Revista CONEXÃO

PIRATARIA EM AMBIENTES CORPORATIVOS.

PIRACY IN CORPORATE ENVIRONMENTS.

Roger Dos Santos Bieger[1]
Sibele Mueller[2].

RESUMO
O presente artigo trata sobre pirataria em ambientes organizacionais, visando ressaltar e demonstrar as consequências de pirataria bem como possíveis soluções, tanto em *softwares* proprietários quanto em *softwares* gratuitos. Utilizando o método básico de pesquisa e a pesquisa bibliográfica que é elaborar material com base em materiais já publicados o autor conseguiu obter dados expondo-os de forma qualitativa. O trabalho apresenta informações bastante relevantes como: valores das multas cobradas por máquina por uso de *softwares* pirateados específicos, bem como o valor de licenças para regularização de *softwares*.
Palavras-chave: Organização; Pirataria; *Softwares*; Sistemas operacionais.

ABSTRACT
This article deals with piracy in organizational environments, with the purpose to highlight and demonstrate the consequences of piracy as well as possible solutions, with both proprietary software and free software. Using the basic method of research and the bibliographical research, that is to elaborate material based on already published materials, the author was able to obtain data exposing them in a qualitative way. The paper presents very relevant information such as: values of fines charged per machine for use of specific pirated software, as well as the value of licenses for software regularization.
Keywords: Organization; Piracy; Softwares; Operational system.

1 INTRODUÇÃO

Software é um programa ou um grupo de programas que ordenam o hardware da máquina a executar funções. Segundo Cavalcanti ([200-], p.3), *softwares* são algoritmos compilados, escritos em uma linguagem de programação que podem ser executados em toda e qualquer máquina ou dispositivo, podendo ser disponibilizados em suas diversas formas, sempre acompanhada de sua documentação. Inclui-se nessa categoria sistemas operacionais, processadores de texto, programas de aplicação, navegadores web, entre outros.

Softwares proprietários são diferentes de *softwares* livres, os proprietários geralmente são adquiridos através de uma licença, já os livres, além de serem gratuitos, tem seu código fonte aberto, que pode ser alterado e personalizado conforme o gosto do usuário (BUENO,

[1] Graduando do curso de Gestão da Tecnologia da Informação pelo Centro Universitário FAI – Uceff Itapiranga, rogerdossantosbeiger@gmail.com.
[2] Mestranda em Educação pela Universidade Federal Fronteira Sul, desenvolvedora de software e professora do curso de Gestão da Tecnologia da Informação do Centro Universitário FAI de Itapiranga, SC, sibele@uceff.edu.br.

2011). De acordo com Las Casas et al. (2012), *softwares* livres não são muito populares, pois há resistência em testar algo novo e existe falta de conhecimento sobre programas gratuitos existentes bem como sua eficácia. Outro motivo é a cultura de dar maior valor ao que tem custo, pois, liga-se custo a qualidade. Porém grande parte dos usuários desconhecem que *softwares* livres oferecem as mesmas funcionalidades e ferramentas que os *softwares* proprietários.

Este artigo aborda o estudo de viabilidade de implantação de *softwares* livres e proprietários em um ambiente organizacional, comparando os *softwares* e apontando vantagens e desvantagens de cada um. A motivação para a escolha do tema deu-se pelo fato do o autor possuir afinidade com *softwares* e por considerar o tema relevante, bem como ter interesse de se aprofundar na área e desta maneira adquirir maior conhecimento no assunto. Outra razão para a elaboração do tema é pela preocupação do autor com a pirataria em organizações, procurando apresentar as complicações geradas pelo uso de *softwares* piratas.

Objetiva-se com este trabalho aprofundar os conhecimentos, tanto em *softwares* livres quanto proprietários, avaliar custos de implementação dos dois *softwares* em organizações, assim como demais *softwares* de uso pessoal, elencando vantagens e desvantagens da utilização destes, realizando um levantamento de custos da utilização de cada um e ao final apresentar os resultados dos estudos.

Este artigo irá aprofundar os temas sobre pirataria e *softwares* livres e proprietários. Por conseguinte, o artigo se organiza da seguinte forma: no capítulo 2 serão apresentados o que é segurança da informação, política de segurança, pirataria, bem como *softwares* para auxiliar na prevenção da mesma e apresentar casos de pirataria que já aconteceram com empresas. O capítulo 3 consiste em expor a metodologia de pesquisa do trabalho, ou seja, de onde e como o autor conseguiu dados para a realização do presente artigo. No capítulo 4 são abordados e apresentados os resultados, que diz respeito a elaborar e apresentar dados sobre pirataria e análise de viabilidade de implantação de *softwares* proprietários ou livres em organizações, por fim serão apresentadas as conclusões deste estudo.

2 REVISÃO TEÓRICA

2.1 SEGURANÇA DA INFORMAÇÃO

Já passou o tempo em que as organizações conseguiam ser gerenciadas de forma manual, se conhecia todos os clientes, se controlava as entradas e saídas sem o auxílio de uma

máquina. Com as organizações crescendo, cresce junto a estrutura e também o número de clientes, contudo aumenta a complexidade dos processos que são desenvolvidos no dia a dia. Neste cenário, a TI vem para auxiliar tanto na interação com o cliente quanto na tomada de decisões da organização, como diz Laurindo et al. (2001, p.2):

> A TI evoluiu de uma orientação tradicional de suporte administrativo para um papel estratégico dentro da organização. A visão da TI como arma estratégica competitiva tem sido discutida e enfatizada, pois não só sustenta as operações de negócio existentes, mas também permite que se viabilizem novas estratégias empresariais.

Para que a tomada de decisões e estratégias sejam planejadas da melhor forma, sistemas de informação e ERP (Enterprise Reforce Planning) podem auxiliar a organização.

Toda organização possui ativos, que foram denominados os bens mais preciosos do século XXI (LYRA, 2017). Parafraseando Galvão (2015, p.13) ativos são “informações que possuem muito valor e são de fundamental importância para os negócios, que, por isso, precisam ser devidamente protegidos”. Como todo e qualquer bem precioso, as informações devem ser zeladas, essas informações podem estar em papel, e-mail, bancos de dados ou outra forma de armazenamento. Diante da necessidade das organizações protegerem seus ativos, surge a segurança da informação, que, por sua vez, tem por objetivo proteger todos os ativos (informações) de todas e quaisquer ameaças, garantindo a continuidade dos negócios, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio.

Hintzbergen et al. (2017) afirma que todos os riscos, ameaças, vulnerabilidades, são medidos pela sua capacidade potencial de comprometer um ou todos os princípios do triângulo CIA, (*Confidentiality*, *Integrity and Availability*) também conhecido como CID em português, que é formado pela Confidencialidade, Integridade e Disponibilidade. Estes três aspectos são princípios críticos de segurança e, na falta de um deles, o ambiente é afetado significativamente.

Oliveira, Moura e Araújo (2012) asseveram que desastres naturais ou humanos são vulnerabilidades de ativos da empresa, também são fraquezas, desastres tecnológicos; por exemplo, equipamentos sem devidas atualizações de antivírus e rede local, ou seja, rede acessível por senha, padrão ou pública. Além destas fragilidades, sérios danos empresariais podem ser causados por políticas de segurança da informação, desde as malformadas até as inexistentes.

Para finalizar o pensamento, segurança da informação nada mais é que assegurar que os ativos da empresa estejam protegidos. Por este motivo, organizações buscam implementar políticas de segurança da informação, para que seus ativos estejam mais protegidos de causas naturais ou tecnológicas.

2.1.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Hummes (2017, p. 17) afirma que a maneira mais eficaz de conseguir assegurar os ativos da organização é implantar a política de segurança da informação, que consiste em "[implementar] um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e hardware". Os controles adequados, aos quais Hummes (2017) se refere, precisam ser construídos, colocados em prática, monitorados, estudados criticamente e, caso necessário, sejam melhorados para que continuem cumprindo seus objetivos.

Políticas de segurança servem para o gerenciamento da segurança da informação em uma empresa ou organização, estabelecendo regras e padrões para a proteção da informação. A implantação desta possibilita a garantia na confidencialidade e a integridade dos dados, ou seja, garante que os dados não sejam alterados e estejam disponíveis quando necessário (OLIVEIRA, MOURA; ARAÚJO, 2012).

Por este motivo, a segurança da informação pode auxiliar no caso da pirataria. Podem ser criadas medidas de prevenção contra a pirataria, pois, como citado acima, são normas internas que policiam o que o funcionário pode ou não fazer, se pode utilizar redes sociais, mídias próprias, instalação de quaisquer programas, são exemplos de ações que o funcionário pode ou não executar.

Organizações, com a política de segurança da informação, conseguem vigiar melhor, os programas instalados nas máquinas de seus funcionários, pois, por mais que a organização saiba que esse ato que segundo Júnior (2004) é considerado pirataria os funcionários podem não saber. Para melhor combater esse problema em específico, faz-se essencial que todos os funcionários, usuários de máquinas e equipamentos informáticos, vulneráveis a instalação de *softwares*, participem de uma palestra de conscientização sobre pirataria, ou que a organização tome medidas que impeçam os colaboradores de instalar softwares sem autorização.

2.2 *SOFTWARES* DE MONITORAMENTO AUXILIARES NO COMBATE À PIRATARIA

Para assegurar as informações, além da segurança da informação, há outra alternativa que as organizações poderiam usufruir, que seria gerenciar todos os equipamentos informáticos através da rede, com *softwares* de monitoramento. A seguir serão apresentados alguns desses tópicos.

2.2.1 TI Monitor.

TI Monitor é um *software* que monitora tanto a internet quanto os aplicativos abertos no computador ou celular. É capaz de analisar todas as redes sociais, teclas digitadas, sites e pastas acessados. Dados disponíveis em nuvem, é capaz de gerenciar mais de um computador ao mesmo tempo (TI MONITOR, 2018).

2.2.2 PRTG network monitor.

Monitora todo o computador, com painéis "sensores" totalmente personalizáveis, controla várias telas ao mesmo tempo, possibilidade de monitorar qualquer computador conectado na rede por completo, desde o uso da memória, temperatura, espaço livre no disco rígido, informações do sistema até o que é acessado na internet (PRTG NETWORK MONITOR, 2018).

2.2.3 WinMonitor.

Capaz de espiar em tela cheia e exibi-las em um computador em tempo real, permite acessar a Webcam e configurá-la para detectar movimentos, exibe as teclas que o usuário digita bem como a localização do dispositivo, informa sites acessados, possibilita a captura de tela de trabalho de usuários bem como gravação de Webcam, gravação de tela e de áudio. Exibe estatísticas de trabalho que nada mais são que um relatório de quanto tempo o usuário permaneceu em cada aplicativo. Grava a estrutura de arquivos de qualquer mídia inserida na máquina e com esse *software* é possível efetuar o bloqueio de sites e aplicativos no computador. (WINMONITOR, 2018).

Estes *softwares* auxiliam muito as organizações na inspeção de *softwares* pirateados instalados em computadores, pois a maioria dos usuários que instalam *softwares* pirateados não sabem o que estão fazendo e nem sabem que a pirataria acarreta em tantos problemas à organização. Outra opção válida é a de colocar senha de usuário administrador para instalação

de programas, assim, sempre que alguém quiser instalar um software terá que chamar o técnico de informática para verificar se o software é pirateado ou não e autorizar a instalação.

2.3 PIRATARIA

A pirataria está relacionada à *pilhagem*[3], furto ou roubo do resultado do trabalho e ou de propriedade de alguém, que com esforço mínimo faz-se de dono de algo que não é seu. Usado geralmente por bens materiais por exemplo: quando é feita a falsificação de mídias originais, utilização de produto original em local ou país não licenciado, utilização do *software* fora do prazo da licença ou então download pela internet. Contudo, hoje vale também para ideias ou criações intelectuais e todas as formas de pirataria têm o mesmo valor perante a lei. (JÚNIOR, 2004). Para amparar quem sofre pirataria existe a lei 9.609/98 ou lei do *software* que "dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências." (BRASIL, 1998).

Falando sobre *software*, a lei 9.609/98 protege da pirataria quem produz *softwares* que possui todo direito sobre produtos de sua autoria, direito de tutela para 50 anos a partir do ano subsequente ao da sua publicação ou, na ausência desta, da sua criação (BRASIL, 1998).

Júnior (2004) diz ainda que licenciamentos de *softwares* proprietários são feitos individualmente por números de série, ou seja, *softwares* "pagos" são geralmente vendidos através de um número de série estipulados pelo fabricante, números esses que funcionam como placas de carros, que dão direito a uma pessoa de usufruir daquele produto com tais características, que podem ser iguais a outro produto e, o que as diferencia, é justamente o número de série.

2.5 CASOS DE PIRATARIA

Muitas pessoas físicas e jurídicas já tiveram que arcar com as consequências de usar *softwares* piratas. Alguns exemplos são apresentados a seguir:

O primeiro caso a ser citado aconteceu na universidade de Cândido Mendes que teve sua sede leiloada pela Justiça, para que a sua dívida com a Microsoft fosse quitada. O prédio localizado em Ipanema, Zona Sul da cidade do Rio de Janeiro foi oferecido pela universidade como garantia do pagamento de R$ 42 milhões a Microsoft, já que a universidade efetuava o

[3] Ato de pilhar ou roubar; saque, devastação. A coisa pilhada ou roubada. (DICIONÁRIO AURÉLIO, 2018)

uso de seus *softwares* pirateados por 17 anos. Porem o valor de R$ 4.3 milhões relativos em honorários de advogados ainda ficou em aberto. (FARINACCIO, 2017).

O segundo caso citado aconteceu com a empresa de alimentos Zaeli Ltda, que teve que pagar R$ 151 mil, corrigidos a partir do ano de 2003 à Microsoft em razão do uso de programas de computador (*softwares*) sem autorização. (NOTÍCIA, 2005).

O terceiro exemplo é da empresa Ediba S/A Edificações e Incorporações Barbieri e Planab Planejamento e Assessoria Imobiliária Barbieri Ltda. Que terão que indenizar a Microsoft por danos materiais. O STJ determinou que fosse pago R$ 12 mil pelo uso ilegal de programas de computador (*softwares*).

O quarto exemplo aconteceu com uma rede de lojas de roupas, chamada Forever 21. Adobe garantiu que a empresa a Forever 21 utilizou 63 de seus *softwares*, pirateados, dentre eles Photoshop, Acrobat e Illustrator. Autodesk e Corel se juntaram ao processo alegando utilização de Autodesk, Winzip e PaintShop Pro pirateados. Mesmo sendo contactada pelas empresas a Forever 21 continuou a utilizar as versões pirateadas dos *softwares*.

Como vimos acima, muitas empresas já foram multadas por utilizar softwares pirateados. Buscando obter informações sobre pirataria o autor realizou entrevistas com revendedores de softwares e sistemas operacionais da região, todos comentaram que já houveram muitos casos de empresas desenvolvedoras de *softwares* proprietários buscarem qualquer possível pirataria em massa em nossa região, Oeste Catarinense, principalmente em empresas, onde geralmente não possui somente um *software* pirateado. Por esse motivo, não deve haver pirataria em empresas, pois, como apresentado nos casos acima, muitas empresas já foram multadas e, como será exposto no capítulo 4, as multas são de alto valor.

3 METODOLOGIA

Este trabalho é um artigo científico e foi realizado utilizando o método básico de pesquisa, que visa aprofundar os conhecimentos em relação à pirataria de *softwares* em organizações. GERHARDT e SILVEIRA (2009, p. 34) afirmam que método básico "objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses locais."

Quanto aos objetivos, o presente artigo é descritivo. Segundo Triviños (1987, apud GERHARDT e SILVEIRA, 2009, p. 34) "a pesquisa descritiva exige do investigador uma série de informações sobre o que deseja pesquisar. Esse tipo de estudo pretende descrever os fatos e

fenômenos de determinada realidade". Essa pesquisa, por investigar a realidade de um determinado local, onde pode haver pirataria e como ela se originou, pesquisando máquina por máquina, para descobrir se os *softwares* utilizados nas mesmas são originais ou provenientes de pirataria se caracteriza como descritiva. Tudo no presente artigo retrata de forma íntegra, ou seja, sem alterar, apenas coletar, analisar e expor os dados analisados e estudados e, por fim, pretende-se apresentar todos os resultados desta pesquisa através de um estudo de viabilidade para a utilização de *softwares* legalizados e de uso livre.

Em relação à abordagem, este artigo se enquadra na forma qualitativa, pois a exposição dos dados é feita de forma qualitativa, onde a principal ferramenta de pesquisa foi o autor, que pesquisou e efetuou a análise dos dados pesquisados. Nesse estilo de abordagem não são utilizados números, mas números aparecem no artigo, porém estes são utilizados em grau de probabilidade e não de certeza.

> Os pesquisadores que utilizam os métodos qualitativos buscam explicar o porquê das coisas, exprimindo o que convém ser feito, mas não quantificam os valores e as trocas simbólicas nem se submetem à prova de fatos, pois os dados analisados são não-métricos (suscitados e de interação) e se valem de diferentes abordagens (Gerhardt e Silveira, 2009, p. 32).

No artigo serão apresentados os dados extraídos durante a pesquisa em todos os computadores da organização, sem que os mesmos sofram alterações. Serão informados valores atualizados das licenças de *softwares* geralmente utilizados em empresas, bem como a cotação das multas geradas pelo uso indevido de *softwares* piratas.

A pesquisa bibliográfica é o procedimento utilizado para a realização deste trabalho. Ela "é elaborada com base em material já publicado. Tradicionalmente, esta modalidade de pesquisa inclui material impresso, como livros, revistas, jornais, teses, dissertações e anais de eventos científicos" (GIL, 2010, p.29). O autor ainda diz que, com tanta tecnologia, a informação pode chegar de muitas outras formas como: meios eletrônicos e mídias digitais, que também foram utilizadas como fonte de pesquisa para este trabalho.

Para a coleta de dados, o autor utilizou do método de entrevista, que, segundo Marconi e Lakatos (2008, p.278) "trata-se de uma conversa oral entre duas pessoas, das quais uma dela é o entrevistador e a outra o entrevistado." Os autores ainda afirmam que entrevistas são divididas em dois tipos, a padronizada ou estruturada e a despadronizada ou semiestruturada. O autor do presente artigo utilizou a entrevista do tipo semiestruturada, que acontece

“[...]quando o entrevistador tem liberdade para desenvolver cada situação em qualquer direção que considere adequada.” (MARCONI; LAKATOS, 2008, p.279).

Apresentada a metodologia que foi utilizada para o desenvolvimento do artigo científico, no próximo capítulo serão apontados os resultados desta metodologia.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

4.1 ENTREVISTA REALIZADA SOBRE A UTILIZAÇÃO DE *SOFTWARES* NA ORGANIZAÇÃO.

Em visita à organização, realizou-se entrevista com o setor administrativo. Foram feitas perguntas sobre informática, em busca de encontrar algum problema ou necessidade para o ambiente. Foi relatado pelos mesmos que eram utilizados vários notebooks e computadores na organização e que existiam muitos exemplares espalhados pelos diversos setores da organização.

Durante a entrevista os participantes, esclareceram que o sistema operacional utilizado pela organização é Windows na maioria dos computadores, portanto estão licenciados somente os equipamentos que são licitados com a licença do sistema operacional. Muitos computadores que já pertencem à organização por mais tempo não possuem licença, então utilizam sistema operacional pirata. Computadores específicos são equipadas com SO livre. Outro *software* pirata encontrado é o pacote Office (Microsoft) instalado nas máquinas que possuem SO proprietário. A organização não possui nenhuma licença, ou seja, todos os computadores que possuem pacote SO e pacote Office são pirateados.

4.2 MULTAS PARA UTILIZAÇÃO DE *SOFTWARES* IRREGULARES.

Sistemas operacionais proprietários geralmente são adquiridos por meio de chave de licença, que você paga por ela e tem direito a instalar em seu computador e fazer o uso tranquilamente; a pirataria ocorre quando hackers criam esses códigos e então são colocados em máquinas sem que seja paga a licença.

Em entrevista com empresários da região, o autor questionou sobre multas aplicadas a organizações que utilizam de sistemas operacionais proprietários (Windows) pirateados e sobre os valores das licenças tanto do SO quanto do pacote Office. O entrevistado respondeu que “se for realmente seguir a Eula (acordo de licença do usuário final), o montante da multa pode

chegar 3.000 vezes o valor do original". Por exemplo: digamos que o Microsoft Office R$ 1.095,00 então R$ 1.095,00 x 3000, o valor final é de R$ 3.285.000,00 por máquina com *software* pirata. Além da multa, a empresa tem que regularizar o *software*, ou seja, você ganha um tempo estipulado pela empresa que investiga o caso para regularizar o computador pirata, sendo necessário comprar a licença e instalá-la dentro do prazo estipulado.

Este procedimento é geralmente realizado pela empresa Microsoft para com seu sistema operacional Windows. Para o SO Windows ocorre o mesmo processo de multa, porém a multa é de 3000 x 845,00 = R$ 2.535.000,00 por máquina com SO pirata, também é necessário regularizar os sistemas operacionais. Os custos de licença por unidade com ativação permanente são de R$ 845,00 para o SO Windows 10 Professional 64 Bits COEM e para o pacote Office home & Business FPP 2016 32/64 Bits é de R$ 1.095,00 a unidade.

Em redação do dia 29/11/2013, o Supremo Tribunal da Justiça (STJ) definiu que indenização por pirataria de *software* deve ter caráter punitivo e pedagógico. Em casos de pirataria de *software*, apenas o pagamento do valor dos programas de computador que foram utilizados sem licença não indeniza todos os prejuízos causados à vítima. Por esse motivo, a multa é elevada, pois, a empresa desenvolvedora e o STJ acreditam que, dessa forma, podem educar as pessoas, para que não façam uso de *softwares* pirateados.

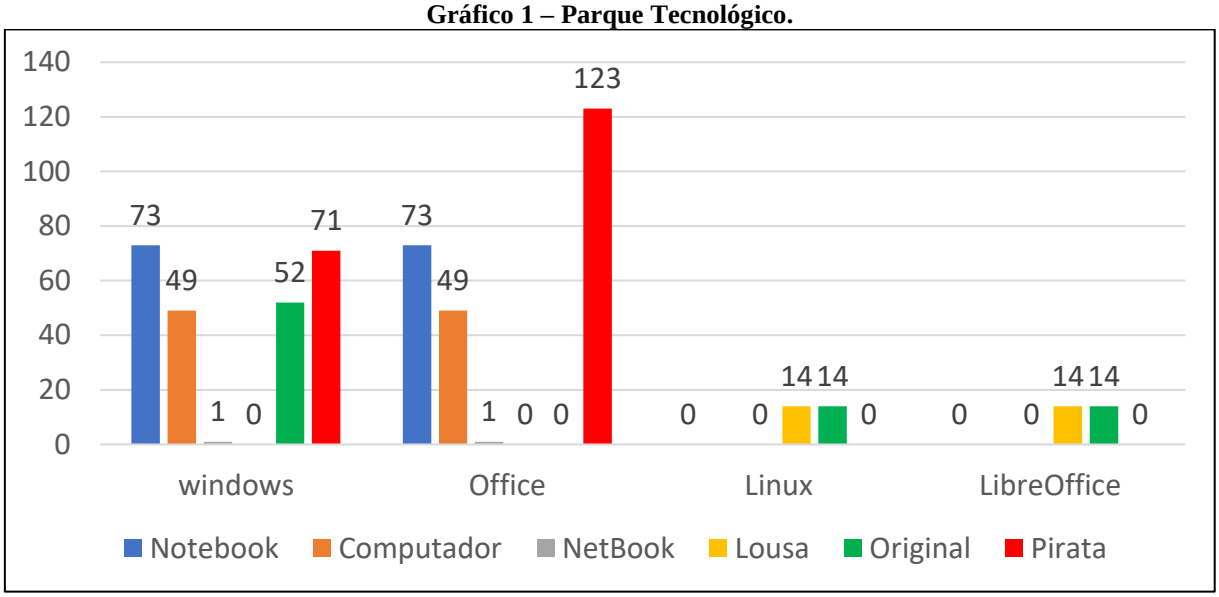
No próximo capítulo será confirmado que ainda há organizações que possuem pirataria em seus setores, o caso utilizado, contém vários *softwares* irregulares.

4.3 APRESENTAÇÃO DO PARQUE TECNOLÓGICO DA ORGANIZAÇÃO.

Em pesquisa realizada em todos os setores da organização, o autor obteve os seguintes dados: a organização possui 73 notebooks, 49 computadores, 1 netbook e 14 Computadores específicos, totalizando 137 máquinas. Destas 52 têm licença para o SO proprietário e 71 não têm licença, sendo que as lousas utilizam de SO livre. Lembrando que todos os computadores da organização que utilizam o SO proprietário possuem o Office pirata, ou seja, 123 máquinas não estão regularizadas.

Veja o gráfico 1 que apresenta os itens do parque tecnológico.

Gráfico 1 – Parque Tecnológico.



Autor: Do Autor, 2018.

4.4 POSSIBILIDADES DE REGULARIZAÇÃO DO PARQUE TECNOLÓGICO DA ORGANIZAÇÃO.

Softwares gratuitos são isentos de licença e de taxas, e qualquer pessoa pode fazer o Download dos *softwares* e instalá-los em sua máquina sem nenhuma complicação. Geralmente esses *softwares* são livres (*free*) e seus códigos-fonte podem ser acessados por quaisquer usuários que tenham conhecimento básico em informática, podendo assim, alterá-lo e personalizá-lo de acordo com sua preferência.

A organização conta hoje com 71 máquinas irregulares, contando todos os setores da mesma, inclusive áreas externas. Algumas alternativas de regularização podem ser: regulamentar as áreas externas com SO livre Linux e a área interna da organização com SO proprietário Windows. Todos os setores e áreas externas com SO proprietário Windows, ou então, todos os mesmos, com SO livre Linux.

A implantação dos *softwares* proprietários é a mais fácil, após adquiridas as licenças, cadastra-se cada Sistema Operacional e pacote Office em um computador e este deverá ser identificado com a chave utilizada.

A implantação do *software* livre é feita através de backup de dados da máquina específica, formatação da mesma e instalação do sistema operacional livre, juntamente com o pacote de produtividade, que no ambiente gratuito é chamado de LibreOffice, e por fim é feita a transferência dos dados antigos para o novo SO. Pode-se observar na tabela 1 a comparação entre as ferramentas disponíveis entre o SO proprietário e livre.

Tabela 1 - comparação entre pacotes de produtividade.

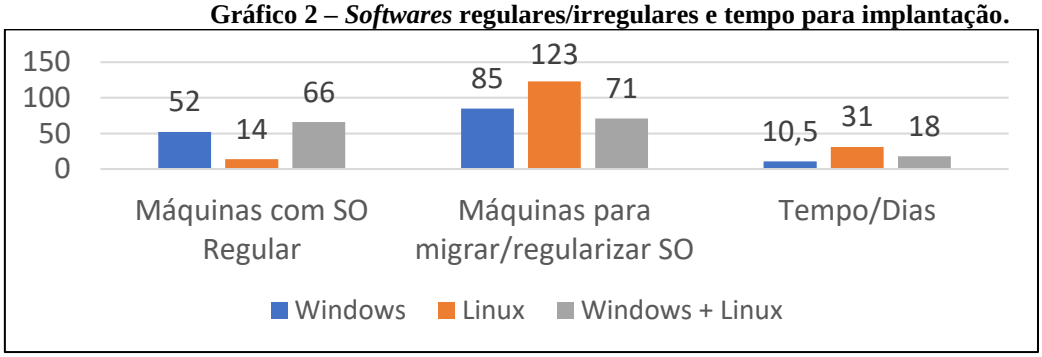
LibreOffice (Linux)	Ferramentas	Office (Windows)
Writter	Processador de texto	Word
Calc	Planilhas de calculo	Excel
Impress	Apresentações	Power Point
Base	Gestor de banco de dados	Access
Draw	Editor gráfico	
Math	Editor de formula matemática	
	armazenamento de arquivos em nuvem	OneDrive
	Anotações	OneNote
	Publicidade	Publisher

Fonte: Adaptado de Mined, 2012.

A organização de pesquisa deste artigo possui a área de Tecnologia como um dos setores internos, constituído por uma pessoa. Levando em consideração que essa pessoa trabalha 8 horas por dia 5 dias da semana, será necessário criar um cronograma para a migração ou a regularização do sistema, cada setor na sua respectiva vez. Contando com a colaboração de todos para que a regularização possa ser feita em horário comercial.

Geralmente o tempo utilizado para formatar e instalar os programas necessários para o bom rendimento da máquina é de noventa minutos. Por mais que o técnico procure realizar apenas a formatação de computadores, a qualquer momento podem surgir imprevistos e ele terá a obrigação de atender os chamados realizados; por esse motivo estima-se que com duas mídias, o técnico consiga deixar pronto 4 computadores por dia. Caso a opção de regularização seja adicionar as licenças faltantes nos computadores piratas, o tempo que o técnico levará para efetuar a regularização é menor; levará cerca de 30 minutos por computador, então, estima-se que conseguirá ajustar 8 máquinas por dia, pois adicionar as licenças demanda menor tempo do que formatar o computador e instalar os *softwares* essenciais, podendo ser observado no Gráfico 2.

Gráfico 2 – *Softwares* regulares/irregulares e tempo para implantação.



Fonte: Do Autor, 2018.

Caso a opção escolhida seja migrar para o SO livre, é necessário que todos os computadores sejam alterados, inclusive os que têm licença do SO proprietário adquirida, para que assim não haja a tentativa de escolha de computadores, por usuários.

4.5 BENEFÍCIOS E DESVANTAGENS.

O que determina um *software* livre de proprietário é o direito autoral que se aplica sob ele, seu licenciamento ou distribuição. Ou seja, o desenvolvedor do programa decide se deixa o código fonte do *software* aberto ou fechado e se cobra ou não pelo mesmo. Geralmente para *softwares* proprietários são cobradas taxas de licença, essas então, dão liberdade ao usuário para utilizar o *software* regularmente, já os livres são comumente gratuítos e seu código fonte são de acesso livre por qualquer usuário (BUENO, 2011). A seguir serão apresentadas as vantagens e desvantagens de cada um:

4.5.1 *Software* Proprietário.

Segundo a Microsoft, fabricante do Sistema Operacional Windows, estas são algumas funcionalidades que o sistema possui:

- Visualizar criações em 3D no mundo real;
- Acesso rápido aos contatos;
- Salvar etapas com o compartilhamento em primeiro lugar;
- Conectar-se rapidamente com emojis;
- Está interligado com o telefone do usuário;
- Comandos de energia ativados por voz;
- Arquivos do OneDrive sob demanda;
- Controle com os olhos.

4.5.2 *Software* Livre.

Já no site do Linux, *software* gratuito, podem se encontrar as seguintes funcionalidades:

- Sem custo;
- Livre de complicações judiciais;
- Totalmente personalizável;
- Código fonte acessível a qualquer usuário;
- Totalmente transparente;

4.6 GASTOS PARA REGULARIZAÇÃO

Para evitar possibilidades da organização ser multada por uso de licenças irregulares, a mesma deve regularizar esses *softwares*. O custo de regularização para o sistema operacional WINDOWS PRO 10 32/64 bits ESD DOWNLOAD a organização terá que desembolsar R$ 831,70 x 71 = R$ 59.050,70. Para regularizar o pacote Office, com o *software* OFFICE PRO 2016 ESD DOWNLOAD ALL LNG, a organização gastaria R$ 1.697,09 x 123 = R$ 208.742,07. Totalizando, a organização irá pagar em licenças o valor de R$ 59.050,70 + R$ 208.742,07 = R$ 267.792,77, sendo que o profissional da área de TI, responsável pela instalação dos softwares ganha R$ 1.500,00 por mês, ou seja R$ 8,53 por hora trabalhada o valor acrescentado para pagar o profissional é acrescido aos demais custos na tabela 2.

Tabela 2 – Valor gasto para regularizar.

	WINDOWS PRO 10 32/64 bits ESD DOWNLOAD	OFFICE PRO 2016 ESD DOWNLOAD ALL LNG	Linux
Tempo gasto para regularizar (horas)	84	123	246
Valor Licença	R$ 831,70	R$ 1.697,09	*free*
Softwares irregulares	71	123	123
Valor gasto com licenças	R$ 59.050,70	R$ 208.742,07	*free*
Hora Técnica (R$)	8,53	8,53	8,53
Regularização + instalação	716,52+ 59.050,70	1.049,19+ 208.742,07	2.098,38 + 0
Total	R$ 59.767,22	R$ 209.791,26	R$ 2.098,38

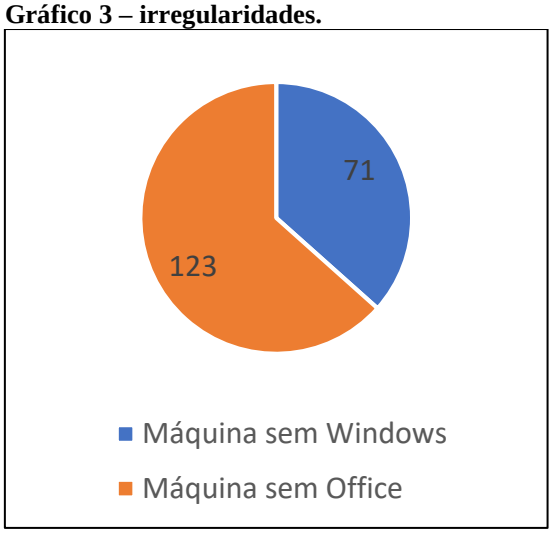
Fonte: Do Autor, 2018.

4.7 ESTUDO DE VIABILIDADE

Caso hoje a organização pesquisada neste artigo fosse denunciada e houvesse uma ouvidoria na mesma, utilizando o que diz no EULA, os valores seriam os apresentados na tabela 5, tendo

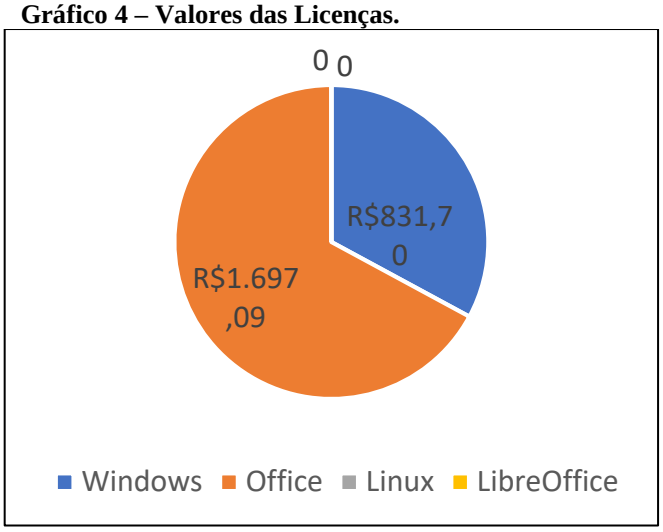
como referência as irregularidades e valores das licenças apresentados no Gráfico 3 e Gráfico 4, respectivamente.

Gráfico 3 – irregularidades.



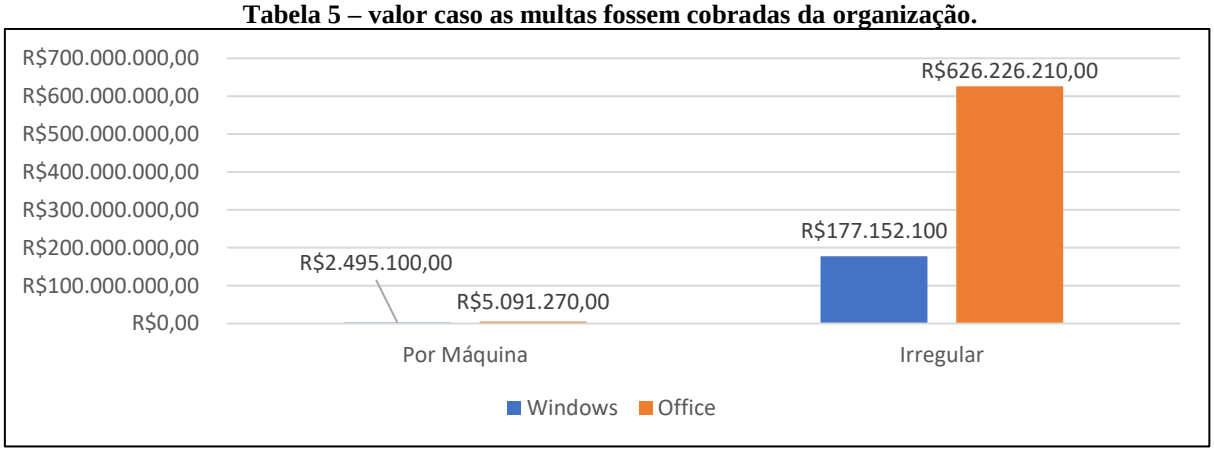
Fonte: Do autor, 2018.

Gráfico 4 – Valores das Licenças.



Fonte: Do autor, 2018.

Tabela 5 – valor caso as multas fossem cobradas da organização.



Autor: Do autor, 2018.

Considerando a multa conforme diz o EULA que é 3000 vezes o valor da licença, a organização gastaria R$ 803.378.310,00 (oitocentos e três milhões e trezentos e setenta e oito mil e trezentos e dez reais) + as licenças dos *softwares* pirateados que é de R$ 267.792,77 (duzentos e sessenta e sete mil e setecentos e noventa e dois reais e setenta e sete centavos), então a organização gastaria - para estar totalmente dentro da lei - o valor de R$ 803.646.102,77 (oitocentos e três milhões e seiscentos e quarenta e seis mil e cento e dois reais e setenta e sete centavos).

Por esse motivo a viabilidade do projeto se torna possível a partir do momento em que se faz a migração do sistema operacional proprietário pirata para o livre nas áreas externas da organização e utilizar as chaves encontradas nos mesmos para regularizar os outros setores da organização e em caso de falta de licenças, deverá ser efetuada a compra e deixados todos os computadores regularizados. Entende-se que a migração total para o sistema operacional proprietário tem um custo elevado, embora o sistema operacional livre garanta maior proteção aos ativos da organização. Por ser necessário um pouco mais de conhecimento para instalar programas adicionais na máquina, a migração para o sistema operacional livre não tem grande aceitação, pois além de ser algo novo e diferente, acredita-se que o tempo investido em adaptação e custos com treinamentos, são elevados, proporcionando assim a diminuição de produtividade dos colaboradores.

5 CONCLUSÕES E CONSIDERAÇÕES FINAIS

O objetivo geral do artigo é que o autor adquira experiência em organizações, aprofunde os conhecimentos tanto em *softwares* livres quanto proprietários.

O propósito do estudo foi alcançado através de objetivos específicos, tais como: conhecer a atuação de uma organização na área de *Softwares* Livres e Proprietários, ou seja, aprofundar os conhecimentos nos dois tipos de *Softwares* na vivência da organização; entender e estar apto a explicar sobre ambos, ter os dados já transformados em informação e poder usá-los em qualquer situação perante a administração da organização; identificar as habilidades e competências necessárias à atuação do profissional de TI em organizações, além de identificar em si próprio tais habilidades e se caso não possuir se há como adquiri-las e, por fim, avaliar custos de implementação dos *softwares* livre e proprietários na organização, assim como demais *softwares* de uso pessoal (pacote Office).

A partir de pesquisa realizada em todos os setores da organização extraiu-se dados sobre *softwares* livres e proprietários, *softwares* tanto legais quanto ilegais e pesquisa com revendedores de *softwares* e sistemas operacionais, foram averiguadas as informações necessárias para efetuar a cotação de multas geradas por computadores irregulares na organização. Ao elencar vantagens e desvantagens da utilização de *softwares* livre e proprietários na organização, o autor conseguiu elencar pontos fortes e fracos da utilização de *softwares* livres e proprietários na organização, pesquisas essas que foram de extrema importância para o presente artigo, pois, com estes dados o autor conseguiu compará-los e foram utilizados na viabilidade do projeto. Além de realizar um levantamento de custos da

utilização de cada *software*, o autor ainda efetivou o estudo e pesquisa de custos para a utilização de cada *software* na organização, e conseguiu apresentá-los no presente artigo que servirá de relatório para a mesma.

O estudo se mostrou válido - tanto para o autor quanto para a organização, pois, além do autor ter adquirido maior conhecimento na área que já lhe era de interesse, conseguiu atingir seu objetivo pessoal que era demonstrar para a organização, que algo que parece inofensivo, pode causar um grande prejuízo para a organização, assim como problemas perante à justiça.

6 REFERÊNCIAS

BRASIL. Constituição (1998). Lei nº 9609, de 19 de fevereiro de 1998. Lei do *Software*. Presidência da República Casa Civil, Brasília, DF, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.htm>. Acesso em: 17 set. 2018.

BUENO, Neide. **CONCEITOS E DISCUSSÃO SOBRE SOFTWARE LIVRE, SOFTWARE ABERTO E SOFTWARE PROPRIETÁRIO.** 2011. Disponível em: <http://oer.kmi.open.ac.uk/wp-content/uploads/2012/05/USP-D-.pdf>. Acesso em: 03 dez. 2018.

CAVALCANTI, Anderson. **Introdução a Engenharia de *Software*.** [200-]. Disponível em: <https://www.dca.ufrn.br/~anderson/FTP/dca0120/P2_Aula1.pdf>. Acesso em: 25 ago. 2018.

DAVENPORT, Thomas H. **Putting the Enterprise into the Enterprise System.** 1998. Disponível em: <https://hbr.org/1998/07/putting-the-enterprise-into-the-enterprise-system>. Acesso em: 03 set. 2018.

DICIONÁRIO Aurélio de Português Online: < https://dicionariodoaurelio.com/pilhagem>. Acesso em: 30 dez. 2018.

FARINACCIO, Rafael. **Universidade do Rio tem prédio leiloado por ter usado Windows pirata.** 2017. Disponível em: <https://www.tecmundo.com.br/mercado/121539-universidade-rio-tem-predio-leiloado-ter-usado-windows-pirata.htm>. Acesso em: 18 set. 2018.

GALVÃO, Michele da Costa (Org.). **Fundamentos em segurança da informação.** São Paulo: Pearson Education do Brasil, 2015. 114 p. (1). Disponível em: <http://faifaculdades.bv3.digitalpages.com.br/users/publications/9788543009452/pages/-3>. Acesso em: 13 set. 2018.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo (Org.). **Métodos de Pesquisa.** Porto Alegre: Ufrgs, 2009. 114 p. Disponível em: <http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf>. Acesso em: 29 set. 2018.
GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 5. ed. São Paulo: Atlas, 2010. 184 p.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002.** 3. ed. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2017. (Best Practices). Disponível em: <http://faifaculdades.bv3.digitalpages.com.br/users/publications/9788574528670>. Acesso em: 13 set. 2018.

HUMMES, Alex Artur. **PROPOSTA DE IMPLANTAÇÃO DE UMA NOVA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM UMA EMPRESA DE SEGURANÇA NACIONAL.** 2017. Disponível em: <https://riuni.unisul.br/bitstream/handle/12345/3043/Artigo%20-%20Alex%20Artur%20Hummes%20Final.pdf?sequence=1&isAllowed=y>. Acesso em: 16 set. 2018.

LASCASAS, Alice Carvalho et al. *Software* livre: por que usar? **Anais do Congresso Nacional Universidade, Ead e *Software* Livre**, Belo Horizonte, v. 2, n. 3, p.1-1, fev. 2012. Semestre. Disponível em: <http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/view/3868/3812>. Acesso em: 18 ago. 2018.

LAURINDO, Fernando José Barbin et al. **Gestão & Produção:** O PAPEL DA TECNOLOGIA DA INFORMAÇÃO (TI) NA ESTRATÉGIA DAS ORGANIZAÇÕES. 2001. Disponível em: <http://www.scielo.br/pdf/gp/v8n2/v8n2a04>. Acesso em: 03 set. 2018.

Linux.org, 2018, **Linux**, disponível em:< https://www.linux.org/>. Acesso em 05 nov. 2018.

LORENTI, Gilson. **Adobe processa Forever 21 por uso de *software* pirata.** 2015. Disponível em: <https://meiobit.com/308787/adobe-processa-forever-21-por-uso-de-*software*-pirata/>. Acesso em: 18 set. 2018.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação.** 2. ed. Rio de Janeiro: Ciência Moderna Ltda., 2017. 316 p.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia Científica.** 5. ed. São Paulo: Atlas S.a., 2008. 312 p.

Microsoft Windows, 2018, Windows, disponível em:< https://www.microsoft.com/pt-br/windows>. Acesso em 05 nov. 2018.

Mined, 2012, **LibreOffice The Document Foundation,** disponível em: < http://www.miportal.edu.sv/blogs/blog/administrador/libre-office/2012/02/28/qu-herramientas-proporciona-libre-office>. Acesso em 12 nov. 2018.

Monitoramento de computador com PRTG, 2018, **PRTG NETWORK MONITOR**, disponível em: <https://www.br.paessler.com/computer_monitoring>. Acesso em 05 nov. 2018.

NOTÍCIA, Expresso da. **Empresa pagará R$ 150 mil por usar *software* pirata.** 2005. Disponível em: <https://expresso-noticia.jusbrasil.com.br/noticias/141513/empresa-pagara-r-150-mil-por-usar-*software*-pirata>. Acesso em: 18 set. 2018.

OLIVEIRA, Gabriella Domingos de; MOURA, Rafaela Karoline Galdêncio de; ARAÚJO, Francisco de Assis Noberto Galdino de. **GESTÃO DA SEGURANÇA DA INFORMAÇÃO: perspectivas baseadas na tecnologia da informação (T.I.).** 2012. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/moci/article/viewFile/2111/1311>. Acesso em: 16 set. 2018.

ORRICO JÚNIOR, Hugo. **Pirataria de *Software*.** 2. ed. São Paulo: Mm Livros, 2004. 230 p.

PADILHA, Thais Cássia Cabral; MARINS, Fernando Augusto Silva. **Sistemas ERP: características, custos e tendências.**2005. Disponível em: <http://www.scielo.br/pdf/%0D/prod/v15n1/n1a08.pdf>. Acesso em: 03 set. 2018.

Programa espião TI Monitor, 2018, **TI MONITOR,** disponível em: <https://www.timonitor.com.br/mono/>. Acesso em 05 nov. 2018.

Programa Espião WinMonitor, 2001, **WinMonitor**, disponível em: <https://security.winmonitor.com.br/>. Acesso em 05 nov. 2018.