Métodos de autenticação em serviços digitais considerando aspectos de segurança, privacidade e experiência de uso

Ronald C. R. de Araujo[1], **Letícia Lopes Leite**[1]

[1]Departamento de Ciência da Computação – Universidade de Brasília (UnB)
Brasília – DF – Brasil

ronald.ecomp@gmail.com, llleite@unb.br

Resumo. *Com a crescente oferta de serviços digitais, é comum que diversos serviços online necessitem de uma forma de identificação dos seus usuários. Neste contexto, é fundamental que se tenha um sistema de gerenciamento de identidades (IdM) para viabilizar o processo de autenticação dos usuários. Este trabalho apresenta os resultados de um questionário aplicado a usuários de serviços on-line, onde as unidades de avaliação foram profissionais de Tecnologia da Informação e não profissionais de Tecnologia da Informação. O objetivo foi investigar o comportamento destes usuários quando confrontados com sentenças a respeito do processos e métodos de autenticação, tais como usuário e senha, biometria e código de acesso. O estudo traz como contribuição um ensaio sobre a crença dos usuários finais sobre aspectos de experiência de uso, segurança e privacidade.*

1. Introdução

Vivenciamos uma crescente oferta de serviços on-line, movimento que tem acelerado em função da necessidade de distanciamento social provocado pela pandemia da Covid-19 [Kutnjak 2021]. Sendo assim, se faz necessário um novo olhar sobre as soluções que são ofertadas aos usuários finais e um maior entendimento das necessidades e desejos destes usuários. A oferta de serviços em meio virtual é comum em diversas iniciativas que, rotineiramente, necessitam de uma forma para autenticar seus usuários, caracterizando um processo de identificação eletrônica. Identificação eletrônica é entendida como o processo de representação de "*quem você é*", compreendendo um conjunto limitado de atributos da sua vida real [Berbecaru, Lioy e Cameroni 2019]. A identificação eletrônica é um facilitador essencial no processo de transformação digital, inclusive na prestação de serviços públicos [Nielsen 2019].

Uma vez que se tem confiança de que um determinado usuário é quem diz ser, um passo adicional é conhecer atributos deste usuário, possibilitando que as aplicações ofereçam uma experiência de uso customizada de acordo com o seu perfil e necessidades, contribuindo para sua adesão ao processo de digitalização e evidenciando o valor percebido pelo mesmo sobre o serviço oferecido [Filho, Ribeiro e Zefferer 2016]. Neste contexto, é importante que os serviços on-line apresentem uma método de autenticação que seja seguro, proteja os dados do usuário e que tenha uma experiência de uso facilitada.

Este trabalho apresenta um questionário aplicado a usuários de serviços on-line que investiga o comportamento destes quando confrontados com sentenças a respeito de processos de autenticação. Foram definidas as unidades de avaliação como sendo profissionais de Tecnologia da Informação (TI) e não profissionais de TI. A escolha por estas

unidades visou investigar se um maior fluência em TI reflete em diferenças de comportamento frente a soluções de identificação eletrônica.

A contribuição desejada com esta pesquisa é um ensaio sobre a crença dos usuários finais no que diz respeito à experiência de uso, segurança e privacidade. Uma limitação inerente ao ensaio diz respeito a não possibilidade de generalização dos resultados. É esperado que o método apresentado nesta pesquisa possa ser utilizado como suporte no desenho de soluções de identificação orientadas aos usuários.

O artigo está organizado da seguinte forma: a Seção 2 apresenta a metodologia aplicada no estudo. Os resultados e a discussão destes são apresentados na Seção 3 e, a Seção 4, traz as conclusões e endereça uma visão de futuro.

2. Metodologia aplicada

A metodologia aplicada neste estudo compreende a elaboração e aplicação de um questionário com o objetivo principal de investigar a crença dos indivíduos em relação a soluções de identificação para acesso a serviços on-line, considerando aspectos como segurança, privacidade e experiência de uso, estes aspectos foram selecionados por serem considerados fundamentais para que uma solução de IdM conte com maior probabilidade de adesão dos usuários e consequente manutenção e longevidade da solução [Cameron 2006] [Cavoukian 2006]. Já a população-alvo a ser abordada considera dois grupos profissionais de TI e não profissionais de TI. A escolha por estas unidades visou investigar se maior fluência com TI se reflete em diferenças de crenças com relação a soluções de identificação digital.

O passo seguinte foi a elaboração do projeto de amostragem. Considerando que este trabalho é focado em sistemas de IdM e, que estes são utilizados por diversos setores da sociedade, optou-se por utilizar uma abordagem acidental, não probabilística. Este tipo de amostragem é caracterizada pela utilização do critério de conveniência para a seleção das amostras e é comum a sua utilização em pesquisas de Engenharia de Software [Linåker et al. 2015]. As amostras se deram por meio de contatos pessoais e o método de levantamento foi o de questionário web, distribuído através de redes sociais e via e-mail.

Por se tratar de uma pesquisa quantitativa e com característica de levantamento, foram utilizadas questões fechadas. Já para as respostas, foi utilizada a escala Likert [Joshi et al. 2015], visando determinar a intensidade e a frequência de uma opinião ou comportamento [Kasunic 2005]. Foram elaboradas sentenças afirmativas e as opções de respostas variam entre os números um e cinco, indicando a intensidade da concordância com a afirmação. O número 1 (um) indica discordância forte e o número 5 (cinco) concordância forte.

3. Resultados e Discussão

O questionário foi aplicado no período de 21/01/2021 a 31/01/2021 e apresentou um total de 132 respostas, sendo a distribuição dos respondentes na proporção de 2/3 dos não profissionais de TI. Pouco mais de metade dos respondentes se declararam como mais identificados com o gênero feminino, 60% possui curso superior e 50% pertencem à faixa etária dos 25 aos 39 anos.

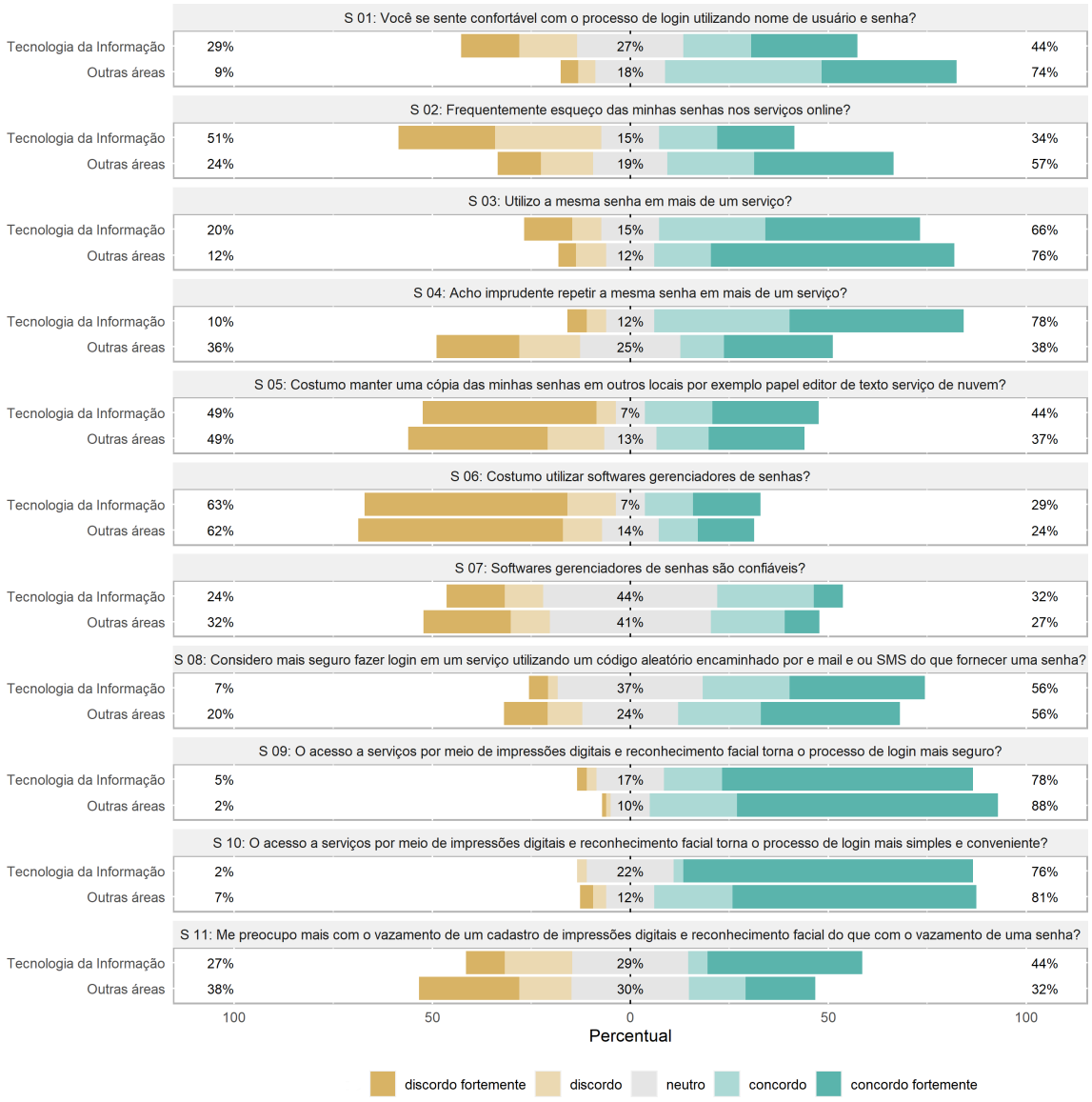

Figura 1. Resultado da aplicação do questionários para as Sentenças de 1 a 5.

A inapropriada medida de segurança de reutilização de senhas é um traço comum em ambos os grupos (Figura 1, S 03). Na percepção dos dois grupos de estudo, o uso de biometria torna o processo de autenticação mais seguro e conveniente.

4. Conclusão

A análise dos resultados do ensaio realizado aponta que os usuários de sistemas online valorizam com maior intensidade o aspecto da experiência de uso, independente do usuário ser ou não um profissional de TI, sendo os aspectos de segurança, proteção e privacidade de dados menos valorizados. Tal constatação, reforça o essencial compromisso dos provedores de identidade com relação à segurança e à privacidade, uma vez que são pilares importantes no estabelecimento de um efetivo sistema de IdM [Cavoukian 2006]. Mesmo em cenários em que os usuários reconhecem que determinada abordagem é arriscada em termos de segurança, eles ainda a utilizam em prol de uma maior comodidade

durante a identificação. O desafio posto é o de se encontrar o equilíbrio entre as dimensões segurança, privacidade e usabilidade.

Um exemplo que reforça essa conclusão é a observação de que cerca de 88% das contas ativas do sistema Gov.Br utilizam como meio de autenticação apenas usuário e senha [Brasil 2021]. Atualmente, o Gov.Br conta com mais de um milhão de contas ativas. Com larga margem é observado que, do ponto de vista dos entrevistados, o uso de biometria é considerado um processo mais simples e conveniente, frente às demais opções. Se por um lado a adoção de biometria nos processos de autenticação de usuário torna o processo com ótima experiência de uso, por outro a utilização de biometria requer controles eficientes no que diz respeito à proteção e à privacidade dos usuários. Métodos de autenticação puramente baseados em biometria ainda correm o risco de vazamentos destes dados inviabilizarem por completo o sistema, uma vez que não é possível a redefinição de um dado biométrico.

A evolução dos métodos de autenticação é constante e o futuro indica para a adoção de autenticação baseada em risco como uma possibilidade (*Risk Based Authentication*). Nela, uma combinação de fatores e técnicas instituem um contexto de confiança que habilita o processo de autenticação com maior ou menor fluidez com relação à experiência de uso.

Referências

BERBECARU, D.; LIOY, A.; CAMERONI, C. Providing digital identity and academic attributes through european eid infrastructures: Results achieved, limitations, and future steps. *Software: Practice and Experience*, v. 49, 08 2019.

BRASIL. Acesso gov.br. *Secretária de Governo Digital*, s.n, 2021.

CAMERON, K. The laws of identity. 2006. Disponível em: <https://www.identityblog.com/?p=352>. Acesso em: 24 maio. 2021.

CAVOUKIAN, A. *7 Laws of Identity - The Case for Privacy-Embedded Laws of Identity in the Digital Age*. Ontaria, Canada, 2006. Disponível em: <http://www.ipc.on.ca/index.asp?navid=46fid1=470>. Acesso em: 2020-10-15.

FILHO, W. P.; RIBEIRO, C.; ZEFFERER, T. An ontology-based interoperability solution for electronic-identity systems. In: . [S.l.: s.n.], 2016.

JOSHI, A. et al. Likert scale: Explored and explained. *British Journal of Applied Science Technology*, v. 7, p. 396–403, 01 2015.

KASUNIC, M. Designing an Effective Survey. 9 2005. Disponível em: <https://kilthub.cmu.edu/articles/journal_contribution/Designing_an_Effective_Survey/6573062>. Acesso em: 10 out. 2020.

KUTNJAK, A. Covid-19 accelerates digital transformation in industries: Challenges, issues, barriers and problems in transformation. *IEEE Access*, v. 9, p. 79373–79388, 2021.

LINÅKER, J. et al. *Guidelines for Conducting Surveys in Software Engineering*. [S.l.: s.n.], 2015.

NIELSEN, M. M. Tackling identity management, service delivery, and social security challenges: technology trends and partnership models. In: . [S.l.: s.n.], 2019. p. 1–5.