# PERDI MEU CELULAR: RELATO DE EXPERIÊNCIA DE UM MINICURSO DO GRUPO MENINAS DIGITAIS - REGIONAL BAHIA

*I LOST MY CELL PHONE: EXPERIENCE REPORT OF A MINICOURSE OF THE GROUP MENINAS DIGITAIS - REGIONAL BAHIA*

**Mônica de Sá Dantas Paz -** Doutorado em Comunicação e Cultura Contemporânea pela Universidade Federal da Bahia. Professora substituta do Instituto Federal de Educação, Ciência e Tecnologia da Bahia. E-mail: profmonicapaz@gmail.com

**Juliana Maria Oliveira dos Santos -** Mestranda em Ciência da Computação pela Universidade Federal da Bahia (UFBA), Bacharela em Sistemas de Informação (UFBA) Diretora Geral do Projeto Meninas Digitais - Regional Bahia. E-mail: julyms.85@gmail.com

**Jessica Ellen Miranda Barbosa -** Graduanda em Sistemas de Informação na Universidade Federal da Bahia. E-mail: jessbarbosa2000@gmail.com

**Paula da Cunha Vilas Boas -** Graduanda no Instituto de Psicologia - Universidade Federal da Bahia. E-mail: paulacunhavillasboas@gmail.com

**Débora Abdalla Santos -** Doutorado em Ciências da Computação pela Universidade Federal de Pernambuco. Professora Titular da Universidade Federal da Bahia. E-mail: debora.abdalla@gmail.com

## RESUMO

Este relato de experiência apresenta o minicurso intitulado “Perdi meu celular Android: o que fazer antes e depois do acontecimento?” cujo objetivo foi conscientizar sobre a importância da segurança digital em um mundo altamente informatizado e móvel. Para tanto, o minicurso abordou, de forma lúdica e informativa, medidas preventivas e corretivas contra ameaças digitais, principalmente, as relacionadas à privacidade diante da possibilidade da perda do dispositivo móvel.

**Palavras-chave:** segurança digital; privacidade; ameças digitais; Android; meninas digitais.

## INTRODUÇÃO

É cada vez maior a relevância dos dispositivos móveis no cotidiano brasileiro. Segundo o Relatório de Acompanhamento do Setor de Telecomunicações referente ao 2º semestre de 2020, em dezembro, o Brasil registrou 234,07 milhões de acessos à internet através da telefonia móvel, o que representou um aumento de 3,26% em relação ao mesmo período em 2019 (ANATEL, 2020). Na sequência, houve um aumento de 3,59% dos acessos, comparando-se o primeiro semestre de 2021 com o final de 2020 (ANATEL, 2021). Tal intensificação do uso de dispositivos móveis

para acessar a internet pode ser justificada pela necessidade de isolamento social causada pela pandemia de COVID-19, o que ocasionou muitas demandas por digitalização nos âmbitos educacional, social, cultural e econômico.

Contudo, os dispositivos móveis armazenam diversos dados e informações importantes de seus usuários. Apesar das facilidades, há também diversas ameaças decorrentes da sua perda ou roubo, como os riscos à privacidade devido ao vazamento de dados sensíveis e até mesmo transações indevidas, que ocasionam danos financeiros, emocionais, psicológicos, físicos e reputacionais (CERT.BR, 2020).

A Secretaria de Segurança Pública do Estado da Bahia (SSP-BA) registrou, no período de janeiro até outubro de 2020, 20.641 ocorrências de roubo ou furto de celulares em Salvador (G1 BAHIA, 2021). Já o Portal da Transparência da Secretaria de Segurança Pública de São Paulo (SSP-SP) revela que 160 mil aparelhos celulares foram roubados ou furtados, entre janeiro e julho de 2021 (GALVÃO, 2021). Além dos crimes de furto e roubo envolvidos em tal cenário, ressalta-se que a invasão de dispositivos alheios é tipificada como crime cibernético pela Lei Carolina Dieckmann ou Lei nº 12.737 de 2012 (BRASIL, 2012).

Cabral e Pontes (2021) afirmam que a combinação de grande volume de dados armazenados e manipulados nos dispositivos móveis com o desconhecimento das boas práticas sobre proteção de dados e medidas de segurança expõem os usuários a muitos riscos e ao sentimento de insegurança.

Lemos *et al.* (2021) alertam sobre o uso de técnicas de engenharia social que induzem os usuários a comprometerem a segurança de seus aparelhos com a instalação de *malwares* disfarçados de aplicativos populares, uso de redes *wi-fis* espionadas e acesso a URL falsas. Por isso, os autores defendem o uso de mecanismos de detecção de *malwares* no Android que utilizam metadados dos aplicativos.

Já Moraes e Vilela (2021) apontam outra prática que coloca os usuários de Android em risco, que é a busca pelo acesso *root* do sistema com a finalidade de instalar certos aplicativos e desinstalar outros aplicativos indesejados, bem como personalizar o sistema operacional. Como resultado, os celulares podem ficar vulneráveis a *malwares* e a vazamentos de dados pessoais, bem como a erros internos. Como contramedida, os autores indicam a importância das técnicas de detecção de *root* empregadas pelos desenvolvedores com o intuito de proteger os usuários menos experientes.

Todos estes riscos podem afetar a privacidade dos usuários de dispositivos móveis. Segundo o Dicio - Dicionário Online de Português (2022), privacidade é definida como a "qualidade do que é privado, do que diz respeito a alguém em particular: não se deve invadir a privacidade de ninguém. Intimidade pessoal; vida privada, particular".

A legislação brasileira, assim como tem ocorrido em outras partes do mundo, vem aprimorando-se no tocante ao direito à privacidade e à proteção de dados. Privacidade é um direito garantido pela Constituição Federal de 1988, pois esta garante no seu Art 5º que "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988). Aprofundando tal ideia no que se refere aos dados pessoais, a Emenda Constitucional nº 115 de 2022 inclui na Constituição Federal de 1988 a proteção de dados pessoais como um dos direitos e garantias fundamentais dos brasileiros (BRASIL, 2022).

O Marco Civil da Internet ou a Lei nº 12.965, de 23 de abril de 2014 também versa no seu Art. 3º sobre a privacidade como um dos princípios do uso da internet no Brasil (BRASIL, 2014). Princípio este que também é fundamental para a Lei Geral de Proteção de Dados Pessoais (LGPD) ou a Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018).

Segundo a disciplina de Segurança da Informação, a privacidade, principalmente dos dados pessoais, pode ser alcançada garantindo-se a confidencialidade, ou seja, restringindo-se o acesso à informação a apenas quem lhe é de direito. Para tanto, contramedidas de proteção devem ser asseguradas para mitigar os riscos à segurança, podendo ter o objetivo de reduzir as chances do risco ocorrer (preventivas e de redução), de amenizar os danos causados por tais riscos (detecção e repressivas), ou atuar em ambas abordagens, utilizando-se tanto de controles físicos, quanto lógicos (HINTZBERGEN *et al.*, 2018).

Portanto, os cuidados que as pessoas precisam ter ao utilizar seus dispositivos móveis envolvem medidas que devem ser tomadas antes e após os incidentes de segurança, como a perda do aparelho, o que resulta não apenas em uma perda financeira relativa ao valor do aparelho, mas que pode resultar em violação de privacidade, com graves consequências na ordem financeira, social e pessoal.

Para tanto, é preciso investimento em Educação. Dados da pesquisa TIC Educação 2020 da CETIC (2020) demonstram a necessidade de ações no intuito de promover a segurança digital e a proteção de dados, nas seguintes categorias: "cursos promovidos pela escola", "palestras com especialistas", "distribuição de materiais educativos, como cartilhas e panfletos"; "eventos promovidos pela escola, como exposições, feiras ou gincanas"; e "grupo de mediação de conflitos mantido pela escola". Por outro lado, a referida pesquisa destaca os bons índices alcançados para o indicador "Projetos interdisciplinares desenvolvidos com os alunos".

Neste contexto, o minicurso "Perdi meu celular Android. O que fazer antes e depois do acontecimento?" foi planejado visando conscientizar os participantes sobre a importância da segurança digital em um mundo altamente informatizado e móvel. Para tanto, no minicurso, foi apresentado, de forma lúdica e informativa, dicas de prevenção contra ameaças digitais, principalmente, as relacionadas à privacidade diante da possibilidade da perda do dispositivo móvel.

O minicurso é uma das ações do projeto de extensão "Segurança Digital para Mulheres e Ativistas", que é uma iniciativa do projeto Meninas Digitais – Regional Bahia. O projeto visa produzir conteúdos sobre segurança digital para a sociedade em geral, em especial as mulheres, suprindo demandas específicas do período pandêmico e de isolamento social, bem como busca aproximar as estudantes extensionistas do mercado e da pesquisa na área da segurança da informação.

Portanto, o objetivo deste relato de experiência é apresentar o planejamento, execução e avaliação do minicurso, que acontece com caráter extensionista, a partir das perspectivas de seus públicos-alvo.

## MATERIAL E MÉTODOS

Este relato de experiência aborda duas edições do minicurso, ambas planejadas e realizadas de forma remota em decorrência das medidas de proteção contra a COVID-19. A primeira ocorreu em 06 de outubro de 2021, na Semana de Ciência e Tecnologia Onda Digital (SCTOD) durante o evento Semana Nacional de Ciência e Tecnologia, que teve como tema "A transversalidade da ciência, tecnologia e inovações para o planeta", sendo voltado para comunidades escolares e acadêmicas, especialmente, estudantes e professores(as) das licenciaturas, e demais pessoas interessadas em Educação. O evento nacional visou explicitar a transversalidade da ciência nas interações humanas e o seu impacto na vida cotidiana da sociedade.

A segunda edição do minicurso ocorreu no dia 18 de fevereiro de 2022 durante o VI Fórum Interdisciplinar sobre Formação Docente com Tecnologias (VI FIFDT), que foi promovido pelo Grupo Onda Digital no âmbito do Programa Permanente de Ações Pedagógicas para Formação

Docente em Computação (PROFCOMP) da Universidade Federal da Bahia (UFBA) e teve como tema "Computação na Ação-Formação Humanística", sendo orientada para docentes de colégios estaduais e federais, mais especificamente da educação básica.

Visando os públicos-alvo dos eventos, o minicurso foi planejado para jovens e adolescentes e seus professores, sem restrição de gênero e sem exigência de conhecimentos prévios de informática. A única restrição era ser usuário de smartphones. Para contemplar o maior número de pessoas, adotou-se como padrão os smartphones Samsung (mais de 40% dos aparelhos no Brasil) (STATCOUNTER, 2022) e o sistema operacional Android (presente em mais de 88% dos smartphones brasileiros) (STATCOUNTER, 2022).

Em termos de conteúdo, o minicurso foi dividido em dois momentos: 1) medidas de proteção preventivas, que devem ser tomadas após a aquisição do dispositivo móvel; e 2) medidas de proteção corretivas, no caso de ocorrer a perda do aparelho. A primeira sessão do minicurso denominada "o que fazer agora?" aborda temas como dados e dados pessoais, bloqueio de tela, senhas fortes, pasta segura, backups, ou seja, configurações que devem ser realizadas ao adquirir o produto. A segunda sessão "o que fazer após perder o celular?" trata da localização e desconexão da conta Google do dispositivo perdido e de outros mecanismos de bloqueio e recuperação.

Buscou-se aplicar uma metodologia diversificada para tornar o minicurso mais interessante e lúdico. As estratégias didáticas estipuladas foram a apresentação oral dialogada, visando a interação com o público, sempre suportadas por slides com conteúdos textuais e imagéticos. Fez-se uso de memes de Internet para tornar mais divertidos os debates teóricos, como o "dados são o novo petróleo". Já para facilitar o entendimento sobre as configurações das medidas de segurança, usaram-se vídeos, como "Bloqueio de tela" do canal no *YouTube* da Samsung, e capturas de tela sobre como localizar o número IMEI do aparelho. Além do conteúdo de terceiros, também foi produzido material, como o vídeo "confirmação em duas etapas".

Como estratégias avaliativas foram feitas perguntas ao público tanto pelas expositoras, quanto no *chat* para provocar o debate, como "vocês usam dispositivos Android?" e perguntas que provocassem reflexão sobre a segurança de dados pessoais como "você deixaria seus documentos pessoais em um banco da praça?", "iria a uma agência bancária e sairia com um grande montante de dinheiro despreocupadamente?" e "daria as suas senhas bancárias a qualquer pessoa?", além da realização de uma dinâmica de criação de senhas. Inicialmente, foi criado um grupo no aplicativo de mensagens instantâneas *Telegram* cujo link de convite foi divulgado através de *QRcode* publicado nos slides desde o início da apresentação. Após o tema das senhas ser abordado no minicurso, deu-se início à dinâmica. Cada participante criou a sua proposta de senha, enviando-a através de um *Google Forms* divulgado através do chat do *Webconf* (plataforma de webconferência utilizada) e também no *YouTube*. Fez-se então uma enquete para eleger a melhor das senhas propostas de acordo com as boas práticas. As pessoas que criaram as senhas escolhidas ganharam brindes do grupo Meninas Digitais Regional-BA, como bottons e camisas.

O planejamento foi todo feito de forma colaborativa, utilizando-se ferramentas online, como Google Docs, Google Apresentações, Google Meet e Telegram. Para a realização, usou-se a plataforma Webconf, com transmissão feita no canal do Onda Digital no Youtube, porém apenas os inscritos no evento podiam interagir através do microfone e do chat para fazer comentários e tirar dúvidas.

## RESULTADOS E DISCUSSÃO

Na SCTOD, o minicurso durou 2 horas e 15 minutos e contou com 55 inscrições, dos quais 23

estiveram presentes, sendo 10 mulheres e 13 homens. O público foi diverso, com estudantes, funcionários administrativos e indivíduos interessados na temática. Houve bastante participação e engajamento espontâneo do público através de diversas perguntas e debates sobre o conteúdo.

Já no VI FIFDT, a duração foi de 2 horas, sendo 28 inscrições e 19 participantes efetivos, sendo 13 mulheres e 6 homens. Por outro lado, no VI FIFDT, o público foi formado em sua maioria por docentes da rede Estadual e Federal, seguindo o foco do evento. Contudo, a participação do público teve que ser estimulada por questionamentos e outras intervenções feitas pela equipe do minicurso.

Os números de participantes podem ser explicados pelo tempo de divulgação que cada evento teve: o primeiro foi divulgado nas redes sociais entre os dias 29/09/2021 e 06/10/2021, ou seja, uma semana de divulgação; o segundo apenas três dias de divulgação de 15/02/2022 até 18/02/2022. Esses dados fazem pensar que um maior tempo de divulgação poderia significar uma maior adesão ao evento.

Em relação à dinâmica, as senhas elaboradas no minicurso da SCTOD foram mais simples e mais memorizáveis, apesar de muitas seguirem os critérios expostos para a criação de uma boa senha. No VI FIFDT, as senhas foram mais elaboradas e mais difíceis de serem lembradas. Os participantes foram orientados a não usar dados pessoais e nem a reutilizar as senhas divulgadas na dinâmica, dentre outras precauções. Apesar do público do VI FIFDT ser mais tímido em relação ao público da SCTOD, notou-se que a presença da dinâmica - forma de tirar o público de um lugar de apenas ouvinte - foi bem recebida já que 15 dos 19 presentes na atividade participaram também da dinâmica.

Ao final do minicurso, os participantes preencheram a lista de presença e uma breve pesquisa de satisfação com as seguintes questões: qualidade do conteúdo (Q1), clareza na apresentação (Q2), metodologia dos materiais utilizados (Q3), duração (Q4), qualidade da transmissão (Q5), relevância do conteúdo (Q6) e divulgação do evento (Q7). Para entender a percepção do público, cada uma dessas seções podiam ser avaliadas com a escala: ótimo, bom, regular, ruim, péssimo, e prefiro não avaliar.

Apesar de a primeira edição ter recebido quase o dobro de inscrições do segundo (53 e 28, respectivamente), o número de participantes nas duas edições do minicurso foi bem próxima (23 e 19). Contudo, as respostas dos participantes sobre a divulgação do evento foi positiva: 1) dos 23 presentes na SCTOD, 15 tiveram a percepção de que foi ótima, 6 entenderam como boa, 1 regular e 1 preferiu não avaliar; 2) das 19 respostas do VI FIFDT, 8 entenderam como ótimo, 9 como bom e 2 como regular.

Outro ponto significativo da pesquisa de satisfação foi que nenhum participante avaliou alguma questão como ruim ou péssima. Isso é, sem dúvidas, um reflexo positivo das duas edições do minicurso. De forma geral, as percepções do público dos dois eventos foi similar. Os dados do formulário foram organizados na Tabela 1:

**Tabela 1.** Número absoluto de participantes que avaliaram cada questão da atividade na SCTOD e no VI FIFDT

| | SCTOD | | | | VI FIFDT | | | |
|---|---|---|---|---|---|---|---|---|
| | **Ótimo** | **Bom** | **Regular** | **NA** | **Ótimo** | **Bom** | **Regular** | **NA** |
| **Q1** | 21 | 2 | 0 | 0 | 17 | 2 | 0 | 0 |
| **Q2** | 21 | 2 | 0 | 0 | 17 | 2 | 0 | 0 |
| **Q3** | 20 | 2 | 0 | 1 | 15 | 4 | 0 | 0 |
| **Q4** | 15 | 7 | 0 | 1 | 15 | 4 | 0 | 0 |
| **Q5** | 17 | 6 | 0 | 0 | 12 | 7 | 0 | 0 |
| **Q6** | 21 | 2 | 0 | 0 | 17 | 1 | 1 | 0 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Q7** | 16 | 6 | 1 | 1 | 8 | 9 | 2 | 0 |

Pode-se perceber, a partir da Tabela 1, que a maioria dos participantes escolheu "ótimo" ou "bom" para classificar os itens da atividade. Merecem especial destaque às questões 1, 2 e 6, referentes à qualidade do conteúdo, clareza na apresentação e relevância do conteúdo, respectivamente. Tais avaliações dos participantes reforçam a importância do tema ministrado no minicurso para o público em questão.

Além dessas seções voltadas para que o público avaliasse a atividade, o formulário ainda contou com uma pergunta sobre como a pessoa ficou sabendo do evento e um último espaço para sugestões, críticas e comentários gerais. Os participantes da SCTOD tiveram alta taxa de resposta a essa seção, contabilizando 9 respostas, que foram majoritariamente positivas, como: "Excelente, parabéns pelo minicurso" e "Muito bom o evento! Parabéns! Que venham outros", mas teve uma sugestão que foi a solicitação de mais vagas. A única resposta dos participantes do VI FIFDT foi uma sugestão: "Como foi muito conteúdo e não deu para anotar tudo, por favor deixe o vídeo da aula no YouTube por uma semana para podermos rever e fazer anotações. Tem muita coisa para registrar".

Como autoavaliação no pós-evento, as alunas extensionistas foram convidadas a falar sobre suas impressões em relação à experiência de ministrar um minicurso sobre segurança digital. Jéssica Barbosa, estudante de Sistemas de Informação, considerou que "foi uma possibilidade de atravessar o contorno da Universidade e estabelecer uma interlocução com a sociedade. A configuração remota do minicurso demandou um novo formato de produção do conteúdo e forma de transmitir esse conteúdo. Este último foi o ponto de maior dificuldade, já que a dinâmica com o público fica limitada, às vezes, a uma mensagem no chat. Com relação à temática de Segurança Digital, novos conhecimentos foram adquiridos e mais interesses surgiram. Já é notório que a tecnologia ocupa amplo espaço e possui diversas áreas do conhecimento e, dentre estas, muitas coisas precisam ser exploradas, e a cibersegurança é uma dessas, já que se apresenta como uma parte da computação considerada complexa. Sendo aluna de Sistemas de Informação, já tinha um pouco de conhecimento acerca da segurança digital para dispositivos Android, mas o aprendizado pôde ser reforçado, além de incrementado com mais conteúdos e curiosidades".

A outra ministrante, Paula Cunha, estudante de Psicologia, pôde perceber que "a transversalidade que o fenômeno da segurança digital tem e o quanto profissionais de outras áreas devem acrescer ao debate, sobretudo, na não culpabilização das vítimas de golpes".

A avaliação dos participantes e a percepção das instrutoras sobre as contribuições da atividade para a formação pessoal, acadêmica e profissional mostram a importância do desenvolvimento de atividades de extensão sobre o tema da segurança digital.

## CONCLUSÃO

As intervenções dos participantes ao longo das apresentações de ambas edições do minicurso e os resultados das suas pesquisas de satisfação corroboram a importância do tema da segurança digital, apontando que iniciativas neste sentido são muito necessárias em um mundo que é cada vez mais mediado pelas tecnologias digitais. Portanto, atividades de extensão são uma alternativa para fomentar a consciência sobre a importância da privacidade e da proteção de dados pessoais como direitos dos cidadãos, bem como alertar sobre as consequências de ameaças digitais que atacam tais direitos.

Como trabalhos futuros, este relato de experiência servirá como ponto de partida para a melhoria das próximas edições do minicurso, bem como para que novas ações sejam propostas

pelo grupo Meninas Digitais - Regional Bahia, aprendendo com os acertos e os erros, e contribuindo assim, para melhoria de iniciativas futuras. Além disso, os slides utilizados no minicurso serão adaptados para as redes sociais do grupo para que mais pessoas possam acessar e compartilhar os conteúdos.

Destaca-se ainda a composição da equipe multidisciplinar deste projeto de extensão universitária feito para e por mulheres de diferentes áreas, como computação, comunicação e psicologia. Isto enriqueceu o material produzido e as atividades realizadas, pensando-se a temática da segurança digital para dispositivos móveis a partir de diferentes pontos de vista, considerando os aspectos técnicos a nível da cibersegurança, sem ofuscar os aspectos psicossociais que atravessam cada indivíduo, como o cuidado de não culpabilização da vítima e o destaque para os possíveis danos financeiros, emocionais, psicológicos, físicos e/ou reputacionais.

Por fim, o minicurso também foi uma ótima primeira oportunidade para as extensionistas terem contato com o planejamento, produção e execução de uma atividade instrucional, mesmo que de forma remota, preparando-as para novos desafios na área de Gênero e Segurança da Informação.

## AGRADECIMENTOS

Agradecemos ao Programa Institucional de Bolsas de Iniciação à Extensão Universitária da Pró-Reitoria de Extensão Universitária (PROEXT) da Universidade Federal da Bahia (UFBA) pelo fornecimento de bolsa para o projeto “Segurança Digital para Mulheres e Ativistas” e ao professor coordenador do projeto, Paul Regnier.

## REFERÊNCIAS

ANATEL, Agência Nacional de Telecomunicações. **Relatório de Acompanhamento do Setor de Telecomunicações.** 2020. Disponível em: https://bit.ly/3DiQQXK. Acesso em: 06 fev. 2023.

ANATEL, Agência Nacional de Telecomunicações. **Relatório de Acompanhamento do Setor de Telecomunicações.** 2021. Disponível em: https://bit.ly/3tTEGBG. Acesso em: 06 fev. 2023.

BRASIL. **Constituição da República Federal do Brasil de 1988.** 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 06 fev. 2023.

BRASIL. **Lei Nº 12.737, de 30 de novembro de 2012.** 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 06 fev. 2023.

BRASIL. **Lei Nº 12.965, de 23 de abril de 2014.** 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 06 fev. 2023.

BRASIL. **Lei Nº 13.709, de 14 de agosto de 2018.** 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 06 fev. 2023.

BRASIL. **Emenda Constitucional Nº 115, de 10 de fevereiro de 2022.** 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 06 fev. 2023.

CABRAL, J., & PONTES, H.. **Segurança em Dispositivos Móveis:** Um Estudo Sobre a Adoção de Boas Práticas para Proteção em Celulares. In Anais do XLVIII Seminário Integrado de Software e Hardware, (pp. 58-68). 2021. Porto Alegre: SBC. doi:https://doi.org/10.5753/semish.2021.15807

CETIC. **TIC Educação 2020:** Pesquisa sobre o Uso das Tecnologias de Informação e

Comunicação nas Escolas Brasileiras. 2020. São Paulo, Fevereiro.

G1 BA. **Salvador tem cerca de três celulares roubados ou furtados por horas diz SSP-BA.** 2021. Disponível em: https://g1.globo.com/ba/bahia/noticia/2021/01/22/salvador-tem-cerca-de-tres-celulares-roubados-ou-furtados-por-hora-diz-ssp-ba.ghtml. Acesso em: 06 fev. 2023.

CERT.BR. **Cartilha de Segurança para Internet.** 2020. Disponível em: https://cartilha.cert.br/. Acesso em: 06 fev. 2023.

GALVÃO, C.. **Cerca de 160 mil celulares já foram roubados ou furtados no estado de SP entre janeiro e julho de 2021, diz levantamento**. 2021. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2021/09/09/cerca-de-160-mil-celulares-ja-foram-roubados-ou-furtados-no-estado-de-sp-entre-janeiro-e-julho-de-2021-diz-levantamento.ghtml. Acesso em: 06 fev. 2023.

HINTZBERGEN, J; HINTZBERGEN, Kees; SMULDERS, A.; BAARS, H. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. Brasport: 2018, Tradução: Alan de Sá.

STATCOUNTER. **Mobile Operating System Market Share in Brazil** - March 2022. 2022. Disponível em: https://gs.statcounter.com/os-market-share/mobile/brazil. Acesso em: 06 fev. 2023.

STATCOUNTER. **Mobile Vendor Market Share in Brazil** - March 2022. 2022. Disponível em: https://gs.statcounter.com/vendor-market-share/mobile/brazil. Acesso em: 06 fev. 2023.

LEMOS, R. HEINRICH, T.; MAZIERO, C.. **Utilizando Metadados de Aplicações e Comunicação entre processos para Identificar Ameaças no Android**. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/17307. Acesso em: 06 fev. 2023.

MORAES, V.; VILELA, J.. **Uma avaliação do cenário de detecção e evasão do acesso root no Android**. 2021. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/17306. Acesso em: 06 fev. 2023.