REVISTA CONEXÃO ELETRÔNICA

SOFTWARES DE CÓDIGO ABERTO E LIVRES: Conceitos, Definições e Ferramentas para Segurança da Informação

Alexandre Honorato Sabino
Graduando em Engenharia da Computação,
Faculdades Integradas de Três Lagoas – FITL/AEMS

Jonathan Yukio Sakata
Graduando em Engenharia da Computação,
Faculdades Integradas de Três Lagoas – FITL/AEMS

Lucas Matheus de Carvalho Gomes
Graduando em Engenharia da Computação,
Faculdades Integradas de Três Lagoas – FITL/AEMS

Vinícius Paggioli de Carvalho
Mestre em Engenharia Mecânica - UNESP
Docente das Faculdades Integradas de Três Lagoas – FITL/AEMS

Richard Vieira do Espirito Santos
Graduado e Esp. em Engenharia Mecatrônica – UniSALESIANO
Docente das Faculdades Integradas de Três Lagoas – FITL/AEMS

André Aparecido Leal de Almeida
Graduado em Análise e Desenvolvimento de Sistemas – FITL/AEMS;
Docente das Faculdades Integradas de Três Lagoas – FITL/AEMS

RESUMO
Este projeto teve como objetivo mostrar as possibilidades de utilização de softwares de código aberto, focados na segurança de rede. Ao longo do artigo foi discutido o motivo da importância da segurança, definições de softwares livre e código aberto, apresentando seus conceitos e ideias propostas pelos mesmos. Por último são exemplificados softwares para uma rede segura. O exemplo utiliza alguns dos softwares mais atuais e comuns em meio corporativo, e que são gratuitos.

PALAVRAS-CHAVE: internet; software livre; código aberto; linux; segurança.

1 INTRODUÇÃO

Na internet usuários fazem transações bancárias; armazenam arquivos pessoais em nuvem; empresas transmitem informações confidenciais; governos transferem arquivos, são inúmeras as transações que podem ser realizadas na rede. No entanto, com os benefícios da expansão da internet, existem também os malefícios. Assim como no mundo real existem roubos, sequestros, falsificação de documentos, no mundo digital o mesmo também ocorre, porém com relação aos dados. Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de

Segurança no Brasil (Cert.br), em 2018 houveram 676.514 mil incidentes reportados ao grupo. Embora os incidentes tenham sido reduzidos com relação ao ano anterior, o número ainda é alarmante. Uma organização precisa proteger seus dados. É neste ponto que a segurança deve se mostrar forte.

A segurança é um assunto antigo, porém se desenvolveu à medida que novos desafios foram surgindo. É a responsável pela proteção dos dados da organização. Hoje existem diversas técnicas de segurança de redes, desde recursos que demandam alto custo à aquelas que utilizam um baixo custo de implementação.

Este projeto demonstra a importância da segurança e como é possível montar uma infraestrutura que protege os dados. Tudo com um custo zero ou custo minimizado utilizando Softwares Livre/Código Aberto.

2 OBJETIVOS

O objetivo deste trabalho é apresentar a importancia da segurança da informação usando ferramentas e software livres bem como diferenciar os tipos de licenciamentos usados nesses Softwares e apontar as principais vantagens de sua utilização. E por fim, comparação de custos de ferramentas com licenças pagas e software livres.

3 MATERIAL E MÉTODOS

A metodologia utilizada neste trabalho baseou-se em pesquisa bibliográfica da literatura científica nacional e internacional publicada em livros e artigos específicos do tema. Os últimos encontram-se indexados em plataformas especializadas de divulgação científica como o Google acadêmico e pesquisas online em websites dos desenvolvedores dos softwares e ferramentas em questão. As palavras chaves utilizadas foram Internet, Software Livre, Código Aberto, Linux, Segurança. Priorizaram-se dados recente, embora não se excluíram publicações antigas contendo material relevante.

4 EXPANSÃO DA INTERNET

As novas tecnologias de informação e comunicação que surgiram após os

anos de 1960, mudaram a forma comum, a qual o mundo se comportava, sob diferentes dimensões (CASTELLS; CARDOSO, 2005). O surgimento da internet é um exemplo. A internet vem transformando completamente a forma com que usuários lidavam com os dados. As informações agora podem ultrapassar fronteiras e viajar vários quilômetros. A interconexão de redes contribuiu de forma imensurável ao mundo, possibilitando o que nem os cientistas imaginavam.

No entanto, com mais dados sendo trafegados é necessário um esquema de segurança mais forte. Com a alta expansão da internet, usuários dispõem grandes quantidades de informações valiosas na rede e, tendo conhecimento deste fato, pessoas mal-intencionadas podem tentar tirar vantagem sobre este ponto.

Em decorrência, novas técnicas de segurança tiveram de ser descobertas, a fim de acompanhar tamanha expansão e ainda assim proteger os dados, como o caso da criptografia por exemplo (DEITEL; DEITEL; CHOFNES, 2005).

O avanço tecnológico e a inovação são de grande contribuição à humanidade, porém, se não receberem a devida atenção e deixarem que seu encanto ofusque outras questões importantes, pode acabar por se tornar um ponto negativo ao invés de auxílio à quem a utiliza.

5 SEGURANÇA DA INFORMAÇÃO

No decorrer do tempo, a informação foi ganhando cada vez mais seu espaço. Seja em guerras, revoluções, ou a competitividade, a informação sempre esteve presente se mostrando um diferencial na obtenção dos objetivos (SÊMOLA, 2015). No presente, a informação é um patrimônio de extrema importância às empresas. A norma brasileira NBR ISO/IEC 17799:2005 diz que “A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida” (ABNT, 2005, p. ix). Sendo assim, a informação tem grande valor à organização e, observando sua importância, sua proteção necessita de uma grande consideração. Somada a ideia do compartilhamento de dados que se desenvolveu ao longo dos anos, a informação acabou por se tornar ainda mais vulnerável, necessitando de um zelo muito maior.

A segurança deve ser levada a sério, principalmente se em meio corporativo. Muitos usuários e gerentes somente percebem a necessidade de investimentos em

segurança até que uma falha ocorra (STALLINGS, 2015). Uma situação que se deve evitar ao máximo, pois uma falha pode representar grandes danos à organização.

Estudos já definiram os pontos que uma rede deve seguir pra ser considerada segura. Obedecendo a estes critérios o usuário obterá uma rede mais protegida e confiável.

5.1 Definição de Segurança da Informação

Conforme diz o Manual de segurança do NIST[1], a segurança da informação é "A proteção de informações e sistemas de informação contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizada, garantindo a confidencialidade, integridade e disponibilidade." (NIST, 2017, p. 2). Desta forma, assegurando estes pontos, a segurança pode ser atingida.

A confidencialidade diz respeito a restrição de acesso a informação. Somente o remetente e o destinatário devem entender conteúdo da mensagem transmitida (KUROSE; ROSS, 2012). A integridade significa que os dados não podem ser alterados de maneira não autorizada. Por fim, a disponibilidade diz que deve-se garantir o acesso e uso confiável da informação (NIST, 2017).

Além destas propriedades já definidas, Kurose e Ross (2012) elencam ainda outros dois pontos em que a segurança da informação deve atuar, sendo a autenticação de ponto final e a segurança operacional. A autenticação de ponto final define que o remetente e destinatário devem confirmar suas identidades, a fim de provar que a outra parte alega quem é ser. Já a segurança operacional diz respeito a mecanismos operacionais da organização, a fim de auxiliar os administradores de rede a proteger o sistema. *Firewalls* e sistema detectores de invasão são exemplos (KUROSE; ROSS, 2012). No entanto, conhecer somente as defiinções de segurança da informação não é o suficiente. É necessário um "esquema" para atingí-la. A norma ABNT NBR ISO/IEC:17799:2005 propõe um modelo para implementar a segurança da informação em uma organização. Seguindo este padrão da ABNT (2005), a organização deve: (i) estabelecer seus requisitos de segurança (definição dos pontos a serem protegidos. Uma análise de riscos à organização é um exemplo) e (ii) prover

[1] *National Institute Standards and Technology (NIST) – Instituto Nacional de Padrões e Tecnologia: Laboratório de Ciências Físicas dos Estados Unidos que fornece medição e padrões de tecnologia para promover a inovação e competitividade do país. (https://www.nist.gov/about-nist).*

uma seleção de controles (esta parte constitui a maior parte da gestão da segurança da informação).

Depois de estabelecidos os requisitos, esta etapa provê um conjunto de controles apropriados para assegurar que os riscos sejam reduzidos a um nível aceitável. Alguns métodos de controles que são fornecidos pela norma estão listados a seguir: documento de política de segurança da informação; atribuição de responsabilidades para a segurança da informação; conscientização, educação e treinamento em segurança da informação; processamento correto nas aplicações; gestão de vulnerabilidades técnicas; gestão da continuidade do negócio; gestão de incidentes de segurança da informação e melhorias.

Tendo o conhecimento sobre a importancia e o que é a segurança da informação, e, seguindo a este método proposto pela norma, a organização deverá ser capaz de implementar uma gestão da segurança da informação eficiente.

Existem também outros modelos de Gestão da segurança da informação. Este projeto citou a NBR ISO/IEC:17799:2005 de forma bem resumida. Ao leitor interessado em se aprofundar mais no tema, recomenda-se a leitura da própria norma, ou outros materias a respeito do tema.

6 SOFTWARES DE SEGURANÇA

Os passos para atingir a segurança podem ser minimizados utilizando do auxílio de aplicações de segurança. Um software de segurança tem a função de prevenir, identificar, eliminar e reparar ameaças ao sistema e seus possíveis danos causados. Atualmente existem diversos tipos de softwares de segurança: Pfsense, Admfirewall, Kaspersky, Norton, Malwarebytes, Ccleaner, BitDefender, IPFire, ESET, Mcafee, Zabbix, entre uma variedade de outros softwares.

Muitos destes softwares disponíveis são oferecidos sob uma licença paga. Estes oferecem um manuseio simples do software e garantias quanto aos serviços adquiridos. Além do mais, softwares pagos podem oferecer serviços exclusivos em relação aos outros softwares.

Em contrapartida existem também os softwares gratuitos, que simplesmente são softwares que podem ser adquiridos e manuseados sem custo.

Nesta seção é apresentada a definição de Softwares Livres e Código Aberto, a idéia proposta por seus projetos e as possíveis vantagens e desvantagens de sua

utilização.

6.1 Software Livre

Software Livre nasceu do ideia do compartilhamento do conhecimeto. Para o fundador do movimento, Richard Stallman, o conhecimento que constitui um programa (o código-fonte) deve ser livre e não restrito. Isto contribui para a computação e é necessário para que a inovação ocorra (O'REILLY, 1999).

Conforme a definição da *Free Software Foundation* (FSF), a organização que promove e incentiva o uso do *software* livre, "Software livre é um software que oferece ao usuário a liberdade de compartilhá-lo, estudá-lo e modificá-lo". Ainda conforme definição do sistema GNU (acrônimo para "GNU is Not Unix"), o *software*, para ser considerado livre, deve atender a quatro requisitos: (i) liberdade 0 (a liberdade de executar o programa como você desejar, para qualquer propósito); (ii) liberdade 1 (a liberdade de estudar como o programa funciona, e adaptá-lo às suas necessidades); (iii) liberdade 2 (a liberdade de redistribuir cópias de modo que você possa ajudar outros) e (iv) liberdade 3 (a liberdade de distribuir cópias de suas versões modificadas a outros). Desta forma, pode-se dar a toda comunidade a chance de beneficiar de suas mudanças.

De maneira informal, este é o tipo de software que, depois de adquirido, o usuário tem o direito de usar, mudar o software, desinstalá-lo, instalar novamente em 10 máquinas diferentes, copiar o software e compartilhar as cópias, compartilhar cópias modificadas, tudo isso sem nenhuma restrição. O usuário tem "liberdade para usar o software".

É importante não confundir *software* "livre" como *software* "gratuito". Embora a ideia do movimento remeta a essa noção, não significa que o autor do *software* deve disponibilizá-lo gratuitamente (mas, é o que geralmente ocorre). O *software* é livre no sentido de liberdade e não como se fosse algum "objeto" gratuito (O'REILLY, 1999).

Todos esses direitos do usuário são garantidos por licenças que atendam a estes quatro princípios de liberdade. A primeira licença criada e muito comumente utilizada é a *GNU General Public License*, conhecida como GNU GPL ou simplesmente GPL.

6.2 Software Código Aberto

A proposta de Stallman não foi bem aceita pela indústria. Muitos acreditavam

que usar este tipo de abordagem era “anti-capitalista”. A resposta que surgiu devido a esta recusa foi a ideia de software *open source* (código aberto), que em parte seguia a ideia de *software* livre (SABINO, KON, 2004).

Segundo a *Open Source Initiative* (OSI), corporação formada para educar e defender os benefícios do código aberto, para ser considerado *Open Source* o software deve obedecer a dez critérios, tais como: Redistribuição Livre (a licença não deve impedir ninguém de vender ou distribuir o software como parte de uma outra distribuição agregada de software); código fonte (o código-fonte deve ser distribuido); trabalhos derivados (a licença deve permitir modificações e trabalhos derivados); integridade do código fonte do autor; não discriminação contra pessoas ou grupos; não discriminação contra campos de atuação (a licença não deve impedir ninguem de usar o programa); distribuição de licença (os direitos associados ao programa devem ser aplicados a todos a quem o programa é redistribuído); a licença não deve ser específica para um produto; a licença não deve restringir outro software; a licença deve ser neutra em termos de tecnologia (nenhuma disposição da licença pode ser baseada em nenhuma tecnologia ou estilo de interface individual).

Em comparação à proposta do Software Livre, o modelo de Código de Aberto permitia uma “mistura” melhor com a ideia de propriedade:

> A definição de código aberto permite maiores liberdades com licenciamento do que a GPL. Em particular, a definição de código aberto permite maior promiscuidade ao misturar software proprietário e de código aberto (O’REILLY, 1999, p.11).

Assim, organizações que tinham certo receio com as licenças do tipo Software Livre viram que suas ideias eram mais compatíveis com o movimento do código aberto, podendo então alterar sua licença para o novo modelo proposto e manter sua postura proprietária (O’REILLY, 1999).

6.3 Motivos para Utilizar

O sentimento de que um software “gratuito” é inferior aos demais *softwares*, é uma ideia errada a respeito do mesmo, o que pode ser comprovado pelo conceito que os envolve (HEXSEL, 2002). Na verdade, softwares livre e código aberto são desenvolvidos e testados por toda uma comunidade de desenvolvedores que trabalham em busca de um software melhor (GARCIA et al., 2010; O’REILLY, 1999). Raymond (2010) define isto como Lei de Linus quando diz que “Havendo olhos suficientes todos os erros são óbvios”. Isto é, com mais pessoas vendo o código, maiores são as chances de encontrar erros e bugs (RAYMOND, 2010).

Poucos projetos de software têm um alcance tão grande em número de desenvolvedores quanto a de projetos de software livre já existentes. Ainda conforme o mesmo, cerca 400 mil desenvolvedores contribuíram para o projeto GNU/ Linux, o que resulta em um software mais robusto (SILVEIRA, 2005).

Castells (2003) tambem faz a mesma afirmação ao falar sobre a forma como estes sistemas são desenvolvidos:

> Só uma rede de centenas, milhares de cérebros trabalhando cooperativamente, com divisão de trabalho espontânea, e coordenação maleável, mas eficiente, poderia levar a cabo a tarefa extraordinária de criar um sistema operacional capaz de lidar com a complexidade de computadores cada vez mais potentes interagindo por meio da Internet (CASTELLS, 2003, p. 49).

De forma resumida, as principais vantagens do software livre/código aberto são apresentados no Quadro 1, de acordo com diferentes autores.

Quadro 1: Vantagens do Software Livre e Código Aberto.

Vantagem	Referência
Compartilhamento do Código	(SABINO, KON, 2004), (O'REILLY, 1999), (RAYMOND, 2010)
Liberdade do uso	(O'REILLY, 1999)
Custo reduzido	(SABINO, KON, 2004), (KAVANAUGH, 2004)
Segurança	(HEXSEL, 2002); (GARCIA et al., 2010).
Customização	(HEXSEL, 2002)
Compatibilidade com equipamentos mais antigos	(HEXSEL, 2002)
Comunidade na internet para auxilio	(GARCIA et al., 2010)
Não monopolização do software.	(HEXSEL, 2002)
Independência de fornecedor	(HEXSEL, 2002), (KAVANAUGH, 2004)

Fonte: Elaborado pelos autores.

Observando suas vantagens, pode-se ver que este tipo de software se sobressai em muitos aspectos sobre o software proprietário, com ênfase na grande comunidade de desenvolvedores que atuam na confecção do software, possibilitando um software mais satisfatório.

A principal desavantagem desta abordagem esta relacionada à manutenção, suporte e a difícil configuração do mesmo (GARCIA et al., 2010; KON; SABINO, 2004; HEXSEL, 2002). Pontos que podem ser corrigidos pela próprio uso do software, pois sua utilização pode proporcionar o surgimento de empresas de suporte e até mesmo empresas de soluções particulares, adaptando a aplicação conforme a necessidade

do usuário (SILVEIRA, 2005).

O Software Livre/Código Aberto já é uma opção viável às organizações devido a sua forma de desenvolvimento, que permite a confecção de uma aplicação mais completa. Grandes empresas já perceberam tal ponto e aproveitam das vantagens. Alguns autores já afirmam que em um futuro estes softwares estarão cada vez mais presentes entre usuários finais (SABINO; KON, 2004; KAVENAUGH, 2004).

7 ARQUITETURAS UTILIZADAS PARA A SEGURANÇA DA INFORMAÇÃO

Esta seção apresenta definições e funcionalidade de alguns software do tipo Livre ou Código Aberto, utilizados atualmente na área de segurança de rede. Ambas as licenças dos dois tipos de software não obrigam a disponibilidade de forma gratuita. A ideia é elaborar um ambiente seguro de rede com custo mínimo ou custo zero, com o uso destes softwares.

Como um caso motivador, tem-se o exemplo da Assessoria de Informática da Companhia de Entrepostos e Armazéns Gerais de São Paulo (Ceagesp). Em entrevista a Comunidade de Software Livre do Governo Federal (SoftwareLivre.GOV.BR), José Geraldo da Silva Neto, coordenador da Ceagesp, disse que ao migrar todos os seus antigos sistemas para Software Livre, economizou cerca de R$1.000.000,00 de reais em licenças e utilizou R$38.000,00 em novos treinamentos. Desta forma, é notável como a diferença de custo em relação a softwares proprietários é grandre, sendo o Software Livre/Código Aberto sendo gratuito ou não.

7.1 CentOS

O sistema operativo optado foi o CentOS (Community Entreprise Operating System). Essa distribuição Linux é uma plataforma ustentada pela comunidade Linux, resultante de fontes provido gratuitamente ao público pela Red Hat, desde março de 2004. O objetivo principal no projeto CentOS é distribuir uma plataforma simples, porém rica para as comunidades de códigos aberto o desenvolverem. Ele oferece estrutura de desenvolvimento para provedores em nuvem, hospedagem e processamento de dados científicos e etc (CENTOS, 2019).

No Centos pode ser instalado ferramentas e aplicações de segurança, como o Zabbix e o Samba, que serão citados nos tópicos abaixo. Porém, sistema

operacional também precisa possuir alguma segurança para não ficar vulnerável. O Linux, tem uma vantagem no quesito segurança, pois vem com o SELinux habilitado, nele é possível criar restrições e controle de acessos e aumentar a segurança do sistema.

De acordo com Hertzog e Mas (2015) o SELinux (Security Enhanced Linux) trata-se de ser um sistema de controle de acesso obrigatório, foi construído sobre a interface LSM (Linux Security Modules) do Linux, ou seja o kernel verifica o SELinux antes de cada solicitação do sistema para determinar se o processo está autorizado a realizar a operação solicitada. Ele utiliza um conjunto de regras ou políticas, usada para autorizar ou proibir as operações (HERTZOG; MAS, 2015).

7.2 Zabbix

Uma solução de nível enterprise, de código aberto e com suporte a monitoração distribuída. A solução foi criada por Alexei Vladishev, e atualmente é mantido e suportado pela Zabbix SIA.

O Zabbix é um software que monitora vários parâmetros da rede, dos servidores e da saúde dos serviços. Utiliza-se de um mecanismo flexível de notificação que permite configurar alertas por e-mail para praticamente qualquer evento. O Zabbix oferece excelentes recursos de relatórios e visualização de dados armazenados. Isso faz com que o Zabbix seja a ferramenta ideal para planejamento de capacidade. Para possibilitar um teste rápido da solução existe o Zabbix Appliance essa é uma alternativa à instalação manual do Zabbix para um ambiente de testes opção vem com o banco de dados MySQL (ZABBIX, 2019).

7.3 Pfsense

O pfSense foi desenvolvido em meados de setembro de 2004 por Cris Buechler e Scott Ullrich, é um firewall gratuito e baseado no sistema operacional FreeBDS com um Kernel personalizado incluindo funcionalidade de terceiros. Mesmo sendo um software gratuito, é possivel adquirir o Appliance do PfSense, que já vem pré configurado e pronto para uso. Um dos beneficios da utilização do Appliance é que não são necessarias licenças adicionais para outros recurso. Com a ajuda de sistemas de pacotes, o pfSense é capaz de fornecer as mesmas funcionalidades ou até mesmo, funcionalidades a mais do que softwares comerciais do segmento. Com o pfSense é possível substituir com êxito firewalls comerciais de grande nome, como

Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro (PFSENSE, 2019).

Dentre os muitos recursos do pfSense o que tem chamado a atenção é que em seu nível mais “básico” é possível instalar o pfSense em um hardware simples e substituir um roteador domestico e/ou comercial. Já em configurações mais avançadas é possível configurar serviços de VPN ou controle a carga de tráfego da rede (WILLIAMSOM; PERSAUD, 2012).

Pode-se ver alguns dos recursos disponíveis no pfSense: Firewall; DHCP; NTP; Squid + SquidGuard; Snort; NAT; DNS; VPN; Redundância, Balanceamento de Carga e Failover.

7.4 Samba Linux

Segundo Castro (2017, p.14) “Samba é uma suite de software que permite um sistema UNIX surgir e funcionar como um servidor Microsoft Windows, quando visto por outros sistemas numa rede”. Com o uso do Samba é possível o compartilhamento de arquivos e impressoras sistemas Windows e Linux, por exemplo (CASTRO, 2017).

Dentre os vários motivos para se utilizar o Samba, Castro (2017, p.14) diz que “muitos administradores de redes experientes podem testemunhar, o Samba oferece uma constante viabilidade, escalabilidade e flexibilidade”. Além de possuir uma Licença Publica Geral GNU e ser compatível com diversas plataformas como FreeBDS, Linux, Solaris ou OS X (CASTRO, 2017).

7.4.1 Características do Samba

De acordo com (MAZIOLI, 2010), algumas das funcionalidades do Samba são: Compartilhamento de arquivos entre máquinas Windows e Linux; Servidor de compartilhamento de impressão; Controle de acesso aos recursos compartilhados no servidor através de diversos métodos; Controle de acesso leitura/gravação por compartilhamento; Controle de acesso de leitura/gravação por usuário autenticado; Possibilidade de definir contas de ”Convidados“, que podem se conectar sem fornecer senha; Possibilidade de uso do banco de dados de senha do sistema; Controle de cache e opções de tunning por compartilhamento; Possui suporte completo a servidor WINS; Faz auditoria tanto dos acessos a pesquisa de nomes na rede como acesso a compartilhamentos. Entre os detalhes salvos estão a data de acesso, IP de origem,

etc; Permite montar unidades mapeadas de sistemas Windows ou outros servidores Linux como um diretório no Linux; Permite executar comandos no acesso ao compartilhamento ou quando o acesso ao compartilhamento é finalizado.

8 CORRESPONDÊNCIA ENTRE SOFTWARES LIVRES E PROPRIETARIOS

O Quadro 2 informa algumas ferramentas livres que oferece serviços equivalentes as ferramentas pagas.

Quadro 2: Softwares Proprietários × Livres/Open Source

Serviço	Proprietário	Livre/Open Source
Servidor de Arquivos	Serviços de Arquivos - Windows	Samba 4
Firewall	Sonicwall	pfSense
Monitor de Rede	PRTG	Zabbix
Produtividade	MS Office	LibreOffice

Fonte: Elaborado pelos autores.

9 CONSIDERAÇÕES FINAIS

Este artigo científico teve como proposta informar sobre segurança da informação para que se tenha um entendimento sobre o funcionamento e sua importância, abordando em conjunto o a definição sobre softwares Código Aberto e Softwares Livres voltados a segurança, de forma a proporcionar a compreensão para o tema. Foi retratado questão de se haver uma preocupação a mais com a segurança da informação, devido ao avanço tecnológico e a forma de como os dados são tratados atualmente, principalmente em organizações com alta quantidades de dados sigilosos. A pesquisa proporcionou que é possível optar por utilizar ferramentas e serviços código aberto ou livres, como opção eficiente. Foi realizado um levantamento bibliográfico, onde diferentes autores levantam as vantagens sobre a adoção a estes sistemas, sendo a redução de custos um dos pontos que mais se destaca.

Trabalhos futuros podem complementar estas ideias com objetivo de proporcionar uma implementação dessas ferramentas em redes e ir além, esboçando uma arquitetura de infraestrutura de rede mais rigorosa e completa.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 17799:2005: Tecnologia da informação — Técnicas de segurança — Código de

prática para a gestão da segurança da informação. 2.ed., Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

CASTELLS, M. A Galáxia da Internet: Reflexões sobre a Internet, os Negócios e a Sociedade. Rio de Janeiro: Zahar, 2003.

CASTELLS, M.; CARDOSO, G. A Sociedade em Rede: Do conhecimento à Acção Política. In: Conferência promovida pelo Presidenet da República, Centro Cultural de Belém, Portugal, 2005.

CASTRO, J. P. L. Integração do Samba 4 na plataforma IPBRICK para criar um Active Directory Open Source. [*S. l.*], p. 14. Disponível em <https://repositorio-aberto.up.pt/handle/10216/102488>. Acesso em 30 set. 2019 16 set. 2019.

CENTRO DE ESTUDOS, RESPOSTA, E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Estatísticas dos Incidentes Reportados ao CERT.br. Disponível em <https://www.cert.br/stats/incidentes/>. Acesso em 12 out. 2019.

DEITEL, H. M.; DEITEL, P. J.; CHOFFNES, D. R. Sistemas Operacionais. 3. ed., São Paulo: Person Education do Brasil, 2005.

GARCIA, M. N. et al. Software Livre em Relação ao Software Proprietário: Aspectos Favoráveis e Desfavoráveis percebidos por Especialistas. Revista Gestão & Regionalidade, São Caetano do Sul, vol. 26, n. 78, p. 106-120, set. 2011.

HEXSEL, R. Software Livre: Propostas de Ações de Governo para Incentivar o Uso de Software Livre. Relatório Técnico RT-DINF 004/2002. Curitiba, Paraná, 2002.

KAVANAUGH, P. Open Source Software: Implementation and Managment. Burlington: Elsevier Digital Press, 2004.

HERTZOG, R.; ROLAND, M. The Debian Administrator's Hnadbook: Debian Jessie from Discovery to Mastery. Freexian Sarl, 2015

KUROSE, J. F.; ROSS, K. W. Redes de Computadores e a Internet: Uma abordagem top-down. 6. ed. São Paulo: Person Education do Brasil, 2013.

MAZIOLI, G. S. Guia Foca GNU/LINUX. Ano: 2010. Disponível em <https://www.pfsense.org/>. Acesso em 30 set. 2019.

NATIONAL INSTITUTE STANDARDS AND TECHNOLOGY. NIST SP 800-12: An Introduction to Information Security. Jun. 2017.

OPEN SOURCE INITIATIVE. The Open Source Definition. Disponível em

<https://opensource.org/osd>. Acesso em 04 set. 2019.

PFSENSE, Firewall (ed.). Getting Started. [*S. l.*]: Netgate, 2019. Disponível em < >. Acesso em 30 set. 2019 25 set. 2019.

RAYMOND, E. S. A Catedral e o Bazar. Disponível em <https://www.ufrgs.br/soft-livre-edu/arquivos/a-catedral-e-o-bazar-eric-raymond.pdf>. Acesso em 30 set. 2019

SABINO, V.; KON, F. Licenças de Software Livre: Histórias e características. Relatório Técnico RT-MAC-IME-USP 2009-01. São Paulo, 2009.

SILVEIRA, S. A. Inclusão Digital, Software Livre e Globalização Contra-Hegemônica. In: Conferência Nacional De Ciência, Tecnologia E Inovação, Brasília, Brasil, 2005.

SOFTWARE LIVRE NO GOVERNO DO BRASIL. Ceagesp deixa licenças de lado e economiza R$ 1 milhão. Disponível em <http://www.softwarelivre.gov.br/artigos/ceagesp-deixa-licencas-de-lado-e-economiza-r-1-milhao/>. Acesso em 30 set. 2019.

STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas. 6. ed. São Paulo: Person Education do Brasil, 2015.

THE CENTOS PROJECT. CentOS Project. Disponível em <www.centos.org/>. Acesso em 4 out. 2019.

WILLIAMSOM, M.; PERSAUD, C. (ed.). Livro do pfSense: Um guia prático com exemplos ilustrados de configurações, para usuários iniciantes e avançados sobre o PfSense. 2.0. ed. rev. [*S. l.*]: Netgate, 2012. Disponível em <https://www.pfsense.org/>. Acesso em 24 set. 2019.

ZABBIX. Versão 4.0. [*S. l.*]: Zabbix SIA, 2019. Disponível em <https://www.zabbix.com/documentation/4.0/pt/start>. Acesso em 26 ago. 2019.