



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DO TOCANTINS
CAMPUS COLINAS DO TOCANTINS
CURSO SUPERIOR LICENCIATURA EM COMPUTAÇÃO

LISS VITORIA RODRIGUES ALVES

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE ESCOLAR

COLINAS DO TOCANTINS

2022

LISS VITORIA RODRIGUES ALVES

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE ESCOLAR

Projeto de Conclusão de Curso apresentado à Supervisão de Trabalho de Conclusão de Curso do Curso de Licenciatura em Computação do Instituto Federal do Tocantins – Campus Colinas do Tocantins, como exigência à obtenção do grau de Licenciado em Computação.

Orientador: Prof. Luís Alberto Libanio Lima

COLINAS DO TOCANTINS

2022

“O cientista não é o homem que fornece as verdadeiras respostas, é quem faz as verdadeiras perguntas”

(Claude Lévi-Strauss)

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus pelo seu amor e por me guiar até aqui, aos professores do Curso de Licenciatura em Computação do Campus Colinas do Tocantins, pela minha excelente formação acadêmica no decorrer desse curso. Ao professor Luís Alberto Libanio Lima, meu orientador de TCC, que pode me ajudar a concluir com êxito este excelente trabalho. Quero agradecer também a minha mãe que sempre me apoiou na busca pelo conhecimento, e aos amigos próximos que me deram força durante a construção desse projeto. Projeto esse, que foi enriquecedor para minha vida acadêmica e profissional.

RESUMO

Numa sociedade cada vez mais digitalizada, onde a informação se tornou o recurso capaz de gerar valor para as empresas é notória a necessidade da segurança da informação, seja em organizações públicas ou privadas, a partir disso foi desenvolvido este trabalho sobre políticas de segurança da informação no ambiente escolar, com intuito de apresentar um plano de políticas de segurança da informação voltado para uma escola pública, baseado nas falhas e vulnerabilidades identificadas. Para tanto, foi realizada uma pesquisa bibliográfica para compreender a relevância que é dada para este tema dentro das escolas, utilizando-se de apoio literário para ser desenvolvido políticas que atendam a demanda das escolas com relação a este tema. Diante disso, verifica-se que as escolas apresentam um nível baixo de consciência sobre o valor das informações, não possuindo políticas de segurança estabelecidas e pessoal com baixo conhecimento sobre o assunto, o que impõe a constatação de que definir Políticas de segurança é importante, mas além disso é necessário transmitir conhecimento sobre o tema entre os usuários, a fim de garantir maior eficiência das políticas.

Palavras-chave: Políticas de segurança da informação. Segurança da informação no ambiente escolar. Valor das informações.

ABSTRACT

In an increasingly digitized society, where information becomes the resource capable of generating value for companies, the need for information security is evident, whether in public or private institutions, this work on information security policies was developed from this in the school environment, in order to present an information security policy plan aimed at a public school, based on the identified flaws and vulnerabilities. Therefore, a survey was carried out to understand the relevance given to this theme within schools, using bibliographic support to develop policies that meet the demand of schools in relation to this theme. Therefore, it appears that schools have a low level of awareness about the value of information, not having established security policies and staff with low knowledge on the subject, which requires the realization that defining security policies is important, but in addition, it is necessary to transmit knowledge about the topic among users, in order to ensure greater efficiency of policies.

Keywords: Information security policies. Information security in the school environment. Value of information.

SUMÁRIO

1 INTRODUÇÃO	8
2 OBJETIVOS	9
2.1 Objetivo Geral	9
2.2 Objetivos Específicos	9
3 METODOLOGIA	10
4.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	12
5 PROCEDIMENTOS METODOLÓGICOS	14
5.1 ANÁLISES DOS RESULTADOS	15
6 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO PARA UM AMBIENTE ESCOLAR	15
7 CONCLUSÃO	18
FONTES BIBLIOGRÁFICAS	19

1 INTRODUÇÃO

Dentre muitas definições de Escola tem-se a de instituição de ensino e aprendizagem, segundo Paulo Freire diz que “não é a educação que forma a sociedade de uma determinada maneira, senão que esta, tendo-se formado a si mesma de uma certa forma, estabelece a educação que está de acordo com os valores que guiam essa sociedade” (1975, p. 30). A partir desse pensamento pode-se analisar a sociedade atual e ver o quanto ela tem evoluído e os valores têm mudado cada vez mais, se nos anos 50 a 70 os homens disputavam uma guerra fria e uma corrida espacial, nos dias atuais uma das grandes disputas é pela informação. A escola é um ambiente que circula muita informação, além da constante aprendizagem seja através do ensino de conteúdos teóricos ou através da prática, a vivência em um espaço escolar influencia diretamente o consciente dos estudantes, sendo assim não se pode ser indiferente à evolução digital crescente no mundo.

A sociedade está cada vez mais digitalizada e online, o que traz muitos benefícios para o dia a dia, porém exige cuidados redobrados, principalmente quando o assunto é “segurança da informação”. O ambiente escolar assim como outras organizações movimentam muitos dados diariamente, as quais também devem seguir os mesmos critérios de disponibilidade, integridade e confiabilidade. Segundo (Kruger & Kearney, 2008), os usuários devem ser sensibilizados para as questões de segurança, nomeadamente para os efeitos negativos que uma falha ou quebra de segurança podem provocar. O que pode-se analisar é que o usuário desenvolve papel crucial nesse sentido e que é necessário cultivar a importância da segurança da informação, tornando –se algo natural para os usuários ao longo do tempo, deve-se destacar que o conhecimento é a chave para essa conquista.

Com a crescente necessidade de segurança da informação, seja em organizações públicas ou privadas, a preocupação com os dados/informação tem crescido constantemente. “Atualmente, mais do que em outras épocas, a informação assume o palco principal e figura como um ativo dotado de extremo valor para as organizações. Desde os tempos mais longínquos até a atualidade, a informação

ganhou importância, significações e representações diversas que demandaram ações para dotá-las de algum grau de segurança”(NETO E ARAÚJO,2019 pag. 14). A partir disso ver-se também essa necessidade nos ambientes estudantis, espaço em que à grande circulação de dados, além de ser um local propício para ação de pessoas má intencionadas, por nem sempre haver meios de segurança eficazes. Partindo do que já foi dito, este trabalho tem como intuito mostrar a importância do conhecimento em segurança da informação em um ambiente escolar, e de como essa prática pode beneficiar inclusive os estudantes. O foco deste estudo está em evidenciar as falhas de segurança da informação em um espaço escolar por meio de uma visão ética, tendo como motivação a segurança dos dados e dos usuários deste local, além de propor um plano de segurança que se utilizado venham amenizar problemas relacionados ao tema, mostrando quais os benefícios e vantagens de se utilizar a segurança da informação no dia a dia de uma organização estudantil.

2 OBJETIVOS

2.1 Objetivo Geral

Elaborar políticas de segurança da informação para um ambiente escolar.

2.2 Objetivos Específicos

- Identificar falhas de segurança da informação mais recorrentes no ambiente escolar.
- Evidenciar aspectos éticos da segurança da informação no dia a dia das pessoas, que por muitas vezes são deixados de lado.
- .Listar ferramentas de segurança da informação, além de destacar a importância desses recursos.
- Esquematizar um plano de segurança da informação voltado para uma escola pública, seguindo os padrões e normas existentes dentro da segurança da informação.

3 METODOLOGIA

Para elaboração deste trabalho será feita uma pesquisa bibliográfica, explorando relatos evidenciados por outros autores sobre o tema, além das experiências através dos estágios em escolas públicas da cidade de Colinas do Tocantins. Através desse estudo tem-se o intuito de desenvolver um plano que possa servir de apoio em escolas públicas.

4 COMPREENSÃO DA INFORMAÇÃO NO AMBIENTE ESCOLAR

A escola é uma “espelho” da sociedade, o que se vivencia no meio social será expresso de alguma forma dentro do ambiente escolar, tendo em vista o avanço tecnológico e a crescente valorização da informação, põe se em discussão a importância da segurança da informação dentro do ambiente escolar e de se estabelecer políticas de segurança dentro do espaço educacional. Para o Tribunal de Contas da União (2012), a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob o conhecimento de pessoas de má-fé ou concorrentes podem comprometer significativamente não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. As escolas trabalham com informações e dados sigilosos em grande parte de sua rotina. Os dados de alunos e suas famílias, funcionários e colaboradores são registrados nos sistemas e precisam ter a sua segurança e privacidade garantidas. Por tanto, a segurança da informação nas escolas é uma questão importante de ser discutida, é possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações.

Assim como em qualquer outra organização a escola possui ativos, com os quais deve direcionar a devida atenção. Segundo Neto e Araújo (2019), de uma forma geral, pode-se entender um ativo como qualquer elemento de valor para uma organização, seja humano, tecnológico ou software, como, por exemplo, banco de dados, softwares, equipamentos (computadores e notebooks), servidores, elementos

de rede (roteadores, switches, entre outros), pessoas, processos e serviços. Compreender o que são Ativos dentro de uma instituição e a sua importância para a informação é crucial para que os processos ocorram de forma eficaz dentro da organização educacional.

Ao longo das últimas décadas a informação tornou-se o mais importante recurso para organizações, se sobrepôs diante do paradigma de sociedade industrial que tinha como recursos a terra, o trabalho e capital como forma de gerar riquezas, hoje a informação e como ela é tratada é o recurso capaz de gerar valor dentro das empresas, seja pública ou privada. De acordo com a NBR 27002 (2005, p. 16) a informação pode existir em diversas formas, ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Independentemente de como essa informação estiver sendo armazenada ou compartilhada é aconselhável o seu resguardo de forma apropriada.

As instituições públicas de ensino estão inseridas em um mundo cada vez mais digital, esses avanços tecnológicos trazem inúmeros benefícios para o dia dia das escolas, principalmente quando o assunto é armazenar dados, com o tempo essas instituições vêm migrando para as ferramentas tecnológicas, deixando de lado as montanhas de papel com dados pessoais sejam de estudantes, colaboradores, informações administrativas e relatórios, porém a informação se transformou em uma moeda de grande valor monetário, pois através dela pode-se alcançar vantagens indevidas em uma sociedade cada vez mais competitiva. O que nos remete a necessidade da segurança da informação, seja por meios digitais ou físicos, uma das principais ferramentas é estabelecer políticas de segurança. Para Almeida (2000, p. 6), “as políticas ou diretrizes são planos gerais de ação, guias genéricos que estabelecem guias mestras, orientam a tomada de decisão e dão estabilidade à organização”. Definir controles de acesso é uma boa prática de manter controle sobre a informação.

A internet é uma das ferramentas tecnológicas mais utilizadas nos dias de hoje, e um ponto em comum entre a internet e a escola é a informação, de acordo com Rocha (2012, p. 6), a informação “[...] é entropia negativa; é o contrário da desordem. No ensino, significa capacidade de produção de sentido e de influenciar o

comportamento do decodificador semântico, o estudante”. Compreendendo a importância da informação no ambiente escolar, deve-se destacar também a ética profissional dos servidores. Segundo Andrade (2017), “o profissional deve seguir os padrões éticos da sociedade e as normas e regimentos internos das organizações”. A ética profissional trata-se de um conjunto de atitudes e valores aplicados no ambiente de trabalho, sendo de essencial importância para o funcionamento das atividades da organização e das relações de trabalho. Proporcionando um local mais honesto, confiável e comprometido com as metas e objetivos da instituição de ensino.

4.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação tem como base a confidencialidade, a integridade e a disponibilidade, sendo estes critérios necessários para garantir a eficiência dos dados a serem tratados, armazenados ou compartilhados. De acordo com a NBR 27002 (2005, p.16) “a segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas”. O ambiente escolar ainda se mostra pobre em políticas de segurança da informação, deve-se compreender também que o contato das escolas públicas com o mundo digital ainda está lento se comparado às organizações privadas, seguindo essa linha de raciocínio, pode-se analisar o pensamento de Ubiratan Rocha:

Os estabelecimentos de ensino, se comparados com o seu entorno digitalizado, parecem um mundo à parte, sem novidades. Um mundo do esperado, das rotinas conhecidas, dos antigos conhecimentos. Entretanto, um olhar mais atento pode descortinar marcas digitais indiretas em seu cotidiano. Professores e alunos acessam a internet, utilizam telefones celulares, textos são digitados e fotocopiados, o livro didático em papel é perpassado, da concepção à impressão, por tecnologias digitais etc. (ROCHA, 2012, p. 6).

A ação dos usuários está diretamente ligada a eficiência das políticas de segurança, as organizações necessitam de profissionais que apresentem compromisso ético profissional, que respeitem as regras impostas pela instituição. Para Neto e Araújo (2019, p. 33), “as vulnerabilidades são falhas que, por si só, não provocam incidentes, pois são elementos passivos que dependem de um agente

causador ou favorável que a explorem tornando-as ameaças para a segurança da organização”. Rocha defende que “A Web lembra um território de caça. Não se sabe bem quem é a caça e quem é o caçador. O usuário captura informações, mas deixa rastros, sendo, portanto, capturado. Informações-chave circulam pela capilaridade da rede. São dados estratégicos para os diferentes mercados e para a segurança das organizações e do Estado”. Identificar as dificuldades enfrentadas pelos usuários podem contribuir para desenvolver políticas de segurança eficazes, lembrando que a falta de conhecimento sobre a segurança da informação está entre as principais barreiras encontradas.

Segundo Peltier (2001, p.8), “a segurança da informação compreende o uso de controles de acesso físicos e lógicos, com o intuito de proteger os dados contra modificações acidentais ou não autorizadas, destruição, quebra de sigilo, perda ou dano aos ativos informacionais”. A partir disso, entende-se a carência de controle de acesso e a criação de Políticas de segurança nesse ambiente, para tanto Neto e Araújo (2019, p. 35) defende que a “falta de treinamento ou de conscientização das pessoas e de avaliação psicológica adequada ou de verificação de antecedentes que identifiquem objetivos escusos, problemas anteriores, má-fé ou descontentamento de um funcionário, entre outros, podem levar ao compartilhamento indevido de informações confidenciais, à não execução de rotinas de segurança ou a erros e omissões que ponham em risco as informações”. É em virtude disso que muitas organizações investem em criptografia de arquivos, softwares antivírus, redes estruturadas, profissionais da área, controle de acesso, além de muitas outras ferramentas, porém o que tem mais impacto nesse sentido é a promoção da ética e valores entre os funcionários.

Summers (1997, p.21) “percebe a segurança da informação como um componente intrínseco ao uso dos computadores e a considera como uma meta a ser atingida para proteger os sistemas computacionais contra ameaças à **confidencialidade, à integridade, à disponibilidade**” e autenticidade das informações tratadas na organização, estes termos são definidos pelo Tribunal de Contas da União (2012) como:

- **Integridade** - Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados[...].
- **Confidencialidade** - Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação[...].
- **Autenticidade** - Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações[...].
- **Disponibilidade** - Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática[...].

Sendo estas características fundamentais dentro da Segurança da Informação, toda estrutura de segurança deve respeitar esses princípios. Para Dhillon (2001),” os problemas relacionados com a segurança ocorrem devido à ausência de medidas de segurança da informação na organização”(Pimenta & Quaresma, 2016, p. 536). Por muitas vezes até pode existir uma estrutura de segurança nas escolas, porém se não transmitida da forma correta há grandes chances de não ser eficaz. Como já mencionado anteriormente o usuário desenvolve importante papel nas medidas de segurança de uma organização, mas sem a existências de Políticas de Segurança da informação não há como se exigir dos usuários ações colaborativas nesse sentido.

5 PROCEDIMENTOS METODOLÓGICOS

Conforme o objetivo deste trabalho, foi realizada uma pesquisa bibliográfica, o intuito é analisar qual a importância e relevância que os usuários de um ambiente

escolar dão para a segurança da informação, se baseando nos dados já evidenciados de outros autores. Apesar do material coletado ter poucos exemplos de ambientes escolares, os questionamentos serão todos direcionados ao ambiente escolar, relacionando a importância da informação que circula dentro da instituição, se existem políticas de segurança para tratar essas informações e principalmente a participação dos usuários. Alguns questionamentos serviram de apoio durante a pesquisa para manter o foco no tema, como a importância que as empresas dá para essas informações tratadas; os tipos de políticas existentes em empresas e órgãos públicos; a ética profissional entre o funcionários; as medidas tomadas para se evitar perdas de dados importantes ou até desvio de informação; como seria o comportamento ideal dos usuários nas redes internas e de acesso externo da empresa; se é de costume contratar alguém especializado para os serviços relacionados à informática ou se já tem alguém na empresa para essa função; dentre outros questionamentos que conduziram a pesquisa, tendo em vista que o objetivo é desenvolver um plano para escolas públicas.

5.1 ANÁLISES DOS RESULTADOS

A seguir são analisados e discutidos os dados levantados, tanto do ambiente das organizações com relação à política de segurança da informação como dos controles citados nas mesmas, com base nos dados coletados foi possível compreender algumas dificuldades encontradas por empresas ao tentar implantar políticas de segurança, inclusive a dificuldade dos usuários ao tentar se adaptar às regras.

As análises feitas a partir desta pesquisa servirão de norte para o desenvolvimento das políticas de segurança da informação para um ambiente escolar.

6 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO PARA UM AMBIENTE ESCOLAR

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos,

estruturas organizacionais e funções de software e hardware (NBR 27002, 2005, p. 10). Um dos primeiros passos para se estabelecer políticas e controles adequados para uma organização é fazer uma análise ativos e dos seus fatores de riscos mais recorrentes, os investimentos devem ser balanceados com possíveis perdas ou danos a estas informações.

A norma ABNT NBR ISO/IEC 27002:2013 trata sobre a Tecnologia da Informação, das Técnicas de Segurança e do Código de prática para a gestão da segurança da informação que atende desde grandes organizações como para pequenas, sejam públicas ou privadas, servindo então como critério base para este trabalho, além também da Lei Geral de Proteção de dados que entrou em vigor a partir de agosto de 2018 que regulamenta os dados tratados por empresas seja por meio físico ou digital, com base nesses documentos e no que foi estudado até o momento, foi elaborado boas práticas de Políticas de Segurança pensadas para um ambiente escolar:

1. Políticas de Controle de Acesso:

- Definir os níveis de autorização para que sejam claramente estabelecidas e documentados;
- Controles de acesso físico e digital a fim de proteger os ativos da organização contra o uso ou acesso não autorizado;
- Os controles de acesso às informações da instituição podem ser estabelecidos tanto através de sistemas da informação com controle de níveis de acesso por usuário, como por meios físicos proibindo a entrada de pessoas não autorizada a certos ambientes principalmente administrativos;
- Estabelecer senhas confiáveis para acesso a equipamentos e sistemas utilizados pela escola;

2. Políticas de Armazenamento:

- Criar rotinas de backups de informações importantes como documentos e base de dados dos sistemas usados pela instituição;
- Utilizar serviços de armazenamentos em nuvem, evitando perdas por falhas em equipamentos como pendrive, computadores e HD;

- Para informações armazenadas de forma física ter o devido zelo, de forma a garantir que não sofra danos como fogo, inundações, estragos por pessoas, além de outros fatores;

- Controle de mídias, evitando a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada;

3. Políticas de controle da Rede:

- Controle de acesso de novos dispositivos na rede a fim de evitar o uso de sites, programas e outros que ofereçam riscos a rede;

- Utilizar ferramentas de segurança como Firewall, além de senhas de acesso ao computador, evitando o tráfego de informações indevidas entre os dispositivos;

- Fazer uso de serviços de proteção a rede que controlem o acesso a internet evitando acesso a sites maliciosos, downloads de programas piratas, além de diminuir qualquer possível infecção dos dispositivos da rede por agentes externos;

4. Políticas de Segurança de Pessoal:

- Transmitir aos usuários as políticas de segurança da informação da instituição, além da divulgação seja por meio de tutoriais, assim como o treinamento dos colaboradores caso necessário.

- Atenção quanto a admissão de novas pessoas ou a contratação de prestadores de serviço, a fim de garantir que funcionários e partes externas entendem as suas responsabilidades e estão de acordo com os papéis para os quais eles foram contratados;

- Divulgar entre os funcionários o código de ética, englobando a missão, os valores e princípios que norteiam a organização e que devem ser conhecidos e respeitados pelos funcionários.

As políticas mencionadas acima foram desenvolvidas para escolas públicas, envolvendo principalmente o comportamento moral e ético dos usuários, pois só a criação de políticas não é suficiente para garantir a segurança das informações, mas também a construção de um pensamento computacional, ético e conscientes por parte dos usuários, onde as práticas de políticas de segurança estarão inseridas no

cotidiano das escolas. Essas ações constroem a reputação da escola perante a sociedade, a ética profissional é umas das ferramentas que podem ser amplamente utilizada no ambiente de trabalho, pois possui fatores como respeito às normas da instituição, respeito entre os funcionários, à hierarquia dentro da organização, promove a imparcialidade e um ambiente mais confiável.

Para uma boa implementação das políticas de segurança se faz necessário investimentos financeiros e de pessoal qualificado, tendo em vista que para aplicação dessas políticas pode ser necessário atualizações da estrutura física e lógica da instituição. Dentro dos aspectos físicos a adição ou aprimoramento de controles de acesso a ambientes, à equipamentos e até mesmo ao lixo descartado são boas práticas de segurança, outro aspecto físico é a estruturação da rede da escola que por muitas vezes é negligenciada assim como na maioria das empresas, a contratação de técnico qualificado e comprometido pode ajudar. Já nos aspectos lógicos, são vários os fatores que podem ser citados aqui, dentre eles está o uso de sistemas originais nos equipamentos das escolas, oferecendo mais segurança e confiabilidade, a internet de qualidade que atenda demanda da instituição, programas que auxiliem no controle da estrutura lógica de rede, os backups de documentos importantes da instituição que podem ser feito de forma automática com o uso de softwares confiáveis, uso de anti-virus de qualidade nos equipamentos e muitos outros. Porém é sabido que nem sempre as escolas públicas possuem meios para investimento diante das várias demandas, além da administração que deve está comprometida com a aplicação das políticas de segurança da informação.

7 CONCLUSÃO

Por meio do estudo realizado foi desenvolvida uma proposta de políticas de segurança da informação, de acordo com a análise das vulnerabilidades e mais recorrentes falhas de segurança relatadas no dia a dia de empresas, seguindo princípios estabelecidos pelas normas existentes nos dias de hoje. Dentre as principais dificuldades identificadas nas escolas, está a falta de conhecimento na área, o que problematiza a implementação de políticas de segurança da informação e potencializa possíveis riscos à segurança. Ao longo deste trabalho foi apresentado a importância da informação e da segurança da informação, sendo estes ativos imprescindíveis dentro das escolas, vivencia-se uma era onde ter informação é ter poder, e informação demais em mãos erradas pode gerar danos inimagináveis a qualquer organização.

As políticas de segurança apresentadas no decorrer deste trabalho está relacionado principalmente ao comportamento dos servidores, para que a implementação dessas políticas ocorram de forma mais eficaz, é importante que eles recebam uma apresentação detalhada dessas políticas, para compreender a relevância dos dados tratados nas escolas, de como essas ferramentas irão operar dentro das instituições e da importância do seu papel dentro aplicação dessas políticas.

Sendo a escola um espaço de constante aprendizagem, fazer o uso de tecnologias digitais no dia a dia das escolas, promove a cultura digital, sabendo que os meios sociais hoje é movida por dispositivos eletrônicos e redes online, ter na escola exemplos de políticas de segurança sendo usados pode contribuir para a vida em sociedade dos estudantes.

FONTES BIBLIOGRÁFICAS

FREIRE, P.& ILLICH, Ivan. Diálogo. In: Seminario Invitación A Concientizar y Desescolarizar: Conversación permanente, Ginebra, 1974. Atas. Buenos Aires, Búsqueda Celadec. 1975, 109 p.

NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. Segurança da Informação: uma visão sistêmica para implantação em organizações. João Pessoa: Editora da UFPA, 2019.

Kruger, H. A., & Kearney, W. D. (2008). Consensus Ranking - An ICT security awareness case study. *Computers & Security*, 27 (7), 493-508.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ALMEIDA, M. C. B. Planejamento de bibliotecas e serviços de informação. Brasília: Briquet de Lemos, 2000.

ROCHA, Ubiratan. Revista Querubim – revista eletrônica de trabalhos científicos nas áreas de Letras, Ciências Humanas e Ciências Sociais – Ano 08 – 2012 ISSN 1809-3264.

SUMMERS, R. C. Secure computing: threats and safeguards. New York: McGraw-Hill, 1997.

TRIBUNAL DE CONTAS DA UNIÃO. Boas práticas em segurança da informação. 4. ed. Brasília. 2012.

PELTIER, T. R. Information security policies, procedures, and standards: Establishing an Essential Code of Conduct. USA: Auerbach Publications, 2001.

Andrade, Inacilma Rita Silva. Ética geral e profissional / Inacilma Rita Silva Andrade. - Salvador: UFBA, Faculdade de Ciências Contábeis; Superintendência de Educação a Distância, 2017.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A.. Information security policy: An organizational-level process model. *Computers & Security*, 28 (7), 2019, 493-508.

PIMENTA, A.M.S., QUARESMA, R.F.C. . A Segurança dos Sistemas de Informação e o Comportamento dos Usuários. **JISTEM - Journal of Information Systems and Technology Management**. Brasil, Vol. 13, No. 3, Set/Dez., 2016 pp. 533-552.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 22 nov. 2021.