FAQI – FACULDADE DE TECNOLOGIA DE GRAVATAI

ELTON RODRIGO DA COSTA FERRO

eltonferro80@gmail.com

INTERNET NO AMBIENTE DE TRABALHO: IMPLICAÇÕES AOS USUÁRIOS QUE DELA DEPENDEM PARA SEU TRABALHO

GRAVATAI

2016

RESUMO:

Esta pesquisa tem como objetivo mostrar como um utilizador de computador e importante para a segurança da informação em um ambiente informatizado. Não é de agora que se fala do uso da internet em ambientes de trabalho, pois atualmente não se pode ficar sem ela. Nota-se o quanto ela relevante num ambiente escolar, onde não só os alunos são os únicos utilizadores, mas sim todos no ambiente escolar, desde a direção até os funcionários da instituição. Observa-se que cada um tem suas motivações para uso desta ferramenta. Portanto, o uso correto e eficiente da internet dentro da escola, necessita preservar a segurança das informações que nela trafegam. Nessa pesquisa são mostradas as principais boas práticas para o uso não só da internet, mas também, do computador como ferramenta de trabalho e instrumento de ensino.

Palavras-Chaves: Internet. Usuários. Segurança.

ABSTRACT:

This research aims to show how a computer user is important for the security of information in a computerized environment. It is not from now that is spoken of the use of the internet in work environments, because currently can not be without it. How relevant it is in a school environment where not only students are the only users, but yes everyone in the school environment from the direction to the staff of the institution. Observed that where everyone has their motivations to use more everyone is important for a correct and efficient use of the internet. Within the school and of course preserve the security of the information that travels through it. This research shows the main good practices for the use not only of the internet, but also, of the computer as a work tool and teaching tool.

Keywords: Internet. Users. Security.

INTRODUÇÂO

O uso da internet está cada vez mais necessário no mundo, especialmente no ambiente de trabalho. Imagina-se que ela é uma ferramenta indispensável na atualidade. Os jovens, por exemplo, já nascem utilizando e beneficiando-se dessa tecnologia. As antigas formas de arquivos de papel e de máquinas de escrever deram lugar aos teclados e monitores. Os quais se tornam menores no momento atual, em que informações e conhecimentos no mundo necessitam a comunicação entre eles, como forma de compartilhar informações e conhecimento. Assim, com o uso do computador que, quase todo mundo, com um *clic* é possível diminuir as distâncias e isto permite acessos sem deslocamentos, que por vezes são onerosas. O mundo virtual provoca significativa mudança nos conceitos em que era virtual reina. Nota-se que se tornou necessário à adaptação a essa tecnologia. Verifica-se que as crianças estão com facilidades de lidar com aparelhos de última tecnologia, por exemplo, os *smartphones*, que de certa forma causa o conflito, ou

estranhezas com gerações, mas houve a modernização de modelos de golpes com o uso de ações de má fé.

A Partir desta contextualização é que se apresenta a questão problema para o estudo: como o uso da internet no ambiente de trabalho causa implicações aos usuários que dela dependem para a execução do seu trabalho? Nota-se que nessa questão há um triângulo em que a empresa disponibiliza o serviço, o trabalhador, usuário do serviço depende da ferramenta e é vigiado pelos *hackers* ou pessoas oportunistas que se beneficiam de lacunas do sistema ou falhas.

Na busca de resposta ao problema apresenta-se o objetivo do estudo que é: identificar no uso da internet no ambiente de trabalho a causa que implicam aos usuários transtornos para a execução de seus trabalhos. Nos objetivos específicos definiram-se os seguintes: caracterizar os possíveis oportunistas para a apropriação de dados e sugerir formas ou maneiras de dificultar o acesso aos dados do usuário.

Como justificativa da pesquisa, é a constatação de que, às vezes, os usuários não estão preparados para utilizar as ferramentas de trabalho, até desconhecem os malefícios do uso incorreto. Por vezes acabam sendo vítimas deles mesmos, pois por não estarem preparados para isso, acabam executando funções em que têm limitações por entenderem ser mais fácil aceitar ajuda de estranhos e acabam por passar informações sigilosas “senhas” que permite que outros usuários usem a sua sessão ou terminal de trabalho.

O estudo está estruturado em tópicos, sendo que o primeiro é a introdução que apresenta o contexto, o problema, os objetivos e a justificativa. No segundo traz a fundamentação teórica sobre a internet, os usuários e a segurança que deve ser dada para evitar os invasores. No terceiro escreve-se sobre a metodologia do trabalho e os dados coletados. Sendo que no último tópico faz-se uma discussão dos dados e a consideração final.

INTERNET – USUARIOS E SEGURANÇA

A grande rede, que atualmente conecta muitos a muitos, com certeza foi uma das primeiras ferramentas de comunicação a realizar isso. A internet faz parte da vida das pessoas, dos negócios, e foi criada com o intuito de ser uma rede

autossuficiente, descentralizada para fins militares no final da guerra fria. A partir de então a rede começou a ser utilizada com fins de estudo interligando centros de tecnologia no mundo. Para que, dessa forma, disseminar o conhecimento não deixando restrito a apenas um local. Isto permitiu com que as informações percorressem grandes distâncias com o passar dos anos e inclusive o barateamento da tecnologia. Os computadores começaram a tornar-se algo mais acessível para as pessoas comuns, tanto em questão de valor, quanto também de acessibilidade ao seu uso.

Esta constatação é possível, pois o usuário não necessita de conhecimentos profundos em informática para operá-lo. Partindo desses fatos, nota-se a busca pela internet, e ela teve um gigantesco avanço no ano de 1995. Este salto que nem os idealizadores da nossa "*www* ou *world wide web*" Rede mundial de computadores, e conforme Castells,(2001, p.17) poderiam imaginar. Com a internet pública, não está mais restrita apenas aos grandes centros informatizados. A internet veio para ficar e dia após dia, ela só aumenta e traz cada vez mais usuários ao mundo virtual. Pode-se afirmar que essa é uma das invenções de maior impacto que faz parte da vida de todos os usuários da internet com destaque a introdução do correio eletrônico.

O "*E-mail"* (Correio eletrônico, método de troca de mensagens por meio de dispositivos eletrônicos) de acordo com Castells (2001, p.28) não substituiu os correios tradicionais, mas trouxe uma significativa mudança no meio empresarial e se tornou uma ferramenta vital na área virtual. Nos seus primórdios a internet era um mundo totalmente novo sobre informações e conhecimentos, que com a entrada de empresas e indústrias na internet ela teve uma nova onda ou uma segunda geração, em que se iniciou a ter serviços baseados na internet. Assim, as empresas começaram a ver o potencial que ela tinha de alcançar muito mais pessoas que apenas os serviços normais na época.

Neste contexto houve uma nova revolução na internet em que não só as empresas estavam se adaptando, como também os usuários dela, que agora tem um papel mais relevante, não apenas sendo usuários, mas como clientes e prestadores de serviços. Então dela, surgem novas empresas e serviços.

Na atualidade, a internet se tornou uma ferramenta necessária para realizar as atividades pelo simples fato de ligar boa parte do mundo e pelo seu alcance as informações. Nota-se que as informações correm o mundo em questão de

minutos. Portanto, através das famosas redes sociais que tiverem um destaque maior na nova geração da web.

OS USUARIOS

Ao procurar se a definição para a palavra usuário no dicionário encontra-se, conforme Merovingio (2015) “Aquele que usa e desfruta de algo coletivo”. Assim sendo, parte-se do ponto que o usuário deve saber: o que vai fazer? O que está usando? E, como deve ser feito?

Na realidade, atualmente não é assim, foi o tempo em que se exigia de funcionários cursos e conhecimento em sistemas operacionais de computadores. Com as facilidades e a proliferação de computadores pelo mundo pressupõe-se que o funcionário ou futuro funcionário saiba manusear qualquer computador ou sistema informatizado, constatação realmente vital para certas funções.

Um dos problemas dos usuários é pensar: só por que uma criança tem facilidade em utilizar acaba achando que isso é fácil. Pressume-se que no entendimento esteja o risco de que não vale apena investir em treinamento. No entanto, a realidade acaba se apresentando em outra forma. Embora haja pessoas que tenham facilidade em aprender, outras têm dificuldade e, às vezes a, dificuldade de entender o que está fazendo e o seu papel na empresa ou mesmo na internet. E ainda, às vezes com o seu próprio computador em casa, por vezes simplesmente não entende isso. Assim, o usuário acaba facilitando a ação de “*crackers”.* Indivíduos que não apenas burlam sistemas, mas que também buscam notoriedade e fama. Estes muitas vezes deixam um recado ou aviso de que invadiram o sistema, que segundo oliveira (2006, p.26), inclusive de até colegas de serviço que possuem um conhecimento melhor do que acontece a sua volta. Então ele acaba culpando o sistema ou mesmo o computador pelos seus problemas ou por não conseguir realizar uma tarefa. Nota-se, que na verdade nunca reconhece a sua parcela de culpa nesse processo, seja por não ter recebido treinamento adequado ou por sua própria falta de experiências com sistemas automatizados.

Desta forma o usuário pode afetar todo um sistema quando ele não atende aos três requisitos acima? Sim, pode. E ainda pode ate mesmo afetar os outros usuários que trabalham com ele, pois basta imaginar a seguinte situação: um

usuário sem treinamento começa a trabalhar no RH de uma empresa, e ele sendo do RH acaba tendo acessos aos dados dos funcionários da empresa. Citam-se alguns tipos que são confidenciais, como: salários, cargo, perfil psicológico, endereço e telefone. Com essas informações disponíveis um usuário mal treinado pode solicitar ajuda por conveniência a outro funcionário que não seja da mesma área. A lógica é de que o funcionário ajuda e inadvertidamente ficam expostos as informações que não são pertinentes a sua área. Assim pode acabar tirando proveito disso de várias formas. Por exemplo: usar os dados de telefone e endereço daquela colega do serviço, pedir aumento de salário baseado num mesmo colega que ganha mais e faz a mesma função, enfim, causar transtorno no ambiente de trabalho pelo simples fato de um único usuário, não treinado, expos informações para outros. Então com esse exemplo justifica-se a importância de um usuário, com vista aos questionamentos, saber o que ele quer fazer? , saber onde ele esta usando? E o que tem que ser feito? Há possibilidade de que isso impacta também na questão da segurança das informações, pois um software é tão seguro quanto o usuário que o utiliza.

EM RELAÇÃO À SEGURANÇA

Atualmente, com o mundo tão globalizado a informação e a sua distribuição começaram a ter um valor bastante elevado, às vezes, a segurança da informação vale mais do que dinheiro. Ela é algo vital na era virtual e ao falar em segurança lembra-se de cofres e vigilantes. Mas no mundo virtual, a segurança depende de nós mesmos, já que quase tudo se pode comprar ou vender pela internet. Movimenta-se dinheiro com o uso de computadores o que faz com que a segurança seja algo valioso para instituições financeiras (Bancos), e inclusive para grandes corporações em que suas decisões movimentam milhões em lucros ou prejuízos. Desta forma, a segurança da informação torna-se um dos grandes problemas na era digital, mas há aspectos relacionados com esse tema que todas as organizações devem saber, ou seja, as boas práticas, que são elas:

Quadro 1: itens de boas práticas

Item	Descrição
a) Não e um assunto de tecnologia:	Na atualidade armazenamos todos os documentos e tecnologia nos nossos computadores, onde os mesmos devem possuir o mínimo de segurança, de acordo com o porte da empresa, onde nem sempre só o uso de tecnologia pode resolver o problema, às vezes sendo necessária a contratação de pessoal qualificado que deve analisar o grau de segurança necessário.
b) É uma decisão empresarial:	Sim a segurança deve ser levada em conta durante cada decisão que envolva prejuízo ou lucro, pois os investidores podem perder dinheiro ao confiarem em um sistema que não possua segurança.
c) Não acontece por milagre:	A segurança da informação exige dedicação e preparo de todos os envolvidos inclusive investimentos financeiros e a segurança deve ser mencionada nos negócios.
d) Deve fazer parte dos requisitos de negócio:	Sim e deve estar também envolvia no custo do negocio.
e) Exige postura profissional das pessoas:	As regras de segurança devem ser claras a todos os colaboradores da empresa para que cada um faça a sua parte e saiba agir de acordo com o seu posto para que só assim haja segurança da informação.
f) É liberar a informação apenas para quem precisa:	A informação deve ser liberada apenas as pessoas que precisem dela, ou melhor, nem de mais nem de menos, as pessoas devem ter acessos a apenas os documentos que são pertinentes para realizar o seu serviço e nada mais, por isso é sempre importante verificar constantemente as atividades dos funcionários para saber se seus acessos estão de acordo com suas atividades.
g) É implementar o conceito de gestor da informação:	É bem comum a área de TI ser responsável pelos acessos às informações das empresas, mas ela nem sempre é a dona ou proprietária dessa informação para conceder o acesso o correto é o proprietário dela conceder uma autorização para que a área de TI disponibilize o acesso ao usuário.
h) Deve contemplar todos os colaboradores:	As regras de segurança da informação devem contemplar a todos os colaboradores inclusive os que não utilizam computadores para que estejam cientes das regras e que não tente utilizar acessos aos terminais de outros usuários, pois eles também fazem parte para que a segurança da informação seja segura.
i) É considerar as pessoas um elemento vital:	As pessoas ou colaboradores são a parte mais importante da segurança da informação elas fazem parte da empresa e, portanto devem ser responsáveis pelas seguranças da mesma, pois não existe software ou arquitetura de segurança que seja totalmente eficiente em uma organização, onde os funcionários não são instruídos adequadamente a utilizar.
j) Exige alinhamento com o negócio:	As medidas de segurança devem ser tomadas sempre juntas e de acordo com o negócio para que sempre estejam alinhadas desde o início, pois não podemos tomas decisões de segurança depois de ter um negócio já totalmente estruturado ou já em andamento.

Fonte: Fontes (2008, p.33)

Verifica-se no quadro uma série de boas práticas para a segurança da informação. Porém, é Claro que não se pode deixar de mencionar os *hackers* de computadores, esses sempre virão na mente quando se fala em segurança de computadores. Além de todas as medidas e casos comentados sobre o usuário, os *hackers* também merecem seu ponto de destaque, em que se pode caracteriza-los em diferentes categorias.

Á começar pelo mais popular e mais comum termo usado que seria o *hacker*. Este é visto da seguinte forma um individuo que possui um vasto conhecimento em informática e sistemas informatizados com uma profunda capacidade de analise, com vista na procura de brechas e falhas em sistemas. Diante disso sabe-se que não existe sistema perfeito a prova de falhas. Ele então vasculha o sistema na busca dessas falhas até conseguir ter acesso ás informações contidas neles e param por ai. No entanto, neste espaço entra outra categoria que vai alem disso, que são os *crackers.*

Os *crackers* esses sim fazem o mesmo processo dos *hackers* só que para eles apenas invadir e analisar um sistema não basta. Querem popularidade na internet, querem ser conhecidos e famosos. Então eles costumam deixar recados que estiveram lá sem rodeios ou cerimônias. Eles podem apenas deixar um simples aviso que invadiram o sistema ou até mesmo destruí-lo por completo e como se não bastassem eles também se apoderam de informações privilegiadas para mostrar seu poder perante as suas comunidades no mundo virtual. Para eles, a informação é muito mais valiosa que dinheiro, não que os *crackers* menosprezem o dinheiro, pois com certeza quando eles invadem instituições financeiras o dinheiro acaba sendo mais um extra do que realmente eles estão buscando.

Os últimos a partir da classificação dos dados surgem os *Phreaker,* que têm as mesmas intenções que os *crackers,* terem fama e notoriedade na internet. Porém também, invadem sistemas telefônicos, alteraram números de telefones ou até mesmo clonam os mesmos com o objetivo de adquirir informações que normalmente não estão disponíveis em computadores.

Por fim, existem mais algumas subcategorias para denominar os *hackers* de acordo com suas metas ou tipo de ataques a sistemas informatizados, como

apropriação de informação mediante á resgate e outros tipos de extorsões através do mundo digital.

METODOLOGIA DO ESTUDO

Com base no que se sabe agora sobre a internet, usuários e o bom uso da segurança no ambiente de trabalho, traz-se o estudo da utilização da internet num ambiente educacional, onde foram coletados os dados através de algumas entrevistas e com os históricos de uso da internet dos utilizadores de computadores, *smatphones* e *tablet* que utilizam ou trabalham com a internet provida pela escola.

Seguindo a metodologia os dados foram coletados em três etapas:

a) Coletar e observar;

b) Coletar e verificar os hábitos de utilização da internet;

c) Ensinar boas prática aos utilizadores sobre a internet, uso de computadores e a sua importância para o ambiente da escolar;

Ao analisar os dados também foram analisados os tipos de utilizadores da rede da escola em que são três grupos distintos: os Professores e administração da escola, funcionários de infraestrutura da escola, e alunos.

Cada grupo tem suas características e objetivo ao utilizar a internet na escola. Ao analisar o grupo de alunos este tem como objetivo o uso de rede social e vídeos na internet. Já os funcionários além de acessar as redes sociais têm consulta a bancos e serviços online. E os professores e administradores acessam os mesmos serviços, mas também sistemas automatizados para lançamentos de avaliação de alunos e contas bancárias da escola e próprias.

Sendo assim foram também, avaliados os equipamentos utilizados quanto a sua segurança para exercer essas funções. Foram analisados os sistemas quanto a sua versão, se era atual e se necessitava ser atualizada, e ainda, se as senhas utilizadas na rede sem fio eram seguras e quem tinha acesso a ela.

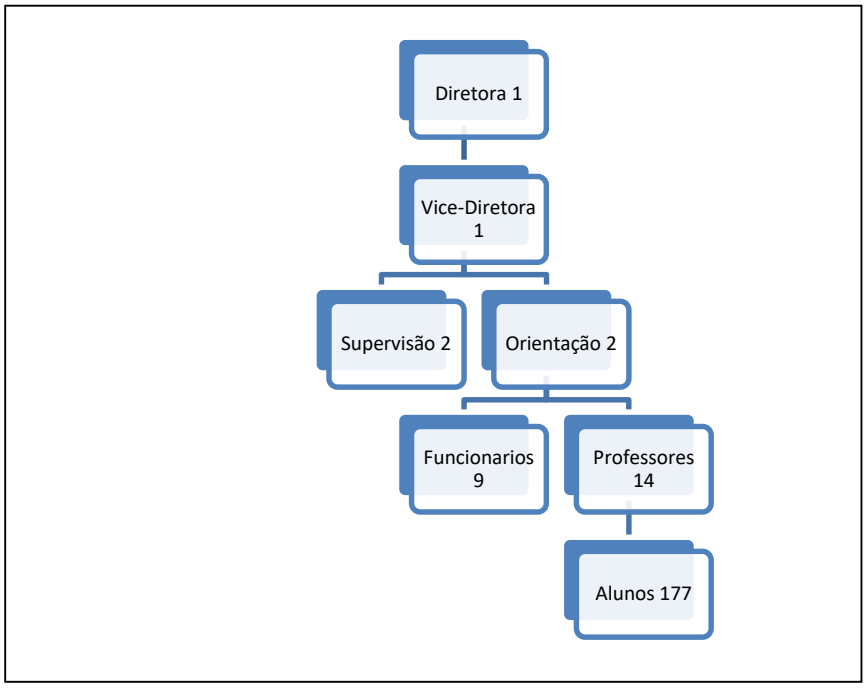
Por último, foi analisada a infraestrutura da rede escola. Nesse sentido, verificou-se se havia necessidade de uma melhora ou se ela poderia ficar mais eficiente aos seus usuários. Partindo destes aspectos metodológicos, no próximo tópico apresenta-se o ambiente do estudo prático.

AMBIENTE DO ESTUDO PRÁTICO

O estudo tem como lócus a Escola Municipal de Ensino Fundamental José Mariano Garcia Mota, situada no município de Gravataí. Possui prédio próprio sendo que nele estão estruturadas Salas: de diretoria, de professores, laboratório de informática, de ciências, de recursos multifuncionais para atendimento educacional especializado. Contém ainda: quadra de esportes descoberta, cozinha, biblioteca, parque infantil, banheiros adequados à educação infantil, banheiros adequados aos alunos com deficiência ou mobilidade reduzida, banheiro com chuveiro, refeitório, pátio coberto e pátio descoberto.

Quanto á hierarquia da escola está organizado da seguinte forma: diretora, vice-diretora, supervisão manhã e tarde, professores, funcionários e alunos. A escola não possui turno noturno e orientação. Sua estrutura de informática está distribuída da seguinte forma: cinco computadores na área administrativa, dois notebook para uso em salas de aula, sete computadores no laboratório de informática pelo projeto Proinfo e dois computadores na sala de recursos multifuncionais, também do Proinfo. Possui dois *access point* para acesso sem fio e duas redes de computadores: uma no laboratório e sala funcional, a outra atende separadamente na administração, cada uma com seu acesso a internet independente. Segue um organograma da estrutura funcional:

Figura 1: organograma funcional com nome dos postos e número de usuários



Fonte: dados da escola

Em relação ao projeto Proinfo ou Programa nacional de tecnologia educacional, este é um programa educacional criado em nove de abril de 1997, para promover o uso pedagógico de Tecnologias de Informática e Comunicações (TIC) na rede pública de ensino fundamental e médio.

Para isso o Ministério da Educação e Cultura - MEC compra, distribui e instala laboratórios de informática nas escolas públicas de educação básica. Em contrapartida, os governos locais (prefeituras e governos estaduais) devem providenciar a infraestrutura das escolas, indispensável para que elas recebam os computadores.

Desta forma as escolas estaduais são selecionadas pela Coordenação do Proinfo de cada estado, já as escolas municipais são selecionadas pelos Prefeitos dos municípios. (fonte portal do MEC. http://portal.mec.gov.br/proinfo/proinfo)

Nota-se que, o programa Proinfo foi uma boa ideia na teoria, mas que acabou sendo mal executada já que as escolas não possuem uma área de tecnologia ou suporte interno ao uso de computadores TI. Sendo assim, os professores tinham que buscar conhecimento para aprender a utilizar um sistema pouco usual para usuários domésticos, que no caso é o Linux.

Esta constatação gera por vezes abandono dos equipamentos após o término da garantia e do suporte. Em que só algumas escolas poderão realmente tirar o real proveito do que o projeto lhes oferecia que era a inclusão digital dos jovens.

Outro aspecto verificado são os pontos de *wifi.* Estes alocados em dois pontos estratégicos: um no laboratório de informática e outro na administração. Sendo que o do laboratório é utilizado por maioria dos usuários, grupos de alunos e funcionários. E o outro é utilizado por professores e funcionários do administrativo.

ESTUDO PRÁTICO DOS RELATÓRIOS

Agora se apresenta a análise dos relatórios feitos na escola em que se podem constatar os problemas e as soluções que serão aplicadas para alcançar um ambiente seguro para os grupos de usuário, para as informações que ali trafegam. Os relatórios foram sendo registrados semanalmente e para um melhor entendimento foram divididos em três etapas:

a) Análise da estrutura de informática da escola;
b) Análise dos equipamentos que fornecem acesso aos usuários;
c) Situar o usuário do ambiente de internet e boas práticas para o uso da internet e das informações;

A coleta dos dados foi realizada entre o período de 30/08/2016 a 19/10/2016 sedo ao todo oito relatórios. A seguir o relatório da primeira semana que fica compreendido entre os dias 30/08/2016 a 31/08/2016 ainda dentro da primeira etapa.

Atividades desempenhadas na **primeira semana** foram feita uma apresentação da escola, conhecendo os pontos de acesso as salas os terminais usados por alunos e professores, equipamentos de *wifi* e demais dispositivos que proviam acesso à internet no ambiente da escola. Nessa primeira semana foram analisadas versões dos dispositivos, aspecto visual dos cabos de rede, disposição dos equipamentos e afins.

Segundo relatório, compreendido entre as semanas 31/08/2016 a 07/09/2016 ainda dentro da primeira etapa de análise da estrutura. Na segunda semana ainda houve um estudo sobre os equipamentos e estrutura da escola, desta vez pesquisando na internet sobre os equipamentos disponíveis para situar sobre seu funcionamento e atualizações existentes. Para isso foi conversado também com alguns utilizadores sobre desempenho da mesma, questionamentos simples sobre a utilização ou problemas de acesso a mesma. Os equipamentos utilizados foram notebook pessoal para anotações e pesquisa na internet.

Terceiro relatório compreendido entre os dias 08/09/2016 a 14/09/2016 ainda na primeira etapa, agora com um conhecimento de toda a estrutura e equipamentos da escola e dado início ao plano de atualização dos equipamentos. As atualizações consistiam em sistema operacional dos computadores, *firmware* de *Access point*, *switchs* e antivírus conforme a necessidade dos mesmos. Nesse processo foi utilizado notebook pessoal para pesquisar as atualizações e logo em seguida colocá-las no *pendrive* e atualizar os equipamentos. Em seguida ocorreram às atualizações de todas as máquinas, foram scaneadas e analisadas pelos softwares antivírus para garantir que estavam seguras para o uso dos utilizadores.

Quarto relatório entre os dias 15/09/2016 a 21/09/2016 após garantir que os sistemas estivessem seguros em nível de software e equipamentos, iniciou-se a

análise sobre os equipamentos disponíveis na escola para as funções que eles exercem aos usuários, prover acesso à internet.

Ao verificar os equipamentos eles atendem bem a esse propósito fornecendo acesso satisfatório á demanda dos usuários. Talvez a área que precise de mais atenção sejam as salas do Proinfo que possuem um acesso bastante compartilhado, pois tem uma estação para cada quatro alunos através do sistema multi-monitor. Este disponibiliza através de um único computador CPU a conexão de até três monitores e consequentemente três teclados e mouses. Mas, a questão é que esses computadores não são dimensionados para um uso tão extensivo causando lentidão e dificuldade de acesso a tarefas mais pesadas, como: vídeos e chats em tempo real. Pode-se verificar que o responsável não é a rede e nem a internet, porque o mesmo evento não ocorre na administração onde existem computadores para uso individual.

Quinto relatório entre os dias 22/09/2016 a 28/09/2016 ainda na segunda etapa de análise dos equipamentos que provem internet aos utilizadores. Como analisado no relatório anterior, o acesso à maioria dos alunos se dá através do laboratório de informática, onde estão os equipamentos do Proinfo que não fornecem um acesso adequado aos alunos. Isto ocorre devido a sua configuração de *hardware,* sendo assim a única solução para deixar mais eficiente o acesso para os utilizadores dessa área seria a troca dos equipamentos para uma configuração que atenda o uso de vários usuários ao mesmo tempo. Poderia ainda, ser mediante a aquisição de várias máquinas para o uso individual, como ocorre nos equipamentos da administração.

Sexto relatório as atividades referente a esse relatório foram realizadas entre os dias 29/09/2016 a 05/10/2016 e iniciou-se a última etapa da à análise em que se citou o usuário de sua importância no uso da internet e as informações contidas nelas. Antes de tudo foi feita uma análise dos hábitos de uso da internet na escola através dos registros de navegação contida nas mesmas. Para saber-se que tipos de mídias e serviços são mais utilizados na escola e o nível de segurança que é aplicada nas mesmas.

Sétimo relatório compreendido entre os dias 06/10/2016 a 12/10/2016 na ultima etapa de analise da internet. Ao verificar os históricos pode-se observar que vários usuários não possuem noções básicas de uso de computadores, como exemplo: podem-se citar contas de e-mails que são deixadas logadas, contas de

redes sociais e outros serviços que necessitam de identificação do usuário, que não e finalizada após o uso. Esse problema também ocorre no administrativo, mas como lá os computadores são individuais o problema não é tão visível, mas isso não evita que algum colega mal intencionado tenha acesso a essas informações já que elas estão totalmente desprovidas de qualquer proteção. Esse fato também ocorre com a rede *wifi* que tem a sua senha espalhada para todos os alunos e usuários que nem frequentam a escola e acabam usufruindo da internet, pelo simples fato de não haver uma política ou regra de troca de senha mais corriqueira.

Oitavo relatório realizado entre os dias 13/10/2016 a 19/10/2016 última etapa da análise de segurança. De posse das informações pertinentes a escola foi possível estabelecer um plano de ação e boas práticas para cada grupo de usuários da internet. Assim pode-se verificar a relevância de cada usuário no uso da internet na escola. Iniciou-se pelo administrativo em que os utilizadores foram aconselhados a não utilizar as opções, de se manter logado e lembrar senha, pois essas opções facilitam em muito o acesso às informações sigilosas e o uso da estação por pessoas não autorizadas. Este fato ocorre naquela sala, pois não há nenhum controle de acesso. Outras medidas que foram elucidadas é evitar o uso do computador para fins pessoais e que seja utilizado preferencialmente para funções do ambiente de trabalho. Também foi comentado o uso de senhas mais elaboradas e tentar fugir do básico com senhas com: endereço de casa, placa do carro ou número de telefone. O ideal para considerar-se uma senha elaborada seria o uso de letras e números e não somente um dos tipos.

Quanto aos outros grupos, que utilizam acessos a internet para fins pessoais, foi recomendada a troca mais seguida da senha do ponto de *wifi* para dois em dois meses, a fim de estabelecer que realmente só as pessoas que estejam frequentando a escola tenham acesso a ela e uma senha elaborada também esteja aplicada ao mesmo.

Por ultimo foi sugerido aos utilizadores que façam a identificação a algum serviço quando solicitado e que o mesmo faça a seu logoff “Finalizar o uso” assim que tiver terminado a utilização do serviço. Esta prática evita que todos usem uma mesma identificação, já que nos laboratórios as estações são compartilhadas com muitos alunos.

CONSIDERAÇÕES FINAIS

Ao concluir o estudo verifica-se o quanto é importante que o usuário de um computador possua conhecimentos básicos de boas práticas para um ambiente de trabalho seguro e proveitoso. Ao analisar-se isto, verificou-se que as falhas e reclamações que existem num ambiente informatizado provêm das próprias limitações do usuário do que do próprio sistema.

Atualmente não e raro ver-se casos de roubo de informações, em que toda a culpa recai erroneamente sobre os *hackers*, mas ao se aprofundar nesse estudo sabe-se que nem tudo pode se atribuir a eles. Às vezes a falta de conhecimento e um colega mal intencionado podem fazer tantos problemas como os maiores *crackers* da informática. Recomenda-se que cada usuário faça a sua parte: procure sempre questionar e manter-se atualizado sobre suas funções e atividades e repasse as boas práticas a todos os usuários. Pode não existir um sistema a prova de falhas, mas quanto melhor os usuários dificultarem as atividades de pessoas oportunistas, maior será a segurança do ambiente de trabalho.

REFERÊNCIAS

BAWA, Joanna. **Computador e Saúde**. São Paulo: Summus Editora, 1997.

CASTELLS, Manuel. **A galáxia da internet reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro RJ: Zahar, 2003.

FONTES, Edison; CISM; CISA. **Praticando a segurança da informação**. Rio de Janeiro RJ: Brasport, 2008.

MEROVÍNGIO. **O usuário o computador e você**. Disponível em Http://www.vivaolinux.com.br/artigo/O-usuario-o-computador-e-voce/, acessado em: 23/11/2016.

OLIVEIRA, Wilson Jose. **Dossie Hacker técnicas profissionais para conhecer e se proteger de ataques.** São Paulo: Digerati Books, 2006.