MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA BAHIA
CAMPUS VALENÇA

MARIA RITA DE JESUS SANTOS

ANÁLISE DA PROTEÇÃO DOS DADOS DE ALUNOS NAS ESCOLAS PÚBLICAS DE VALENÇA: UMA ABORDAGEM DE CIBERSEGURANÇA

VALENÇA-BA
2023

MARIA RITA DE JESUS SANTOS

ANÁLISE DA PROTEÇÃO DOS DADOS DE ALUNOS NAS ESCOLAS PÚBLICAS DE VALENÇA: UMA ABORDAGEM DE CIBERSEGURANÇA

Trabalho de Conclusão de Curso do Curso ADS, do Instituto Federal de Educação, Ciência e Tecnologia da Bahia, como requisito parcial para a obtenção do título de Tecnólogo em ADS

Orientador: Prof. Dr. Rafael Freitas Reale

VALENÇA

2023

FICHA CATALOGRÁFICA ELABORADA PELO SISTEMA DE BIBLIOTECAS DO IFBA, COM OS DADOS FORNECIDOS PELO(A) AUTOR(A)

S237r Santos, Maria Rita de Jesus

Análise da proteção dos dados de alunos nas escolas públicas de Valença: uma abordagem de cibersegurança/ Maria Rita de Jesus Santos; Orientador Marcelo de Araújo Lino; coorientador Diogo S. D. da Silva -- Valença : IFBA, 2023.

44f.

TCC (Tecnólogo em ADS) -- Instituto Federal de Educação, Ciência e Tecnologia da Bahia – Campus Valença, 2023.

1. Segurança da informação 2. Documentação 3. Escolas públicas. I. Lino, Marcelo de Araújo, orient. II. Silva, Diogo S. D. da, coorient. III. TÍTULO.

CDD: 005.8

FOLHA DE APROVAÇÃO

MARIA RITA DE JESUS SANTOS

ANÁLISE DA PROTEÇÃO DOS DADOS DE ALUNOS NAS ESCOLAS PÚBLICAS DE VALENÇA: UMA ABORDAGEM DE CIBERSEGURANÇA

Trabalho de Conclusão de Curso de graduação apresentado como requisito parcial para obtenção do título de Bacharel em Tecnologia em Análise e Desenvolvimento de Sistemas, do Instituto Federal de Educação, Ciência e Tecnologia da Bahia (IFBA), *campus* Valença.

Aprovado em

Valença, 24 de julho de 2023

Banca examinadora

Rafael Freitas Reale

Prof. Dr. Rafael Freitas Reale – Orientador

Instituto Federal de Educação, Ciência e Tecnologia – Campus Valença

Addson Araújo da Costa

Prof. Me. Addson Araújo da Costa

Instituto Federal de Educação, Ciência e Tecnologia – Campus Valença

Matuzalém Guimarães Leal

Prof. Esp. Matuzalém Guimarães Leal

Instituto Federal de Educação, Ciência e Tecnologia – Campus Valença

DEDICATÓRIA

Dedico este trabalho aos meus pais e meu irmão que sempre me apoiaram em todas as etapas da minha vida, me ajudando a encarar riscos, a vencer desafios e a comemorar as minhas vitórias. A participação de vocês na minha vida acadêmica foi essencial, amo vocês. Dedico também a família PRD que encontrei pelos corredores do IFBA que participaram das alegrias e tristezas de algo muito além da minha formação, fazendo parte da minha jornada e me permitindo chegar até aqui. A todos vocês, meu profundo agradecimento.

AGRADECIMENTOS

Agradeço aos meus pais e irmão por me ensinarem a olhar para o céu e amar as estrelas. Vocês me mostraram que o passado brilha tanto quanto o futuro. E eu fico imensamente grata por todos os desafios que passamos juntos.

Agradeço aos meus amigos que compartilharam, risos, lágrimas, momentos difíceis, fáceis, brincadeiras e todas as realizações desse período juntos. Criamos uma família, somos irmãos de alma.

Por fim, agradeço aos meus professores queridos que, em meio a todas as dificuldades desses últimos anos, se dedicaram com todas as energias para colaborar com a minha formação e dos meus amigos. Eterna gratidão a todos vocês.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

LGPD	Lei Geral de Proteção de Dados
CERT	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança da Informação
CID	Confiabilidade, Integridade e Disponibilidade
ISO	*International Organization for Standardization* - Organização Internacional de Padronização
IEC	*International Electrotechnical Commission* - Comissão Eletrotécnica Internacional
CGI	Comitê Gestor da Internet no Brasil
ECA	Estatuto da Criança e do Adolescente
DTI	Departamento de Tecnologia da Informação
AWS	*Amazon Web Services*

SUMÁRIO

ANÁLISE DA PROTEÇÃO DOS DADOS DE ALUNOS NAS ESCOLAS PÚBLICAS DE VALENÇA: UMA ABORDAGEM DE CIBERSEGURANÇA

RESUMO

Com o avanço da tecnologia e as transformações digitais em curso, é essencial dedicar atenção e cuidado à segurança da informação e às políticas de segurança adotadas por instituições que lidam com dados sensíveis e pessoais, especialmente quando se trata de crianças e adolescentes. Por conta disso, o presente trabalho tem como objetivo investigar a proteção de dados dos estudantes das escolas públicas da cidade de Valença, considerando o contexto da cibersegurança. Foram adotadas abordagens qualitativa e descritiva, buscando conceituar e compreender as práticas e medidas implementadas para garantir a segurança desses dados. Foram realizadas entrevistas com gestores acadêmicos e no Departamento de Tecnologia da Informação, a fim de identificar os procedimentos e desafios enfrentados nesse contexto. Além disso, foram analisadas as normas e diretrizes, como a LGPD e a família ISO/IEC 27000, que orientam as boas práticas de segurança da informação. Os resultados e análises obtidas oferecem um norte sobre a atual situação da proteção de dados nas escolas públicas de Valença e destacam a importância de medidas preventivas e atualizadas para garantir a segurança e privacidade dos dados dos estudantes. O trabalho também ressalta a necessidade de conscientização e capacitação dos profissionais envolvidos nesse processo, bem como o constante acompanhamento e aprimoramento das políticas e práticas de segurança da informação nas instituições educacionais.

Palavras-chave: Segurança da informação. Documentação. Escolas públicas.

ABSTRACT

With the advancement of technology and ongoing digital transformations, it is essential to dedicate attention and care to information security and the security policies adopted by institutions that deal with sensitive and personal data, especially when it comes to children and adolescents. Therefore, the present study aims to investigate the data protection of students in public schools in the city of Valença, considering the context of cybersecurity. Qualitative and descriptive approaches were adopted, seeking to conceptualize and understand the practices and measures implemented to ensure the security of this data. Interviews were conducted with academic managers and the Department of Information Technology to identify the procedures and challenges faced in this context. Additionally, standards and guidelines such as LGPD and the ISO/IEC 27000 family were analyzed, which guide best practices in information security. The results and analyses obtained provide insights into the current state of data protection in public schools in Valença and highlight the importance of preventive and up-to-date measures to ensure the security and privacy of student data. The study also emphasizes the need for awareness and training of professionals involved in this process, as well as the continuous monitoring and improvement of information security policies and practices in educational institutions.

Key words: Information security. Documentation. Public schools.

1. INTRODUÇÃO

O avanço tecnológico possibilitou um maior acesso à informação para a população, ao mesmo tempo em que proporcionou a disponibilidade de uma grande variedade de dispositivos que permitem o acesso à internet. Surgiu então a necessidade de verificar, não só a qualidade de armazenamento de informações que envolve a manipulação correta, cuidados e manutenção, como também abordar quesitos de segurança de quem está acessando e consumindo esses dados.

Conforme apontado por Semeler e Pinto (2019), um dado é a menor unidade de informação quando considerado isoladamente. Entretanto, ao reuni-los e analisá-los em um contexto adequado, os dados recebem significado e podem ser utilizados para compreender e tomar decisões em diversas situações. Os dados, nesse sentido, servem como blocos de construção para a obtenção de informações relevantes e são fundamentais para embasar processos de análise e tomada de decisão.

Segundo Vangller (2017), informação é um conjunto de dados que pertence a uma pessoa ou a uma organização. Sendo assim, uma informação é o resultado do processamento e interpretação dos dados, o que lhe confere significado e utilidade, tornando-se, portanto, um recurso importante para quem as possui. A Segurança da Informação é a garantia de que os dados pessoais e corporativos estarão protegidos.

O conceito de segurança da informação não abrange somente a ideia de informações dispostas em ferramentas eletrônicas, e sim possibilita a proteção de informações pessoais, corporativas e nacionais armazenadas em qualquer lugar. Nesse contexto, esta pesquisa teve como objetivo investigar como ocorre a proteção de dados dos estudantes das escolas públicas na cidade de Valença, considerando os conceitos de cibersegurança.

Para a coleta de dados para esta pesquisa abordou parâmetros cruciais para entender como ocorre a proteção dos dados dos estudantes. Portanto teve como objetivos específicos identificar as formas mais relevantes de armazenamento dos dados, os formatos de acesso a essas informações, os responsáveis por esse acesso e se possuem qualificação relacionada aos conceitos de cibersegurança. Além disso, foram identificados os dados sensíveis compartilhados na instituição e, por fim, foi analisada como ocorre efetivamente a proteção dessas informações.

Dado o grande fluxo de informações mantidas dentro de uma escola, onde a maior parte desses dados são manuseados diariamente, esse trabalho se justifica com o entendimento

sobre a necessidade de abordagem com os funcionários das instituições sobre os conceitos de segurança da informação, criação de políticas de segurança de dados, o entendimento sobre dados sensíveis e as implicações de descumprimento da Lei Geral de Proteção de Dados (LGPD). As instituições acadêmicas devem possuir mecanismos de segurança para evitar, além de ataques cibernéticos, ataques que envolvem engenheiros sociais.

Essa monografia possui a estrutura de cinco capítulos onde são abordados desde conceitos importantes de segurança da informação, até os dados de resultados colhidos através de entrevistas com os gestores do departamento de tecnologia da informação e das escolas examinadas. No primeiro capítulo, foram abordadas as motivações da sua construção e como foram estabelecidos parâmetros para seu desenvolvimento. No segundo capítulo, é feita a revisão bibliográfica, que nos permite compreender os conceitos de redes de computadores, cibersegurança, aborda as ameaças à segurança da informação, traz alguns procedimentos que podem mitigar as ameaças à segurança da informação e por fim, aborda as legislações que gerenciam juridicamente a proteção de dados e direitos da criança e adolescente. No terceiro capítulo, são apresentados os processos de desenvolvimentos utilizados para chegar aos resultados, abordando o formato descritivo e qualitativo aplicado nas entrevistas com os gestores. No quarto capítulo, são apresentados os resultados da pesquisa em conjunto com a análise dessas informações trazidas. Por fim, no capítulo cinco, temos as considerações finais que perpassam pelos conceitos abordados anteriormente e traz a relevância desse trabalho e seus resultados.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentadas a revisão de literatura utilizada para esse estudo. Por tanto, são abordados os conceitos importantes, legislações e ainda, procedimentos de segurança da informação.

2.1. REDES DE COMPUTADORES

Redes de computadores, ou simplesmente Redes, segundo Sousa (1999), é a troca de conteúdos e recursos por meio de equipamentos que estão interligados, compartilhando arquivos, conectando em uma mesma infraestrutura ou até mesmo espalhados pelo mundo.

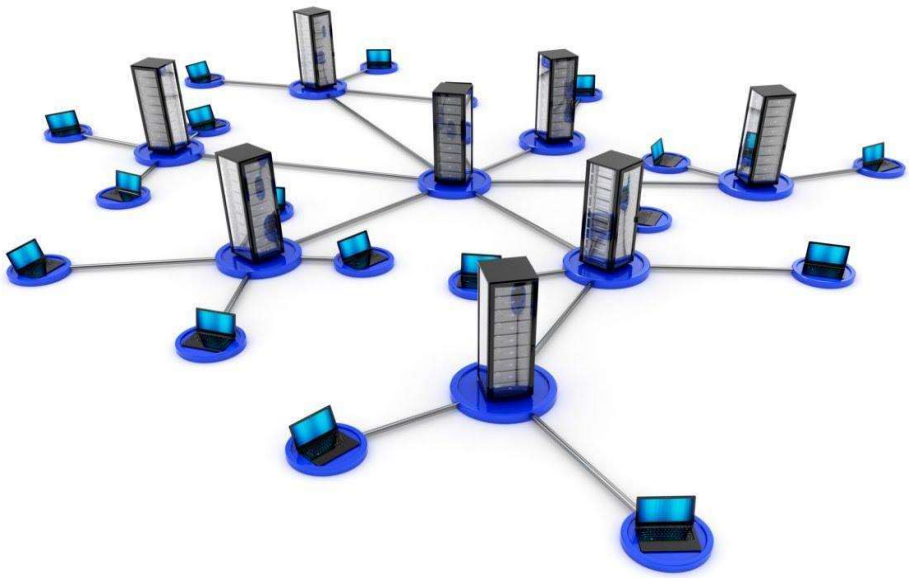

Figura 1 - Representação das redes de computadores (JONER, 2017)

Uma rede é uma estrutura de pontos de conexão que se tornou muito importante no cotidiano. Teixeira (2021) discorre sobre sua ampla utilização nos contextos corporativos, acadêmicos e governamentais, contando com sua característica de distribuição de conteúdo para facilitar a vivência daqueles que dependem do seu uso.

O que chamamos de Internet foi definido por Almeida e Rosa (2000), como um conjunto dessas redes, que estão conectadas entre si, espalhadas pelo mundo inteiro. A Internet, a fim de conectar o mundo, tem a capacidade de direcionar os usuários a uma ampla variedade de recursos, como pesquisas, arquivos diversos e notícias. Entretanto, estar conectado é um processo que é mais complexo do que pode parecer à primeira vista. Esses processos englobam conjuntos de dispositivos interligados, utilizando camadas de comunicação, protocolos que regulamentam e regras de normatizações que garantem o bom funcionamento dessas redes. Esse conjunto de elementos, por sua vez, necessita de um gerenciamento eficiente, a fim de garantir a qualidade necessária para que um usuário possa acessar livremente os conteúdos disponíveis.

Para acessar a Internet é possível a utilização de diversos aparelhos que passaram a ser parte integrante do dia a dia. Celulares, computadores, relógios, impressoras, são exemplos de equipamentos que ao se conectar em rede, possibilitam a comunicação contínua

entre as pessoas. Magrani (2018) ressalta que estamos vivendo um momento de hiperconectividade, que trata sobre a disponibilidade de comunicação constante das pessoas. À medida que a tecnologia avança, novos equipamentos continuam a se integrar à rede, aprimorando ainda mais a capacidade das pessoas de se comunicarem e compartilharem informações.

2.2. CIBERSEGURANÇA

Com o passar do tempo, os avanços tecnológicos e a busca pelos dados cada vez mais frequentes, tornou-se evidente que, assim como o uso legítimo e relevante da internet, surgiram diversas fraudes e golpes envolvendo as redes. De forma que muitas informações ficaram expostas, levando ao surgimento do conceito de cibersegurança, que agora ganha um direcionamento a proteger as redes e tecnologias da informação. O objetivo da cibersegurança é suprir o déficit da segurança dos dados que passou a existir com o crescimento e popularização dos computadores.

A cibersegurança, portanto, é o esforço para proteger sistemas, documentos e todos os dados de usos não autorizados ou prejudiciais. É possível dizer a partir disso que uma pessoa deve proteger suas informações, uma instituição deve proteger a informação de todos as pessoas que fazem parte daquele contexto e uma nação, por sua vez, deve proteger a população para que essas informações não se tornem alvos de criminosos. Só se faz isso seguindo diretrizes e leis que permitem que esses grupos sejam possibilitados de criar esse ambiente seguro.

Vangller (2017) ainda mostra que a segurança de uma informação vai estar relacionada possivelmente ao comportamento do usuário ou ainda, ao ambiente onde aquele dado está sendo utilizado. Dessa forma, é possível que certos conteúdos sejam modificados ou manipulados, especialmente quando o acesso a eles está disponível para qualquer pessoa.

Kurose (2013) mostra em seu conteúdo uma analogia que confirma exatamente essa ideia da possibilidade de manipulação, onde traz uma comunicação entre dois indivíduos e ilustra sobre a dificuldade de se falarem em um ambiente inseguro. Toda a comunicação deve conter propriedades que garantam a segurança seja ela: uma conversa, uma documentação, um arquivo em um computador, ou ainda, a disponibilização de imagens do usuário. Esses

contextos determinam que haja regras no monitoramento e armazenamento dos dados, para isso, existem as diretrizes CID, que são os pilares na cibersegurança.

A Tríade CID consiste principalmente nos conceitos de Confidencialidade, Integridade e Disponibilidade da informação. Esses são os parâmetros que garantem, se seguidos, uma maior segurança dos dados.

A **confidencialidade** diz respeito à privacidade de uma informação. Vangller (2017) comenta que ela tem o papel de limitar o acesso, fazendo com que ela seja apenas acessada por pessoas legalmente autorizadas a aquele conteúdo. É nela que a criptografia é utilizada, junto a um grupo de técnicas, sejam elas eletrônicas ou não, que visam garantir a proteção do conteúdo compartilhado, restringindo sua informação entre emissor e receptor. Dessa forma, a confidencialidade garante que para acessar um dado, é necessário que o usuário passe por algum tipo de verificação de identidade, a autenticação, que suas atividades sejam verificadas, de forma a averiguar se elas cumprem as disposições planejadas e estabelecidas, a auditoria, e por fim, a partir da autorização, garantir que o usuário possa ter direito ao acesso, levando em consideração o grupo a que pertence.

A **Integridade** está relacionada a não alteração ou manipulação de informações, sejam elas armazenadas ou compartilhadas. Não é possível confiar em algo que pode ser modificado durante a comunicação, como por exemplo, na brincadeira de telefone-sem-fio, onde as pessoas falam aos ouvidos uns dos outros e ao fim, nem sempre o que foi dito no início, chega a última pessoa da roda. Portanto, a integridade, segundo Vangller (2017) , é a garantia de que todo o conteúdo se mantenha inalterado durante o manuseio.

Vangller (2017) destaca que a **Disponibilidade** é a diretriz que visa garantir que o conteúdo esteja disponível sempre que o usuário necessitar dele. Ela é importante para a validação do conteúdo para a garantia de qualidade e dos pontos anteriores, e o acesso à informação. Não adianta que a criptografia, através da confidencialidade seja feita e que a Integridade tenha sido atendida, se no fim, quem for utilizar não puder acessar o dado.

Outros dois pilares que podem ser acrescentados são: autenticidade e irretratabilidade. Autenticidade consiste, segundo Ferreira(2021), em garantir que as informações partam de uma origem confiável. Por isso, através da autorização do acesso de um usuário a um determinado sistema, visa, por meio de senhas ou recursos de biometria, por exemplo, garantir a maior confidencialidade, já que isso limitaria o acesso de terceiro.

Ferreira(2021) ainda traz o conceito de irretratabilidade, que também pode ser chamado de não repúdio, que tem a ver com a responsabilização do fornecedor de informações, garantindo que possa ser possível de provar o que foi feito, quem fez e quando fez em um determinado sistema, não sendo possível a negação das ações causadas pelos seus usuários.

2.3. AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

A CID viabiliza a diminuição de ataques cibernéticos e contra a segurança da informação, prevenindo de fatores que possam causá-los. Para existir um ataque é importante que existam fatores anteriores com um potencial para que isso ocorra.

Na Cartilha de Segurança da Internet, desenvolvida em 2012, pelo Comitê Gestor da Internet no Brasil, CGI.br, a vulnerabilidade é definida como: uma situação de fraqueza a um objeto, indivíduo ou informação, onde essa fraqueza pode ser utilizada para criar estratégias de ataques. Uma ameaça é a possibilidade que exista um prejuízo a esses elementos que ocasionalmente possam se tornar ataques. E ainda segundo a cartilha, ataques a essas vulnerabilidades são a tentativa de execução de ações que resultem em perdas, uso indevido, sequestro ou perdas de dados.

As pessoas que idealizam ataques cibernéticos são indivíduos muito inteligentes popularmente conhecidos como Cibercriminosos. Porém existem outras terminologias que se referem a categorias de profissionais especialistas em invasões. Beaver (2013) tenta trazer na sua descrição dessas terminologias relacionadas alguns termos e eles são: Hackers são indivíduos que possuem uma predisposição e grande curiosidade para lidar com sistemas e, muitas vezes, acabam descobrindo vulnerabilidades; Crackers são os Hackers “do mal”, indivíduos que exploram essas falhas a fim de receber algum reconhecimento, dinheiro ou simplesmente prejudicar pessoas ou instituições, são os Cibercriminosos; e ainda temos os Hackers éticos, que são aqueles que trabalham para fins de conseguir descobrir falhas internamente, antes que outras pessoas descubram e possam explorá-las.

Vale ressaltar que apesar de grandes habilidades com softwares e hardwares, os Crackers são especialistas em pessoas. As técnicas usadas para explorar vítimas podem partir de inúmeros tipos de golpes diferentes que envolvem manipulação e criação de sistemas específicos para usar da falta de conhecimento ou habilidade da população vulnerável.

Existem inúmeros tipos de ataques que podem ser motivos de acessos indevidos a dados pessoais, muitos deles, aplicados unicamente a computadores. Temos os chamados

Malwares, que segundo Melo e Amaral (2011), são códigos maliciosos que tem o objetivo de explorar vulnerabilidades presentes nos computadores ou em áreas adjacentes ao uso de equipamentos eletrônicos. Como visto abaixo, na Tabela 1, a variedade desses malwares e suas descrições.

Tabela 1 – Malwares (Adaptado da Cartilha de Segurança na Internet)

Nomenclatura	Descrição
Vírus de computadores	É um código malicioso que se propaga, infectando vários dispositivos. Geralmente dependem de uma ativação, como a execução de um programa no computador
Worm	É um programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades, enviando cópias de si mesmo de computador para computador
Bot	É um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente
Botnet	É uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots
Spyware	É um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros
Keylogger	É um tipo de Spyware é que capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador
Screenlogger	É um tipo de Spyware é que similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado
Adware	Projetado especificamente para apresentar propagandas, podendo ser usado tanto para fins legítimos, quanto para fins maliciosos, fazendo o monitoramento do usuário
Backdoor	É um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim
Cavalo de troia (Trojan)	É um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário
Rootkit	É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido

Segundo as estatísticas do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança da Informação, a CERT.br, existiu um número considerável de envio de Spams notificados nos primeiros meses de 2023, que são definidos pelo CERT.br na Cartilha de Segurança na internet como uma forma de comunicação indesejada enviada por e-mail para

um grande número de destinatários. Essas mensagens geralmente contém propagandas, mas também podem representar uma ameaça à segurança, pois podem conter códigos maliciosos que comprometem a segurança dos computadores. Na Figura 2, é possível ver um gráfico estatístico dos ataques de 2023 notificados ao CERT.br.

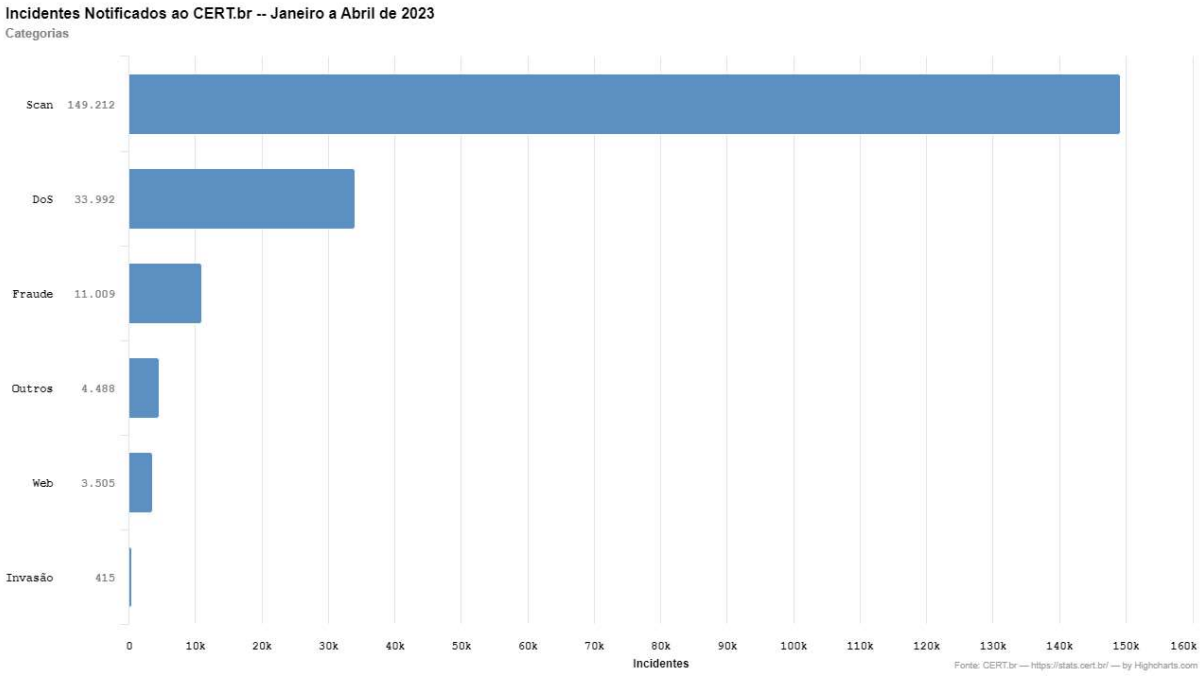

Figura 2 - Incidentes Notificados ao CERT.br entre janeiro e abril de 2023 (CERT.br)

Ransomware, segundo De Mendonça (2020) é um sequestro digital que pode se dar por diversas motivações, como por exemplo, ganhos financeiros. Geralmente são aplicados em grandes empresas ou pessoas famosas que acabam por ter seus dados bloqueados e a partir disso, é solicitado um valor em “resgate” para esses dados.

O ransomware é um tipo de malware altamente prejudicial que pode causar danos permanentes ao proprietário das informações afetadas. A perda de acesso a arquivos importantes pode ter consequências graves, interrompendo operações de negócios, resultando na perda de dados valiosos e comprometendo a privacidade de informações sensíveis.

Além dos malwares, existem diversas outras formas de ataques de invasão, e uma das estratégias mais eficazes para comprometer a segurança da informação é a engenharia social. A engenharia social é uma técnica que é um ataque de acesso, utilizada por invasores com o

objetivo de manipular indivíduos, levando-os a realizar ações ou divulgar informações confidenciais.

Em A arte de enganar, Mitnick (2003) aborda que o elo mais fraco da segurança de uma instituição é o humano. A segurança é ilusória quando não exercida envolvendo todos os fatores que a cercam. Uma escola, um banco, uma clínica podem possuir os melhores e mais sofisticados sistemas de segurança que existem no mercado. Entretanto, quando existe confiança exagerada apenas nesses recursos técnicos, somente o mau treinamento da secretária ou do porteiro pode desencadear em um ataque.

Acessar ambientes usando a Engenharia social é fácil, porque ela é cercada por mentiras e pela segurança convincente do cracker. Essa pessoa dissimula de maneira tão tranquila, que passa a ter acesso a ambientes, muitas vezes, restritos da instituição. Ela usa uma tática que pode passar despercebida por não utilizar necessariamente alguma ferramenta tecnológica de forma que provoca situações que fazem com que as vítimas se sintam confusas, confortáveis diante de uma posição de liderança manipulada, ou ainda vulnerabilidades na disponibilidade de informações em ambientes que podem ficar acessíveis a pessoas suspeitas. E isso se dá graças ao não acesso das pessoas a técnicas básicas de identificação de ataques de cibersegurança, fazendo com que elas não percebam que estão sendo atacadas e acabam passando informações de forma indevida.

2.4. Mitigação de Riscos à Segurança Da Informação

Com o objetivo de mitigar os riscos associados às vulnerabilidades encontradas no uso de recursos tecnológicos ou nas interações sociais, é possível adotar diversas medidas para reduzir a ocorrência de incidentes. Dentre elas destacamos: Políticas de segurança da informação, backups, criptografia, manutenção de equipamentos e treinamento de funcionários.

2.4.1. Políticas de segurança da informação

As políticas de segurança da informação, segundo Spanceski(2004), têm como objetivo garantir que o uso dos recursos da instituição sejam utilizados corretamente. Para alcançar isso, é essencial que os usuários estejam cientes das regras e diretrizes para o uso seguro das informações, evitando a exposição de dados que possam prejudicar a instituição de ensino, seus funcionários ou alunos.

A criação de regras e diretrizes internas tem a responsabilidade de mitigar riscos sobre os dados e quem os detém, bem como, é importante que o conteúdo utilizado seja protegido por uma política de respeito a Tríade de segurança da informação, que irá fornecer ao usuário a garantia de atendimento de regras de proteção de dados necessária.

2.4.2. BACKUPS

Backups são cópias de segurança dos dados e essenciais para garantir a preservação dos dados em caso de comprometimento do ambiente de armazenamento original. De acordo com Fialho Jr.(2007), a importância das cópias de segurança está relacionada à sua capacidade de mitigar interferências externas ou internas na gestão da qualidade do armazenamento da informação. Eles desempenham um papel crucial na proteção contra perdas de dados e garantem a continuidade das operações, permitindo a recuperação das informações em caso de falhas, desastres ou ataques cibernéticos.

Dentro do processo de criação de cópias, é importante levar em consideração algumas medidas que podem ajudar que esse processo seja mais eficaz. Moraes(2007), traz a perspectiva sobre a localização do backup, citando o evento de 11 de setembro de 2001, quando as Torres Gêmeas foram atacadas. Em um dos prédios estava a base de dados e no outro seu backup, isso impossibilitou a recuperação daquelas informações perdidas durante o incidente.

Outro aspecto trazido por Moraes(2007) que deve ser analisado é em qual ambiente essas informações ficarão armazenadas, se localmente em computadores na própria instituição, se eles serão colocados em armazenamentos em nuvem, ou ainda em computadores em outros ambientes, mantendo uma segurança de localização. Por fim, a frequência é imprescindível para garantir a eficiência do backup, visto que, um dia comum em um ambiente com muito fluxo de dados, possui atualizações dinâmicas que precisam ter sua integridade, disponibilidade e confiabilidade garantidas.

2.4.3. CRIPTOGRAFIA

De acordo com Terada (2008), a criptografia é uma técnica que utiliza algoritmos para criar uma chave de acesso, tornando difícil para pessoas não autorizadas decifrarem informações ou obterem acesso a sistemas específicos. Dois exemplos de uso de criptografia são: assinaturas digitais e certificados digitais. Segundo a CERT.br (2012), as assinaturas digitais permitem a comprovação da autenticidade e a integridade de uma informação, tendem a garantir que apenas quem gerou a chave primária a conheça. O certificado digital é um

registro eletrônico que é composto por um grupo de informações que pode diferenciar entidades e associá-las a chaves públicas, sendo assim emitido para inúmeros grupos, como pessoas físicas ou jurídicas, que estão também associados a equipamentos e serviços Web.

A criptografia desempenha um papel fundamental na proteção da confidencialidade e da integridade dos dados, fornecendo uma camada adicional de segurança contra ameaças externas. Ao aplicar técnicas criptográficas adequadas, é possível proteger informações sensíveis e manter a privacidade das comunicações em ambientes digitais.

2.4.4. MANUTENÇÃO DOS EQUIPAMENTOS

No contexto de segurança, para além da ideia de garantir que existam senhas e cópias de segurança, é importante um olhar especial para os equipamentos que serão utilizados pelos usuários dentro da instituição.

Conforme descrito na Cartilha de Segurança da Internet do CERT.br (2012), é importante adotar cuidados específicos em relação aos equipamentos utilizados. Alguns desses cuidados incluem:

Tabela 2 – Segurança dos equipamentos (Cartilha de Segurança na Internet)

Ações de prevenção	Descrição
Atualização do sistema operacional	Manter o sistema operacional atualizado é fundamental para garantir que possíveis falhas e vulnerabilidades de versões anteriores sejam corrigidas
Uso de programas originais	Ao instalar programas em computadores, é importante utilizar versões originais. Isso se deve ao fato de que, ao executar o código de um programa, é possível que partes desse código tenham funções programadas para atacar o dispositivo. A utilização de programas originais minimiza o risco de instalação de software malicioso ou modificado
Cuidado ao manipular arquivos e links	É importante ter em mente que os malwares entram nos computadores através de interações entre usuários e arquivos ou links que possuem infecções. Por isso o cuidado ao clicar em links ou executar arquivos suspeitos deve ser evitado
Administração de senhas e usuários	Devem ser verificados os acessos aos equipamentos por meio de senhas e usuários determinados pelas políticas da empresa para que exista um filtro do que foi acessado dependendo do nível dos usuários
Utilização de mecanismos de	Uso de antimalwares, antispans, firewalls, ferramentas que

Ações de prevenção	Descrição
segurança	bloqueiam propagandas em sites, como o Adblock, entre outros, são uma forma de mitigar a aparição de programas maliciosos no computador

Esses cuidados visam proteger os equipamentos contra potenciais ameaças, mantendo a integridade do sistema e evitando a exploração de vulnerabilidades. Ao adotar as práticas citadas, é possível reduzir os riscos de comprometimento da segurança e garantir um ambiente mais seguro para a utilização dos equipamentos.

2.4.5. TREINAMENTO DOS FUNCIONÁRIOS

Em A arte de enganar, Mitnick (2003) diz que o principal trunfo do engenheiro social é sua habilidade de usar a culpa e a empatia dos outros ao seu favor, destacando que, ao ser iniciante, um funcionário tende a ser mais manipulado pela simpatia das pessoas que pedem algum tipo de ajuda. Entretanto, em circunstâncias onde uma pessoa já possua experiência, isso também pode acontecer, já que os engenheiros sociais são astutos e causam inúmeras situações que possam usar a seu favor e conseguir informações importantes.

É necessário que na criação das regras de políticas internas da instituição seja levado em consideração algo muito além dos equipamentos, que tenham em vista a qualificação dos funcionários. As regras podem envolver acesso de estranhos desacompanhados aos ambientes internos, o que pode ou não ser dito para pessoas que buscam alguma informação e ainda sobre o posicionamento de equipamentos na busca de evitar a visibilidade das telas dos computadores, uso de redes públicas de wifi, entre outros.

Se torna importante portanto, um treinamento que passe pelos conceitos cibersegurança onde serão abordados: Informações sobre malwares, mostrando ameaças que podem acontecer no ambiente de trabalho; explicar como a engenharia social tem um papel importante nos golpes aplicados em alguns ambientes corporativos e instituições; ensinando também em como usar corretamente os dispositivos de redes e por fim, fornecer atualizações contínuas de treinamento para que essas pessoas possam lidar com os problemas que envolvem a segurança da informação.

2.5. LEGISLAÇÕES

Nesta subseção, serão trazidas as legislações que garantem a segurança dos dados e os direitos das crianças e adolescentes. Serão abordadas: A Lei Geral de Proteção de Dados, Estatuto da criança e do adolescente e a ISO 27000.

2.5.1. LEI GERAL DE PROTEÇÃO DE DADOS

Segundo Botelho(2020), a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, foi uma lei brasileira criada com a intenção de proteger e assegurar a integridade dos dados nos meios físicos e digitais de pessoas físicas. A LGPD tem como objetivo estabelecer que dados pessoais são qualquer informação relacionada a uma pessoa natural identificada ou identificável. Por isso, essa legislação define os princípios e diretrizes que devem ser seguidos no tratamento desses dados, visando proteger a privacidade e os direitos dos titulares.

A LGPD trata um dos conceitos fundamentais desta pesquisa, sendo ele o dado sensível. Segundo Pinheiro(2020), dados sensíveis são dados de natureza individual que possua caráter capaz de identificar, localizar um indivíduo, ou ainda que possa descrever de forma detalhada uma situação de saúde, por exemplo.

A legislação LGPD busca assegurar que os métodos indicados pela Cibersegurança, em conformidade com a Tríade CID, sejam respeitados e atendidos. Essa lei foi criada com o objetivo de promover a proteção dos dados pessoais, garantindo que o tratamento dessas informações seja feito de forma adequada e segura. Desse modo, nos ambientes corporativos, é importante destacar que a LGPD estabelece diretrizes para o tratamento de dados pessoais pelas empresas, incluindo a definição de políticas internas e práticas que visem à proteção da privacidade dos indivíduos.

As organizações devem estar cientes das obrigações impostas pela LGPD e implementar medidas para garantir a conformidade. Isso envolve a adoção de políticas e procedimentos claros para o tratamento de dados pessoais, a realização de avaliações de risco e a implementação de medidas de segurança adequadas para proteger essas informações.

2.5.2. ESTATUTO DA CRIANÇA E DO ADOLESCENTE

O Estatuto da Criança e do adolescente (ECA), sancionado em 13 de julho de 1990, foi uma iniciativa de vários órgãos que tem como objetivo assegurar os direitos das crianças e adolescentes no Brasil.

Botelho(2020) ressalta em seu trabalho que instituições públicas e privadas devem cumprir com o direito da criança, fazendo com que suas necessidades sejam atendidas independentemente. Ainda, que o estado deve estabelecer regras que garantam a proteção dos direitos desses indivíduos.

O Estatuto estabelece a responsabilidade compartilhada entre a família, a sociedade e o Estado na proteção dos direitos das crianças e dos adolescentes. Ele enfatiza a importância de políticas públicas voltadas para esses grupos, bem como a participação dos jovens na construção de suas próprias vidas e na sociedade.

O Art. 14. da Lei n° 13.709/2018 (LGPD), traz no seu texto que o tratamento dos dados das crianças e adolescentes devem ser feito respeitando seus direitos, com a autorização de um responsável legal e devem conter características que possam ser entendidas pelas crianças e adolescentes, bem como pelos seus pais ou responsáveis. Dessa forma, as leis conversam para manter os direitos das crianças e adolescentes garantidos quanto a LGPD e a segurança da informação.

2.5.3. ISO 27000

Baldissera(2021) traz que as normas da família ISO/IEC 27000, são responsáveis por padronizar o funcionamento do Sistema de Gestão de Segurança da Informação. Como já foi dito nesta fundamentação, a segurança da informação vai além dos dados eletrônicos, sendo assim, as normas ISO/IEC 27000 são uma garantia no funcionamento da disponibilidade, integridade e disponibilidade de todos os tipos de dados pertencentes a um indivíduo que estejam armazenados em qualquer meio.

Baldissera(2021), também diz que a série ISO 27000 é um conjunto de 45 normas que pertencem ou são seguidas por vários países. Entre essas normas, destaca-se a ISO 27701, que é a certificação mais recente e está relacionada à conformidade com a Lei Geral de Proteção de Dados (LGPD) no Brasil.

É relevante enfatizar que a norma ISO 27000 não possui caráter de certificação, mas sim de referência. Ela oferece um conjunto de termos e definições comuns utilizados no contexto da segurança da informação, contribuindo para a compreensão e aplicação adequada dos padrões de segurança em diferentes organizações.

3. PROCEDIMENTOS METODOLÓGICOS

Neste capítulo são apresentados os procedimentos metodológicos utilizados para a realização da pesquisa. Portanto, são abordados os seguintes tópicos: caracterização da pesquisa, critérios de seleção de público-alvo, etapas da pesquisa e instrumento de coleta de dados.

3.1. CARACTERIZAÇÃO DA PESQUISA

Esta pesquisa foi conduzida com o objetivo principal de compreender como ocorre a proteção de dados dos estudantes nas escolas municipais da cidade de Valença. Para alcançar essa compreensão, optou-se por uma abordagem qualitativa, que, de acordo com Prodanov (2013), envolve a coleta de dados e a interpretação de fenômenos cotidianos, atribuindo significados aos mesmos.

O estudo busca, de forma descritiva, expor as características da população acadêmica da cidade, analisando como esse grupo lida com os dados dos estudantes e como busca garantir a segurança das informações contidas nos documentos arquivados nas instituições. Além disso, o estudo também aborda a qualificação adequada dos atores envolvidos nesse processo, visando compreender as práticas adotadas e identificar possíveis lacunas ou áreas de melhoria relacionadas à proteção de dados.

3.2. CRITÉRIOS DE SELEÇÃO DO PÚBLICO-ALVO

Ao executar a busca pelo público-alvo desta pesquisa, foi necessário entrar em contato com o Departamento de Tecnologia da Informação (DTI) de Valença, já que era necessário estabelecer critérios para a seleção das escolas que seriam entrevistadas. No processo de entrevista com o gestor do departamento, foi possível identificar a criação de um sistema de gestão acadêmica e saber sobre sua implementação.

O sistema consiste em uma ferramenta que possibilita a criação de cadastros, roteamento de estudantes entre escolas e armazenamento de todos os documentos pessoais e dados sensíveis desses estudantes ingressos e, ainda, promove o arquivamento dos documentos dos egressos. Esse sistema atualmente se encontra presente e implementado em todas as 137 escolas do município, porém por questões de adaptação dos funcionários ou

ainda por falta de equipamentos que possam contribuir efetivamente para seu uso contínuo, ele está em fases diferentes de implantação.

Usando os diferentes níveis de implantação, foi possível definir quais escolas seriam utilizadas como fonte de pesquisa. Foi levantado durante a entrevista com o gestor de DTI, que existem três níveis de implantação.

Nível 1 - Escolas que possuem o sistema, entretanto nem todos os funcionários utilizam, pois falta qualificação suficiente para o uso ou não possuem equipamentos disponíveis para sua utilização;

Nível 2 - Onde os funcionários já utilizam, porém ainda existem algumas ressalvas sobre a utilização, ou dificuldade na obtenção de equipamentos;

Nível 3 - Onde os funcionários possuem equipamentos e utilizam contínua da ferramenta.

Dadas essas informações, a seleção foi definida como um gestor de escolas em cada um dos níveis, levando em consideração limitantes como tempo e disponibilidade dos entrevistados.

3.3. ETAPAS DA PESQUISA

O trabalho foi desenvolvido sendo organizado em três etapas:

1. Definição do escopo da pesquisa;
2. Elaboração dos meios de coleta de dados;
3. Análise dos dados adquiridos;

Durante a primeira etapa da pesquisa, foram realizadas análises e levantamentos de informações técnicas relevantes para embasar a formulação do problema de pesquisa e dos objetivos do estudo. Essa etapa demandou aproximadamente três meses para sua conclusão e foi essencial para a estruturação de todo o desenvolvimento da pesquisa.

Na segunda etapa, foi conduzida uma conversa inicial com o gestor do DTI da prefeitura. Essa conversa teve grande importância, pois permitiu obter uma visão geral sobre como a gestão do município encara as necessidades de armazenamento de informações pessoais dos estudantes e quais medidas são adotadas para mitigar possíveis problemas nessa área.

Essas etapas iniciais proporcionaram a base necessária para direcionar o estudo e estabelecer um panorama da situação da proteção de dados e cibersegurança nas escolas municipais de Valença. A partir dessas informações, foi possível avançar desenvolvendo formulários e roteiros de entrevistas, bem como sua aplicação.

Na terceira etapa, realizou-se uma análise dos dados coletados nas entrevistas, a fim de obter uma compreensão mais aprofundada da proteção de dados e cibersegurança nas escolas. Nessa etapa, os dados foram organizados, categorizados e interpretados, utilizando-se métodos adequados de análise qualitativa.

Com base nessa análise, foi possível avançar mais, e esse avanço envolveu a discussão e interpretação dos resultados, a fim de responder ao problema de pesquisa e alcançar os objetivos estabelecidos.

3.4. INSTRUMENTOS DE COLETA

Para a obtenção dos dados, foram feitas entrevistas estruturadas e semi estruturadas, consistindo em perguntas em dois formulários disponibilizados na ferramenta Google Forms, anexados a essa monografia, e também com perguntas abertas objetivando saber mais sobre as dinâmicas individuais dos ambientes de trabalho.

Com a realização das entrevistas, buscou-se identificar como é feito o armazenamento dos dados estudantis, como eles são acessados e principalmente quem são os agentes que são responsáveis pela manutenção e manipulação dessas informações. Também foi parte da investigação, compreender a qualificação acerca de conceitos de Segurança da informação dentro da instituição pelos funcionários.

As entrevistas foram conduzidas de forma presencial e por telefone, permitindo que os participantes compartilhassem informações sobre as dinâmicas internas de segurança nas escolas municipais da cidade. Antes do início das entrevistas, os participantes receberam e tiveram acesso ao termo de consentimento, no qual foram informados sobre os objetivos da pesquisa, os procedimentos envolvidos e seus direitos como participantes. Esse termo de consentimento assegurou que os participantes estavam cientes e concordavam voluntariamente em participar da pesquisa, garantindo assim a ética e a confidencialidade dos dados coletados.

Durante as entrevistas, foram abordados conceitos relacionados à proteção de dados, conforme apresentados no formulário de entrevista. Cada entrevista teve uma duração média

de uma hora contínua, desde o início da intervenção até a conclusão. Essas abordagens variadas de coleta de dados permitiram obter uma visão mais abrangente e aprofundada da proteção de dados nas escolas municipais.

Como dificuldades encontradas durante a pesquisa, destacam-se a indisponibilidade de alguns profissionais das escolas contatadas, o que dificultou a realização das entrevistas planejadas. Além disso, um processo de parada de aulas em determinado período impactou a disponibilidade e disposição dos diretores para participarem das entrevistas. Também foi observada a dificuldade de conciliar agendas e encontrar horários adequados para a realização das entrevistas em campo, devido às demandas e restrições de tempo do entrevistador. Essas dificuldades foram superadas por meio de flexibilidade na programação das entrevistas e busca de alternativas de comunicação, como entrevistas por telefone, visando obter as informações necessárias para a pesquisa.

4. ANÁLISE DOS RESULTADOS

Neste capítulo, serão apresentados os resultados e a análise realizada com base nas entrevistas conduzidas. Serão, portanto, apresentadas as respostas e informações fornecidas pelos entrevistados em relação aos temas abordados na pesquisa.

Com o objetivo de geral, essa pesquisa buscou compreender como se dá a proteção de dados dos alunos da escola de Valença, por isso foram guiadas entrevistas com setores que desempenham funções de controle de dados e implementação de ferramentas dentro do contexto acadêmico municipal. Foram feitas entrevistas com um grupo de três gestores de escolas e com o gestor do DTI da cidade.

Para as entrevistas com a gestão acadêmica, foram respondidas 29 questões ligadas à estrutura, à qualificação dos funcionários, bem como, às políticas internas que são empregadas dentro da instituição (ANEXO II). Para a entrevista com o DTI, foram respondidas 18 questões referentes à visão geral acadêmica do município, como funciona a disponibilidade de equipamentos e qualificação profissional fornecida pela prefeitura para uso e manutenção dessas máquinas (ANEXO I).

4.1. Entrevista com Departamento de Tecnologia da Informação

Foi realizado um encontro com o diretor do DTI a fim de obter informações relevantes sobre a integração entre as escolas municipais e o departamento. A entrevista foi conduzida de forma semi-estruturada, o que permitiu uma abordagem abrangente dos tópicos relacionados à segurança da informação.

Durante a entrevista, foram exploradas questões relacionadas ao conhecimento do corpo acadêmico sobre Segurança da Informação. O objetivo foi investigar o nível de conscientização dos professores, funcionários e estudantes em relação às práticas de segurança e proteção de dados. Foram abordados temas como a importância da proteção dos dados dos estudantes, a necessidade de manter informações confidenciais em segurança e os possíveis riscos associados à exposição de dados sensíveis.

Além disso, foram realizadas perguntas sobre o armazenamento dos dados dos estudantes ingressos e egressos. Essas questões visavam obter informações sobre a existência de políticas de segurança no ambiente acadêmico, o uso de sistemas de armazenamento seguro e as medidas de proteção contra acessos não autorizados.

Através da entrevista, foi explorada a existência e o estágio de implementação de um sistema de gestão acadêmica no município. Foram investigadas informações sobre a integração desse sistema com as escolas e o progresso da implantação nas 137 escolas municipais. Logo, foi possível obter informações relevantes sobre a integração entre as escolas e o departamento de Tecnologia da Informação.

Entende-se, portanto, que a implementação de um sistema de gestão acadêmica está em curso, com integração paralela em todas as 137 escolas, todas em diferentes fases de implantação. Essas informações obtidas foram importantes para a compreensão do cenário atual de proteção de dados nas escolas municipais, bem como para subsidiar a análise dos métodos utilizados atualmente e por fim, definir os próximos atores entrevistados.

Foi observado que, as situações de nivelamento em relação a implementação do sistema são referentes às dificuldades que estão ligadas aos déficits estruturais e de acordo com a familiaridade e ao domínio das tecnologias por parte dos docentes e funcionários. Embora tenha havido tentativas de aquisição de novos equipamentos e a tentativa de fornecer treinamento para toda a população acadêmica, vale lembrar a quantidade de escolas e as necessidades paralelas que contribuíram para o atraso dessas aquisições. Dessa forma, quando

usamos parâmetros para a escolha das escolas, foi possível encarar que independentemente da quantidade de escolas visitadas em um nível, os problemas enfrentados seriam iguais.

Quanto ao sistema, foi perguntado sobre a frequência de backup dos dados, de como funciona o armazenamento dessas informações e sobre o controle do acesso aos dados. Foi informado que o sistema foi desenvolvido por uma empresa terceirizada que é responsável pela segurança dos dados, seguindo as políticas de privacidade e segurança do município. O armazenamento é feito em nuvem e quando o controle de acesso, o público que utiliza o sistema dentro das instituições são: professores, diretores, coordenadores, estudantes, pais e secretários. Para o controle da estrutura e inserção de dados de estudantes egressos, o DTI ficou responsável, existindo assim dentro do setor usuários com o maior nível de acesso com o intuito de exercer essas funções.

Em relação a estrutura que foge ao uso do sistema, foi questionado sobre manutenções das ferramentas e instalações de sistemas de segurança, entre outros. Segundo o gestor, o sistema de segurança não é mantido em todos os prédios, porém a manutenção de todas as ferramentas de tecnologias passam por manutenções frequentes.

4.2. Entrevista com Gestores das escolas

Na entrevista com os gestores acadêmicos, as perguntas giraram em torno de compreender como são armazenados os dados dos alunos, quem teria acesso a esses dados, qual a qualificação dessas pessoas, quais são os dados sensíveis compartilhados nas escolas e quais os mecanismos de proteção de dados ali presentes.

A primeira parte do questionário que foi utilizado como roteiro da entrevista, teve como foco a instituição, com perguntas que foram de quem tem acesso aos dados até equipamentos que estão presentes, como são utilizados e como é feita a sua manutenção.

Em todos os ambientes pesquisados, foi possível observar que apenas um grupo seleto de pessoas possuíam acesso a esses dados, e entre esses, existe um nivelamento de permissão, como por exemplo, professores não podem entrar em salas onde estão arquivados os documentos que possuem dados sensíveis dos estudantes. É uma medida de segurança instaurada pelos gestores para diminuir a falha de segurança dos dados.

A maioria dos documentos e arquivos ainda estão armazenados em formato físico, como papéis e pastas, devido aos desafios enfrentados no processo de digitalização. Esses

desafios incluem a falta de equipamentos adequados em alguns ambientes e a escassez de profissionais qualificados para lidar com a integração dos sistemas.

Também foi questionado a utilização do sistema acadêmico desenvolvido pela prefeitura e os gestores trouxeram pontos positivos e negativos nas suas falas. Dentro de um contexto de adaptação, apesar da criação de um curso de qualificação para uso do sistema, muitos ainda possuem ressalvas para sua utilização, principalmente entre os professores, que precisam fazer a utilização diária dessa ferramenta. Profissionais com mais antigos alegam dificuldade de se adaptar ao novo método e preferem os métodos tradicionais. Já outros, concordam que o sistema trouxe benefícios significativos para a instituição e acreditam que após a implementação completa, nos casos onde isso ainda não ocorreu, os funcionários irão poder ter maior flexibilidade em procedimentos, antes complexos, como fazer matrículas e transferências, facilitando muito o seu trabalho.

Apesar de algumas instruções serem levadas em consideração, quanto a não entrada de estranhos na instituição, ou restrições em áreas que possuem documentação acadêmica, não existem regras de conhecimento geral para os funcionários, isto é, não existem políticas de segurança de dados. Ademais, foi relatado que não existiu nenhum tipo de qualificação referente a Segurança da informação ou a Legislações que possuem o propósito de garantir a segurança dos dados, em alguns casos, inclusive, não existia nem conhecimento do que se tratava a Lei Geral de Proteção de Dados (LGPD).

Ao serem questionados sobre os equipamentos existentes, existiu uma dificuldade de identificação da existência de antimalwares instalados ou sobre a existência de backups, sendo presente apenas o uso de senhas nos computadores como um mecanismo de segurança. O uso de câmeras é praticamente inexistente e o seu uso não viola práticas de segurança da informação, não estando direcionados para computadores ou ambientes de arquivamento.

Dentre as informações obtidas, a falta de conhecimento sobre os conceitos de segurança da informação em ambientes escolares foi o que causou mais preocupação, visto que durante a conversa, entrevistados compreenderam a importância de adesão a regras de segurança que poderiam ter sido pensadas a partir de uma qualificação básica. Foram relatados ainda algumas situações onde a remoção de documentos dos arquivos precisaram ser feitas para garantir que pessoas com segundas intenções não tivessem acesso a essas informações com o uso de engenharia social. Por fim, ainda foi questionado sobre as redes sociais e sobre o consentimento dos pais e responsáveis sobre a publicação de fotos e vídeos

dos estudantes, nesses casos, na matrícula existe um termo de consentimento que deve ser assinado pelos pais permitindo as publicações.

4.3. ANÁLISE DOS DADOS

Segundo Fonte(2012), a Segurança da Informação é um conjunto de políticas, procedimentos, estruturas organizacionais e funções que envolvem hardware e softwares que são implementados em função do objetivo de garantir a integridade, confidencialidade e disponibilidade dos dados.

Após a análise dos questionamentos respondidos, é possível observar a forma como os dados são armazenados, manipulados e protegidos dentro da instituição. Embora nem sempre sejam utilizadas técnicas de segurança da informação atualizadas, é evidente que tanto a prefeitura quanto os funcionários das instituições estão se esforçando para garantir a segurança dos dados dos estudantes.

Fica claro que as estratégias de armazenamento e proteção dos dados dos estudantes possuem ainda algumas lacunas importantes a serem preenchidas. Spanceski(2004) enfatiza no seu estudo que, todas as instituições sofrem ameaças, mas que com a aplicação de condutas de segurança, é possível diminuir a possibilidade de que essas ameaças se tornem um ataque real.

Embora o armazenamento seja feito de forma a sanar algumas questões de ataques, isso não significa que os documentos estejam livres de danos físicos, já que não possuem uma cópia de segurança, por exemplo, algo que exigiria bastante trabalho e tempo. Como Fialho Jr.(2007), busca trazer em sua discussão os incidentes que podem acontecer com a disposição indevida de backups.

5. CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Neste capítulo serão apresentadas as conclusões e as recomendações para a continuidade de futuras pesquisas nesta área de estudo.

5.1. CONSIDERAÇÕES FINAIS

Essa pesquisa buscou compreender como se dá a proteção dos dados nas escolas públicas da cidade de Valença, e apesar de com níveis diferentes, foi interessante perceber a relevância que vêm sido dada a essa questão. A prefeitura tem buscado implementar, de forma permanente, uma ferramenta que tem a intenção de diminuir a falta de segurança dos arquivos

físicos, seja por tentativas de uso indevido dos dados, como por falta de manutenção adequada.

É importante salientar que iniciativas de prevenção de ataques, como treinamentos adequados, criações de políticas internas da instituição e ainda maior proteção dos equipamentos, têm como objetivo mitigar déficits na segurança, que futuramente podem ser muito graves.

Vale lembrar do que Mitnick(2003) quer trazer quando ele enfatiza que um atacante sempre começa por informações que podem parecer irrelevantes demais para serem protegidos. Portanto, é indispensável que as instituições estejam constantemente vigilantes em relação à proteção dessas informações, adotando medidas adequadas e atualizadas de segurança da informação para garantir a segurança e a privacidade dos dados dos seus proprietários.

No contexto atual, em que a tecnologia desempenha um papel fundamental nas instituições de ensino, é fundamental que os gestores, professores e demais envolvidos estejam conscientes dos riscos relacionados à segurança da informação e adotem medidas adequadas para proteger os dados dos estudantes. A pesquisa ressalta a importância de investimentos em recursos tecnológicos, capacitação dos profissionais e adoção de práticas de segurança efetivas para garantir a proteção dos dados e a privacidade dos estudantes.

5.2. TRABALHOS FUTUROS

Conforme mencionado durante o trabalho, houve dificuldades na realização das entrevistas devido à falta de disponibilidade de tempo e de profissionais dispostos a participar.

A implementação em andamento proporcionou uma visão geral do funcionamento atual, com todas as dificuldades e processos de adaptação existentes. Portanto, é recomendado realizar uma nova série de entrevistas para validar a adaptação dos funcionários ao sistema, abrangendo um maior número de escolas, a fim de obter uma visão mais abrangente da situação.

Por fim, sugere-se também uma intervenção como a criação de uma cartilha de cibersegurança para os funcionários, apontando questões relacionadas a políticas de segurança dentro dos setores, regras e medidas que são capazes de implementar nos ambientes escolares.

REFERÊNCIAS

ALMEIDA, Marcus; ROSA, Priscila. Internet, Intranet e Redes corporativas. Rio de Janeiro: Brasport, 2000.

MITNICK, Kevin D., SIMON, William L. A arte de enganar. 2002; Versão brasileira da Editora Pearson Education do Brasil Ltda, 2003.

VANGLLER, Thompson. Técnicas de invasão. Londres: 2017.
BR, C.E.R.T. Cartilha de segurança para Internet. 2008. Disponível: http://cartilha.cert.br. Acesso em: 19 de maio de 2023.

SOUSA, Flávio RC; MOREIRA, Leonardo O.; MACHADO, Javam C. Computação em nuvem: Conceitos, tecnologias, aplicações e desafios. II Escola Regional de Computação Ceará, Maranhão e Piauí (ERCEMAPI), p. 150-175, 2009.

CERT.br "Incidentes Notificados ao CERT.br". Disponível em: https://stats.cert.br/incidentes/. Abril/2023. Acesso: 01 de junho de 2023.

DE MENDONÇA, Júlia Fernandes. A responsabilidade civil e penal dos envolvidos em sequestros digitais em face da legislação brasileira de proteção de dados pessoais. Revista do CEPEJ, n. 22, p. 156-173, 2020.

FIALHO JR, Mozart. Guia essencial do backup. Universo dos Livros Editora, 2007.

MORAES, Eliana Márcia. Planejamento de backup de dados. 2007.

TERADA, Routo. Segurança de dados: criptografia em rede de computador. Editora Blucher, 2008.

SPANCESKI, Francini Reitz. Política de segurança da informação–Desenvolvimento de um modelo voltado para instituições de ensino. Monografia do Trabalho de Conclusão de Curso em Sistemas de Informação, 2004.

PRODANOV, Cleber Cristiano; DE FREITAS, Ernani Cesar. Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição. Editora Feevale, 2013.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. Revista Direitos Sociais e Políticas Públicas–Unifafibe, v. 8, n. 2, p. 18, 2020.

GARCIA, Lara Rocha et al. Lei Geral de Proteção de Dados (LGPD): guia de implantação. Editora Blucher, 2020.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018-LGPD. Saraiva Educação SA, 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 01 de julho de 2023.

BALDISSERA, Olívia. ISO 27000: tudo o que você precisa saber para se destacar na segurança da informação, [2021]. Disponível em: https://posdigital.pucpr.br/blog/iso-27000#iso-27000. Acesso em: 01 de julho de 2023.

FONTES, Edison. Praticando a segurança da informação. Brasport, 2008.

FERREIRA, Haroldo. Cibersegurança. Editora Senac São Paulo, 2021.

ANEXOS

Anexo I - QUESTIONÁRIO APLICADO PARA A PREFEITURA

1) Quantas instituições atualmente possuem o sistema acadêmico implementado?
2) Existem restrições de acesso ao sistema acadêmico na utilização de equipamentos pessoais?
    a) sim
    b) não
3) O que o sistema acadêmico abrange no armazenamento dos dados dos estudantes?
    a) Cópia da documentação
    b) Dados relacionados a saúde do estudante
    c) Dados acadêmicos
    d) Diários
    e) Documento dos responsáveis
    f) Dados financeiros
    g) Outros
4) Em quantos por cento das escolas já foi feita a implementação do sistema acadêmico do município?
5) Quais são os perfis de usuários que possuem acesso a informações que estão presentes no sistema?
    a) Professores
    b) Servidores
    c) Diretores
    d) Alunos
    e) Coordenadores
    f) Outros
6) Com qual regularidade é feita a manutenção efetiva dos computadores nas escolas do município?
    a) Nunca
    b) Raramente
    c) Frequentemente
7) Existe um mapeamento dos equipamentos existentes nas escolas (Computadores, Câmeras de vigilância, equipamento de internet)

a) Sim
b) Não
c) Não possuo conhecimento

8) As salas que existem computadores que são utilizados para armazenamento de dados acadêmicos, possuem câmeras de segurança?
   a) Sim
   b) Não
9) Se possuía câmeras, o posicionamento das câmeras foi pensado para que pudesse evitar o acesso visual do que é digitado ou visualizado na tela de computadores da instituição?
   a) Sim
   b) Não
   c) Em alguns casos
   d) Não se aplica
10) Os computadores disponibilizados para as instituições possuem antivírus?
   a) Sim
   b) Não
   c) Em alguns casos
   d) Não se aplica
11) Como é feito o armazenamento dos dados cadastrados no sistema?
12) Existem rotinas de backups dos dados no sistema implementado?
   a) Sim
   b) Não
   c) Em alguns casos
   d) Não se aplica
13) Se sim, onde o backup é armazenado?
   a) Armazenamento em nuvem
   b) Armazenamento interno
   c) Não se aplica
14) A equipe recebeu alguma qualificação de Cibersegurança?
   a) Sim
   b) Não
   c) Em alguns casos
   d) Não se aplica

15) A equipe recebeu alguma qualificação de LGPD?
    a) Sim
    b) Não
    c) Em alguns casos
    d) Não se aplica
16) Quais as estratégias são garantidas pela prefeitura para assegurar que os dados sejam protegidos dentro de um contexto da Cibersegurança?
    a) Câmeras de vigilância
    b) Armários com chave
    c) Uso de senhas nos computadores
    d) Diferentes acessos de usuário
    e) Treinamento da equipe
    f) Controle dos horários de login
17) Existem normas estabelecidas pela prefeitura para a utilização dos dados dos alunos?
    a) Sim
    b) Não
18) Se sim, os servidores responsáveis conhecem e praticam essas normas?
    a) Sim
    b) Não
    c) Não se aplica

Anexo II - QUESTIONÁRIO APLICADO PARA OS GESTORES DAS ESCOLAS

1) Quais funcionários têm acesso aos dados pessoais dos alunos?
    a) Secretários
    b) Diretores
    c) Vice-diretores
    d) Professores
    e) Coordenadores
    f) Auxiliares de limpeza
    g) Porteiros
    h) Merendeiros
    i) Inspetores
2) Quais formatos de armazenamentos utilizados na instituição?
    a) Arquivos físicos (Papéis e pastas)
    b) Computadores da instituição
    c) Computadores pessoais dos funcionários
    d) Computação em nuvem (Dropbox, AWS, Google)
    e) Sistema de gestão acadêmica
3) Como se dá o acesso aos dados dos estudantes?
    a) Computadores pessoais
    b) Equipamentos fornecidos pela prefeitura (Como tablets, notebooks)
    c) Arquivos físicos (Papéis e Pastas)
    d) Computadores da instituição
    e) Não se aplica
4) Caso o sistema acadêmico tenha sido implementado, quais informações ainda persistem fora do sistema?
    a) Cópia da documentação
    b) Atestados médicos
    c) Relatórios acadêmicos
    d) Diários
    e) Não se aplica
5) Ainda caso o sistema acadêmico tenha sido implementado, quantos por cento foi implementado, na sua opinião?

6) Quais dos elementos abaixo fazem parte da rotina de armazenamento e preservação dos arquivos físicos guardados na instituição?
    a) Ambiente com boa circulação de ar
    b) Limpeza adequada
    c) Seleção utilizando alguma regra de arquivamento (Ordem alfabética, Ordem de ano de matricula)
    d) Ambiente com fechadura
    e) Ambiente com sistema de monitoramento
7) No uso dos computadores, é comum que as telas fiquem visíveis para pessoas além daquelas que estão utilizando?
    a) Sim
    b) Não
    c) Não se aplica
8) As salas que existem computadores que são utilizados para armazenamento de dados acadêmicos, possuem câmeras de segurança?
    a) Sim
    b) Não
    c) Alguns ambientes
9) Se possua câmeras, o posicionamento das câmeras pode favorecer o acesso visual do que é digitado ou visualizado na tela de computadores da instituição?
    a) Sim
    b) Não
    c) Em alguns casos
    d) Não se aplica
10) Os computadores possuem antivírus?
    a) Sim
    b) Não
    c) Em alguns casos
    d) Não se aplica
11) Além de computadores, em quais outros equipamentos os funcionários, cujo acesso é permitido, podem acessar informações dos alunos?
12) Existem rotinas de backups dos dados?
    a) Sim
    b) Não

c) Em alguns casos
d) Não se aplica

13) A equipe recebeu alguma qualificação de Cibersegurança?
a) Sim
b) Não
c) Parte da equipe

14) A equipe recebeu alguma qualificação de LGPD?
a) Sim
b) Não
c) Parte da equipe

15) Quem tem acesso a áreas reservadas para a documentação acadêmica dos discentes?
a) Secretários
b) Diretores
c) Vice-diretores
d) Professores
e) Coordenadores
f) Auxiliares de limpeza
g) Porteiros
h) Merendeiros
i) Inspetores

16) Quais as estratégias para garantir que os dados sejam protegidos dentro de um contexto da cibersegurança?
a) Câmeras de vigilância
b) Armários com chave
c) Uso de senhas nos computadores
d) Diferentes acessos de usuário
e) Treinamento da equipe
f) Controle dos horários de login

17) A instituição possui redes sociais onde postam imagens dos estudantes?
a) Sim
b) Não

18) Existiu em algum momento alguma documentação de consentimento para que as imagens fossem divulgadas em alguma rede social?
a) Sim

b) Não
c) Não se aplica

19) Existem normas estabelecidas pela instituição para a utilização dos dados dos alunos?
a) Sim
b) Não

20) Se sim, os servidores responsáveis conhecem e praticam essas normas?
a) Sim
b) Não
c) Não se aplica

21) Existem procedimentos em caso de violação de dados ou incidentes de segurança?
a) Sim
b) Não

22) Como a escola garante o consentimento adequado dos pais ou responsáveis para coletar e processar os dados dos alunos, de acordo com as exigências da LGPD?

23) Em caso de incidente de segurança cibernética, como são comunicados e gerenciados os incidentes?

24) Existe um processo de revisão e atualização das políticas e práticas de segurança de dados da escola?
a) Sim
b) Não

25) Existe um encarregado de proteção de dados (DPO) designado na escola para garantir o cumprimento da LGPD?
a) Sim
b) Não

26) A escola realiza avaliações de impacto à proteção de dados (DPIA) para identificar e minimizar riscos à privacidade dos alunos?
a) Sim
b) Não

27) A escola realiza treinamentos e capacitações regulares para os funcionários sobre a LGPD e as melhores práticas de proteção de dados?
a) Sim
b) Não

28) Quais são os procedimentos estabelecidos para o compartilhamento de dados pessoais dos alunos com terceiros, como fornecedores de serviços ou outras instituições educacionais?
29) A escola mantém registros das atividades de processamento de dados pessoais dos alunos, conforme exigido pela LGPD?