necessidade de otimização dos recursos de tecnologia da informação do setor público para construção de soluções, que viabilizassem seus serviços, como o acesso seguro às bases de dados dos seus clientes.

O Serpro mantém em suas bases de dados informações extremante importantes e sigilosas dos cidadãos brasileiros, como imposto de renda de pessoas físicas e jurídicas, cadastro de pessoas físicas e jurídicas dentre outros. A empresa fez a opção estratégica pelo software livre para o desenvolvimento de tecnologias e soluções em informática para o acesso a esses dados, visando maior agilidade e controle administrativo dos seus clientes internos, que são seus funcionários, e externos, que são os órgãos da administração pública federal. O interesse desse trabalho é mostrar a importância e os impactos do software livre na segurança da informação, que é caracterizada pela preservação da disponibilidade, integridade, confidencialidade e autenticidade dos dados.

Os procedimentos metodológicos utilizados neste estudo referem-se à pesquisa de natureza qualitativa com coleta de dados de forma quantitativa, com o objetivo de identificar a percepção de forma genérica, e para complementar a análise, outros dados foram coletados através de questionário virtual encaminhado as áreas de segurança, e entrevista encaminhada via correio eletrônico a três gestores nas áreas de segurança, Software Livre e tecnologia do Serpro.

Este trabalho está dividido em capítulos, organizados da seguinte forma: O primeiro refere-se a introdução. O capítulo 2 apresenta uma contextualização teórica sobre software livre e segurança da informação, identificando as razões que levaram o governo brasileiro a adotar políticas públicas de incentivo ao Software Livre. Apresenta a definição do conceito de Software Livre e segurança da informação, e como eles se relacionam, traz um panorama do Software Livre no Brasil e fora dele, e por fim, fala da espionagem no mundo do software. O terceiro capítulo refere-se as políticas públicas de Software Livre em escala nacional e sua internalização pelo Serpro. O quarto capítulo refere-se ao Serpro como agente de fomento do Software Livre. O quinto capítulo apresenta os procedimentos tecnológicos, descrevendo o método escolhido para a pesquisa e a justificativa. Os instrumentos de coleta de dados, a

amostra dos respondentes do instrumento de pesquisa, a aplicação do instrumento e a análise dos dados. O sexto capítulo 6 refere-se a apresentação e análise dos resultados da pesquisa. Por fim, o sétimo capítulo apresenta as considerações finais do presente estudo.

2 CONTEXTUALIZAÇÃO TEÓRICA EM SOFTWARE LIVRE E SEGURANÇA DA INFORMAÇÃO

A segurança da informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, por problemas no software, ambiente ou infraestrutura que a cerca ou pelo acesso indevido de pessoas com o objetivo de furtar, destruir ou modificar as informações. Apresenta-se neste capítulo conceitos da literatura que abordam as questões teóricas de software livre e segurança da informação, e auxiliam no processo de análise dos impactos das políticas de software livre no Serpro em relação a segurança das informações dos seus clientes internos e externos.

2.1 RAZÕES QUE LEVARAM O GOVERNO BRASILEIRO A ADOTAR POLÍTICAS PÚBLICAS DE INCENTIVO AO SOFTWARE LIVRE

O Governo Brasileiro tem adotado um novo modelo em se tratando do uso de softwares, o do Software Livre; isto é, incentivando a utilização de tecnologias de informação preferencialmente não proprietárias como forma de acelerar a inclusão do país na economia global, baseada em tecnologia e desenvolvimento de software. Dentre as razões para adoção de Software Livre pelo Governo, Brasileiro , destacam-se a garantia da independência de fornecedores, o não aprisionamento a tecnologias, a possibilidade de desenvolver tecnologia própria e o fomento de iniciativas de inovação. Assim, pode-se oferecer liberdade aos atores envolvidos nos relacionamentos com o governo: cidadãos, setores produtivos, outros governos e o próprio governo, internamente.

O Brasil tem mais que o direito, tem a necessidade de utilizar tecnologias que permitam aumentar a sua autonomia tecnológica, a sua participação como desenvolvedor de soluções na sociedade da informação (SILVEIRA, 2003).

Para Borges (2014) a adoção de Software Livre pelos governos e a criação do chamado Governo Eletrônico são revoluções na interação do cidadão com o governo. Ele cita as principais razões que levariam os governos a adotar o Software Livre como padrão em suas instalações:

> […] proteção contra coerção ou ameaças por parte de entidades corporativas que desenvolvem e controlam softwares do qual os governos dependem; maior controle de um software do qual depende a segurança nacional; maior potencial econômico

> para companhias internas propiciando o desenvolvimento nacional, melhoria e suporte ao software sem dependência de sociedades com corporações fora do país; redução de litígios e pressões internacionais acerca de questões relacionadas a "pirataria"; redução de custos que facilita a obtenção de financiamento, além do fato de que estes podem ser distribuídos (BORGES, 2014, p.11).

Em síntese, quando o Governo Federal define o Software Livre como direcionamento estratégico através de políticas públicas, ele dá densidade aos fundamentos do Estado brasileiro (à soberania, à cidadania e à dignidade da pessoa humana), bem como aproveita aos seus objetivos de construir uma sociedade livre, justa e solidária e visando garantir o desenvolvimento nacional.

Finalmente, reduzir o debate da adoção do software livre pelo setor público aos estreitos limites da licitação como pretendem os opositores, significa desprezar a real dimensão do tema, consistente na democrática atuação da Administração Pública.

2.2 O SOFTWARE LIVRE E A SEGURANÇA DA INFORMAÇÃO

Com o desenvolvimento de soluções em software livre espera-se incrementar o nível de segurança das informações processadas, pois o livre acesso ao código permite ao usuário alterá-lo de acordo com seus interesses, e no caso, aos interesses do Estado de auditar suas soluções. Silveira (2004) coloca que usando o software livre, o governo pode analisar todo o código que adquire, e retirar rotinas duvidosas que estariam presentes no software em uso; enfim, pode alterá-lo para dar maior segurança. Com o software proprietário não é possível saber se ele possui falhas graves, podendo deixar no computador um caminho de invasão sem despertar a desconfiança de seu operador. Para Ferraz (2002) a segurança é um dos aspectos em que o Software Livre mais se destaca. Um argumento comum é que, como o código-fonte está amplamente disponível, os erros não permanecem escondidos por muito tempo. O fato dos erros tornarem-se visíveis pode parecer assustador à primeira vista, mas a realidade mostra que a visibilidade dos problemas é uma qualidade, e não um defeito.

Os defensores do software proprietário contra-argumentam que o quase domínio da Microsoft no mercado de sistemas operacionais levaria a uma maior exposição, e por consequência uma maior investida das pessoas mal intencionadas em invadir o sistema. Entretanto não se pode esquecer alguns softwares livre, como o Servidor web Apache, que

domina grande parte do mercado e é preferido por enormes vantagens de segurança em relação a servidores proprietários. A segurança dos sistemas é uma das grandes preocupações dos desenvolvedores de software, organizações e governos. A Agência Espacial Americana, Nasa, já usa programas em software livre no controle de suas missões, isso inclui o sistema operacional Linux, mas também uma série de softwares científicos. Além disso lançou o portal (NASA,2014) para ampliar o desenvolvimento e o uso de software livres pela agência espacial. Além de disponibilizar códigos-fontes desenvolvidos internamente, o site é um convite aos desenvolvedores para participar de forma colaborativa de novos projetos. No próximo subcapítulo será apresentado o processo colaborativo de desenvolvimento de software.

2.3 PROCESSO COLABORATIVO DE DESENVOLVIMENTO DE SOFTWARE

Em 1998, Eric Raymond publica o primeiro documento que descreve o processo desenvolvimento de software livre. Raymond descreve esse processo no artigo *The Cathedral and the Bazaar* (RAYMOND, 1998) através de metáforas. A catedral foi escolhida para representar o processo de desenvolvimento de software proprietário e para o desenvolvimento de software livre foi escolhido o bazar. A indústria de software proprietário seria semelhante ao projeto de uma catedral medieval, na qual um pequeno grupo de gestores exerce forte controle sobre o trabalho de um pequeno exército de programadores. Segundo Raymond, Este modelo descreve o relacionamento entre os gestores do projeto, que definem metodologias e cronograma, com tarefas e prazo, que devem ser cumpridos pelos programadores.

A comunidade de software livre é semelhante um anárquico bazar, onde não há hierarquia entre os participantes, e todos cooperam para que o bazar seja atrativo aos compradores, ao mesmo tempo em que competem pela atenção destes mesmos compradores. Na produção de software no bazar os projetos são informalmente organizados em torno da proposta de desenvolvimento de algum software considerado importante, do qual os interessados participam voluntariamente, porque tem interesses pessoais ou comerciais no projeto. O processo de liderança é por meritocracia, ou seja, os líderes são os programadores que mais se destacam no projeto.

Um dos grandes problemas do desenvolvimento no modo catedral, é que os arquitetos de software definem os requisitos do produto a ser desenvolvido pelos programadores. Quando o desenvolvimento é finalizado, um grupo restrito de testadores valida o produto, que é então liberado para ser comercializado. Temos muitos exemplos de produtos que foram colocados a venda antes de atingirem estabilidade ou maturidade, simplesmente porque o prazo de desenvolvimento se esgotou.

No processo de desenvolvimento Catedral: ambiente é fechado e altamente hierárquico; pequeno grupo de líderes e programadores; desenvolvimento centralizado; somente versões estáveis ou que ainda se encontra em fase de desenvolvimento e testes e modelo de desenvolvimento clássico. Já no desenvolvimento Bazar: ambiente aberto onde todos podem participar; número indefinido de líderes e desenvolvedores; desenvolvimento colaborativo; liberação de várias versões e sem metodologia definida (RAYMOND, 1998).

Um projeto de Software Livre passa por diversas fases, que se inicia quando o autor desenvolve uma versão inicial do software e pública o código-fonte em um ambiente de acesso público, se o software for interessante, outros programadores o instalam e experimentam. Os possíveis erros são descobertos e corrigidos, e melhorias são propostas ou já implementada no software. Estas modificações são submetidas ao autor, que as incorpora e pública uma nova versão do software. Para os softwares que atraem mais programadores, o processo de evolução do software é mais rápido. O processo de desenvolvimento garante a continuidade do projeto e por consequência o suporte aos usuários por parte da comunidade.

Uma parte considerável do agrupamento de pessoas em torno dos softwares livres se dá por meio da participação em comunidades, que reúnem pessoas ou empresas em espaços reais ou virtuais, interessadas em agregar experiências e interesses mútuos em torno da disseminação do software livre junto a governos, empresas e centros de pesquisa científico-tecnológica, ou simplesmente desenvolver um software juntando a experiência e colaboração de milhares de programadores. Exemplos de destaque incluem o Linux, um núcleo de sistema operacional; Apache, o servidor web mais difundido na Internet; o Sendmail e o QMail, juntos responsáveis por transferir mais de 50% do tráfego de correio eletrônico mundial [3]. No Brasil temos como destaque a comunidade Demoiselle[4], que é uma plataforma de desenvolvimento de aplicações na linguagem Java, mantida e evoluída pelo Serpro e outras entidades de governo, além de universidades e empresas privadas. “O trabalho colaborativo e em rede é a essência do desenvolvimento do software livre [...] e existem dezenas de projetos

de software bem sucedidos que contam com colaboradores espalhados pelo planeta, sejam oriundos de países ricos ou pobres" (SILVEIRA, 2004, p. 41).

2.4 SOFTWARE

Software ou programa de computador é, segundo a Lei Federal nº. 9.609/98 (BRASIL, 1998) a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados. O que define um software como livre ou proprietário não está dado em sua arquitetura, mas pela sua forma de licenciamento isto é, no modo como é regulamentado juridicamente, regulamentação que configura/ autoriza determinadas relações na sociedade, não outras (Evangelista 2003, p. 10).

Todo software existe em duas formas: uma lida somente por computadores e outra que pode ser lida pelas pessoas. A forma que o computador lê é a forma que é executada por ele. Esta forma é chamada de código binário ou executável. A forma que pode ser lida por humanos é chamada de código-fonte. É assim que os programas são desenvolvidos e através de um compilador é que se gera o código binário ou executável (CHASSEL, 2000). É possível, através de engenharia reversa, que consiste em usar a criatividade para, a partir de uma solução pronta, retirar todos os possíveis conceitos novos ali empregados, obter o código-fonte de um programa a partir do código binário, mas além de se tratar de um processo trabalhoso, o código-fonte normalmente contém comentários que auxiliam seu entendimento e manutenção.

2.4.1 Software Livre

Quando alguém compra um software ou programa de computador, recebe o código de máquina, e não o código-fonte. O código de máquina contém as instruções a serem

executadas pelos compiladores, que fazem a tradução do código-fonte para uma linguagem que a máquina consiga executar. Alguns tipos de software ou programa, no entanto, possuem código-fonte aberto, ou comumente chamados de software livre. Quando você compra um software live ou baixa de forma gratuita pela internet, além do código de máquina, você também leva o código-fonte, que uma pessoa com conhecimento técnico na linguagem em que ele foi desenvolvido, pode alterar a forma como ele funciona, adicionar melhorias, enfim, pode adaptá-lo as suas necessidades.

No passado era comum os programadores de computador trabalharem de forma colaborativa, compartilhando os seus códigos-fontes, o que tornava a evolução e resolução de erros no código muita mais rápida. Nas grandes universidades dos Estados Unidos, o compartilhamento de código-fonte era muito difundido, o que é condizente com os princípios de liberdade e cooperação do mundo acadêmico.

Segundo a *Free Software Foundation,* muitas empresas ganhavam dinheiro vendendo o computador, mas com o início da sua popularização, decidiram como estratégia comercial vender seus softwares, e não mais disponibilizar seus códigos-fonte. O comprador só recebia o software ou programa na linguagem de máquina, o que permitia sua utilização, mas não mais possibilitava o acesso ao código-fonte. As empresas além de abrir um novo segmento de mercado, detinham o conhecimento sobre o software, assim criavam barreiras à entrada de novas empresas, menores, no mercado. Para manter o conhecimento do software restrito, os programadores dessas empresas eram obrigados a assinar termos de compromisso de não divulgação dos segredos do código-fonte; e os softwares eram comercializados com licenças restritivas, que previam além de impossibilitados de modificar o software ou programa, a impossibilidade de fazer cópias. Resumindo, o cliente não tinha o direito de controlar o programa ou software executado em seu computador. Ele podia somente comprar uma licença que permitia o uso daquele programa em apenas um computador.

O programador Richard Matthew Stallmann foi uma das pessoas contrárias ao processo de restrição das empresas comercializadoras de software, e, unido a vários outros programadores, criou um movimento para produzir programas que resguardassem liberdades destinadas as pessoas que desejassem alterar o programa. Então, em 1985 foi criada a *Free Software Foundation*, cujo principal objetivo é apoiar o desenvolvimento de software livre, seja contratando desenvolvedores, seja fornecendo infraestrutura para o desenvolvimento, ou com ações de “evangelizando”, isto é, fazendo campanhas para o convencimento sobre as

vantagens do uso de software livre. O foco do discurso usado é o convencimento dos desenvolvedores e usuários sobre a liberdade. Segundo Stalman, as pessoas devem ter consciência que a escolha do software que ela utilizará, influencia a liberdade do conhecimento tecnológico embutido

> Richard Stallman nasceu em 1953 e teve contato com computadores em 1969, aos 16 anos. Após concluir o ensino médio foi contratado pela IBM em Nova Iorque, onde escreveu seu primeiro programa de computador, Graduou-se em física na Universidade Harvard em 1974. Mais tarde, tornou-se programador do laboratório de IA (Inteligência Artificial) do MIT (*Massachusetts Institute of Technology - Instituto de Tecnologia de Massachusetts*).

O primeiro projeto da fundação foi o GNU, que tinha como objetivo a concepção de um sistema operacional, SO, completo e totalmente livre. Os sistemas operacionais surgiram com dois objetivos principais: criar uma camada de abstração entre o hardware e as aplicações, e gerenciar os recursos de forma eficiente (TANENBAUM AND WOODHULL, 1997). Esse sistema seria compatível com UNIX, que surgiu nos anos 60, e que deu origem a praticamente todos os SO existentes hoje em dia. Já que o sistema seria parecido com o UNIX, sem ser o UNIX, Richard Stallman resolveu batizar o seu sistema de GNU, que significa GNU is Not Unix, ou seja: GNU não é UNIX.

A *Free Software Foundation*, criou a primeira licença para software livre, a Licença Pública Geral, GPL em inglês, o copyleft, garantindo que os trabalhos desenvolvidos coletivamente não se tornem propriedade de ninguém, afirmou Silveira (2005). Esta licença além de garantir as quatro liberdades fundamentais descritas pela Free Software Foundation, garante que este software permanecerá com estas liberdades no futuro e também para trabalhos derivados. Assim, Bretthauer (2002) entendeu que as principais licenças de software livre tem como objetivo manter a propriedade intelectual dos autores originais, sem que, para isso, seja preciso restringir os direitos dos usuários.

As Quatro Liberdades Fundamentais propostas pela *Free Software Foundation* (Foundation, 2014):

- A liberdade de executar o programa, para qualquer propósito; (liberdade 0);
- A liberdade de estudar como o programa funciona, e adaptá-lo às suas necessidades (liberdade 1). Para tanto, acesso ao código-fonte é um pré-requisito;
- A liberdade de redistribuir cópias de "modo que você possa ajudar ao próximo

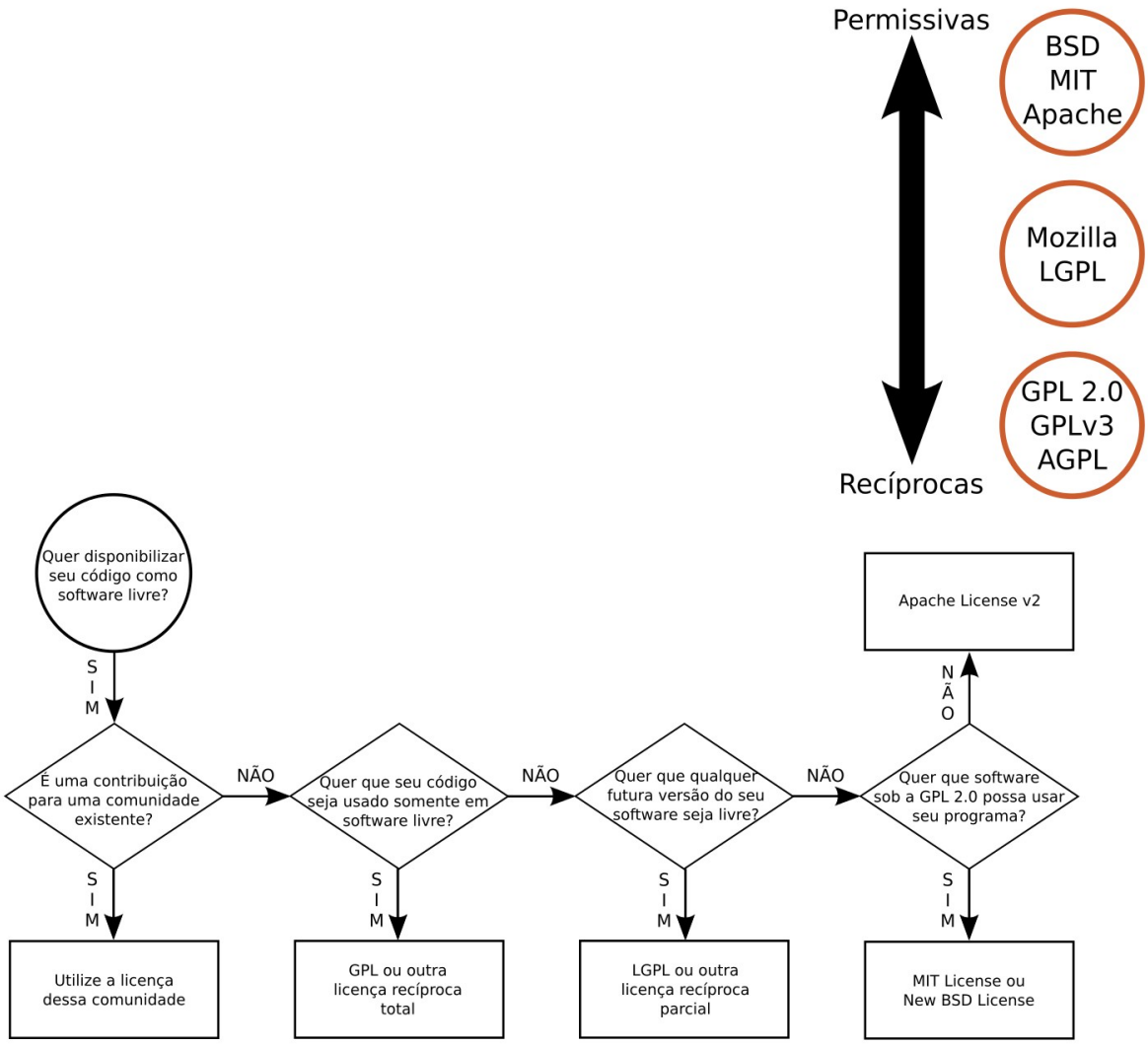
(liberdade 2);

- A liberdade de distribuir cópias de suas versões modificadas a outros (liberdade 3);

No final do século XX, como parte de uma campanha de marketing para o software livre, a *Open Source Iniciative*, OSI, (OSI 2014) criou o termo código aberto, ou *open source* em inglês, que salienta os benefícios técnicos e econômicos do código-fonte aberto e livre ao desenvolvimento, e pouco ou nada sobre os aspectos éticos. A diferença entre esses movimentos, do software livre e do código aberto, são mínimas; centrando-se apenas na argumentação em favor dos mesmos softwares, os dois grupos se unem em diversas situações ou são mencionados, agregadoramente, pela sigla FLOSS, *Free/Libre and Open Source Software*.

Atualmente existem muitas licenças, cada qual com características e finalidades específicas. A OSI mantém uma lista de licenças aprovadas. O programador pode redigir o texto de uma licença de software livre, mas a prática mais comum é reaproveitar alguma das licenças já consolidadas na comunidade, reduzindo a proliferação de licenças, pois gera trabalho adicional para os usuários que precisam estudar os termos de cada nova licença presente no software que utilizarão. A figura 1 propõe um mecanismo de seleção de licença para os desenvolvedores que decidam compartilhar seu código-fonte como software livre.

Figura 1 - Mecanismo de seleção de licença



Fonte: Sabino (2011, p. 56).

Caso o programador não queira redigir o texto de uma licença de software Livre, o importante é escolher uma licença que já seja conhecida e cujo texto seja verificado juridicamente, pois isto facilita a sua adoção e evita problemas legais no futuro. No próximo subcapítulo será apresentado um panorama do Software Livre fora do Brasil.

2.4.2 Panorama do Software Fora do Brasil

O uso de software livre no mundo tem crescido de forma vertiginosa, nas empresas públicas e órgãos governamentais, sendo uma das principais motivações o desejo dos governos da independência tecnológica, encontrando alternativas a monopólios no mercado de software, que é dominado em grande parte por empresas dos Estados Unidos. A grande preocupação é ter operações governamentais sigilosas e essenciais sob a dependência de um único fornecedor e de suas decisões. As empresas privadas enxergaram no software livre um negócio lucrativo, uma vez que é possível cobrar para dar suporte e treinamento, e podem também vender mão de obra para quem quiser criar soluções específicas, o que faz com que a dinâmica da indústria de software evolua, trazendo fortes efeitos sobre a estrutura da indústria: as empresas dominantes do setor de TI estão mudando as suas estratégias competitivas; de outro, tem fomentado a entrada de novas empresas competindo no mercado e novas modalidades de competição e de aquisição de posições e vantagens.

Segundo avaliações da União Europeia, em documentos como "*Free Software/Open Source: Information Society Opportunities for Europe*", o Software Livre está entrando com força na agenda política de diversos países e blocos econômicos. A Alemanha, Áustria, Bélgica, Bulgária, Eslováquia, Eslôvenia, Estônia, Espanha, Finlândia, França Holanda, Irlanda, Itália, Noruega, Portugal, Reino Unido, Suécia e Suíça são exemplos de países que desenvolvem ações e projetos envolvendo software livre na esfera estatal. Em 2009, 231 candidatos a Deputado do Parlamento Europeu assinaram o Pacto do Software Livre, que é um documento simples com os quais os candidatos podem informar o público votante que favorecem o desenvolvimento e a utilização de Software Livre. O pacto também é uma ferramenta para os cidadãos que valorizam o tema para educar os candidatos sobre a sua importância, se eleitos, protegerem a comunidade Europeia de Software Livre.

No mundo dos negócios, pesquisas como da *Open Source Actuate* demonstram como está a saúde do software livre no mundo. A pesquisa entrevistou 1.500 gerentes de TI, programadores e executivos, incluindo pela primeira vez a China, juntando-se o Reino Unido, Estados Unidos, Alemanha e França. O resultado identificou que as empresas europeias são as líderes mundiais na implementação de software livre, mas a China está investindo, e está prestes a superar os europeus. A França está a frente entre os países europeus entrevistados, sendo que 67 por cento relataram que eles estão usando software livre. Alemanha ficou com

60,7 por cento, e Reino Unido, com 42,1 por cento. Os Estados Unidos ficou com 41,0 por cento, sendo que os maiores obstáculos citados pelos pesquisados para uso do software livre foi a falta de documentação adequada e suporte.

Na China 72,7 por cento dos entrevistados responderam que o maior benefício do software livre é o acesso ao código fonte sem a necessidade de pagar pela licença. Essa taxa, com as condições econômicas na China, poderia fazer um grande impacto sobre o lugar da China no uso de software livre.

A China é atualmente o quarto maior mercado de software do mundo, com milhares de programadores, que recebem muito pouco pelo seu trabalho. Além dos fatores culturais e econômicos que explicam por que os programadores e gerentes chineses estão muito interessado em ter em suas mãos o código-fonte. O acesso ao código aberto fornece uma maneira para os chineses gerarem inovação com um custo muito abaixo de softwares proprietários.

Tabela 1 - Quanto as vendas de Linux movimentam no mundo

Mercado bilionário	
Quanto as vendas de Linux movimentam no mundo (em US$ bilhões)	
2002	8,5
2003	11,2
2004	14,5
2005	19,8
2006(1)	24,3
2007(1)	29,4
2008(1)	35,7

Fonte: IDC

(1) Previsão

De acordo com a consultoria IDC, a previsão é que o mercado mundial de programas de software livre crescerá a uma taxa anual de 22,4%. De acordo com o vice-presidente do grupo de soluções corporativas da IDC, o mercado de software livre teve um grande impulso nos últimos 12 meses, mesmo com a crise econômica mundial, e grandes empresas como IBM, Sun, Dell, HP e Oracle têm bom faturamento oferecendo suporte e sistemas de software livre (FAUSCETTE, 2014).

A IBM, Intel e Sun possuem áreas específicas para o desenvolvimento dessas

soluções, empregando centenas de milhares de profissionais, e aplicam com êxito o modelo Bazar, tornando o processo de desenvolvimento mais rápido e com custos menores. A IBM anunciou em 2013 um investimento de 1 bilhão de dólares no desenvolvimento de novas tecnologias baseadas em Software Livre e Linux. Portanto, esta e outras iniciativas apontam a tendência de crescimento do Software Livre no mercado de TI mundial. No próximo capítulo será apresentado um panorama do uso de Software Livre no Brasil.

2.4.3 Panorama do Software Livre no Brasil

A Associação Brasileira das Empresas de Software, ABES, divulgou dados de pesquisa da entidade, realizada pela IDC, e divulgados na ABES *Conference* 2014. A pesquisa mostra que os software e serviços baseados em software livre responderam por US$1,192 milhão, ou 4,6% do total produzido na área de software com serviços no país em 2013, que foi de U$ 25.948 milhões.

O segmento de serviços é o grande impulsionador do software livre no Brasil, respondendo por US$ 961 milhões da receita apurada em 2013. O software ficou com US$ 231 milhões. O governo é o grande comprador com uma participação de mercado de 68%, com um volume de US$ 811,9 milhões. Os aplicativos são o maior segmento do software livre, com 40,8% de participação ou US$ 486,5 milhões. Os sistemas operacionais aparecem em seguida com 38,6%, ou US$ 460,2 milhões. As ferramentas de desenvolvimento e os bancos de dados despontam, respectivamente, com 8,3% e 3,5%, ou US$ 98,9 milhões ou US$ 42,9 milhões.

O Mercado comprador, adverte a pesquisa, reclama da falta de mão de obra especializada. O estudo revela também que faltam profissionais qualificados para atender às demandas de desenvolvimento e de prestação de serviços do setor. O levantamento também destaca que, por falta de especialistas, as empresas interessadas no software livre buscam os fornecedores de maior porte, o que fez sucumbir uma série de prestadores de menor poder econômico.

Após mais de uma década de políticas públicas de fomento ao software livre por parte do governo, os dados indicam que os resultados obtidos no setor privado de tecnologia da informação são inferiores ao de outros países onde essas políticas não foram implementadas,

o que serve de alerta em relação à eficácia delas, comenta Roberto Carlos Mayer, presidente da ALETI e vice-presidente de Relações Públicas da Assespro Nacional.

Com base no último levantamento geral realizado pelo Comitê Técnico de Implementação de Software Livre do Governo, CISL, onde 153 empresas de governos, e entidades de ensino federais responderam pesquisa sobre a utilização de ferramentas e soluções desenvolvidas em software livre:

Tabela 2 - Utilização de ferramentas e soluções desenvolvidas em Software Livre

Correio eletrônico	Servidor de internet	Sistemas de informação	Estações de trabalho	Suíte de escritório
45 %	53 %	40%	4%	11%

Fonte: CISL

Para melhorar estes números, o CISL realizou e divulgou o planejamento do software livre para 2013-2014. Foram definidos 25 objetivos:

a) Garantir produção e acesso à informação e conhecimento sobre Software Livre nos mais diversos ambientes e locais;
b) Ampliar a capacitação de pessoal para utilização de Software;
c) Dimensionar o montante gasto com propriedade intelectual, com ênfase em tecnologia da informação;
d) Garantir a sustentabilidade e suporte adequado às soluções livres adotadas pelo Governo Federal.;
e) Ampliar a comunicação, conhecimento e compreensão da política de adoção de Software Livre;
f) Ampliar a proporção de uso de software livre em relação a software privativo;
g) Órgãos da Administração Pública Federal devem definir metas para adoção de Software Livre e o CISL monitorar o cumprimento;
h) Definir ambiente colaborativo de desenvolvimento federado para o setor público;
i) Definir catálogo de tecnologias abertas e livres desenvolvidas e ou utilizadas pelas unidades do governo;
j) Estimular grupos de trabalhos específicos e comunidades temáticas para softwares de código aberto de uso comum;

k) Alocar recursos do orçamento federal para serem investidos nos softwares livres selecionados pela Administração Pública Federal;
l) Estimular a criação de eventos de Software Livre, fortalecer os existentes e promover a participação de integrantes dos governos.;
m) Definir os processos de compartilhamento e colaboração de softwares abertos e livres em documento que seja mantido e atualizado pelo CISL;
n) Identificar e mapear Softwares Livres utilizados pelas instituições do Governo Federal, o estágio atual de adoção de Software Livre e os casos de sucesso ainda não documentados;
o) Sensibilizar a direção das instituições públicas para inserir seus técnicos e gestores em comunidades de desenvolvimento de software livre de interesse estratégico de seus órgãos;
p) Promover a integração e interação com todas as esferas dos três poderes para fomentar a interoperabilidade, colaboração, compartilhamento e o desenvolvimento de soluções livres;
q) Estimular o compartilhamento das vagas de cursos de software livre entre diferentes órgãos;
r) Apoio à inclusão de Software Livre dentro do currículo dos cursos existentes;
s) Apoio a criação de novos cursos superiores, técnicos e de extensão em Software Livre;
t) Fomento à pesquisa científica em tecnologias livres;
u) Fomento à integração de IES com governo;
v) Apoio a startups (empresas jovens) de software livre;
w) Estimular alunos e técnicos a resolverem tickets de projetos de software livre;
x) Promover que as ações de inclusão digital utilizem Software Livre;
y) Estimular a manutenção de um espaço único com cadastros de especialistas em Software Livre atualizado pela própria comunidade;

No próximo subcapítulo será apresentado um panorama sobre segurança no acesso aos dados.

2.5 SEGURANÇA DA INFORMAÇÃO

A segurança é caracterizada pela preservação da confidencialidade, integridade e disponibilidade.

Taurion discorre sobre a questão da confiabilidade (2004. p.97) afirmando:

> A confiabilidade refere-se à capacidade de manter informações confidenciais ou em segredo. A integridade é a capacidade de garantir a exatidão das informações. Disponibilidade refere-se à capacidade de prover acesso, a qualquer momento que for necessário.

O acesso à internet tornou-se recurso indispensável para sociedade e para a economia mundial. Nem mesmo seus inventores poderiam imaginar a extensão que alcançaria, bem como seu uso nos mais diversos segmentos, que causou em todo o mundo a propagação de uma nova cultura digital. Porém é importante lembrar que essa nova cultura está sujeita a várias formas de ameaças e violações da soberania digital, efetuadas por estados nacionais contra indivíduos, contra empresas e organizações públicas ou privadas ou até mesmo contra outros países.

A era digital foi alcançada, mas sem uma grande discussão sobre os conceitos de segurança para esta grande rede, pois o que seria apenas uma pequena rede militar, tornou-se a grande rede mundial. Atualmente no desenvolvimento das aplicações, parte do tempo das equipes é dedicado a análise de possíveis ataques e o modo de cercá-los. Os usuários são alertados através de campanhas sobe comportamentos de risco, senhas seguras, sites e aplicativos maliciosos.

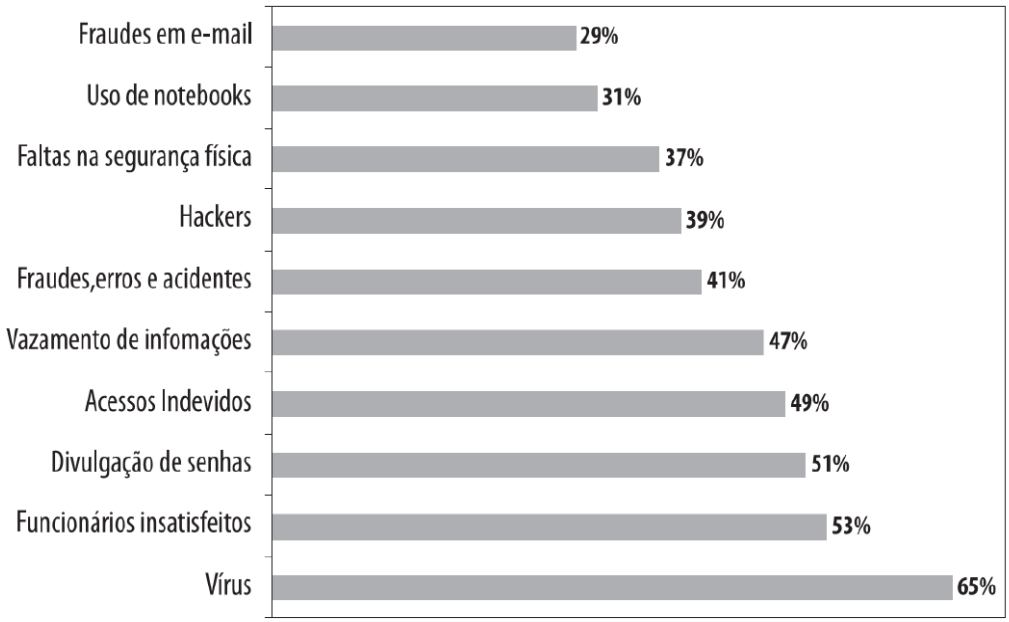
Para Kayworth e Whitten (2010), nenhuma solução ou mecanismo tecnológico é suficiente para garantir a eficácia da segurança da informação nas organizações, pois esta eficácia só pode ser atingida através da aplicação de uma estratégia corporativa de segurança que envolva aspectos técnicos e sociais.

Neste contexto, problemas relacionados à segurança da informação estão cada vez mais evidentes no mundo. Podemos citar o ataque às torres gêmeas em 2001, onde as empresas mantinham suas cópias de segurança na torre vizinha, que também desmoronou, evidenciando a necessidade de práticas de segurança da informação para garantir a continuidade dos negócios (EXAME, 2001).

> Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.
>
> [...]As redes de computadores, e consequentemente da Internet mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas do que em sistemas fechados, assim como os riscos à privacidade e à integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e aos dados desses sistemas (LAURENO, 2005, p. 11).

Na décima edição da pesquisa Nacional de Segurança da Informação, realizada pela Módulo *Security Solutions* (2003), que contou com a resposta de cerca de 600 profissionais atuantes nas áreas de Segurança e Tecnologia da Informação de organizações privadas, públicas e de economia mista, nos seguintes setores: Governo 21%, Financeiro 15%, Informática 14%, Indústria 9%, Prestação de Serviços 8%, Telecomunicações 5%, Comércio 4%, Educação 3%, Energia Elétrica 3%, Saúde 2%, Mineração 0,5%, outros 15%. Com esta pesquisa temos uma noção dos potenciais riscos a que a informação pode estar sujeita dentro da organização, conforme pode ser observado na figura 2.

Figura 2 - Ameças a segurança da informação das instituições



Fonte: Modulo Security Solutions - 10ª Pesquisa Nacional sobre Segurança da Informação.

A pesquisa chegou a conclusão que nos últimos anos houve um avanço na conscientização das empresas em relação à importância da Segurança da Informação para seus negócios. No entanto, a maioria delas ainda não possui planejamento formal de segurança e as ações implementadas normalmente são pontuais. No próximo subcapítulo será apresentado a política de segurança da informação do Governo Federal.

2.5.1 Politica de Segurança do Governo Federal

A Instrução Normativa nº. 1 do Gabinete de Segurança Institucional da Presidência da República, na qualidade de Secretária Executiva do Conselho de Defesa Nacional conceitua Segurança da Informação e Comunicações como:

> [...]ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" e considera as informações tratadas no âmbito da Administração Pública Federal, direta e indireta, como ativos valiosos para a eficiente prestação dos serviços públicos; o interesse do

> cidadão como beneficiário dos serviços prestados pelos órgãos e entidades da Administração Pública Federal, direta e indireta; o dever do Estado de proteção das informações pessoais dos cidadãos; a necessidade de incrementar a segurança das redes e bancos de dados governamentais; e a necessidade de orientar a condução de políticas de segurança da informação e comunicações já existentes ou a serem implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

O principal órgão do Governo Federal na questão da segurança da informação é o Departamento de Segurança da Informação e Comunicação, DSCI, que é ligado ao Gabinete de Segurança Institucional da Presidência da República. A missão do DSCI é: coordenar a execução de ações de segurança da informação e comunicações na administração pública federal; definir requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal; operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal; avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações; coordenar as atividades relacionadas à segurança e ao credenciamento de pessoas e de empresas no trato de assuntos e documentos sigilosos; e exercer outras atribuições que lhe forem delegadas pelo Secretário-Executivo. O DSIC registra milhares de incidentes por hora em redes do governo federal na Internet, sendo que parte destes incidentes está relacionada a tentativa de espionagem e coleta de informações nos bancos de dados do governo.

No próximo subcapítulo será apresentada a questão da espionagem, e como o Governo Brasileiro e as comunidades de software livres estão vendo e tratando o problema.

2.5.2 A Espionagem e a Segurança da Informação

Desde o ataque as torres gêmeas em 2001, os Estados Unidos aprovaram uma lei chamada *USA Patriot Act of 2001* (USA, 2001), que visa unir e fortalecer a América providenciando ferramentas apropriadas e necessárias para interceptar e obstruir o terrorismo. A lei permite, dentre outras coisas, invasão de residências, espionagem de cidadãos, interrogatórios e torturas de possíveis suspeitos de espionagem ou terrorismo.

Nos casos de vigilância existe necessidade de autorização judicial, mas no seu artigo 505 cita a remoção de obstáculos nas investigações de terrorismo, e estende o uso de *NSLs,*

National Security Letters, antes limitadas a investigações sobre terrorismo, à investigações de qualquer natureza. Uma NSL dá *Federal Bureau of Investigation*, FBI, o poder de exigir informações confidenciais de empresas ou órgãos de governo, sem autorização judicial, sem qualquer explicação ou justificativa, e os destinatários devem coletar e entregar os dados sob sigilo, não podendo nem mesmo informar o recebimento da carta. Assim, quando empresas como Google, Microsoft e Facebook, vem a público dizer que só estão cumprindo a lei, neste caso, elas então basicamente falando a verdade. E se explicarem melhor, podem ser acionadas judicialmente pelo governo norte-americano, já que estão legalmente proibidas de informar sobre os dados solicitados através das NSLs. Amparadas legalmente pela *FISA-Foreign Intelligence Surveillance*, as agências de inteligência do Governo Estadunidense requisitam as empresas americanas a instalação de dispositivos que permitem filtrar o fluxo de informações ou sugar os dados constantes em sistemas de informação.

As comunidades de software livre sempre tiveram a preocupação sobre o uso de informações estratégicas dos governos e empresas por parte dos Estados Unidos. As grandes empresas mundiais e governos estavam encurralados. Se proliferam os softwares proprietários e hardwares com softwares embutidos, que não permitem análise e auditoria do software, o que gera um aprisionamento pelo desconhecimento do código como pela falta de alternativa de fornecedores, devido a maioria dos fornecedores de software e hardware serem dos Estados Unidos.

A presidente Dilma discursou na ONU, e estabeleceu dois princípios essenciais da liberdade, da segurança e da governança da internet: ausência do direito à privacidade, não pode haver real liberdade de expressão e opinião e, portanto, democracia; o direito à segurança dos cidadãos de um país não pode ser garantido às custas da violação dos direitos de cidadãos de outro.

O Brasil também aprovou o Marco Civil (BRASIL, 2014), que é uma lei que visa estabelece direitos e deveres na utilização da Internet, que tem como ponto principal a proteção do direito à privacidade e à livre expressão, o que deixa claro o apoio brasileiro à neutralidade da rede como princípio norteador do desenvolvimento futuro da internet. Com software livre é as informações ficam mais seguras? As discussões em relação ao aspecto segurança do software livre em relação ao proprietário não são recentes, Righetti em 2006 levanta uma discussão em relação a segurança da informação e software livre questionando questões que incluem, além dos aspectos técnicos, a própria soberania da nação.

Em outubro de 2003 o Governo Federal Brasileiro criou através de decreto oito comitês executivos do programa Governo Eletrônico, entre eles o Comitê Técnico de Software livre, CISL. Este comitê seria coordenado pela Instituto Nacional de Tecnologia da Informação, ITI, que começou a atuar a definição das diretrizes da implantação do software livre no governo federal. Em novembro de 2003, o então ministro José Dirceu encaminhou carta circular para os Ministérios sobre software livre, recomendando a avaliação da conveniência de se adotar software livre nas futuras aquisições de hardware.

O Brasil adota desde 2004 um conjunto de padrões de interoperabilidade definidos para uso através da arquitetura ePING - Padrões de Interoperabilidade de Governo Eletrônico, que define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação no governo federal, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral, define: item 3.1. Adoção preferencial de Padrões Abertos; Item 3.2. Priorizar o uso do Software Livre. Apesar da obrigatoriedade da adoção destes padrões pouco mais da metade dos gestores públicos afirma a adoção de algum destes (MESQUITA, 2010). Em novembro de 2011, o governo através da Lei Federal nº 12.527 (BRASIL, 2011), no seu artigo primeiro dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. No Art. 8º aberto. § 3º: II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações.

Em novembro de 2013, o governo federal publicou portaria que regulamenta os critérios de auditoria de segurança de sistemas de comunicação do governo e reconhece o Software Livre como auditável, estabelecendo que softwares públicos e livres são considerados auditáveis.

O item 3 das diretrizes do governo eletrônico brasileiro, que consta no portal de governo eletrônico define: O software livre deve ser entendido como opção tecnológica do governo federal. Onde possível, deve ser promovida sua utilização. Para tanto, deve-se priorizar soluções, programas e serviços baseados em software livre que promovam a otimização de recursos e investimentos em tecnologia da informação. Entretanto, a opção pelo software livre não pode ser entendida somente como motivada por aspectos econômicos, mas

pelas possibilidades que abre no campo da produção e circulação de conhecimento, no acesso a novas tecnologias e no estímulo ao desenvolvimento de software em ambientes colaborativos e ao desenvolvimento de software nacional. A escolha do software livre como opção prioritária onde cabível, encontra suporte também na preocupação em garantir ao cidadão o direito de acesso aos serviços públicos sem obrigá-lo a usar plataformas específicas.

Está em tramitação na Câmara Federal um Projeto de Lei nº. 2269/1999, que dispõe sobre a utilização de programas abertos pelos entes de direito público e de direito privado sob controle acionário da administração pública.

No próximo capítulo será apresentada as razões que levaram o Governo Federal a incentivar e adotar politicas públicas de Software Livre.

3 AS POLÍTICAS PÚBLICAS DE SOFTWARE LIVRE EM ESCALA NACIONAL E SUA INTERNALIZAÇÃO PELO SERPRO

A utilização de software livre em órgãos federais faz parte da decisão estratégica da política de tecnologia de informação orientada e difundida pelo Comitê Técnico para Implementação do Software Livre, CISL. O comitê aponta as diretrizes para a implementação de software livre, entre elas popularizar o uso desta tecnologia e ampliar a malha de serviços prestados no governo, garantindo ao cidadão brasileiro o direito de acesso aos serviços públicos sem obrigá-lo a usar plataformas específicas. Além disso fomenta a criação de comunidades e discussões colaborativas e voluntárias, além de fortalecer e compartilhar ações existentes de software livre dentro e fora do governo e incentivar o mercado nacional a adotar novos modelos de negócios em tecnologia baseados em software livre.

Segundo o portal Software Livre no governo do Brasil, as razões para que as instituições públicas federais estabeleçam programas de migração para o Software Livre são:

Macroeconômica: As despesas referentes a licenças de uso não são aplicáveis a soluções baseadas em Software Livre, resultando em economia progressiva, cujos valores podem ser reaplicados em investimentos na área de Tecnologia da Informação, ou outras áreas do governo.

Segurança: As soluções livres oferecem o recurso do acesso aos códigos-fonte, o que proporciona que técnicos do governos possam auditar a solução, verificando possíveis códigos maliciosos que possam infectar os sistemas de governo, ou mesmo a existência de falhas de codificação, abrindo portas para possíveis ataques as bases de governo. Com o acesso ao código fonte, sabe-se exatamente o que o programa executa.

Autonomia tecnológica: com o software livre o governo ou empresas privadas podem alterar a qualquer momento sua estrutura de acordo com as suas necessidades. Já nos sistemas proprietários não se tem acesso ao código fonte e isso faz com que os o governo e as empresas privadas fiquem sempre presas as decisões da empresa que vende a solução. Assim, pode-se oferecer liberdade aos atores envolvidos nos relacionamentos com o governo: cidadãos, setores produtivos, outros governos e o próprio governo, internamente. Segundo Linus Torvalds, criador do Linux, usar Software livre não é somente redução de custos, é questão de controle e autonomia do sistema que você usa. Com os governos, há a questão de segurança de usar um sistema que ninguém pode tirar de você, e não ficar à mercê de uma empresa internacional.

Independência de fornecedores: quando o governo compra software proprietário, ele fica dependente do fornecedor desse software, já com o software livre, a oferta de mercado aumenta. Possuindo o código fonte e as licenças de uso, é possível realizar melhorias não só por quem forneceu a solução, mas por qualquer outro fornecedor ou técnico da própria empresa.

Compartilhamento do conhecimento: o software livre proporciona o compartilhamento das inovações com a comunidade, permitindo que as melhorias sejam adotadas por todos os interessados. O governo ao estimular o uso e o desenvolvimento de software livre, fomenta a produção e qualificação do conhecimento local, a partir de um novo paradigma de desenvolvimento sustentado e de uma nova postura, que insere a questão tecnológica no contexto da construção de um mundo com inclusão social e igualdade de acesso aos avanços tecnológicos.

Segundo o Portal Brasil, a implantação do software livre nos órgãos federais avança, mas é um processo contínuo que acontece de forma gradual e respeita os momentos de substituição da tecnologia em cada instituição. A transição para o software livre se dá quando, por exemplo, há necessidade de se fazer a implementação de nova versão de um sistema ou conforme a maturidade e o momento de descarte de uma tecnologia.

A seguir serão apresentadas formas como o Serpro internalizou as politicas públicas de Software Livre.

4 O SERPRO COMO AGENTE DE FOMENTO DO SOFTWARE LIVRE

O Serpro é o principal agente estatal de fomento da informática pública brasileira, fornecendo a infraestrutura necessária às ações estruturantes do Governo Federal e que permitem à administração pública maior eficiência na sua gestão, controle e divulgação dos dados: receita, investimentos e gastos. A criticidade das informações, o incremento das demandas de serviço, a evolução das tecnologias utilizadas e o surgimento de novos fatores de vulnerabilidade fazem com que a segurança da informação seja tratada, prioritária e permanentemente, como um requisito fundamental para o negócio do Serpro. A segurança da informação protege a informação de propriedade do Serpro, bem como aquele que esteja sob sua guarda, dos diversos tipos de ameaças para minimizar os riscos de falhas, danos ou prejuízos que possam comprometer a qualidade dos serviços, a imagem do Serpro e de seus clientes.

O investimento na qualificação do corpo funcional é constante, visando garantir o permanente incremento da cultura de segurança. Além disso, possui pessoal especializado com certificação profissional e ampla qualificação em segurança. Decisões condicionadas pelo próprio fluxo e pelas reações e modificações que elas provocam no tecido social, bem como pelos valores, ideias e visões dos que adotam ou influem na decisão". Neste sentido, segundo Ruas (2009, p.19) "políticas públicas (*policy*) são uma das resultantes da atividade política (*politics*): compreendem o conjunto das decisões e ações relativas à alocação imperativa de valores envolvendo bens públicos."

O governo brasileiro vem oficializando a opção preferencial pelo Software Livre e promovendo a adoção de padrões abertos, entendendo ser um recurso estratégico para a implementação do governo eletrônico brasileiro. A sociedade também deve se beneficiar das politicas, buscando ampliar o fomento a pesquisa e desenvolvimento a partir do uso de ferramentas livres e melhorando a eficiência das empresas com a adoção de modelos abertos de desenvolvimento.

O estado do Rio Grande do Sul foi pioneiro nas discussões sobre normatização de Software Livre no Brasil, com a proposta do então deputado Elvino Bohn Gass, através de um projeto de lei que determinava o uso preferencial de software livre. Este tipo de proposta ajudou a abrir o debate sobre a importância do Software Livre ser utilizado na administração pública.

Em outubro de 2003 o Governo Federal Brasileiro criou através de decreto oito

comitês executivos do programa Governo Eletrônico, entre eles o Comitê Técnico de Software livre, CISL. Este comitê seria coordenado pela Instituto Nacional de Tecnologia da Informação, ITI, que começou a atuar a definição das diretrizes da implantação do software livre no governo federal. Em novembro de 2003, o então ministro José Dirceu encaminhou carta circular para os Ministérios sobre software livre, recomendando a avaliação da conveniência de se adotar software livre nas futuras aquisições de hardware.

O Serviço Federal de Processamento de Dados, Serpro. é uma empresa pública de tecnologia da informação a serviço do Governo Federal do Brasil. Foi criado pela Lei Federal nº. 4.516, de 1º de dezembro de 1964 (BRASIL, 1964), vinculado ao Ministério da Fazenda, desenvolve programas e serviços visando ao controle e transparência sobre a receita e os gastos públicos. Com 50 anos de existência, tem se afirmado no cenário de TI pública, aprimorando tecnologias adotadas por diversos órgãos federais, estaduais e municipais.

O Serpro, tem investido na internalização de tecnologias livres desde a década de 90, onde os primeiros estudos foram iniciados, o que resultou na criação de um Centro de Especialização em Software Livre, CEUL. Setores interessados em novas soluções em Software Livre podiam solicitar à CEUL um estudo da viabilidade do uso em questão. A partir de 2003 o Governo Federal começa a lançar politicas com direcionamento estratégico para Software Livre, e para atender estes direcionamentos, o Serpro criou o Programa Serpro de Software Livre, PSSL. No final de 2003, o centro de dados começaram a utilizar o Linux. E até final de 2004, seria concluída a grande tarefa de migrar todas as estações de trabalho para o sistema operacional livre.

> O PSSL tem como objetivo fornecer o direcionamento estratégico quanto a internalização, desenvolvimento e o uso de soluções baseadas em Software Livre e padrões abertos, bem como definir um processo de colaboração para fomentar contribuições e melhorias das soluções em software livre utilizadas institucionalmente (SERPRO 2013 - Decisão de Diretoria).

O Serpro também criou a Coordenação Estratégica de Software Livre, CESOL (SERPRO 2007 - Decisão de Diretora), cujas principais atribuições são: coordenar a estratégia de implantação do PSSL e suas ações corporativas; Interagir com os Comitês Regionais de Software Livre; promover ações de sensibilização do corpo funcional e gerencial; manter acompanhamento sobre a prospecção e efetiva implantação de soluções tecnológicas em Software Livre em todas as áreas de atuação da empresa tanto para internalização de novas

tecnologias como para substituição das tecnologias atualmente em uso; recomendar a prospecção, em conformidade com as políticas e diretrizes empresariais, de soluções tecnológicas em Software Livre em todas as áreas de atuação da Empresa; atuar junto as Unidades de Relacionamento com Clientes para que as novas soluções sejam desenvolvidas, sempre que for possível, utilizando infraestrutura em Software Livre, considerando a internalização realizada pela produção; avaliar o ciclo produtivo dos serviços em software livre e propor recomendações a serem adotadas pelas áreas de produção e de desenvolvimento, para garantir a viabilidade de implantação dos serviços e propor, com base em direcionamentos da diretoria, migrações de soluções para infraestrutura baseada em Software Livre. Atualmente a coordenação do PSSL está a cargo da Coordenação Estratégica de Tecnologia, CETEC.

Atualmente o Serpro tem a maior parte de suas estações de trabalho utilizando sistema operacional livre, Ubuntu GNU/Linux, e sua rede local é toda implementada com soluções livres, assim como seu correio eletrônico Expresso, que está sendo utilizado também pela Presidência da República. Buscando padronizar as soluções tecnológicas do governo federal no desenvolvimento de sistemas, o Serpro desenvolve e mantém em comunidade o projeto Demoiselle, que tem como principal objetivo a padronização de processos e códigos de sistemas, consequentemente gera aumento da produtividade, simplifica o processo de construção e manutenção das soluções, incentiva o reuso de artefatos e fomenta o mercado para o uso preferencial de plataformas abertas. Os principais sistemas de governo eletrônico são desenvolvidos com o Demoiselle, como o Sistema de Comércio Exterior, Siscomex, o novo sistema de passaporte brasileiro dentre outros.

O Serpro, como provedor de soluções para o governo federal, tem um papel fundamental na definição e implementação de alternativas livres para o estado brasileiro. A empresa deixa de ser apenas uma receptora de tecnologias oferecidas por fornecedores e toma posição de participante efetiva no desenvolvimento de soluções livres para o país, devendo se portar como agente principal no direcionamento de tecnologia de software livre para o governo federal.

5 PROCEDIMENTOS METODOLÓGICOS

Neste capítulo serão apresentados os procedimentos metodológicos do presente trabalho como o método escolhido e justificativa, instrumento de coleta de dados, a amostra dos respondentes do instrumento de pesquisa, a aplicação do instrumento de pesquisa e análise dos dados.

5.1 MÉTODO ESCOLHIDO E JUSTIFICATIVA

O método escolhido é o estudo de caso, usando como caso as áreas responsáveis pela gestão da segurança da informação do Serpro, que é uma estratégia que permite ao pesquisador um aprofundamento em relação ao objeto a ser pesquisado. Segundo Yin (2001) o estudo de caso é uma estratégia de pesquisa que compreende um método que abrange tudo em abordagens específicas de coleta e análise de dados.

5.2 INSTRUMENTOS DE COLETA DE DADOS

Para atender o objetivo deste trabalho foi realizada uma análise de cunho qualitativo, com coleta de dados primária de forma quantitativa, com o objetivo de identificar a percepção de forma genérica. e, posteriormente foi utilizado questionário estruturado (APÊNDICE A) com 9 questões fechadas que foram enviadas ao público-alvo através de formulário virtual. E uma entrevista semiestruturada (APÊNDICE B) composta de 1 pergunta estratégica, enviada para 3 gestores de áreas ligadas a coordenação de tecnologia, Software livre e segurança da informação do Serpro através de e-mail e complementada por telefone.

A entrevista é uma técnica de pesquisa que visa obter informações de interesse a uma investigação, onde o pesquisador formula perguntas orientadas, com um objetivo definido. Segundo Manzini (2004) as entrevistas podem ser do tipo estruturada, semiestruturada e não-estruturada. A entrevista estruturada é aquela que contem perguntas fechadas, semelhantes a formulários, sem apresentar flexibilidade; semiestruturada a direcionada por um roteiro

previamente elaborado, composto geralmente por questões abertas; não-estruturada aquela que oferece ampla liberdade na formulação de perguntas e na intervenção da fala do entrevistado. A entrevista (APÊNDICE B) é do tipo semiestruturada, o que permite uma organização flexível e ampliação dos questionamentos à medida que as informações vão sendo fornecidas pelo entrevistado.

5.3 A AMOSTRA DOS RESPONDENTES DO INSTRUMENTO DE PESQUISA

O Serpro investe muito em segurança da informação, e atualmente temos as seguintes áreas grupos como responsáveis pelo assunto dentro da empresa: Comitê Estratégico de Segurança do Serpro, COESI; Coordenação de Geral de Segurança da Informação, COGSI; Superintendência de Operações e Centro de Dados, que são Áreas de segurança da produção e Grupo de segurança das unidades de relacionamento com o cliente - URC. A amostra foi formada por especialistas em segurança da informação dos grupos e áreas acima, o que leva a um universo a ser investigado de população de cerca de 118 pessoas, sendo que o questionário (APÊNDICE A) foi enviado a todos.

Foi enviada entrevista composta de uma questão (APÊNDICE B) respondida por e-mail, que foi complementada por telefone, em virtude da impossibilidade de deslocamento para efetuar as entrevistas de forma presencial. A entrevista foi enviada para o responsável pela Coordenação Estratégica de Tecnologia do Serpro, CETEC, que responde pelo tema tecnologia, por meio de sistematização de informações e procedimentos relacionados aos processos de governança de TIC, arquitetura e integração de sistemas, modernização, pesquisa e desenvolvimento em computação aplicada e inovação. Ao Comitê de Implementação de Software Livre do Governo Federal, CISL, que define as diretrizes da implementação de Software Livre no Governo Federal, e a Coordenação de Gestão de Segurança do Serpro, que tem a missão de levar para qualquer unidade da empresa as diretrizes gerais de segurança definidas pelo comitê estratégico da segurança da informação, que é composto por representantes de cada uma das diretorias da empresa.

5.4 A APLICAÇÃO DO INSTRUMENTO DE PESQUISA

O instrumento da coleta de dados foi um questionário e uma entrevista. O questionário (APÊNDICE A) foi aplicado através de formulário eletrônico, enviado para os representantes das áreas de segurança do Serpro. As questões do formulário serão formatadas seguindo a escala de *Liker* de 5 pontos, que é uma escala psicométrica das mais conhecidas e utilizada em pesquisa quantitativa, já que pretende registrar o nível de concordância ou discordância com uma declaração dada. A entrevista (APÊNDICE B) foi enviada para o e-mail corporativo dos entrevistados, e posteriormente complementada por telefone. A entrevista não foi feita de forma presencial devido aos entrevistados fazerem parte do quadro de funcionários do Serpro em Brasília.

5.5 ANÁLISE DOS DADOS

O questionário (APÊNDICE A) passou por um pré-teste com 8 pessoas, de forma a confirmar que ele seja realmente aplicável com êxito no que toca a dar uma resposta efetiva aos problemas levantados pela pesquisa. A partir do resultado da coleta de dados foi realizada uma análise utilizando estatística descritiva. A estatística descritiva é um ramo da estatística que envolve a coleta e a análise de um conjunto de dados com o objetivo de descrever as características desse conjunto (LEVINE, 2000). Posteriormente foi realizada uma análise qualitativa de forma a compreender a forma como o domínio do código fonte afeta a segurança das informações.

6 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Neste capítulo foi realizada uma análise de quanto o domínio do código do software livre afeta a segurança da informação dos clientes do SERPRO.

O questionário (APÊNDICE A) foi enviado para 118 pessoas, sendo que 42 responderam, correspondendo a 35,5 por cento do público-alvo.

A questão 1 foi aplicada como o objetivo de verificar se no processo de internalização de novas tecnologias para a gestão da segurança da informação no Serpro é dada prioridade para ferramentas em software livre pensando na segurança da informação. Questão 1: Na internalização de novas tecnologias no Serpro é dada prioridade as soluções livres pensando na segurança da informação.

Gráfico 1 - Respostas da questão 1

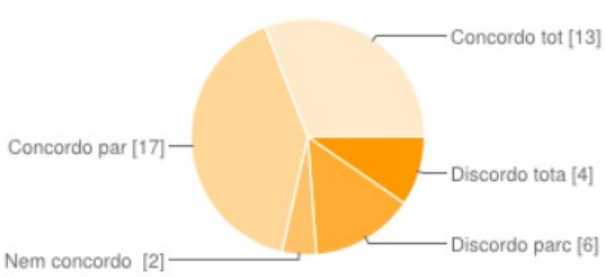
Fonte: Elaborada pelo autor.

O gráfico 1 indica que temos 14 por cento que discordam totalmente, 26 por cento que discordam parcialmente, 2 por cento que nem concordaram e nem discordam, 28 por cento que concordam parcialmente e 19 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 30 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 57 por cento, dando uma diferença de 27 por cento, o que é bastante significativo. Estes resultados sugerem tendência a percepção que é dada prioridade a soluções livres na internalização de novas tecnologias no Serpro. O resultado pesquisa vai de encontro ao direcionamento do estratégico do Serpro em relação a internalização das politicas de software livre do Governo Federal, onde é definido o seu uso como preferencial, desde que atenda todos os requisitos definidos, neste caso os de segurança.

A questão 2 foi aplicada como o objetivo de verificar se o acesso ao código-fonte de uma solução (software livre) tem relação direta a proteção dos dados, e por consequência na

segurança da informação. Questão 2: O código-fonte de uma solução livre tem relação direta com a proteção dos dados.

Gráfico 2 - Respostas da questão 2



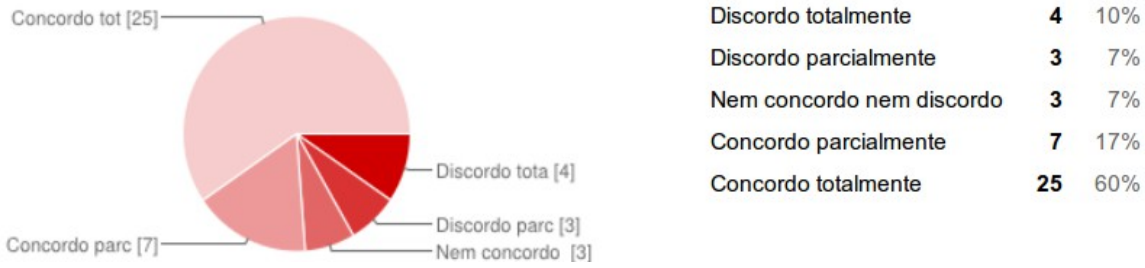
Discordo totalmente	4	10%
Discordo parcialmente	6	14%
Nem concordo nem discordo	2	5%
Concordo parcialmente	17	40%
Concordo totalmente	13	31%

Fonte: Elaborada pelo autor.

O gráfico 2 indica que temos 10 por cento que discordam totalmente, 14 por cento que discordam parcialmente, 5 por cento que nem concordaram e nem discordam, 40 por cento que concordam parcialmente e 31 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 24 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 71 por cento, dando uma diferença de 47 por cento, o que é bastante significativo. Estes resultados sugerem tendência a percepção que o acesso ao código(Software Livre) tem relação direta com a proteção dos dados. O resultado da pesquisa é reforçado por Silveira (2003), que defende que o Software Livre deve ser adotado na área de segurança pelo fato de ter seu código aberto. O referido autor explica como saber se um software é seguro se não temos acesso ao seu código-fonte, e ainda, se um software não pode ser integralmente auditado não pode ser considerado seguro.

A questão 3 foi aplicada como o objetivo de verificar se os responsáveis pela gestão da segurança no Serpro conhecem casos em que foi detectada falha na segurança devido à vulnerabilidade constatada no código-fonte. Questão 3: Conheço caso em que foi detectado falha de segurança no acesso aos dados devido à vulnerabilidade constatada no código-fonte.

Gráfico 3 - Respostas da questão 3



Fonte: Elaborada pelo autor.

O gráfico 3 indica que temos 10 por cento que discordam totalmente, 7 por cento que discordam parcialmente, 7 por cento que nem concordaram e nem discordam, 17 por cento que concordam parcialmente e 60 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 17 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 77 por cento, dando uma diferença de 60 por cento, o que é bastante significativo. Estes resultados sugerem tendência a percepção que o público-alvo conhece casos em que foi detectado falha de segurança no acesso aos dados devido à vulnerabilidade constatada no código-fonte. Um dos problemas de segurança menos lembrado pelos usuários é a vulnerabilidade do software. O usuário na maioria das vezes não se preocupa se o software adquirido, seja ele livre ou proprietário, garante segurança durante sua utilização. É importante lembrar que todo software está sujeito a erros e por isso pode conter falhas que permitem quebras de segurança. Existem casos onde um software instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da internet, e só é possível ter esta certeza analisando o código-fonte. Os softwares livres proporcionam que o usuário possa analisar possíveis falhas ou vulnerabilidades no código-fonte, e isto é possível através de uma das quatro Liberdades Fundamentais propostas pela *Free Software Foundation* (*FOUNDATION*, 2014), a liberdade 1, dá o direito de estudar como o programa funciona, e adaptá-lo às suas necessidades. Para tanto, acesso ao código-fonte é um pré-requisito.

A questão 4 foi aplicada com o objetivo de verificar se uma solução sendo em software livre abre possibilidades para que pessoas descubram suas fragilidades. Questão 4: o acesso ao código-fonte (software livre) abre possibilidade para fragilidades.

Gráfico 4 - Respostas da questão 4

Fonte: Elaborada pelo autor.

O gráfico 4 indica que temos 24 por cento que discordam totalmente, 19 por cento que discordam parcialmente, 14 por cento que nem concordaram e nem discordam, 26 por cento que concordam parcialmente e 17 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 43 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 33 por cento, dando uma diferença de 10 por cento, o que não é significativo. Estes resultados sugerem um leve tendência do público-alvo em achar que ter acesso ao código-fonte (software livre) não abre possibilidade para fragilidades. As vulnerabilidades ou fragilidades são pontos em que o software é susceptível a ataques. A identificação das fragilidades técnicas de um software nem sempre é trivial, requerendo, em geral, profundo conhecimento tecnológico. Segundo Thomas Soares, coordenador de infraestrutura do Fórum Internacional de Software Livre, FISL, a segurança existe quando o processo é aberto e todos sabem como funciona a fechadura. O que os privados vão propõe são soluções confidenciais, que só serão conhecidas por eles, e que poderão ser exploradas através de “portas dos fundos”.

A questão 5 foi aplicada como o objetivo de verificar se os sistemas operacionais livres são menos atacados devido a menor quantidade de usuários em relação aos sistemas operacionais proprietários no mundo. Questão 5: a quantidade de exploradores de falhas de segurança em sistemas operacionais livres é proporcional ao seu uso.

Gráfico 5 - Respostas da questão 5

Fonte: Elaborada pelo autor.

O gráfico 5 indica que temos 10 por cento que discordam totalmente, 14 por cento que discordam parcialmente, 14 por cento que nem concordaram e nem discordam, 45 por cento que concordam parcialmente e 17 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 24 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 62 por cento, dando uma diferença de 38 por cento, o que é significativo. Estes resultados sugerem uma tendência do público-alvo em achar que a quantidade de exploradores de falhas de segurança em sistemas operacionais livres é proporcional ao seu uso. Segundo o manifesto de José Ricardo de Oliveira Damico sobre a eficiência contínua dos ataques cibernéticos, publicado no portal de Software Livre, no que diz respeito a sistemas operacionais populares para computadores pessoais, aquele que se tornar o predominantemente usado naturalmente atrairá mais tentativas de ataque.

A questão 6 foi aplicada como o objetivo de verificar a relação de custos de manutenção entre uma solução de segurança em software livre e uma proprietária. Questão 6: o custo de se manter uma solução de segurança em software livre é maior do que em uma solução proprietária.

Gráfico 6 - Respostas da questão 6

Fonte: Elaborada pelo autor.

O gráfico 6 indica que temos 29 por cento que discordam totalmente, 26 por cento que discordam parcialmente, 21 por cento que nem concordaram e nem discordam, 14 por cento que concordam parcialmente e 10 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 55 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 24 por cento, dando uma diferença de 26 por cento, o que é significativo. Estes resultados sugerem tendência a percepção que o público-alvo acha que o custo de se manter uma solução de segurança em software livre não é maior do que em uma solução proprietária. Em síntese, embora soluções em Software Livre não eliminem os custos de manutenção e suporte, tem a vantagem de poder ser mantido pelo próprio usuário através da contratação de profissionais de informática, ou pela comunidade, através da experiência compartilhada ou por terceiros.

A questão 7 foi aplicada como o objetivo de verificar a maturidade das soluções de segurança em software livre em relação as proprietárias. Questão 7: as ferramentas de segurança em software livre estão no mesmo nível de maturidade em relação as ferramentas proprietárias.

Gráfico 7 - Respostas da questão 7

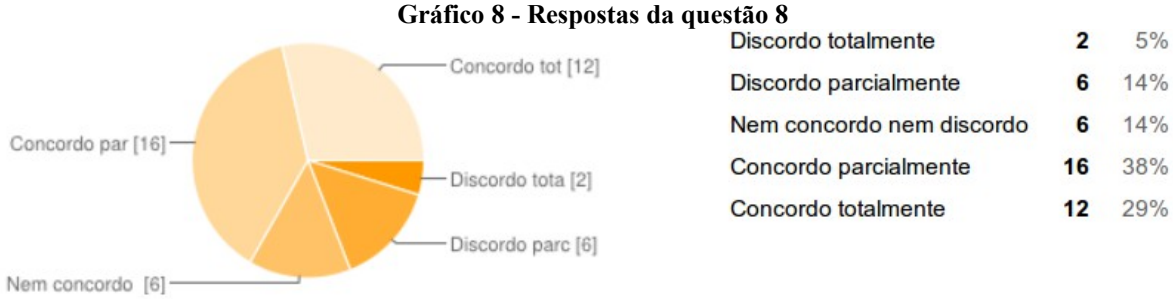
Fonte: Elaborada pelo autor.

O gráfico 7 indica que temos 21 por cento que discordam totalmente, 24 por cento que discordam parcialmente, 5 por cento que nem concordaram e nem discordam, 33 por cento que concordam parcialmente e 17 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 45 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 50 por cento, dando uma diferença de 5 por cento, o que é não significativo. Estes resultados sugerem um leve tendência do público-alvo em achar que ferramentas de segurança em software livre estão no mesmo nível de maturidade das ferramentas proprietárias. As ferramentas em software livre que não estão no mesmo nível podem ser alteradas e evoluídas

para atender aos requisitos de segurança da organização. O que é reforçado por Silveira (2004), que defende que o software livre permite aos técnicos, engenheiros e especialistas que acompanham a evolução do software se capacitarem para alterá-lo e de acordo com os seus interesses.

A questão 8 foi aplicada como o objetivo de verificar se os requisitos de segurança de soluções livres tem a mesma rigorosidade das soluções em software proprietário. Questão 8: os requisitos de segurança das soluções em software livre são tão rigorosos quanto os das soluções em software proprietário.

Gráfico 8 - Respostas da questão 8



Fonte: Elaborada pelo autor.

O gráfico 8 indica que temos 5 por cento que discordam totalmente, 14 por cento que discordam parcialmente, 14 por cento que nem concordaram e nem discordam, 38 por cento que concordam parcialmente e 29 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 19 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 67 por cento, dando uma diferença de 48 por cento, o que é significativo. Estes resultados sugerem uma tendência do público-alvo em achar que os requisitos de segurança das soluções em software livre são tão rigorosos quanto os das soluções em software proprietário. Os sistemas desenvolvidos pelo Serpro são orientados por um ciclo de desenvolvimento seguro, com requisitos de segurança validados em todas as fases do processo. Todo o ciclo é suportado por metodologias, ferramentas e testes especializados na análise de vulnerabilidade do código-fonte.

A questão 9 foi aplicada como o objetivo de verificar se devido ao acesso ao código-fonte (Software Livre) a correção de fragilidades pode ser corrigida rapidamente. Questão 9: o uso de software livre permite que as fragilidades possam ser corrigidas rapidamente.

Gráfico 9 - Respostas da questão 9

Fonte: Elaborada pelo autor.

O gráfico 9 indica que temos 10 por cento que discordam totalmente, 24 por cento que discordam parcialmente, zero por cento que nem concordaram e nem discordam, 33 por cento que concordam parcialmente e 33 por cento que concordam totalmente. A porcentagem de respostas que discordam totalmente e discordaram parcialmente somam 24 por cento, e a porcentagem dos que concordam parcialmente e concordaram totalmente somam 66 por cento, dando uma diferença de 42 por cento, o que é significativo. Estes resultados sugerem que o uso de software livre permite que as fragilidades possam ser corrigidas rapidamente. O acesso ao código-fonte, que é um pré-requisito do Software Livre, permite que as organizações ao detectarem erros ou vulnerabilidades em seus códigos possam rapidamente corrigi-los. No caso dos softwares proprietários, as alterações ou correções só podem ser feitas pela empresa desenvolvedora do software, mediante solicitação formal, o que pode demorar bastante tempo. O processo colaborativo de desenvolvimento de software (subcapítulo 2.3) deste trabalho, explica o modelo Bazar, que é quando um erro ou vulnerabilidade é relatado, este é rapidamente corrigido, simplesmente porque há uma imensa comunidade envolvida e compromissada no processo de correção, e somente encerrarão o processo quando comprovarem que o problema já foi efetivamente solucionado. Portanto, as vezes o erro ou vulnerabilidade detectado pela organização já foi solucionado pela comunidade do software, bastando a empresa baixar o novo código-fonte já corrigido.

A entrevista semiestruturada (APÊNDICE B) foi enviada a três pessoas chaves nas áreas de Software Livre, segurança da informação e coordenação tecnológica do Serpro. Na apresentação e análise das entrevistas será apresentado o resultado analisando o que foi dito pelos entrevistados ou observado pelo entrevistador, com o desejo de responder ao objetivo específico 5, que é de analisar o quanto o domínio do código do software (software livre) afeta a segurança da informação dos clientes internos e externos do SERPRO.

O entrevistado 1, que faz parte da gestão da tecnológica no Serpro, respondeu a entrevista de forma bastante sucinta, mesmo assim ficou claro que no contexto do Governo, o entrevistado entende que a utilização de software livre e padrões abertos traz benefícios, como a independência tecnológica, redução de custos, ampliação da concorrência, desenvolvimento do conhecimento e a inteligência do país na área. Quanto a segurança da informação, que é o objetivo da entrevista, o entrevistado entende que sob as hipóteses de confiabilidade para os sistemas de Governo, que são sistemas complexos com imprevisibilidade estatística, o domínio do código-fonte que o software livre proporciona afeta a segurança da informação no mesmo nível do software proprietário. O entrevistador entrou em contato com o entrevistado por telefone para tentar entender melhor a resposta, porque não ficou claro o quanto o domínio do código-fonte (software livre) afeta a segurança da informação dos clientes internos e externos do SERPRO. A resposta continuou evasiva, não conseguindo o entrevistador se aprofundar na análise. Em relação a independência tecnológica, a resposta do entrevistado está alinhada com (SILVEIRA, 2003), que defende que o Brasil tem mais que o direito, tem a necessidade de utilizar tecnologias que permitam aumentar a sua autonomia tecnológica, a sua participação como desenvolvedor de soluções na sociedade da informação. As discussões em relação ao aspecto segurança do software livre em relação ao proprietário não são recentes, Righetti em 2006 levanta uma discussão em relação a segurança da informação e software livre questionando questões que incluem, além dos aspectos técnicos, a própria soberania da nação. Quanto a segurança da informação, contradizendo o entrevistado, Ferraz (2002) entende que a segurança é um dos aspectos em que o Software Livre mais se destaca. Um argumento comum é que, como o código-fonte está amplamente disponível, os erros não permanecem escondidos por muito tempo.

O entrevistado 2, que faz parte da gestão da segurança da informação no Serpro, respondeu a entrevista de forma bastante detalhada, não necessitando de complementação por telefone. Quanto ao posicionamento do entrevistado sobre a relação entre software livre e segurança da informação, o entendimento é que com o acesso ao código-fonte da aplicação, do sistema operacional ou da solução de armazenamento de dados, na hipótese de descontinuidade do desenvolvimento do produto a empresa ou o usuário terá a possibilidade de promover o desenvolvimento e suporte de sua plataforma a partir de iniciativa própria, com equipe de desenvolvimento específica. A resposta do entrevistado está alinhada com (SILVEIRA, 2003), que defende que o Brasil tem mais que o direito, tem a necessidade de

utilizar tecnologias que permitam aumentar a sua autonomia tecnológica, a sua participação como desenvolvedor de soluções na sociedade da informação, e também está alinhada ao próprio conceito do Software Livre descrita no subcapítulo 2.4.1 deste trabalho.

Quanto a possibilidade de evolução do código-fonte, o entrevistado entende que o Software Livre representa também a possibilidade de, para um determinado produto, o responsável pelo desenvolvimento de uma dada organização garantir a implementação de seus próprios requisitos de segurança, construindo as soluções que julgue mais adequadas à garantia de controle de acesso ao seu ambiente em conformidade com os padrões de segurança que seu negócio necessita, ou seja, com o acesso ao código-fonte podemos alterar o código as nossas necessidades, viabilizando excelentes opções para que o responsável pela estratégia de segurança construa, com as áreas de desenvolvimento, um modelo de desenvolvimento seguro bastante evoluído, bem desenhado e condizente com a política de segurança da organização. A resposta do entrevistado vai de encontro ao conceito do software livre, que é apresentado no subcapítulo 2.4.1 deste trabalho, principalmente a liberdade 1, que cita que com o acesso ao código-fonte temos a liberdade de estudar como o programa funciona, e adaptá-lo às nossas necessidades.

Quanto a ferramentas de análise de forense computacional, que consistem em um conjunto de técnicas para coleta e exame de evidências digitais, reconstrução de dados e ataques, identificação e rastreamento de invasores, o entrevistado ressaltou que o Serpro possui excelentes soluções livres, embora a empresa também utilize algumas soluções proprietárias. A resposta do entrevistado está alinhado com o direcionamento do Serpro, que vem investindo em inteligência artificial e cruzamento de dados para coibir ações fraudulentas, além do constante processo de segurança da informação em que a Empresa está inserida, com utilização de forense computacional, em ações preventivas dentro do Serpro e para o cliente. Reforçando o que foi citado pelo entrevistado em relação a existência de soluções livres, existem hoje, diversos sistemas operacionais baseados em Software Livre, desenvolvidos para gestores da informação e computação forense. Os sistemas possuem ferramentas e aplicativos exclusivos para realização de testes, análises e atividades da área, tais como: recuperação de arquivos apagados, analisadores de logs do sistema e programas, engenharia reversa, testes de invasão, vasculhador de tarefas executadas no sistema, analisador de protocolos enviados e recebidos na rede, programas de força bruta para quebrar senhas, entre outras coisas

Quanto a espionagem (item 2.5.2 deste trabalho), o entrevistado entende que diante do cenário atual em que vimos toda uma ação do governo norte-americano em estreita cooperação com a iniciativa privada, no sentido de fomentar a inserção de "portas de acesso" em aparelhos e software de modo a garantir uma indevida quebra de confidencialidade de sistemas públicos e particulares, o uso de software livre pode representar um robusto ativo na construção de soluções de Estado imunes a esses acertos público-privados espúrios, garantindo maior segurança cibernética e maior efetividade na construção de ferramentas de defesa cibernética. O posicionamento do entrevistado está alinhado com (SILVEIRA,2004), que defende que usando o software livre, o governo pode analisar todo o código que adquire, e retirar rotinas duvidosas que estariam presentes no software em uso; enfim, pode alterá-lo para dar maior segurança. No subcapítulo 2.5.2 deste trabalho, é tratado o assunto da espionagem, onde é citado que em novembro de 2013, o governo federal publicou portaria que regulamenta os critérios de auditoria de segurança de sistemas de comunicação do governo e reconhece o Software Livre como auditável, estabelecendo que softwares públicos e livres são considerados auditáveis.

Quanto a gestão de continuidade, o entrevistado entende que é extremante importante para a segurança da informação, e que a ideia de resiliência e continuidade estão presentes no próprio conceito de software livre e em sua disponibilidade integral (desde o código) para prover solução em circunstâncias de contingência. A resposta do entrevistado está alinhada com o direcionamento estratégico do Serpro, que tem investido na internalização de tecnologias livres, e que está exigindo nas licitações realizadas por sua área jurídica, que o vencedor disponibilize o código-fonte do produto como Software Livre, para garantir que a descontinuidade do produto não afete os seus serviços (SERPRO Informações Normativas, SINOR, 2014).

Quanto a resiliência, a posição do entrevistado é que a busca pela construção de uma engenharia corporativa de resiliência (resiliência corporativa). Para uma empresa que se vê obrigada a utilizar as melhores soluções proprietárias do mercado, em razão dos níveis de serviço e dos elementos estratégicos, poder contar com software livre é muito importante.

Quanto a auditoria, o entendimento eu entrevistado é que existirem inúmeras ferramentas livres de qualidade que oferecem solução na realização de auditorias, a própria concepção geral do software livre guarda extrema afinidade com a geração de trilhas de auditoria. Para que uma solução seja auditável, é necessário ter acesso ao código-fonte, neste

sentido a resposta do entrevistado vai de encontro a própria ausência do viés proprietário tradicional em torno do software livre, o que viabiliza uma maior transparência e rastreabilidade no ambiente livre que no ambiente proprietário.

O entrevistado 3 não respondeu a entrevista.

Por fim, os resultados desta pesquisa apontam que com o modelo do software livre não são necessários investimentos na compra de software, uma vez que este se encontra disponível, sendo possível copiar, alterar e distribui seu código fonte. Do ponto de vista da segurança, é muito importante as organizações terem acesso ao código-fonte das soluções usadas, afinal as empresas desenvolvedoras podem estar abrindo sua rede a qualquer pessoa que conheça o código-fonte que você desconhece. Não é que todo livre seja seguro, mas, como é aberto, é possível saber se é seguro (SILVEIRA, 2006).

Diante desses achados, as seguintes considerações finais e trabalhos futuros foram traçados.

7 CONSIDERAÇÕES FINAIS

O objetivo deste trabalho foi analisar a segurança da informação no Governo Federal Brasileiro a partir da internalização das politicas de incentivo ao Software Livre no SERPRO fazendo a análise de como a internalização destas politicas impacta a segurança das informações dos seus clientes.

Antes de fazermos a conclusão deste trabalho, é importante analisarmos o desenvolvimento dos computadores e a globalização proporcionada pela Internet. A Internet é o principal meio de comunicação existente na atualidade, qualquer informação hoje é compartilhada pela rede, você pode receber informações do outro lado do mundo em questões de segundos. Não se pode considerar a Internet uma tecnologia perfeita, pois se não for utilizada de maneira correta acaba trazendo consequências desagradáveis, provocando vários danos para particulares, empresas ou governos. Existem pessoas que possuem um conhecimento avançado nas tecnologias usadas e do seu funcionamento, e estes utilizam este conhecimento para acessar ilegalmente bases de dados com informações muitas vezes sigilosas. Nesta visão, percebemos a segurança da informação como um ponto extremamente importante, pois ela defende um dos maiores patrimônios das organizações , suas informações. A grande preocupação com a proteção das informações a qualquer custo sob pena de grandes prejuízos é um tema atual. Seguindo esta tendência, surgem tecnologias que prometem elevado nível de segurança e proteção.

Nos últimos anos o Governo brasileiro tem incentivado a adoção do Software Livre como estratégia da sua politica de TI para as empresas da administração Federal, entendendo que uma das vantagens tecnológicas proporcionada é uma melhor segurança das informações, porque tecnologicamente abre à possibilidade de identificar e adaptar a lógica do sistema para um formato confiável de transporte e de divulgação das informações.

O SERPRO trabalha com dados sigilosos dos seus clientes, como o Imposto de Renda da pessoa física e jurídica, por exemplo, e nos últimos anos, tem desenvolvido e utilizado ferramentas livres para o desenvolvimento de soluções que impactam a gestão destas informações.

A análise dos resultados procurou respondeu quais os impactos do uso de Software Livre para a segurança das informações dos clientes do Serpro. Os resultados deixaram a percepção que é dada prioridade a soluções livres na internalização de novas tecnologias na empresa, e que o acesso ao código-fonte tem relação direta com a proteção dos dados, porque

permite que as possíveis fragilidades sejam corrigidas rapidamente. O custo da manutenção de soluções em Software Livre não é maior do que em uma solução proprietária, e que as ferramentas e segurança em software livre estão no mesmo nível de maturidade das proprietárias. Nos casos de espionagem, existe a possibilidade da inserção de "portas de acesso" nos softwares proprietários adquiridos pelo Governo, sendo que com a compra ou desenvolvimento de soluções em software livre o código-fonte podem ser auditado.

O Software Livre ou quaisquer outros mecanismos tecnológicos atuais não são suficientes para garantir a eficácia da segurança da informação nas organizações, pois esta eficácia só pode ser atingida através de uma politica de segurança corporativa, que envolva todos os aspectos, como os técnicos e pessoais. Um sistema seguro depende além dos setores de segurança da informação, de toda a instituição. Afinal, falhas de pessoas tornam vulneráveis tecnologias ou processos implementados para a segurança das informações. Para concluir, no contexto de uma politica de segurança, a organização ter acesso ao código-fonte proporcionada pelo software livre poderá trazer maior segurança as informações, porque terá certeza que não existem códigos maliciosos embutidos no seu código-fonte, e caso necessário poderá alterá-lo para deixá-lo de acordo com a politica de segurança corporativa.

Como possíveis trabalhos futuros, pode-se apontar:

- Neste estudo foram exploradas características de segurança. A identificação de potenciais de melhoria de qualidade e redução de custos na utilização de ferramentas livres oferece a possibilidade de estudos em relação as lacunas existentes entre o tempo no processo de aquisição de produtos demandando estudos futuros para a identificação destas;
- Estudo para criação de um repositório de ferramentas de segurança em software livre para que sirvam como padrão para todas as empresas da administração pública federal;
- As leis e licitações muitas vezes são estruturadas com foco no modelo proprietário, o que traz dificuldade para que o produto em software livre seja oferecido. Como trabalho futuro fazer um estudo nas leis e nos processos de licitação das empresas da administração Pública Federal, para que soluções livres concorram com as proprietárias no mesmo patamar.

REFERÊNCIAS

BRASIL. **Instrução Normativa Nº 1 de 13.06.2008**. Gabinete de Segurança Institucional da Presidência da República, Brasília, 2008. Disponível em: <http://www.mct.gov.br/index.php/content/view/72703.html>. Acesso em: 24 ago. 2014.

BRASIL. **Instrução Normativa Nº 04**, de 12 de novembro de 2010. Disponível em: <https://www.governoeletronico.gov.br/anexos/instrucao-normativa-no-04>. Acesso em: 15 set. 2014.

BRASIL. **Comitê Executivo do Governo Eletrônico**. A política de governo eletrônico no Brasil. Brasília, DF, 2001. 8 p. Disponível em: <www.governoeletronico.gov.br/governoeletronico/index.html>. Acesso em: 25 ago. 2014.

BRASIL. **Federal. Software Livre**. Disponível em: <http://www.brasil.gov.br/>. Acesso em: 14 out. 2014.

BRASIL. **Aviso Circular nº 40 /SE-C.Civil/PR**. Disponível em: <http://www.softwarelivre.gov.br/documentos-oficiais/circulardominstro/?> searchterm=circular. Acesso em: 02 set. 2014

BRASIL. **Projeto de Lei PL 2269/1999**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=17879>. Acesso em: 09 set. 2014.

BRASIL. **Portaria Interministerial nº 141**. Disponível em: <http://www.softwarelivre.gov.br/news/portaria-interministerial-estabelece-normas-de-seguranca-as-informacoes-governamentais/>. Acesso em 21 set. 2014.

BRASIL. **Lei n nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União , Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 out. 2014

BRASIL. Comitê Executivo do Governo Eletrônico. **A política de governo eletrônico no Brasil**. Brasília, DF, 2001. 8 p. Disponível em: <www.governoeletronico.gov.br/governoeletronico/index.html>. Acesso em: 25 ago 2014.

BRASIL. **Razões para adoção de Software livre**. Disponível em: <http://www.planalto.gov.br/>. Acesso em: 14 out. 2014.

BRASIL. **Lei nº. 9.609/98**, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 13 nov. 2014.

BORGES, Job Diógenes Ribeiro. **Governo Eletrônico e Software Livre**: A Tecnologia com a Cidadania a Serviço da Comunidade. Disponível em: <http://buscalegis.ccj.ufsc.br>.

Acesso em: 03 out. 2014.

BRETTHAUER, David. **Open Source Software**: A history.Information Technology and Libraries, v. 21, n. 1, p. 3-10, UConn Libraries Published Works, Connecticut, 2001.

CARDOZO, Richard N. **An experimental study of consumer effort, expectation and satisfaction. Journal of Marketing Research**, v. 2, n. 3, p. 244-249, Chicago, August, 1965.

CHASSELL, R. J., **How to Make a Living with Free Software**, Transcrição da apresentação em Software Park, Tailândia, 24 de Outubro de 2000.

CISL, **Comitê de Implementação de Software Livre do Governo Federal**. Disponível em: <http://www.softwarelivre.gov.br/planejamento-cisl/rascunho-planejamento-2013-2014>. Acesso em: 25 ago. 2014.

DSCI. **Departamento de Segurança da Informação e Comunicação**. Disponível em: <http://dsci.planalto.gov.br>. Acesso em: 25 ago. 2014.

RAYMOND, Eric S. **Homesteading the Noosphere**. Technical report, Abril 1998. Disponível em: <www.tuxedo.org/~esr/writings/homesteading/>. Acesso em: 02 set. 2014.

The USA PATRIOT Act. **Preserving Life and Liberty**. Disponível em: <http://www.justice.gov/archive/ll/highlights.htm>. Acesso em: 15 ago. 2014.

EVANGELISTA, Rafael de Almeida. **Liberdade ? Que Liberdade ?** Disponível em: <http://www.softwarelivre.org/news/8420>. Acesso em: 09 set. 2014.

FALCAO, et.alli, Estudo sobre o Software Livre - 2005,P.20

HEXSEL, Robert A. **Propostas de ações de Governo para incentivar o uso de software livre**. Relatório Técnico do Departamento de Informática da UFPR, n. 004/2002, Curitiba, outubro, 2002. Disponível em: <http://www.inf.ufpr.br/info/techrep/RT_DINF004_2002.pdf>. Acesso em: 29 ago.2014.

LEVINE, D. M. ; BERENSON, M. L.; STEPHAN, D. **Estatística: Teoria e Aplicações**. 1. ed. Rio de Janeiro: LTC, 2000. 811 p.

Mercado Brasileiro de Software: panorama e tendências, 2014 Brazilian Software Market: scenario and trends, 2014 [versão para o inglês: Anselmo Gentile] - 1ª. ed. - São Paulo: ABES - Associação Brasileira das Empresas de Software, 2014.

MESQUITA, Cláudia do Socorro Ferreira. BRETAS, Nazaré Lopes (orgs). **Panorama da Interoperabilidade no Brasil**. Ministério do Planejamento, Brasília, 2010.

NASA. Code Nasa. Disponível em: http://code.nasa.gov. Acesso em: 14 nov. 2014.

OLIVA, Alexandre. **The competitive advantage of free**. Anais do I Fórum Internacional Software Livre 2000 (Workshop Acadêmico - WSL2000). Porto Alegre: Sociedade Brasileira

de Computação. Auditórios do CEPUCRS, 04 e 05 mai. 2000, p.19-22.

[Palmer and Corporation 2001] Palmer, G. and Corporation, M. (2001). **A road map for digital forensic research**. Technical report.

PCSI. **Política Corporativa de Segurança da Informação**. Disponível em: <http://sinor.portalcorporativo.serpro/documento.php?cod=MTM2MTY>. Acesso em: 16 set. 2014.

ACTUATE. Software Livre Na Europa. Disponível em: <http://www.linux.com/news/enterprise/biz-enterprise/111756-europe-leads-oss-adoption-china-rising-fast>. Acesso em: 15 set. 2014.

RIGHETTI, Sabine. **Software livre é prioridade do governo**. Disponível em: <http://www.comciencia.br/200406/reportagens/08.shtml>. Acesso em: 26 ago. 2005.

RUA, M. **Políticas Públicas**. Departamento de Ciências da Administração, Florianópolis, 2009.

SABINO, Vanessa Cristina. **Um estudo sistemático de licenças de software livre**. 2011. Tese de Doutorado. Universidade de São Paulo. OSI, Open Source Iniciative, Disponível em: <http://opensource.org/>. Acesso em: 30 ago. 2014.

SARAVIA, E. **Políticas Públicas - Coletânea**. Escola Nacional de Administração Pública, Brasília, v.1, p. 21-42, 2006.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: Uma visão Executiva. Rio de Janeiro: Campus,

SERPRO 2013 - Decisão de Diretoria (PSSL) SERPRO 2007 - Decisão de Diretoria (PSSL)

SERPRO. **Segurança da Informação**. Disponível em: <https://www.serpro.gov.br/conteudo-tecnologia/infraestrutura/seguranca>. Acesso em: 25 ago. 2014.

SILVEIRA, Sérgio Amadeu da. Software livre: **a luta pela liberdade do conhecimento**. São Paulo: fundação Perseu Abramo, 2004.

SISP. **Sistema de Administração dos Recursos de Tecnologia da Informação**. Disponível em: <http://www.governoeletronico.gov.br/sisp-conteudo/index>. Acesso em: 25 ago. 2014.

e-PING. **Padrões de Interoperabilidade de Governo Eletrônico**. Disponível em: <http://www.governoeletronico.gov.br/anexos/artigo-e-ping-desburocratizacao/view?searchterm=e-ping>. Acesso em: 25 ago. 2014.

PORTUGAL. **Software livre na Europa**. Disponível em: <http://www.softwarelivre.citiap.gov.pt/sw_livre_europa>. Acesso em: 30 ago. 2014.

GNU. **A Definição de Software Livre**. Disponível em: <http://www.gnu.org/philosophy/free-

sw.pt-br.html>. Acesso em: 15 ago. 2014.

STALMANN, Richard. **Histórico**. Disponível em: <http://www.infoescola.com/biografias/richard-stallman/>. Acesso em: 31 ago. 2014.

IBM. **Open Source Innovation on Power Systems**. Disponível em: <http://www-03.ibm.com/press/us/en/pressrelease/41926.wss>. Acesso em: 30 ago. 2014.

BERNSTEIN, D. J. **Internet host SMTP server survey**. 2003. Disponível em: <http://cr.yp.to/surveys/smtpsoftware6.txt>. Acesso em: 30 ago. 2014.

SERPRO. **Framework Demoiselle**. Disponível em: <https://www.frameworkdemoiselle.gov.br/>. Acesso em: 30 ago. 2014.

W. BANK. The World Bank: eGovernment , 2009.

WIRED, "**We Pledge Allegiance to the Penguin**" in Wired Magazine, Issue 12.11, November,2004.

Governo Brasileiro. Adoções de Policias públicas de Software Livre. Disponível em: http://www.softwarelivre.gov.br/publicacoes/guia-livre-referencia-de-migracao-para-software-livre?searchterm=guia+livre. Acesso em: 30 set. 2014.

TAURION, Cezar. Software Livre: **Potencialidades e modelo de negócios**. Rio de Janeiro: Brasport, 2004.

TORVALDS, Linus. **Brasil ganha em independência ao adotar software livre**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/08/brasil-ganha-em-independencia-ao-adotar-software-livre-diz-pai-do-linux.html>. Acesso em: 30 set. 2014.

KAYWORTH, T.; WHITTEN D. **Effective Information Security Requires a Balance of Social and Technology Factors**. MIS Quarterly Executive, v. 9, n. 3, p. 163-175, 2010.

SERPRO. **Segurança da informação**. Disponível em: <https://www.serpro.gov.br/noticias/setor-publico-discute-seguranca-da-informacao>. Acesso em: 06 out. 2014.

EXAME, Revista. **O Plano B**. Edição 0751, Outubro de 2001. Disponível em: <http://exame.abril.com.br/revista-exame/edicoes/0751/noticias/o-plano-b-m0050962>. Acesso em: 03 out. 2014.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 03 out. 2014.

MÓDULO SECURITY SOLUTIONS. **10ª Pesquisa Nacional sobre Segurança da Informação**. Módulo Security Solutions S.A 2003. Disponível em: <http://www.modulo.com.br/software/casos-de-sucesso/99-pesquisas>. Acesso em: Acesso

em: 03 out. 2014.

FSF. **Free Software Foundation**. Disponível em: <https://www.fsf.org>. Acesso em: 03 out. 2014.

SILVEIRA, Sério Amadeu da, **Exclusão Digital: a miséria na era da informação**: São Paulo: Editora Fundação Perseu Abramo, 2001.

FERRAZ, Nelson Corrêa de Toledo. **Vantagens Estratégicas do Software Livre para o Ambiente Corporativo**. São Paulo: MBIS-PUC/SP, 2002.

SecurityFocus. **Pesquisa: Segurança da informação**. Disponível em: <http://www.securityfocus.com/>. Acesso em: 03 out. 2014.

Pacto do software livre. Disponível em: <http://www.freesoftwarepact.eu/post/Signatories-for-the-2009-campaign>. Acesso em: 14 out. 2014.

SILVEIRA, Sérgio Amadeu da. Software livre: a luta pela liberdade do conhecimento / SérgioAmadeu da Silveira. São Paulo : Editora Fundação Perseu Abramo, 2004

YIN, Roberto K. Estudo de caso: planejamento e métodos. 2ª Ed. Porto Alegre. Editora: Bookmam. 2001.

MANZINI, E. J. **A entrevista na pesquisa social**. Didática, São Paulo, v. 26/27, p. 149-158, 1991.

FAUSCETTE, Michael. 2014. Mercado de Software Livre. Disponível em: <http://softwarelivre.org/portal/noticias/mercado-de-software-livre-deve-crescer-acima-de-22-ao-ano>. Acesso em: 06 nov. 2014.

APÊNDICE A - QUESTIONÁRIO

1. Na internalização de novas tecnologias no Serpro é dada prioridade as soluções livres pensando na segurança da informação. *

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo
( ) Concordo parcialmente
( )Concordo totalmente

2. O código fonte de uma solução livre tem relação direta com a proteção dos dados.*

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo
( ) Concordo parcialmente
( )Concordo totalmente

3. Conheço caso em que foi detectada falha de segurança no acesso aos dados devido à vulnerabilidade constatada no código fonte. *

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo
( ) Concordo parcialmente
( )Concordo totalmente

4. O acesso ao código fonte (software livre) abre possibilidades para fragilidades. *

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo

( ) Concordo parcialmente
( )Concordo totalmente

5. A quantidade de exploradores de falhas de segurança em sistemas operacionais livres é proporcional ao seu uso. *

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo
( ) Concordo parcialmente
( )Concordo totalmente

6. O custo de se manter uma solução de segurança em software livre é maior do que em uma solução proprietária. *

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo
( ) Concordo parcialmente
( )Concordo totalmente

7. As ferramentas de segurança em software livre estão no mesmo nível de maturidade em relação às ferramentas proprietárias. *

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo
( ) Concordo parcialmente
( )Concordo totalmente

8. Os requisitos de segurança das soluções em software livre são tão rigorosos quanto os das soluções em software proprietário. *

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo
( ) Concordo parcialmente
( )Concordo totalmente

9. O uso do software livre permite que as fragilidades possam ser corrigidas rapidamente. *

( ) Discordo totalmente
( ) Discordo parcialmente
( ) Nem concordo nem discordo
( ) Concordo parcialmente
( )Concordo totalmente

APÊNDICE B - ENTREVISTA

1. Qual a relação entre software livre e segurança da informação?