

Segurança Digital: Relato de Experiência sobre Projeto Aplicado em Escola do Ensino Médio na Cidade de Mombaça-CE

Digital Security: Report of Experience on Project Applied in High School in the City of Mombaça-CE

João Charllys Brauwol Araújo
Cavalcante
Graduado em Computação
Universidade Estadual do Ceará -
UECE
Mestrando em Computação
Universidade Federal do Ceará - UFC
charllysbrauwolhaha@gmail.com

Erlanio Freire Barros
Graduado em Análise e
Desenvolvimento de Sistemas
Unileão - Centro Universitário
Mestrando em Computação
Universidade Federal do Ceará - UFC
erlanio.dev@gmail.com

Taís Rodrigues Sandes
Graduanda em Computação
Universidade Estadual do Ceará -
UECE
Fecli - Faculdade de Educação,
Ciências e Letras de Iguatu
Campus Avançado de Mombaça
taissandes@gmail.com

Eudásio Rodrigues de Sousa
Graduado em Computação
Universidade Estadual do Ceará -
UECE
Fecli - Faculdade de Educação,
Ciências e Letras de Iguatu
Campus Avançado de Mombaça
rodrigues0117@gmail.com

José Marcelo de Pinho Moreira
Graduado em Computação
Universidade Estadual do Ceará -
UECE
Fecli - Faculdade de Educação,
Ciências e Letras de Iguatu
Campus Avançado de Mombaça
marcelo.moreira@aluno.uece.br

Edinara Lima de Alencar
Graduada em Computação
Universidade Estadual do Ceará -
UECE
Fecli - Faculdade de Educação,
Ciências e Letras de Iguatu
Campus Avançado de Mombaça
edynaraccb@gmail.com

RESUMO

Este trabalho teve como objetivo avaliar a segurança digital dos estudantes de acordo com o seu comportamento com o uso da tecnologia. Os dados da pesquisa foram obtidos com a aplicação de um questionário com os alunos de uma escola de ensino médio da cidade de Mombaça-CE, onde foram obtidas 111 respostas referente ao questionário que continha 25 perguntas. Foi observado que 69,4% dos entrevistados mantiveram contato com alguém que não conheciam pessoalmente. E que 75,7% deixam a senha salva no próprio aparelho. Através da análise dos dados, o trabalho mostra a importância da conscientização dos alunos sobre os perigos do uso da tecnologia sem os devidos cuidados para se manter seguro no mundo digital.

Palavras-Chave

Segurança Digital; Tecnologias; Comportamento Online.

ABSTRACT

The present work aimed to evaluate the digital security of students according to their behavior with the use of technology. The research data were obtained by applying a questionnaire to the students of a high school in the city of Mombaça-CE, where 111 answers were obtained regarding the questionnaire that contained 25 questions. It was observed that 69.4% of the interviewees kept in touch with someone they did not know personally. And that 75.7% left their

passwords saved on their own devices. Through the analysis of the data, the study shows the importance of making students aware of the dangers of using technology without proper care to keep safe in the digital world.

Keywords

Digital Security; Digital Security; Technologies; Online Behavior.

1. INTRODUÇÃO

A definição de segurança da informação é a prática de proteger fisicamente, através da configuração correta de equipamentos ou por meio de conscientização do usuário para evitar ataques virtuais como vírus, Malware ou Phishing, por exemplo. Esses ataques normalmente possuem o objetivo de acessar informações confidenciais, dados bancários, extorquir dinheiro ou expor a intimidade do usuário. Já o significado de crimes cibernéticos é dado por ações criminosas executadas com o uso da internet, na qual o agente explora falhas de segurança nos meios físicos utilizados para acessar a internet ou uso indevido, negligência ou inabilidade por parte dos usuários [Cavalcante, 2016].

A relevância deste estudo é baseada na quantidade de pessoas incluídas no meio digital, usando vários aparelhos diferentes para acessar a internet e no número crescente de violações, ataques, roubos de dados, invasões de dispositivos, entre outros tipos de golpes que acontecem no mundo digital. Todo usuário conectado à internet está vulnerável a ser uma vítima de cibercriminosos. Com o conhecimento dos dados sobre a rotina online da população em

geral, os pesquisadores podem desenvolver materiais informativos de prevenção ou orientação para que o número de vítimas desses criminosos venha a diminuir.

Um estudo realizado com 7000 pessoas de 14 países expôs que 65% dos entrevistados sofreram algum tipo de crime ou ataque cibernético [Norton, 2010]. Já no Brasil, de acordo com os dados da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD) realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), um percentual de 85,4% das pessoas de 14 a 17 anos utilizam a internet, sendo que 94,6 usam a internet por meio do aparelho celular [IBGE, 2018].

Segundo levantamento da Serasa Experian, somente no mês de fevereiro deste ano 326.290 brasileiros sofreram tentativas de golpes — o equivalente a uma vítima a cada 7 segundos. Em resposta, bancos e instituições financeiras estão investindo em segurança e mecanismos de proteção de usuários contra fraudes e golpes [CNN Brasil, 2022]. No meio digital, investir na segurança dos serviços e aplicações se tornou algo fundamental, a fim de garantir a segurança do usuário, protegendo seus dados contra pessoas mal-intencionadas que se aproveitam de diversas maneiras para aplicar golpes.

O campo digital é um amplo espaço, no qual a pessoa tem que ter o mínimo de conhecimento prévio para manter-se segura e aos seus dados. Para VASCONCELOS [2022], os vazamentos podem acontecer por ataques cibernéticos, como vírus, pessoas mal-intencionadas ou mesmo por falta de conhecimento.

Vazamentos de dados sigilosos, como senhas e números de documentos, fotos e vídeos de cunho íntimo, outras tantas são as possibilidades de problemas decorrentes da falta de informação ou uso impróprio dos aparelhos tecnológicos. Segundo LOPES e IGNACZAK [2021], criminosos utilizam os dados para obter lucros após a venda dos mesmos.

Este estudo foi desenvolvido com o objetivo de coletar dados para avaliar o nível de conhecimento e de segurança digital dos estudantes do ensino médio de uma escola, na cidade de Mombaça/CE. Outras questões estão relacionadas ao contexto familiar e os meios tecnológicos, infraestrutura e equipamentos de acesso, comportamentos online e níveis de segurança nesse meio.

Os resultados deste trabalho indicam alguns problemas encontrados na sociedade, principalmente nos jovens, como o uso sem supervisão e conhecimentos sobre segurança adequados de aparelhos tecnológicos, podendo assim, ocasionar vários transtornos.

O restante desse trabalho está organizado da seguinte forma: na Seção 2 está disposta a fundamentação teórica; na Seção 3, a metodologia; na Seção 4 são expostos os resultados; na Seção 5 a conclusão é apresentada.

2. Fundamentação Teórica

O conteúdo teórico deste trabalho baseia-se na área específica de segurança digital e seus componentes principais, como os perigos que podem ser encontrados no meio digital. Uma subseção também de igual importância é a relação entre a utilização dos meios tecnológicos pelos estudantes e o impacto que isso ocasiona em todo ecossistema escolar.

2.1 Segurança Digital

O conceito de segurança digital, segundo a CISCO é a prática de proteger os sistemas de ataques virtuais, que podem ser direcionados a obtenção de vantagens, extorsão, acesso indevidos a dados sigilosos. Exemplos desses ataques são o Phishing (e-mails fraudulentos), ransomware (software mal-intencionado) e engenharia social (manipulação dos usuários).

De acordo com VIANNA E FERNANDES [2015] esses ataques causam diversos problemas em empresas, como danos de reputação e impactos financeiramente negativos.

Como PIMENTA E QUARESMA [2016] destacam, o usuário é a principal fonte de risco das organizações com seus comportamentos e atitudes. Com a pandemia da COVID-19, problemas com segurança no espaço digital se tornaram mais evidente, sendo preciso medidas de proteção e cibereducação [GUILHERME et al, 2021].

O Marco Civil, aprovado em 2014, foi o início de uma tentativa de jurisdição e penalização dos responsáveis por práticas criminosas no ciberespaço. Ele estabeleceu princípios, garantias, direitos e deveres que os usuários deveriam seguir na internet (LEI Nº 12.960, 2014). Já a Lei Geral de Proteção de Dados, aprovada em 2018, tratava mais da esfera de coleta de dados pessoais pelas empresas, o que fazer com esses dados [LEI Nº 13.709, 2018].

Como PEIXOTO [2020] explica, a exposição em larga escala de dados dos usuários está cada vez mais comum, isso demonstra a fragilidade dos sistemas das empresas responsáveis, além disso, a dificuldade de fiscalização pelos órgãos que deveriam atuar nessa área.

2.2 Impactos das Tecnologias nas Escolas

Para GABRIEL [2013] a tecnologia é vista como sendo uma bênção e um fardo, já que com elas surgem novas possibilidades, são novas ferramentas para o homem utilizar e explorar seus limites. Os aparelhos tecnológicos devem ser integrados na educação e seu uso aperfeiçoado e impulsionado, principalmente no contexto das novas gerações, jovens que estão conectados à internet já nos anos iniciais de vida.

Proibir o uso de aparelhos, como celulares em instituições de ensino é um erro, segundo SILVA et al. [2019], proibir ou restringir o uso de das tecnologias é uma negação da realidade encontrada foram dos muros das escolas. Em contrapartida, utilizar os *smartphones*, por exemplo, para uma educação mais digital pode ser uma saída para que aquele aluno consiga ter um melhor desenvolvimento em sua caminhada acadêmica, como afirma ARAÚJO et al. [2019] que é preciso uma inserção consciente de tecnologia nas escolas.

Outras tantas são as formas de educar através de recursos tecnológicos, como grupos em redes sociais, memes, utilizar as Tecnologias Digitais da Informação e Comunicação – TDICs, entre tantas outras. Para LAUDON E LAUDON [2004], a tecnologia da informação pode ser entendida como um conjunto formado por hardware e software e com finalidade diversas como coletar, processar, armazenar e disseminar informação. Essas TDICs são ferramentas digitais para impulsionar a comunicação e a busca de informação, se usadas da maneira correta em sala de aula. Podemos citar como exemplos mais conhecidos de TDICs os seguintes equipamentos: *smartphones*, computadores, *tabletes*.

O professor precisa de uma formação correta e ampla, para uma correta utilização dos meios tecnológicos disponíveis. SCHUARTZ E SARMENTO [2020] evidenciam que o uso das TDICs modificando todo o processo de ensino e aprendizagem, os professores precisam assim, que em suas formações, esses componentes e formas de aplicá-los em sala estejam inclusos.

Tudo está se transformando no mundo, dominar as novas tecnologias é estar integrado a essas transformações. Muitos são os

recursos disponíveis ao professor que podem ajudar nos processos administrativos e pedagógicos. Mas é preciso antes dominá-los de forma adequada, ocasionando assim a otimização de suas utilizações KALINKE [1999].

3. Metodologia

Este trabalho foi desenvolvido por meio de uma abordagem quantitativa, através de uma pesquisa de campo utilizando a ferramenta online do *Google Forms* para a coleta de dados, mediante formulário contendo vinte e cinco (25) questões fechadas sobre segurança digital, com turmas do primeiro (1º), segundo (2º) e terceiro (3º) ano do ensino médio regular, de uma escola estadual no município de Mombaça – Ceará. O formulário ficou disponível entre os dias vinte (20) e trinta (30) de setembro de 2022, para que os discentes respondessem as questões.

O desenvolvimento do questionário foi feito em etapas consistentes para um melhor resultado. A primeira foi reunir informações sobre o tema a ser pesquisado, levantar várias questões pelos autores, e, após esses passos, selecionar as principais e eliminar as perguntas que não trariam valor ao estudo.

A segunda etapa foi de pré-testes do formulário, designado como formulário teste. Foi disponibilizado esses questionamentos aos integrantes do trabalho e ao professor de uma disciplina do curso de licenciatura em computação da UECE, para após análise, alterar ou excluir questões do formulário.

Ao todo, 111 alunos responderam ao formulário. Os dados coletados foram analisados para um melhor entendimento sobre as questões principais que os autores estavam a procurar.

4. Resultados

Os resultados estão apresentados divididos em subseções de acordo com as suas relações: 4.1 Infraestrutura, 4.2 Relação Familiar, 4.3 Comportamento Online, 4.4 Segurança dos Dados e 4.5 Segurança Online.

4.1 Infraestrutura

O tema infraestrutura aborda aparelhos eletrônicos que os alunos utilizam e tipos de internet disponíveis para acesso, por exemplo, se o acesso acontece por meio de fibra óptica ou utilizando antenas via rádio.

Os discentes foram questionados com relação aos aparelhos que mais utilizam para acessar a internet e ao tipo de internet que possuem para navegarem. De todos os dispositivos listados, 94% (104) responderam que utilizam os smartphones, Figura 1. Nas perguntas 3 do formulário, eles foram indagados se possuíam celular próprio, 94,6% (105) responderam que tinham o aparelho. Já na quarta indagação, com relação ao computador, 82,9% (92) disseram não têm um computador próprio em casa. Já as perguntas 5 tinha relação com o tipo de conexão com a internet, 91% (101) possuem acesso em casa e a 6 o tipo, sendo 56,8% (63) do tipo fibra óptica e 29,7% (33) internet via rádio.

3 - Possui celular próprio?

111 respostas

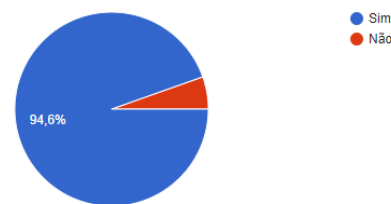


Figura 1. Questão 3.

4.2 Relação Familiar

Nesse grupo encontram-se a relação de uso dos pais dos entrevistados quanto ao acesso à internet e se há participação ativa dos mesmos no conteúdo que os alunos acessam.

O resultado obtido quanto a utilização da internet no dia a dia foram 88,3% (98) para sim. Sobre quais os conteúdos mais frequentemente acessados foram: redes sociais 90,1% (100) e entretenimento 59,5% (66) se destacaram no levantamento de dados. Quanto aos pais acompanharem o conteúdo acessado pelos alunos, Figura 2, nos seus aparelhos eletrônicos 46,8% (52) responderam que não. É notável a grande parcela dos jovens conectados via celulares na atualidade, sendo um objeto de desejo por todos dessa parcela da população. Os pais devem estar atentos para qual fim essa ferramenta está sendo utilizada.

9 - Seus pais verificam ou sabem como vocês estão acessando a internet (redes sociais, conversar online)?

111 respostas

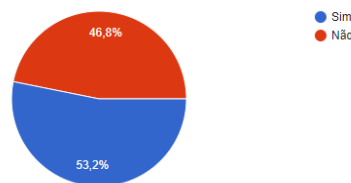


Figura 2. Questão 9.

4.3 Comportamento Online

Os estudantes foram questionados sobre o tempo que utiliza a internet e qual plataforma mais utiliza, para compreender como são seus comportamentos no meio digital.

Os resultados obtidos sobre o tempo gasto na internet com maior porcentagem são que 36% (40) dos alunos ficam online mais de seis (6) horas e 30,6% (34) ficam entre três (3) e seis (6) horas. Já em relação a plataforma que os mesmos mais utilizam são as redes sociais, alcançando um total de 73% (81) dos entrevistados. O público alvo da pesquisa eram jovens do ensino médio, sendo comum que as redes sociais e muitas horas acessando tenham obtido altas porcentagens. Normalmente essas plataformas são as mais utilizadas para socializar e ficar atualizado sobre o cotidiano dos seus grupos sociais.

4.4 Segurança dos Dados

Os itens mais sensíveis foram abordados da pergunta 12 a 22, relacionadas à segurança que emprega ou modo como se comporta online. Um total de 22,5% (25) discentes já forneceram

informações sigilosas (Dados, fotos, vídeos) no meio digital e 21,6% já tiveram problemas com vírus ou contas invadidas. Já relacionado ao vazamento desses dados, 2,7% (3) já teve algum problema. Embora o índice de vazamento de informações ou conteúdos pessoais seja baixo, em relação aos entrevistados, fornecer informações ou mídias particulares por meios de comunicação digital, como *WhatsApp*, gera uma ameaça à privacidade desses jovens.

Tabela 1. Senhas

Questão	Sim	Não
19 - Suas senhas estão salvas no seu aparelho?	75,7%	24,3%
20 - Usa a mesma senha para todas as contas ou redes sociais?	21,6%	78,4%
21 - Usa a autenticação em duas etapas?	48,6%	51,4%

Quando o contexto é o relacionamento com pessoas que conheceram de forma online, 69,4% (77) afirmou que mantiveram contato com alguém que não conhecia pessoalmente e 9,9% (11) compartilharam dados sigilosos com tais pessoas, sendo que 45,9% (51) já se encontrou com essas pessoas. Esse grupo de perguntas em especial é um alerta para o comportamento desses alunos, já que conversar com quem nunca conheceu pessoalmente ou se encontrar com tais pessoas, eleva o nível de preocupação relacionada à segurança física do estudante.

17 - Já se encontrou pessoalmente com pessoas que conheceu pela internet
111 respostas

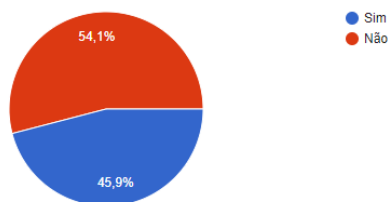


Figura 3. Questão 17.

Nas questões sobre senhas que os estudantes utilizam, 44,1% (49) disseram que eram curtas (somente números ou letras), 75,7% (84) deixam a senha salvas nos aparelhos, 78,4% (87) não utilizam a mesma senha para todas as contas, 51,4% (57) não usam autenticação em duas etapas e, ainda, 58,6% (65) afirmaram que nunca trocaram as suas senhas. Essas porcentagens são um retrato da privação do conhecimento sobre o ambiente digital e seus perigos inerentes. Com uma segurança de suas contas fraca, apontada pela pesquisa, os dados ficam expostos a inúmeros riscos, desde chantagens, vazamentos, uso indevido, entre outros.

4.5 Segurança Online

As duas últimas perguntas do questionário foram sobre a sensação de segurança no meio digital ou falta dela. Um total de 73% (81) afirmaram que se sentem seguros quando estão online e, numa escala de 0 a 10, onde 0 significa muito inseguro e 10 muito seguro, 44,1% escolheram entre 8 e 10 na referida escala. Poucas pessoas possuem de fato algum conhecimento concreto relacionado à segurança dos seus dados ou como mantê-los seguros enquanto estão utilizando a internet. Tendo esses fatos como base para análise do subtópico apresentado, essa falsa sensação de segurança encontrada é justificável.

5. Conclusão

A segurança dos dados dos usuários é uma preocupação recorrente entre as várias plataformas online, como bancos, redes sociais entre outras. Ter conhecimento sobre como os jovens, que estão cada vez mais precocemente conectados, tem uma importância ímpar no desenvolvimento do discente, tanto no ambiente escolar como no pessoal.

O objetivo principal desse trabalho foi avaliar a segurança digital dos alunos do ensino médio daquela instituição. Com os dados coletados e analisados, esse objetivo foi alcançado.

As características de uso que causam uma maior preocupação quanto a segurança desses jovens é a utilização dos aparelhos sem o devido cuidados com seus dados e suas senhas, a falsa sensação de segurança na internet, o convívio com pessoas no meio online sem a devida cautela, além é claro, do acesso irrestrito e sem a supervisão adequada pelos pais ou responsáveis.

Os responsáveis desses alunos devem ter uma atenção maior referente ao meio digital, seus dependentes muitas vezes conversam ou enviam dados sigilosos, fotos ou documentos, sem que ao menos eles saibam do risco que isso pode ser.

O acesso a sites e aplicativos de índole duvidosa, que muitas vezes coletam seus metadados para revenda de informações ou dispor tais para usos em atividades ilícitas, também proporciona um receio quanto a prudência desses jovens. Muitos dizem se sentir seguros, mas, os mesmos não tomam o devido cuidado com as suas senhas, ou mesmo, navegam em sites não confiáveis. Esse fato é muito mais perigoso, já que eles se acham seguros, mas não possuem os cuidados necessários com tal.

Como opções de intervenções e trabalhos futuros: o desenvolvimento de palestras para todos os alunos da instituição de ensino em que o formulário foi aplicado. Nessa palestra é possível abordar os principais pontos que foram observados e que geram preocupação com relação a segurança dos dados dos discentes. Logo após seria sensato aplicar um outro formulário com o objetivo de analisar as mudanças que os alunos podem ter em relação ao modo como se comportam e gerenciam sua segurança quando estão online.

6. REFERÊNCIAS

- ARAÚJO, Allyson Carvalho; et al. Aproximações da formação continuada em Educação Física com as mídias e tecnologias: uma proposta mediada pelos conceitos. In: ARAÚJO, Allyson Carvalho; OLIVEIRA, Marcio Romeu Ribas de; SOUZA JUNIOR, Antônio Fernandes de. Formação continuada em educação física no diálogo com a cultura digital. 1. Ed. João Pessoa/PB: Editora IFPB, 2019. Disponível em: <https://memoria.ifrn.edu.br/handle/1044/1782>. Acesso em: 12 ago. 2020.
- CAVALCANTE, Waldek Fachinelli. Crimes Cibernéticos: noções básicas de investigação e ameaças na internet. Revista Jus Navigandi. Teresina, v. 18, 2016.
- CISCO. O que é segurança digital? Disponível em: https://www.cisco.com/c/pt_br/products/security/what-is-cybersecurity.html. Acessado em: 19/06/2023.
- CNN BRASIL. A cada 7 segundos, uma tentativa de fraude é registrada no Brasil; saiba se proteger. 2022. Disponível em: <https://www.cnnbrasil.com.br/economia/a-cada-7-segundos->

[uma-tentativa-de-fraude-e-registrada-no-brasil-saiba-se-proteger/](#). Acesso em: 12/09/2022.

- [5] GABRIEL, Martha. Educ@r. A (r)evolução digital na educação. 1ª Edição. São Paulo, Saraiva, 2013.
- [6] GUILHERME, Leonardo Pinto, et al. "Uma breve noção sobre o comportamento dos internautas em relação à segurança na rede." Anais da VII Escola Regional de Sistemas de Informação do Rio de Janeiro. SBC, 2021.
- [7] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). P NAD Contínua TIC 2016: 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens. 2018. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073>. Acesso em: 08/09/2022.
- [8] KALINKE, M.A. Para não ser um professor do século passado. Curitiba: Gráfica Expoente, 1999.
- [9] LAUDON, K. C.; LAUDON, J. P. Sistemas de Informações Gerenciais: administrando a empresa digital. 5. ed. Prentice Hall. 2004.
- [10] Lei No 12.965 (2014) Disponível em: www.planalto.gov.br/CCIVIL_03/_ato2011-2014/2014/Lei/L12965.htm. Acessado em: 17/06/2023.
- [11] LEI Nº 13.709. (2018) Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acessado em: 15/06/2023.
- [12] MERRITT, Merian. Norton's Cybercrime Report: The Human Impact Reveals Global Cybercrime Epidemic and Our Hidden Hypocrisy. Symantec Cyber Education. 2020. Disponível em: <https://community.norton.com/en/blogs/symantec-cyber-education/norton%E2%80%99s-cybercrime-reporhuman-impact-reveals-global-cybercrime>. Acesso em: 19/09/2022.
- [13] SCHUARTZ, A. S.; SARMENTO, H. B. de M. Tecnologias digitais de informação e comunicação (TDIC) e processo de ensino. R. Katál, v.23, n.3 set./dez. 2020.

- [14] SILVA, Rayanne Medeiros da; et al., Reflexões de aplicação das narrativas midiáticas na formação continuada dos professores de Educação Física. In: ARAÚJO, Allyson Carvalho; OLIVEIRA, Marcio Romeu Ribas de; SOUZA JUNIOR, Antônio Fernandes de. Formação continuada em educação física no diálogo com a cultura digital. 1. Ed. João Pessoa/PB: Editora IFPB, 2019. Disponível em: <https://memoria.ifrn.edu.br/handle/1044/1782>. Acesso em 12 ago. 2020.
- [15] VASCONCELOS, Márcia Linhares de et al. Vazamento de dados pessoais: um problema em crescimento. 2022.
- [16] VIANNA, E. W. & FERNANDES, J. H. (2015). C. O Gestor da Segurança da Informação no Espaço Cibernético Governamental: Grandes Desafios, Novos Perfis e Procedimentos.

7. ANEXO 1 – FORMULÁRIO APLICADO NAS ESCOLAS

