Segurança da Informação: um estudo em escolas municipais em Girau do Ponciano-AL

Daniese B. da Silva[1], Rômulo N. de Oliveira[2], Edelane N. da Silva[1]

[1]Instituto de Computação – Universidade Federal de Alagoas (UFAL)
CEP 57072-970 – Maceió – AL – Brazil

[2]Campus Arapiraca – Universidade Federal de Alagoas (UFAL)
CEP 57309-005 – Arapiraca – AL – Brazil

danieeseboia@gmail.com, romulo@nti.ufal.br, delanynunes72@gmail.com

Abstract. *In some contexts, information is the most valuable asset of the organization, and face common threats, attacks, and other related concerns. The same happens in all levels of government, including the public sector school management. This study investigated the information security in public schools located in the urban area of the city Girau do Ponciano / AL, observing the practices and procedures used to protect the information in these institutions and that the knowledge of employees about it. This study showed that the current situation of schools is still critical, but with the adoption of some security mechanisms, with the implementation of information security policies, and the training of staff, you can minimize security breaches.*

Resumo. *Em alguns contextos, informação é o bem mais valioso da organização, sendo comum enfrentar ameaças, ataques, e outras preocupações relacionadas. O mesmo acontece em todos os níveis governamentais, incluindo o segmento público de gestão escolar. Este trabalho investigou a segurança da informação nas escolas municipais localizadas na área urbana do município Girau do Ponciano/AL, observando as práticas e os procedimentos adotados para proteger as informações nestas instituições e qual o conhecimento dos colaboradores sobre o assunto. Este estudo mostrou que o cenário atual das escolas ainda é crítico, porém com a adoção de alguns mecanismos de segurança, com a implantação de políticas de segurança da informação e com a capacitação de funcionários, é possível minimizar as falhas na segurança.*

1. Introdução

A informação tornou-se um ativo indispensável e de uso corrente no dia a dia de diversos ambientes corporativos. Esses ambientes vêm produzindo eletronicamente um grande volume de dados e informações com o uso de Sistemas de Informação (SI) e de Tecnologia da Informação e Comunicação (TIC) como ferramenta de apoio. O uso dessas ferramentas vem crescendo bastante nos ambientes escolares, tanto para uso didático, quanto administrativo [Nagy, 2021]. Escolas são exemplos de ambientes que dependem e produzem diariamente dados e informações importantes da vida escolar dos alunos e da própria instituição. É grande o volume de informações manuais armazenadas em armários, gaveteiros e, atualmente, com o auxílio da tecnologia, passaram a produzir mais informações, principalmente digitais. Nesse sentido, além de gerenciar a guarda, as escolas devem também garantir a segurança dessas informações.

Portanto, a importância da informação para as organizações e a necessidade de protegê-la, demanda a adoção de políticas e técnicas a garantia de uma maior proteção, segurança e disponibilidade, inclusive nos ambientes educacionais. No contexto do objeto de estudo deste trabalho, procurou-se responder a seguinte pergunta: Qual a situação atual das escolas municipais localizadas na área urbana de Girau do Ponciano-Alagoas com relação à segurança da informação?

Diante deste contexto, o objetivo geral deste trabalho é investigar a realidade das escolas municipais localizadas na área urbana do município Girau do Ponciano-AL, com relação à segurança da informação, observando as práticas e os procedimentos adotados para proteger as informações e qual o conhecimento dos colaboradores sobre o assunto.

A fim de atingir o objetivo proposto, o trabalho iniciou com uma pesquisa bibliográfica sobre o tema de interesse. Com base nessa pesquisa, foi criado um questionário para ser aplicado nas escolas da rede municipal existentes na área urbana da cidade de Girau do Ponciano-AL. Como se trata de um estudo baseado em questionários para retratar um possível cenário dos municípios de Alagoas, desconsideramos a área rural, tendo a consciência de que os possíveis problemas identificados na área urbana, seriam ainda intensificados nessa região. A escolha do município se deu pela facilidade na coleta de informações, dado o bom relacionamento de um dos autores com o município.

2. Fundamentação Teórica

Devido a informação ser um bem importante para o ambiente organizacional, pode ficar exposta a ameaças e vulnerabilidades. Garantir que essa informação fique segura é um desafio que as organizações têm que lidar [Albuquerque Junior e Santos, 2014]. Nesse contexto, para proteger adequadamente esse bem, é preciso saber destacar quais ativos e consequentemente que informações são mais importante para a organização. Para isso, é necessário compreender a segurança da informação, sua importância, saber classificar a informação que circunda pela organização e que princípios cercam essas informações, além de disso, é preciso conhecer quais ameaças podem afetar os ambientes organizacionais e quais medidas ou mecanismos de segurança podem ser adotados para atingir um nível adequado de segurança da informação. Todos esses temas são tratados nos tópicos a seguintes.

2.1. Segurança da Informação

Conforme Laudon e Laudon (2010), as informações são criadas a partir da coleta, processamento e análise dos dados. Assim, por meio da aplicação do conhecimento humano, novos conhecimentos são gerados. Esses, por sua vez, voltam para aprimorar as informações. Nesse contexto, a informação e o conhecimento adquirido constitui um imprescindível recurso estratégico para o sucesso da empresa, pois sua importância está diretamente relacionada a maneira como ela auxilia a tomada de decisões e o alcance das metas da organização.

A segurança da informação é a proteção da informação e de outros ativos informacionais contra o acesso, divulgação, destruição ou utilização por pessoas não autorizadas [Laudon e Laudon, 2010]. Segundo a Associação Brasileira de Normas Técnicas [ABNT, 2005], a segurança está relacionada com a "preservação da confidencialidade, da integridade e da disponibilidade, além de outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade".

Nos dias atuais, é cada vez mais comum nos depararmos com notícias de ataques cibernéticos em diversos países, inclusive no Brasil. São ataques a grandes e pequenas empresas, agências, órgãos, instituições governamentais, roubo de dados, vazamentos de

informações sigilosas, tentativas de fraudes, entre outras formas maliciosas utilizadas por criminosos para obter vantagens [Nagy, 2021]. Ainda segundo Nagy (2021), esses ataques virtuais acontecem a todo instante e, na maioria das vezes só é percebido pelas empresas, instituições, organizações ou mesmo usuários comuns quando se tem algum prejuízo, tanto financeiro quanto moral. Nesse contexto, inicialmente o principal bem atacado por esses criminosos cibernéticos é a informação, a partir dela que esses criminosos conseguem tirar outras vantagens.

2.2. Incidentes, Vulnerabilidades, Ameaças e Ataques

Segundo a norma ABNT NBR ISO/IEC 27002 (2005), um incidente de segurança da informação é uma série de eventos indesejados ou inesperados que podem comprometer e ameaçar as atividades e os negócios da organização. Como incidentes, Tanenbaum (2003), Kozen (2013), Kurose (2010) e Laudon e Laudon (2010) destacam alguns exemplos: roubo de informações; disseminação de outros códigos maliciosos; perda de informações ou equipamentos que armazenam dados importantes; usar/acessar sem autorização um sistema; ataques de negação de serviço e de engenharia social; descumprimento da Política de Segurança da Informação (PSI) entre outros.

As vulnerabilidades também são outro fator que podem contribuir para impulsionar o crescimento dos incidentes de segurança. Para Dantas (2011, p.24), “vulnerabilidades são fragilidades que, de alguma forma, podem vir a provocar danos”. É importante que a organização saiba identificar as vulnerabilidades existentes em seu ambiente para que, além de eliminá-las, também se previnam das ameaças que por ventura venham explorar essas vulnerabilidades. A norma ABNT NBR ISO/IEC 27002 (2005, p.3) define ameaças como: “a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização”. Laudon e Laudon (2010) consideram que os funcionários são ameaças internas da organização, visto que, devido terem acesso a informações privilegiadas, podem introduzir erros inserindo dados incorretos nos sistemas, como também, podem deixar de seguir as regras impostas para uso adequado dos sistemas.

Várias ameaças também são oriundas do meio eletrônico, projetadas para executarem ações maliciosas contra computadores, redes e sistemas, com intuito de acessar dados sem autorização, alterar seu conteúdo, deletá-los, deixá-los indisponíveis, entre outras ações que acabam prejudicando tanto os processos quanto a própria imagem da organização. Assim, as principais ameaças que acometem com frequência os meios eletrônicos são identificados como códigos maliciosos (Malwares). Eles podem infectar um computador de diversas formas: explorando vulnerabilidades existentes nos programas instalados; acessando páginas maliciosas da Internet; executando arquivos infectados em anexos de e-mails ou em mídias removíveis.

Segundo Lyra (2015), os ataques podem afetar diferentes princípios da segurança da informação. Por exemplo, fere o princípio da disponibilidade quando um atacante invade uma rede corporativa e a deixa inoperante, se esse atacante porventura altera um arquivo, acaba ferindo o princípio da integridade, o ato de conseguir ter acesso a rede corporativa e ver informações privadas e confidenciais sem ser autorizado, já fere o princípio da confidencialidade. As principais técnicas de ataques por meio da Internet que a Cartilha de Segurança para Internet destaca são: exploração de vulnerabilidades, varredura em redes, falsificação de e-mail, interceptação de tráfego, força bruta, desfiguração de páginas, negação de serviço (DoS e DDoS).

2.3. Medidas e Mecanismos para o Controle da Segurança

A informação, independentemente do seu formato, é um ativo valioso e importante. Por esse motivo que os diversos ambientes organizacionais e os equipamentos utilizados para processar, armazenar e transmitir informações devem ser protegidos [Fontes, 2006]. Para isso, esses ambientes devem adotar medidas e mecanismos de segurança. As medidas de segurança podem ser entendidas como práticas, procedimentos e mecanismos usados para proteger informações e ativos. Através delas é possível reduzir riscos, limitar impactos e impedir que ameaças explorem vulnerabilidades [Sêmola, 2003].

Apesar de existirem diversas medidas de segurança e mecanismos de apoio e, mesmo a organização adotando grande parte deles, não significa que estará completamente segura nem tão pouco que essas medidas darão cem por cento de segurança. Moreira (2001) afirma que não existem ambientes totalmente seguros pois, até mesmo as medidas de segurança implementadas pelas empresas possuem vulnerabilidades. Entretanto, isso não significa que não se deva buscar com empenho por uma política de segurança eficiente. Pelo contrário, a política de segurança deve ser constantemente revista e reestruturada.

Nesse sentido, é importante compreender que a segurança da informação de um ambiente organizacional não deve se limitar apenas em mecanismos tecnológicos como *firewall*, antivírus, IDS entre outros. É necessário uma abrangência maior que envolva outros mecanismos. Segundo ABNT (2013), a segurança da informação é alcançada através da implementação de um conjunto adequado de controles, como políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware que precisam ser estabelecidos, implementados, monitorados, analisados criticamente, além de melhorados sempre que necessário para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos.

3. Desenvolvimento da Pesquisa

A pesquisa foi realizada em sete escolas públicas do município de Girau do Ponciano, em sua área urbana. Ela teve como objetivo investigar a realidade das escolas municipais com relação à segurança da informação, observando as práticas e os procedimentos adotados para proteger as informações nestas instituições e qual o conhecimento dos colaboradores sobre o assunto. O instrumento de pesquisa utilizado foi um questionário físico, que teve sua aplicação realizada entre 29 de maio de 2019 a 20 de junho de 2019. O questionário continha questões fechadas e abertas, que foram escolhidas de acordo com o objetivo deste estudo e com base na literatura estudada, assim como uma entrevista semiestruturada, que foi aplicada junto aos diretores escolares. Todos os entrevistados tiveram seu sigilo garantido e, a pedido deles, os nomes das escolas também foram mantidos em sigilo. Antes das entrevistas era lido um texto sucinto de apresentação, para fins de esclarecimento. Os resultados apresentados a seguir representam parte da análise sobre as afirmações prestadas pelos respondentes da pesquisa. Entretanto, a pesquisa completa está disponível no repositório institucional “Universidade Digital”, na url “https://ud.arapiraca.ufal.br”.

3.1. Análise Crítica dos Resultados

A educação básica ofertada pelo município compreende desde a educação infantil ao ensino fundamental (1º ao 9º ano). Algumas escolas disponibilizam a modalidade de educação de jovens e adultos (EJA). Quanto aos horários de funcionamento das escolas, 85,7% funcionam apenas em períodos matutinos e vespertinos, e em 42,9% delas funcionam também no período noturno. O município também oferta em uma das escolas o ensino integral, atendendo apenas a educação infantil. A média de alunos matriculados nas escolas pesquisadas foi de 474

alunos, sendo que a quantidade mínima foi 150 e máxima foi 1200 alunos. A quantidade de funcionários também é relevante, 42,9% das escolas possuem um quantitativo entre 30 a 50 funcionários e em 57,1% delas o número é bem maior, ficando entre 50 a 100. Essa quantidade e proporção entre alunos e funcionários é bem significativa, podendo impactar tanto positivamente quanto negativamente a segurança da informação nessas escolas.

Observou-se que 28,6% dos respondentes desconhecem a segurança da informação e, os demais respondentes (71,4 %) informaram ter conhecimento sobre o assunto, porém demonstraram um pouco de insegurança ao responder, não sabendo nos explicar se é ou como é aplicada a segurança da informação. Com isso, fica evidente que existe uma carência de treinamento, conscientização e educação dos funcionários para com a segurança da informação nos ambientes escolares.

Existe também a necessidade de se estabelecer uma PSI (Política de Segurança da Informação) nesses ambientes, visto que 85,7% informaram não possuir uma PSI explícita e 14,3% responderam não saber da existência de alguma. Ao implantar uma PSI, com o devido treinamento e divulgação, todos os funcionários passarão a ficar cientes de suas responsabilidades para com a segurança das informações no ambiente escolar.

Quando chega um novo funcionário no setor, 28,6% dos entrevistados responderam não ter passado as responsabilidades referente a segurança das informações utilizadas na escola. Apesar de ser uma quantidade relativamente baixa, se estes funcionários não estiverem bem treinados e conscientes de suas responsabilidades perante as informações que produzem, manipulam e armazenam, podem representar sérios riscos, visto que nenhuma das escolas possuem um servidor de arquivos com o objetivo de proporcionar um local principal para o armazenamento compartilhado de arquivos com demais computadores na rede.

Foi observado que, em 42,9% das escolas, os computadores possuíam autenticação por senha. Porém, um ponto que destacamos como uma falha é o fato de que 71,4% das instituições utilizam apenas uma única autenticação comum aos funcionários ou simplesmente não utilizam autenticação alguma (28,6%), como destacado no Gráfico 1. O compartilhamento de senhas é considerado um risco para a segurança das informações de qualquer organização. Usar um único usuário e senha nos computadores para todos os funcionários que trabalham no setor não é seguro para as informações produzidas, visto que fica fácil da senha ser descoberta por qualquer outro funcionário da escola ou pessoa externa, como também, todos poderão ter acesso às informações com perfil de administrador.

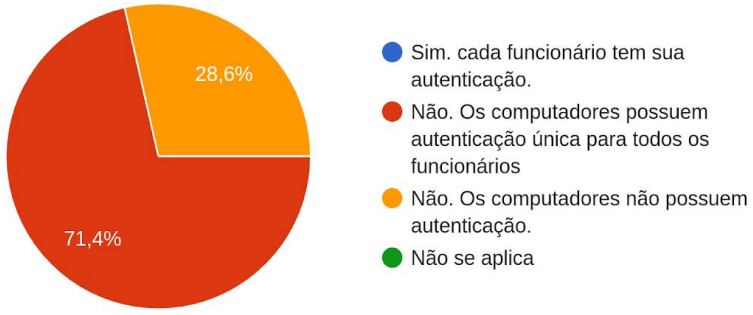

Gráfico 1. Distribuição percentual sobre a prática de autenticação individual para acesso aos computadores.

De acordo com o informado, 42,9% das escolas já procuraram informações (manuais e digitais) que eram importantes e não encontraram. Esse fato além de ocasionar a quebra do

princípio da confidencialidade das informações, também prejudica a disponibilidade, posto que, no momento preciso, a informação procurada não estava disponível. Por essas e outras ameaças que podem afetar os recursos informacionais é importante que as escolas adotem controles físicos e lógicos para assegurar a confidencialidade, integridade e disponibilidade das informações.

Em 42,9% das instituições, os funcionários não fazem uso de bloqueio ou proteção de tela quando se ausentam por algum momento dos computadores. Esse tipo de ação pode colocar em risco a confidencialidade e a integridade das informações, por isso a importância da instituição adotar uma PSI.

Notou-se que 71,4% dos ambientes estudados não alteram com frequência as senhas dos computadores bem como e-mails da instituição, o que pode ocasionar um sério problema, visto que novos ou antigos funcionários poderão ter acesso às informações até mesmo fora do ambiente escolar. É importante que as escolas sempre alterem suas senhas regularmente, principalmente quando funcionários que tinham conhecimento das senhas não trabalham mais na escola.

Foi perguntado aos entrevistados se a escola fazia cópias de segurança com regularidade, e 71,4% disseram que faziam (Gráfico 2). É importante fazer a cópia de segurança de dados, observando principalmente qual o melhor local para guardá-las. 71,4% informaram que armazenam as cópias de segurança em mídias (pen drives, CDs, DVDs). Durante a entrevista, os diretores informaram que a mídia mais utilizada é o *pen drive*. Dos entrevistados, 42,9% responderam que as cópias de segurança são armazenadas também no HD do próprio computador da escola. Essa prática normalmente é considerada um fator de risco pois, se uma ameaça, por exemplo, de *Ransomware*, conseguir explorar alguma vulnerabilidade existente nos computadores e sistemas conseguirá criptografar todos os dados existentes, inclusive as cópias de seguranças que ali forem armazenadas.

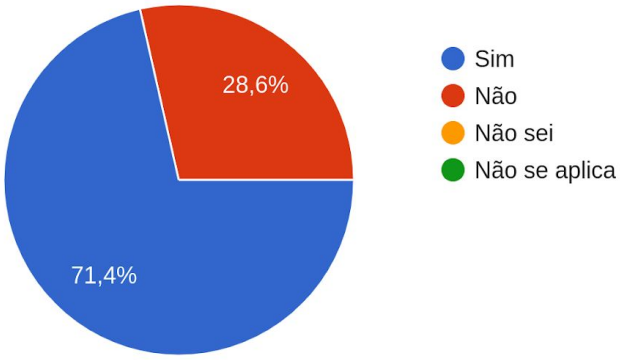

Gráfico 2. Distribuição percentual sobre a prática de backups na instituição

Todas as escolas possuem Internet e uma conexão sem fio (Wi-Fi) com senha de segurança para ser acessada, 57,1% restringem o acesso para a área administrativa e direção escolar. Apesar da maioria das escolas restringirem o acesso à rede, segundo os entrevistados, todos os computadores e dispositivos em funcionamento nas instituições ficam conectados na mesma rede. Consideramos essa ser uma situação potencialmente perigosa para os sistemas de informação das instituições, visto que 42,9% das escolas informaram que já tiveram sua rede invadida, necessitando reconfigurar toda rede para restabelecer o acesso. A mesma porcentagem (42,9%) não souberam informar se isso já havia ocorrido. Invasões ou acessos indevidos às redes e sistemas são considerados incidentes para a segurança da informação. É

preciso que estas instituições saibam identificar as vulnerabilidades existentes em suas redes e sistemas, para assim, evitar que estes incidentes venham impactar negativamente suas informações.

As escolas utilizam diferentes versões do sistema operacional *Windows*. Tal sistema com relação a segurança apresenta problemas, por exemplo: facilidade de instalação de programas sem licença; acesso fácil ao sistema com perfil de administrador, que pode facilitar a instalação de programas maliciosos, reduzindo o nível de segurança para as informações manipuladas nesses sistemas. Em 85,7% das escolas, os sistemas operacionais e os programas instalados são atualizados com frequência, porém, apenas 28,6% utilizam a versão mais recente do sistema. É importante manter os programas sempre atualizados, isso deve ser uma prática constante para a segurança das informações, tendo em vista que nas novas versões ou atualizações foram corrigidas as possíveis falhas e vulnerabilidades identificadas. Observou-se que as escolas utilizam um sistema que por padrão é proprietário, ou seja, é necessário adquirir a licença para usufruir das funcionalidades. Como ilustrado no Gráfico 3, 71,4% informaram que a escola não é responsável e não paga a licença adquirida e 28,6% não souberam informar se o sistema é licenciado. É importante saber a procedência dos sistemas e programas instalados, bem como não permitir a instalação de programas não originais, pois muitos códigos maliciosos se propagam por meio de softwares piratas, como também, muitos fabricantes não permitem a realização de atualizações quando detectam versões não licenciadas.

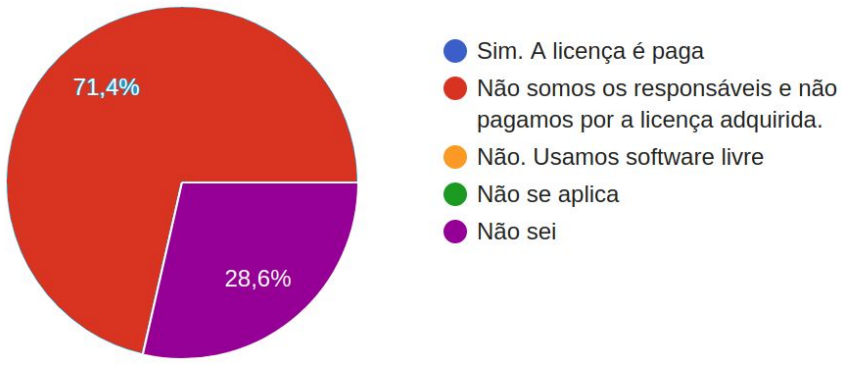

Gráfico 3 – Distribuição percentual sobre o licenciamento do SO e programas instalados.

Outro ponto a ser destacado é o uso do antivírus. Todas as escolas fazem uso de antivírus, observou-se que 85,7% delas utilizam o mesmo antivírus (Avast) e apenas 14,3% utilizam outro software de proteção. Todas elas utilizam a versão gratuita do programa, como também fazem uso apenas do firewall que vem instalado no próprio sistema operacional instalado nos computadores.

Dos entrevistados, 28,6% disseram que os computadores da escola já foram infectados por algum tipo de código malicioso e, a mesma porcentagem informou que nunca foram. Porém, observa-se que 42,9% dos entrevistados não souberam informar se já foi identificado esse tipo de problema nos computadores da escola. Fato que deve ser analisado, visto que 42,6% também disseram não saber identificar se um computador estaria infectado por algum *Malware.* Além disso, todos os entrevistados informaram que os funcionários não recebem orientação sobre o que é e como funciona um software malicioso, porém, consideram importante uma capacitação para docentes, funcionários e alunos sobre o tema.

Em 85,7% das instituições pesquisadas é permitido que docentes, funcionários e alunos insiram mídias como por exemplo, *pen drives*, entre outras, nos computadores principais onde os dados e informações são manipuladas e armazenadas. Mídias podem ser infectadas por códigos maliciosos e, quando infectadas, servem como meio de propagação para essas pragas virtuais. Desse modo, não é seguro permitir que mídias, que não as da própria escola, sejam inseridas nos computadores nos quais são usados principalmente para manipular e armazenar as informações da escola, pois, por mais que os computadores tenham antivírus instalado, esse pode acabar não identificando as ameaças escondida nessas mídias, principalmente se a versão instalada do software é limitada.

Notou-se que 42,9% das escolas permitem em alguns casos o uso dos computadores para fins pessoais. Isso também pode prejudicar a segurança das informações. As escolas podem adotar alguns mecanismos de segurança, como por exemplo, fazer a filtragem dos conteúdos, definindo o que pode ou não ser acessado. Porém, é necessário ter alguém ou uma equipe técnica responsável para fazer as devidas configurações nos computadores da escola. As escolas não possuem uma área de TI e, 71,4% delas não recebem o suporte necessário da equipe disponibilizada pela Secretaria de Educação do município responsável pela área. Outros fatores também são ameaçadores para a segurança das informações das escolas, como por exemplo, não realizar treinamentos para conscientizar os funcionários das consequências e riscos que o uso inadequado dos recursos de informática podem trazer, fato observado em 85,7% das escolas.

Foi questionado aos entrevistados se consideravam que as informações da escola estavam seguras: 71,4% responderam que talvez. Em fase a esse resultado obtido, percebe-se dos entrevistados insegurança quanto à segurança das informações. É preciso entender que a segurança nunca é 100%, porém é necessário que as informações tenham um nível adequado de segurança, adotando as medidas e mecanismos de segurança que visem assegurar esse nível.

4. Conclusão

Este trabalho investigou inicialmente a realidade das escolas municipais, localizadas na área urbana de Girau do Ponciano-AL, com relação a segurança de suas informações. Foi observando se as práticas e procedimentos adotados nos ambientes de pesquisa resguardavam adequadamente seu acervo de dados e qual era o conhecimento dos colaboradores sobre o assunto. Para produzir este trabalho, destaca-se também que foi realizado um estudo sobre os conceitos relacionados à segurança da informação, no qual foi possível descrever os principais incidentes, vulnerabilidades, ameaças e ataques que afetam os ativos informacionais das organizações e apresentar as principais medidas e mecanismos para o controle da segurança. Para pesquisa em si, foi aplicado um questionário junto aos diretores e funcionários das escolas, com intuito de levantar os dados necessários para dar suporte às análises dos resultados. Neste levantamento ficou visível que os colaboradores das escolas, apesar de terem conhecimento sobre o assunto, demonstram uma certa insegurança.

Os objetivos foram traçados e alcançados no decorrer do seu desenvolvimento. Assim, conclui-se que o cenário atual das escolas em relação a segurança da informação ainda é crítico, porém com a adoção de alguns mecanismos de segurança já citados, a implantação de PSI e a realização de capacitações para conscientizar os funcionários podem minimizar as falhas na segurança e preservar as informações contra futuras eventualidades. Desse modo, destacamos que a proteção do acervo de dados e do próprio Sistema de Informação é responsabilidade de todos, uma necessidade essencial para garantir a segurança da informação, não só das escolas estudadas, mas de qualquer organização. Como comentado na

introdução, é possível que esse estudo seja apenas uma amostra de algo pior, que se repita em outros municípios e se agrave na zona rural. São sugestões para continuação deste trabalho.

Referências

Albuquerque Júnior, A. E.; Santos, E. M. (2014) Adoção de medidas de segurança da informação: um modelo de análise para institutos de pesquisa públicos. Revista Brasileira de Administração Científica, Aquidabã, v.5, n.2, p.46-59.

ABNT, Associação Brasileira de Normas Tecnicas. (2005) NBR ISO/IEC 27002. Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro.

ABNT, Associação Brasileira de Normas Tecnicas. (2013) NBR ISO/IEC 27002. Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro.

Dantas, M. L. (2011) Segurança da Informação: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido.

Fontes, E. (2006) Segurança da Informação: O usuário faz a diferença. 1a. ed. São Paulo:Saraiva.

Konzen, M. P. (2013) Gestão de Riscos de Segurança da Informação Baseada na Norma NBR ISO/IEC 27005 Usando Padrões de Segurança.

Kurose, J. F. (2010) Redes de Computadores e a Internet: uma abordagem top-down. 5. ed. São Paulo: Pearson.

Laudon, K. C.; Laudon, J. P. (2010) Sistemas de Informações Gerenciais. Editora: Pearson Prentice Hall. 9. ed.. São Paulo.

Lyra, M. R. (2015) Governança da Segurança da Informação . Edição do Autor – Brasília.

Moreira, N. S. (2001) Segurança mínima: uma visão corporativa da segurança de informações.Rio de Janeiro: Axcel Books.

Nagy, Marcelo (2021) Por onde os Dados Vazam?. São Paulo, Escola Superior de Redes. Webinar medidado por Nicole Rieckmann em 09/07/2021.

Sêmola, M. (2003) Gestão da Segurança da Informação, uma visão Executiva. Rio de Janeiro: Elsevier.

Tanebaunm, Andrew. S. (2003) Redes de Computadores. 4. ed. Rio de Janeiro, Brasil: Ed. Campus.