

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO NAS ESCOLAS MUNICIPAIS DE ARAGUATINS-TO

Vinícius Miranda Aires¹, Lorrain Marinho Sampaio², Rogério Pereira Sousa³

¹Graduando em Licenciatura em Computação – IFTO. Bolsista do Programa Institucional de Bolsa de Iniciação à Docência - IFTO. e-mail: vinnyaires@gmail.com

²Pós graduado em educação especial e licenciado em computação – IFTO. e-mail: lohham@hotmail.com

³Professor especialista em docência no ensino superior, mestrando em engenharia de produção e sistemas pela Universidade do Vale do Rio dos Sinos Unisinos. e-mail: rogerio.pereira@ifto.edu.br

Resumo: O uso da informática por instituições de ensino vem crescendo cada vez mais, devido à praticidade de utilização deste recurso para atingir objetivos ou realizar tarefas do cotidiano. Entretanto atender os requisitos de segurança é essencial, para manter a estação de trabalho segura de possíveis acessos não autorizados. Neste estudo de caso foi analisado as opiniões dos servidores das escolas municipais da cidade de Araguatins - TO, através de questionário aplicado, com a finalidade de descobrir como é feita a *Segurança da Informação* nas instituições, dentre outros aspectos, embasados nos requisitos de segurança.

Palavras-chave: escolas, informática, segurança da informação

1. INTRODUÇÃO

O uso da informática como ferramenta de trabalho vem crescendo bastante nas escolas com o frequente avanço da globalização e avanço das tecnologias, em especial as TIC (Tecnologia da Informação e Comunicação) e TDICs (Tecnologia Digitais da Informação e Comunicação) estes recursos facilitam o trabalho do corpo docente e administrativo das escolas. Antes o trabalho era feito de maneira manual, com o manuseio de papéis para muitos serviços essenciais do professor, por exemplo, diários, enviar documentos para outras instituições, elaboração de provas, seminários, apresentação e exposição de aulas dentre outros. Com a flexibilidade que a informática traz aos usuários, faz com que os trabalhos manuais possam ser realizados digitalmente com o uso dos recursos computacionais facilitando e promovendo a eficácia e eficiência.

Com o frequente uso dos serviços do computador e dos serviços de internet, também cresceu as desvantagens aos usuários da rede mundial de computadores como, por exemplo, a invasão à privacidade com roubo de informações, tanto pessoais como de uso comunitário de alguma empresa ou ambiente de trabalho. Contudo, também aumentou a segurança para proteger esses dados e informações com a criação de sistemas de defesa para impedir que a integridade dos dados esteja vulnerável na rede, adotando os princípios de segurança da informação nos ambientes de trabalho.

“Nos ambientes organizacionais, a prática voltada à preservação da segurança é orientada pelas assim chamadas políticas de segurança da informação, que devem abranger de forma adequada as mais variadas áreas do contexto organizacional, perpassando os recursos computacionais e de infraestrutura e logística, além dos recursos humanos”. (MARCIANO, 2006, p. 16)

Na informática relaciona-se ao nível de segurança que é aspirado para definir uma

determinada política de segurança pela instituição ou pelo usuário, uma vez que as configurações de restrição ao acesso à informação são definidas, apenas o pessoal autorizado através de uma senha podendo ser definida de diversas formas ou formatos, por exemplo, terão o acesso aos dados daquela estação de trabalho, pessoas com a senha de acesso. O acesso por senhas é um critério adotado pela maioria das escolas, instituições ou empresas, para gerenciar o tráfego de usuários que acessam a rede de computadores, sendo muito importante, porque separa as pessoas (peoplewares) autorizadas ao acesso dos conteúdos nos computadores, daqueles que possuem restrições ao uso da rede ou do acervo de dados da escola.

Para que a segurança possa ser eficiente é preciso adotar os princípios da política de segurança sabendo a importância que “a informação é um ativo importante e valioso para os negócios da organização. Portanto, há a necessidade de proteger esse ativo de forma a garantir sua confidencialidade, integridade e disponibilidade”. (NETO, 2010, p. 19)

Confidencialidade

Uma informação confidencial é a informação que não deve ser compartilhada com os demais usuários da rede é de fundamental importância à instituição que possua um servidor de arquivos, para armazenar todas as informações mantendo-as seguras dos demais usuários que não estão devidamente autenticados no ambiente computacional.

Fazer o gerenciamento do controle de acesso aos dados é essencial para o contexto seguro da organização, com as agregações dos usuários por setores de trabalho ou equipes de servidores de uma mesma função. Cada servidor possui suas especificidades distintas um dos outros na questão do acesso, armazenamento e usabilidade do computador e do ambiente de rede do seu local de trabalho, contudo cada profissional deve manter a confidencialidade das suas senhas para aumentar a segurança das informações evitando que outros usuários não autorizados acessem o banco de dados.

Integridade

De acordo com o projeto de lei Marco Civil da Internet, decretada pelo congresso nacional enfatiza na questão do uso da internet e da proteção dos dados e privacidade dos usuários no “Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios: II - proteção da privacidade; III - proteção aos dados pessoais, na forma da lei”. Quando se fala em integridade faz a referência em relação à proteção dos dados, uma vez as informações virtuais estejam protegidas a privacidade do usuário também estará resguardada de usuários não autorizados. A integridade também se relaciona com a proteção da informação, ao trafegar na rede ou de um computador para outro, mantendo a originalidade da mesma sem que seja modificada por outro usuário não autenticado. Dentre as modificações que podem vir a ocorrer, por não haver as precauções com os requisitos de segurança, que um ambiente escolar implica na modificação de dados digitais sendo elas; diários, fichas ou listas, status, exclusão de arquivos dentre outros.

Disponibilidade

Garantir que as informações do ambiente de trabalho estejam sempre disponíveis ao acesso é de fundamental importância para que o usuário sempre que necessário possa usufruir de seus dados. Em um ambiente escolar as informações geralmente ficam em um servidor de arquivos ou compartilhadas em computadores da rede, e estes computadores podem enviar e receber informações confidenciais ou não de acordo com a requisição feita pelo usuário da rede.

A disponibilidade também se relaciona com a proteção de informações, nas escolas onde muitos servidores têm a senha de acesso aos dados disponíveis na rede, devem-se fazer reuniões para tratar de assuntos essenciais de segurança, para que a ética no ambiente computacional prevaleça

entre os funcionários ou servidores, para evitar que o vazamento de informações ocorra por parte de algum integrante.

“Para atingir um patamar do que seria "ideal" em segurança, tem que existir muita conscientização. E a sensibilidade sobre as questões de natureza humana deve ser aflorada quase que diariamente pelos responsáveis de SIC. E isso vai muito além de responsabilidades e deveres de um modo geral. Tem que ser intrínseco!”. (ROCHA, 2010)

Para que os serviços de disponibilidade dos serviços atendam aos requisitos do negócio é de fundamental importância que a T.I (Tecnologia da Informação) possa estar trabalhando em conjunto com os servidores a fim de evitar também o não repúdio, este é um recurso de segurança que almeja que o autor não venha a negar um ato ou ação de sua autoria que realizou no ambiente de trabalho. Portanto é de suma importância que o investimento em qualificações do pessoal envolvido diariamente com a informática como destaca (PALVIA & PALVIA, 1999 apud PRATES, 2003, p.44) “o cenário de segurança atual - com o crescimento dos riscos das empresas frente aos ataques, invasões e vazamentos de informações - parece estar incentivando as Organizações a capacitarem suas equipes...”. Portanto investir na capacitação dos funcionários vem tornando-se algo essencial para um melhoramento na prática de manuseio das Tecnologias Computacionais.

Devido à necessidade em conhecer como é feito o processo da segurança das informações nas escolas municipais da cidade de Araguatins – TO, foi realizada uma pesquisa através de questionários com a finalidade de analisar como é feita a manipulação, armazenamento e a segurança dos dados confidenciais das instituições.

2. MATERIAL E MÉTODOS

As escolas envolvidas no universo da pesquisa nesse estudo de caso, tendo como meta compreender como é feita a segurança e os cuidados básicos na manipulação dos dados de uso cotidiano, no qual, foram avaliadas três instituições através de questionário, sendo elas: Escola Municipal Vanor da Costa Parreão, Escola Municipal Professora Nair Duarte e Escola Municipal Professora Maria de Lourdes Milhomem Fernandes. Estas instituições de ensino dispõem de um quadro de docente significativo e essenciais para o estudo de caso, com profissionais de diversas áreas que abrangem o contexto escolar dentre eles compreende-se professores, diretores, coordenadores, orientadores pedagógicos e secretários.

Neste contexto, o estudo de caso faz inferência aos tipos de situações que contribuem para que os usuários da escola elaborassem meios próprios para cumprirem suas tarefas, mesmo que estes meios voltados à segurança estivessem em desacordo com os procedimentos do Sistema da Informação e Comunicação (SIC) organizacional. Nos dados da pesquisa foi extraído, informações dos setores que compõem a organização, bem como as diferentes características dos usuários em relação às diversas formas de uso da estação de trabalho que em alguns casos não atendem os requisitos de segurança.

3. RESULTADOS E DISCUSSÃO

A pesquisa realizada nas escolas do município. Baseando-se nos acervos e livros didáticos,

necessidades regionais particulares em expor a situação vigente da cidade em relação a um estudo de caso sobre segurança da informação nas escolas municipais de Araguatins – TO. Foram necessários para elaboração e aplicação do questionário com os professores e profissionais da área administrativa das escolas, para descobrir como está ocorrendo os serviços de segurança.

Estas instituições dispõem de um quadro docente significativo, com profissionais de diversas áreas que abrange o contexto escolar, sendo elas: Escola Municipal Vanor da Costa Parreão, Escola Municipal Professora Nair Duarte e Escola Municipal Professora Maria de Lourdes Milhomem Fernandes. Este artigo está explicitando como estes profissionais tratam as informações de interesse da escola, se é feita de maneira segura utilizando os recursos da computação e seus princípios de segurança. Em relação à “*segurança da informação*”, compreende um conjunto de medidas, normas e procedimentos destinados a garantir a integridade, a disponibilidade, a confidencialidade, a autenticidade, a irretratabilidade e a atualidade da informação em todo o seu ciclo de vida”. (BRASIL, 2001, p. 4)

De acordo com os detalhes em relação à pesquisa se faz importante enfatizar que a “*segurança da informação* é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. (ABNT NBR ISO/IEC 27002:20051)

Neste estudo de caso, a pesquisa nas escolas municipais foi realizada através de um questionário em que a coleta e análise dos dados, em relação aos serviços cotidianos como a manipulação de dados, a utilização da internet e suas especificidades para fins educacionais. Abordando os seguintes requisitos essenciais para a pesquisa, dentre eles, quanto à proteção da estação de trabalho, caso haja senha de acesso aos dados do computador. “*Quais as precauções e cuidados os servidores da instituição e usuários da rede adotam em relação as suas as senhas?*”.

Em outra pergunta está sendo abordada a renovação das senhas dos desktops (computadores de mesa), a próxima pergunta diz que, “*De quanto em quanto tempo é feita a renovação das senhas e onde geralmente são guardadas as?*”. Nessa questão é válido ressaltar a importância da autenticação, uma vez que as informações só podem ser acessadas por pessoas devidamente autorizadas naquele perfil e a aquele tipo de conta de usuário.

Outro ponto a ser abordado é “*Como são salvos e preservados os arquivos e documentos digitais da instituição?*”. Também perguntou-se “*você compartilha a senha do seu computador de trabalho com colegas da instituição ou pessoas da sua família?*”.

No decorrer da relação de aprimorar e trabalhar as práticas de ensino de maneira interdisciplinar com as tecnologias da informação e comunicação é de suma importância neste universo de ensino, fazendo com que a informática continue favorecendo essa relação de progresso nos requisitos de segurança destas instituições.

De acordo com a análise dos resultados, na primeira afirmativa do questionário foi perguntado da seguinte maneira; *A sua estação de trabalho é protegida por senha?* Do universo de vinte profissionais quinze confirmaram que existe o serviço autenticação ativo no acesso a estação de trabalho, ou seja, uma senha de acesso. Para uma escola que existe uma rotatividade de pessoas acessando o mesmo computador, é de ampla importância que exista uma proteção para manter um nível de segurança preventiva adequada para o ambiente.

Em outra pergunta foi explorado a questão da confidencialidade e proteção das senhas, a pergunta exposta para analisar tais aspectos; *você compartilha a senha do seu computador de trabalho com colegas da instituição ou pessoas da sua família?* O gráfico a seguir (Figura I) expõe a questão supracitada em porcentagem.

Você compartilha senha do seu computador de trabalho com colegas da instituição ou pessoas da sua família?

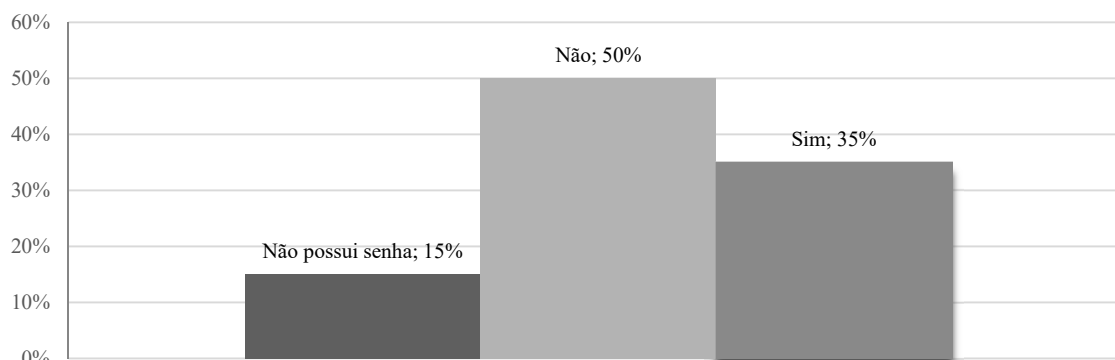


Figura I – Criada pelo autor.

Pode-se perceber que metade dos profissionais pesquisados, mantém a confidencialidade dos seus dados, protegendo suas senhas de acesso aos arquivos, seus interesses pessoais ou de sua responsabilidade. Também se pode notar que 35% destes profissionais não mantêm o segredo e proteção de seus arquivos digitais e 15% não possuem senha ou nenhum serviço de autenticação dos seus dados, a não proteção das informações podem acarretar em algumas desvantagens desagradáveis aos usuários da rede ou dos serviços de informática como um todo, sendo estas; alteração da originalidade dos dados, exclusão, cópias não autorizadas e desorganização do ambiente de trabalho.

Na questão de gerenciamento dos recursos computacionais da instituição, o gráfico abaixo (Figura II) expõe dados relacionados à existência de um setor de T.I. (Tecnologia da Informação) para que haja o controle e gerenciamento, da utilização da informática pela escola.

Existe um setor de T.I. (Tecnologia da Informação) para gerenciar o funcionamento da Rede de Computadores da Escola?

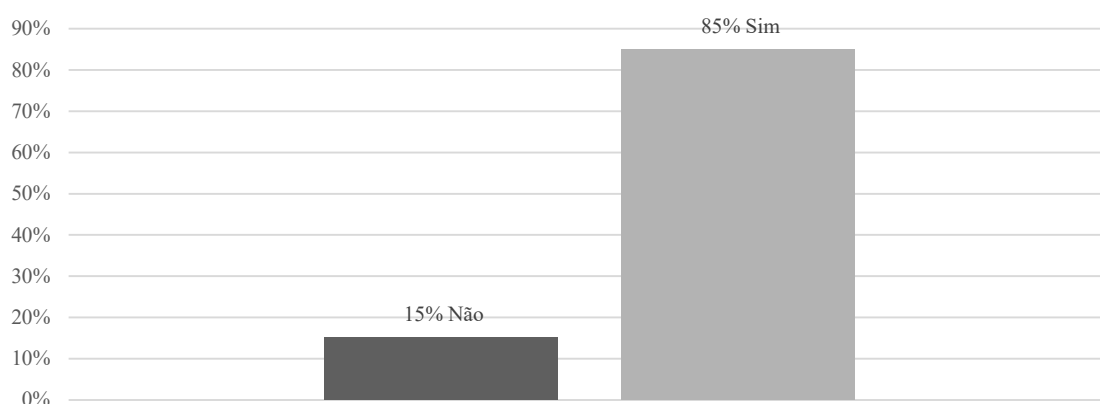


Figura II – Criada pelo autor.

A equipe de T.I faz o serviço preventivo para que os princípios de segurança da informação sejam preservados com eficiência e eficácia, princípios estes, confidencialidade, autenticidade, integridade e disponibilidade, fazem com que os diferentes tipos de ameaça aos dados sejam evitados. Quando questionado sobre a equipe de T.I. ficou constatado que possuía somente um técnico em informática à disposição de todas estas escolas do município, também ficou claro que não havia manutenção preventiva nos laboratórios de informática assim como nos computadores dos servidores e sempre que ocorria algum problema era necessário localizá-lo.

Tendo como última pergunta do questionário foi explícita que os servidores com seus conhecimentos, sugerissem algo para melhorar a segurança, a pergunta foi descrita da seguinte maneira O que você faria para melhorar a segurança de acesso e manipulação dos dados confidenciais da sua estação de trabalho? Houve várias sugestões cogitadas pelos profissionais dentre elas serão destacadas algumas. Profissional um: “faria um controle de usuários com serviços de autenticação bem definido”, profissional dois: “sugeria um usuário para cada computador”, profissional três: “fazer a proteção com antivírus e usar senhas de acesso para restringir o acesso de pessoas não autorizadas”. Estas sugestões comprovam as falhas encontradas que vem prejudicando a todos os usuários e na segurança dos dados das instituições relatadas neste trabalho e demonstram através das opiniões dos próprios servidores algumas possíveis soluções.

6. CONCLUSÕES

O estudo de caso trouxe a possibilidade de conhecer como é atendido os requisitos de segurança nas escolas municipais referidas, interagir com os funcionários e instigar suas opiniões a respeito da temática. De acordo com a análise dos dados é de grande importância apresentar possíveis soluções para o estudo de caso que vão contribuir para a melhora dos setores e dos próprios profissionais.

Uma delas é a organização dos dados em um servidor de Arquivos pela equipe de Tecnologia da Informação, para fazer a armazenagem e gerencia dos dados, para que torne possível atender os requisitos de segurança da informação e manter uma prevenção contra possíveis invasões. Não podendo descartar as sugestões feitas pelos servidores das escolas em relação as melhorias a serem feitas para que evitem o vazamento das informações, por exemplo; submeter os funcionários a um processo de formação continuada com temas voltados à segurança preventiva, para aperfeiçoar as habilidades dos profissionais na utilização dos recursos das Tecnologias da Informação e Comunicação (TIC) e as das Tecnologias Digitais da Informação e Comunicação (TDIC). Neste Sistema de Informação e Comunicação (SIC), as instituições de ensino que adotam a informática como ferramenta são mais preparadas em relação à segurança e sigilo das informações de trabalho e consequentemente os objetivos e metas no âmbito escolar ou pessoal estarão sendo bem realizados.

Quanto aos locais em que não há a estrutura necessária para manter a segurança dos dados, é sugerido que contrate pessoas com o conhecimento técnico comprovado para que possa elaborar uma metodologia de segurança e principalmente resolver os gargalos que envolvem a informática na instituição. As dicas de segurança citadas se encaixam de maneira pertinente em relação às pessoas que acessam a internet, devem tomar os cuidados básicos e essenciais na usabilidade cotidiana do computador e na utilização de seus recursos.

REFERÊNCIAS

ALVES, Gustavo Alberto. **Segurança da Informação – Uma Visão Inovadora da Gestão**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:2008**: Tecnologia da Informação: Técnicas de Segurança: Gestão de Riscos de segurança da informação. Rio de Janeiro: 2008. ASSOCIAÇÃO BRASILEIRA DE NORMAS

BRASIL. **Decreto nº 3.505**, de 13 de junho de 2000. Brasília, 2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 10 maio 2011.

FONTES, Edison. **Praticando a Segurança da Informação**. Rio de Janeiro: Editora Brasport, 2008.

MARCIANO, J. **Segurança da Informação - uma abordagem social**. Tese apresentada ao Departamento de Ciência da Informação e Documentação da Universidade de Brasília como requisito para a obtenção do título de doutor em Ciência da Informação, CID/FACE-UNB, 2006.

NETO, João Souza. **Política e Cultura de Segurança**. Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – CEGSIC, 2009-2011.

NORMA COMPLEMENTAR Nº 07/IN01/DSIC/GSI-PR. **Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta**. Brasília, 2010.

ROCHA, Danielle 2010, fórum 1 sobre Política e Cultura de Segurança

TÉCNICAS. **NBR ISO/IEC 17799:27001**: Tecnologia da Informação - Técnicas de Segurança – Sistema de Gestão de segurança da informação - Requisitos. Rio de Janeiro: 2006.