Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.21, n.1, p.46-66, 2021.
DOI: 10.18762/1982-4920.20210004

INFLUÊNCIA ETÁRIA E SEGURANÇA DA INFORMAÇÃO : ESTUDO SOBRE A PERCEPÇÃO DE SENHAS SEGURAS EM RELAÇÃO A IDADE

Jonathan Gabriel Cardoso **GOES**[1]
Luana Dos Santos **MARTINS**[2]
Wdson **OLIVEIRA**[3]

RESUMO

Atualmente, em um mar tecnológico, ondas de inovação chegam a nossos "barcos" e nos imergem em um oceano de possibilidades e comodidades através de diversos tipos de dispositivos, será que nossos "barcos" estão protegidos? A premissa da autenticação de usuários é garantir o princípio da confiabilidade, onde apenas o usuário específico consegue acessar aquela informação, o que nos leva a um dos métodos de autenticação - as senhas, será que quanto mais complexa a senha, mais protegido estará nosso barco? Com o passar do tempo, como tratamos as senhas e suas complexidades? Será que quanto mais experiente o usuário, maior complexidade da senha e do método utilizado para proteção? A faixa etária pode influenciar na geração de senhas?

Palavras-Chave: Senhas, Influência Etária, Segurança.

ABSTRACT:

Nowadays,in a technological sea, waves of innovation reach our "boats" and immerse us in an ocean of possibilities and facilities through different types of devices, but, are our "boats" protected? The premise of user authentication is to certify the principle of reliability that only access to only users that have been assigned a specific user, which brings ustooneofthe authentication methods - the passwords. In terms of complexity, as safier as passwords more protected will be? Over time, how do we handle passwords and their complexities?Does the most experienced user use more secure methods and passwords to protect themselves? Does the age group influence the generation of passwords?

KEYWORDS: Passwords, Influence of Age, Security.

1 * Graduando de Tecnologia em Segurança da Informação. Graduado em Engenharia de controle e automação. E-mail do autor:jonathangcgoes@gmail.com;
2 *Graduanda de Tecnologia em Segurança da Informação. Especialista em Gestão de Projetos. Graduada em Administração Pública. E-mail do autor: luana.m93@gmail.com;
3 *Mestre. Especialista. Graduado em Ciência da Computação. E-mail do autor: wdson.oliveira01@fatec.sp.gov.br

Recebido em: 05/09/2021 - Aceito para publicação em: 02/12/2021

INTRODUÇÃO

As senhas surgiram por volta dos anos 60, e hoje se apresenta como um dos métodos mais utilizados para comprovar a autenticidade e confiabilidade dos usuários. Fernando J Corbató ajudou a implementar a primeira senha de computador, transformando o uso da tecnologia e nossa percepção sobre privacidade. Agora, na era da Web, o antigo professor do MIT (Massachusetts Institute of Technology) considera as senhas um verdadeiro pesadelo." (GIZMODO UOL 2014).

Segundo Exame (2015) no ano de 2014 a senha mais utilizada pelos populares foi "123456", seguida por "password", "12345", "12345678" e "qwert", todas essas muito intuitivas, nada complexas e que não atende o quesito eficácia.

Quanto a elaboração de senhas:

> "Caso você esteja usando alguma delas, considere trocá-las por algo mais elaborado o quanto antes -- e não, usar o dia de seu aniversário não é recomendável. O ideal é misturar letras maiúsculas e minúsculas a números e símbolos, e até usar um gerenciador de combinações, como o LastPass e ou o Key, para não correr o risco de esquecer algo" . (GUSTAVO GUSMÃO, 2015).

Entre as vantagens, as senhas permitem proteger as informações, e garantir a confiabilidade dos dados, no entanto, alguns usuários podem se sentir incomodados com a complexidade e obrigatoriedade de padrões em algumas tecnologias, levando a repetição em dispositivos e contas diferentes, anotá-las em lugares de fácil acesso ou utilizar padrões simplificados, práticas não recomendadas segundo a pesquisa da SplashData.(GOGONI, 2019)

A realidade deveria ser outra, se por um lado qualquer barreira auxilia na prevenção e dificulta o vazamento de dados e informações, do outro estamos inseridos de maneira crônica neste paradoxo de complexidade e comodidade na escolha das senhas. "Em meio a notícias de golpes de Black Friday e vazamentos de credenciais de acesso, a preocupação do internauta com a proteção por meio de uma senha forte continua em baixa" (ARBULU, 2020).

Apesar de notícias e orientações cada vez mais presentes nas empresas e tentativas de conscientização da população para este risco, a preocupação com as senhas não é considerada na hora de se proteger, "De acordo com a pesquisa da SplashData, a maioria das pessoas usa senhas simples e fáceis de lembrar, por uma questão de conveniência. Mas o problema é que as senhas mais memoráveis são também as mais vulneráveis a invasões" (ARBULU, 2020).

Segundo Diego Macedo :

> “De forma geral, se você seguir as regras para se criar senhas fortes, você já terá uma linha de defesa contra ataques”, “Muitas empresas adotam estas regras no formulário de senhas como um requisito de complexidade da senha.” (MACEDO DIEGO 2017)

Os métodos evoluíram com o tempo, assim como as técnicas para burlar as senhas mudam constantemente, com isso podemos retomar algumas questões: Com o passar do tempo, como tratamos as senhas e suas complexidades? Será que quanto mais experiente o usuário, maior complexidade da senha e do método utilizado para proteção? A faixa etária pode influenciar na geração de senhas?

Esta pesquisa busca verificar os diversos tipos de senhas, suas complexidades e relação com a faixa etária, no que se diz respeito à criação e manutenção das senhas baseados na amostra coletada através do instrumento de pesquisa na forma de um formulário com questões Quali-Quantitativa.

MATERIAL E MÉTODOS

Para atingir os objetivos propostos, testar as hipóteses experimentais formuladas e identificar a relação entre o nível de segurança através de experiências relacionadas a senhas versus idade dos respondentes, foi utilizado a metodologia de pesquisa exploratória a fim de aprimorar ideias e descobrir intuições tendo como instrumento de pesquisa um formulário on-line aplicado a uma população de 160 pessoas, buscando analisar principalmente as respostas da amostra de 37 respondentes que correspondem a faixa etária acima de 38 anos de idade.

A pesquisa visa estabelecer um parâmetro relacional, ainda inexistente, entre ações e métodos de segurança adotados ou não pelos entrevistados e o resultado desta pesquisa colabora com a iniciativas de boas práticas de segurança da informação e desenvolvimento de sistemas seguros.

BREVE REFERENCIAL TEÓRICO SOBRE SEGURANÇA DA INFORMAÇÃO E SENHAS

Na era digital onde o valor dos dados e informações se eleva a cada segundo, a internet é um dos principais pontos por onde a informação é distribuída, e principal meio de comunicação mundial, por essa razão a demanda por segurança de dados em consonância com as preocupações de uso não autorizado de senhas

e consequências relacionadas a vazamento de dados crescem exponencialmente. (SILVA; STEIN, 2007)

Laureano e Moraes (2005) elenca os três princípios básicos da segurança da informação : Confidencialidade para impedir acessos não autorizados, Integridade para que a informação não seja alterada durante seu ciclo de vida, e disponibilidade para estar sempre a mão sempre que necessário.

Silva e Stein (2007) sumarizam a definição de Segurança da informação (SI) como a proteção contra o uso ou acesso não - autorizado à informação, proteção contra a negação de serviço a usuários autorizados, preservando a confidencialidade, um dos pilares da segurança.

A segurança da informação "...se aplica a todos os aspectos de proteção da informação ou dados, de qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma"(SILVA; STEIN, 2007)

A autenticação é conceito chave dentro da segurança da informação, o processo de diferenciar usuários autorizados de outros não-autorizados é registrado desde em 1900 A.C. onde decifrar códigos para que apenas a pessoa certa tenha acesso a mensagem é algo que sempre existiu, embora tenha sido tratado especialmente nos últimos anos. (SILVA,2007)

A diferença sobre a autenticação da informação do ponto de vista do usuário e da S.I., às vezes podem ser distintas, o que para o usuário se torna apenas uma tarefa obrigatória, para a segurança da informação seria um conjunto de recomendações técnicas que podem ser gerenciadas. (Smith, 2002)

Segundo Melo (2017) os mecanismos de autenticação podem ser classificados em 3 tipos: conhecimento, quando se baseia em conhecimentos exclusivos do usuários, propriedade, algo que o usuário possua para se autenticar, ou característica, que se apoia em características físicas, humanas ou comportamentais.

A senha é o esquema de autenticação baseado em conhecimento mais comumente utilizado. Os usuários devem se lembrar de uma sequência alfanumérica de que precisam para fornecer no login (ZIMMERMANN; GERBER, 2020)

Por apresentar muitos problemas de autenticação, Fiorese (2000) destaca que para melhorar o uso de senhas, podem ser utilizados geradores randômicos, checagem pró-ativa, utilização de senhas descartáveis baseadas em software e hardware e sistemas de desafio/resposta, modificações no processo de login e combinação com outros mecanismos de autenticação de usuários como smartcards .

Fiorese (2000) complementa exemplificando:

> "O S/KEY, definido pela RFC 1760, é um sistema que implementa senhas descartáveis. A cada conexão é usada uma senha diferente, impedindo ataques baseados na captura ou adivinhação de senhas. Existem várias implementações compatíveis com S/KEY que podem ser encontradas na Internet."(FIORESE,cap 2)

Cartões inteligentes, chaves e tokens são exemplos de autenticação por propriedade, Melo (2017) descreve como desvantagem desse mecanismo de autenticação a probabilidade de perda desse dispositivo que apoia o processo.

Segundo Fiorese (2000) esquemas de autenticação por propriedade como tokens são apoiados em um dos seguintes esquemas: autenticação por desafio/resposta ou autenticação sincronizada no tempo.

Sistemas baseados em desafio/resposta, o usuário insere sua identificação no sistema,é gerado um desafio a ser respondido, enquanto isso o sistema cria uma resposta correspondente criptografada a ser comparada com a resposta do usuário dentro de suas chaves permitidas. Na Autenticação por tempo a geração é comumente randômica aguardando o usuário por um determinado período de tempo também verificando suas chaves.(FIORESE, 2000)

A Biometria ou autenticação biométrica considera características físicas e comportamentais do indivíduo, que serão comparadas com um banco de dados e tem como garantia a presença da pessoa no ponto de identificação. (Melo,2017)

Para Fiorese (2000) características humanas, físicas ou comportamentais, podem ser utilizadas para a identificação de pessoas nas autenticações baseadas em características desde que satisfaça alguns itens: Universalidade: que todas as pessoas possam possuir essa característica; Singularidade: que não pode ser igual em pessoas diferentes; Permanência: que não deve mudar com o tempo e Mensurabilidade: que a característica pode ser medida quantitativamente.

Autenticar usuários, sistemas ou processos exerce um papel importante para o gerenciamento de controle de acesso, uma vez que suas operações são realizadas com base em uma entidade autêntica. (SOUZA, 2010)

Segundo Albertin e Moura (1998) :

> "sistemas biométricos são considerados como o nível mais seguro de autorização, envolvendo alguns aspectos únicos da pessoa, incluindo comparação de impressão digital, impressões da palma da mão, padrões de retina, verificação de assinatura e reconhecimento de voz. Estes sistemas são muito caros."(ALBERTIN; MOURA, 1998,p.53)

O controle de acesso realiza a mediação das requisições de acesso a objetos iniciados pelos sujeitos, viabilizando a implantação de políticas de segurança específicas. Existem três classes principais de controle de acesso: DAC (Discretionary Access Control); MAC (Mandatory Access Control); e, RBAC (Role-Based Access Control).(Melo,2017)

Samarati e Vimercati (2001) explicam que as políticas DAC controlam o acesso com base na identidade do usuário e nas regras de acesso, que juntas indicam se o mesmo possui ou não permissão de acesso. A política MAC verifica o acesso com base em regulamentos obrigatórios determinados por uma autoridade central e a RBAC controla o acesso dependendo das funções que os usuários possuem dentro do sistema e das regras que indicam quais acessos são permitidos aos usuários em determinadas funções.

Dentre tantos conceitos identificados, torna-se evidente a fragilidade do tema - senhas ; tanto no quesito de criação das mesmas, quanto no gerenciamento, atingindo não apenas aos programadores mas também seus usuários e o risco relacionado a ataques hackers.

EMPODERAMENTO DIGITAL

Através dos dados coletados no processo de pesquisa, constitui-se um levantamento de alguns índices, que podemos relacionar a ideias e conceitos da segurança da informação e a idade.

Em um país como o Brasil, onde uma das maiores dificuldades na implantação de uma cultura sólida de segurança de dados, é a acessibilidade e às informações relacionadas a esse conceito, faz-se necessária a democratização e criação de um processo de empoderamento digital, no que se diz respeito

conexão com a internet e dispositivos para o desenvolvimento e interação seguros no ambiente virtual.(OLIVEIRA; MOTTA; MELO; ESTEVES, 2020)

Para Oliveira, Motta, Melo e Esteves (2020) estamos inseridos e convivemos diariamente com uma alta taxa de desigualdade social, na qual uma parcela muito grande da população não tem condições de adquirir meios para tal nível de segurança, e muitas vezes até quem detêm o poder aquisitivo necessário para tal, ainda não possui esse conceito de segurança digital aplicado em seu cotidiano, com uma internet razoavelmente boa e um dispositivo eletrônico, como computador, notebook ou tablet, estamos inseridos de maneira ativa ou semi ativa em toda a gama de circulação de dados na internet, e expostos a riscos.

A partir disso e concordando com Oliveira, Motta, Melo e Esteves (2020) podemos dizer que existem diversas realidades vivenciadas diariamente por essa grande massa da população, em que não só essas são as dificuldades encontradas, mas muitas outras e este é um dos maiores desafios dos órgãos públicos neste novo cenário tecnológico, equiparar todos os envolvidos em pé de igualdade no quesito segurança de dados, e estamos ainda muito longe de um cenário ideal, onde todos tenham uma consciência dos riscos que nosso dados estão correndo, e pretendemos verificar o quanto a nossa idade pode influenciar nessa conscientização, pois é premissa popular é que quanto mais velhos nós somos mais avessos a tecnologia nos tornamos.

RESULTADOS E DISCUSSÕES

Nesta seção serão abordados os resultados obtidos por intermédio do formulário aplicado a fim de realizar uma análise Quali-quantitativa, retomando a classificação da pesquisa, tratando-se do problema social denominado - a percepção do conceito de senhas seguranças em relação a idade, visando responder a questão principal de pesquisa que é entender se a faixa etária pode influenciar na geração de senhas.

Tabela 1. Definição da faixa etária dos respondentes

Questão	1. Por Favor informe sua faixa de idade	
	Quantidade de respostas	Representatividade (%)
16 - 24 Anos	43	26,9%
24 - 38 Anos	63	39,4%
38 - 55 Anos	40	25%
Mais de 55 Anos	14	8,8%
Total	160	100%

Fonte: Os autores (2021)

Como premissa tínhamos o objetivo de analisar a influência da idade nas decisões que dizem respeito a segurança da informação, aos nossos dados e as práticas seguras ou não que os indivíduos em questão estão relacionados, por outro lado a grande maioria dos entrevistados atingiu uma faixa etária próxima do que se considera nova geração, de 16 a 38 anos, totalizando 66,3 %, e uma outra parte acima de 38 anos totalizando 33,8% conforme demonstrado na **Tabela 1**, a partir da identificação de faixa etária dos respondentes, seguiremos buscando a relação de senhas seguras segundo a idade.

Tabela 2. Identificação dos dispositivos comumente utilizado

Questão	2. Qual dispositivo você mais utiliza?	
(respondentes com mais de uma opção)	Quantidade de respostas	Representatividade (%)
Celular	155	96,9%
Computador (Desktop)	30	18,8%
Notebook	79	49,4%
Tablet	4	2,5%
Total	268	167,6%

Fonte: Os autores (2021)

Na Tabela 2, temos a representatividade dos dispositivos móveis mais utilizados,essa realidade é reflexo do avanço exponencial da tecnologia, nos dias atuais onde a maioria dos brasileiros tem em suas mãos um smartphone, por onde se conecta a internet e grande parte de sua vida on-line é concretizada através do aparelho, as redes sociais são predominantes em nossas vidas, no cenário em que tudo acontece ou é influenciado por posts ou fatos vinculados nas mídias sociais, por isso os aparelhos celulares estão em constante risco no que se diz respeito a vulnerabilidades de informações, por seu uso constante e muitas vezes descuidado, os aparelhos celulares podem ser ferramentas utilizadas para vazamentos de contas, senhas e dados, e podem desencadear demasiado prejuízo aos usuários e as empresas, e em muitos casos o celular é a porta de entrada para os criminosos, uma tentativa válida mas não muito utilizada pelos usuários, para proteção de seus dados, é a autenticação de múltiplos fatores, onde é empregado mais de um fator de autenticação para proteção do dispositivo, além da senha, podemos utilizar pin de segurança, impressão digital, voz, entre outros, mas adesão desse método ainda não atinge a maioria dos entrevistados.

Tabela 3. Preferência de autenticação

Questão	**3. Qual o tipo de autenticação você prefere? Métodos de autenticação, em suma, são métodos utilizados para verificar a identidade do indivíduo que está buscando a informação, podem ser simples, 2 fatores ou multifatorial, podendo apresentar métodos como, senha, reconhecimento, facial, digital, voz, padrões gráficos, PIN,SMS, etc.**	
	Quantidade de respostas	**Representatividade (%)**
Fator Simples (Ex: Apenas senha)	**56**	**35%**
2 Fatores (Ex: Senha+PIN ou Senha+SMS)	**77**	**48,1%**
Multifatorial (Ex: Mais de dois fatores,utilização de biometria etc)	**27**	**16,9%**
Total	**160**	**100%**

Fonte: Os autores (2021)

Como podemos observar na **Tabela 3**, de preferência dos métodos de autenticação, o mais utilizado é o de dois fatores com 48,1%, método este que apresenta uma eficiência mediana na proteção dos dados e informações dos usuários.

Em seguida, temos a autenticação de fator simples com 35% sendo bastante utilizada pelos usuários, esta que utiliza apenas um método de autenticação que se apresenta com maior vulnerabilidade no quesito proteção dos nossos dados, por nos fornecer apenas uma barreira de proteção que pode ser quebrado através de força bruta,o que significa que um ataque desse tipo o atacante consegue a senha por tentativa e erro.

Por último, na última classificação temos o método considerado mais seguro - o multifatorial, escolhido por apenas 16,9% dos respondentes. Autores como Albertin e Moura (1998) mencionam que Sistemas biométricos que utilizam o elemento multifatorial em sua identificação de usuários podem ser considerados como “o nível mais seguro de autorização, envolvendo alguns aspectos únicos da pessoa, incluindo comparação de impressão digital, impressões da palma da mão, padrões de retina, verificação de assinatura e reconhecimento de voz “.

Apesar de ser o mais seguro e menos popular, a autenticação multifatorial é um método que provavelmente se apresenta de maneira mais complexa ao usuário, que supõe um difícil entendimento e manipulação deste fator de autenticação, podemos considerar, como já citado anteriormente nos resultados, que os métodos mais eficazes de autenticação tendem a ser os menos escolhidos pela falta de informação por parte dos usuários, que preferem os meios mais fáceis, que demandem menos atenção e empenho.

Um dos principais desafios de uma sociedade que se preocupa com a segurança dos dados é a conscientização de cada usuário, e o empoderamento digital é um desafio para os governos, empresas e sociedade em um quadro geral, com indivíduos tendendo a cada vez mais exposição e menos segurança, por isso devemos ter em mente que a mudança é cultural, comportamental, a nível coletivo e individual.

Tabela 4. Preferência de tipo de autenticação

Questão	4. Quais os tipos de autenticação que você mais utiliza?	
(respondentes com mais de uma opção)	Quantidade de respostas	Representatividade (%)
PIN	82	51,%
Impressão digital	115	79,9%
Padrão gráfico	28	17,5%
Reconhecimento Facial	34	21,3%
Localização geográfica	2	1,3%
Senha numérica	81	50,6%
Senha Alfanumérica	84	52,5%
Reconhecimento de voz	0	0%
Reconhecimento de íris	3	1,9%
SMS	50	31,3%
Envio de código de segurança	78	48,8%
Total	557	356,1%

Fonte: Os autores (2021)

Como em uma comunidade tecnológica cada dispositivo conectado na rede e a uma pessoa, tem que apresentar os meios mais eficientes de proteção, e como apresentado no **Tabela 4** acima, podemos encontrar a preferência dos usuários entrevistados quanto ao fator de autenticação mais utilizados; como mostrado anteriormente na **Tabela 2** o dispositivo mais utilizado é o celular, este gráfico apresenta tendência de utilização do método presente na maioria dos smartphones, o leitor de impressão digital, que se mostra o preferido entre os entrevistados, podemos considerar a facilidade de acesso e sua velocidade de resposta, como fatores principais para sua fácil e massiva aceitação, apesar de sua eficiência, se utilizado unicamente como autenticação podemos considerar de pouca efetividade em um cenário geral de proteção dos dados do usuário, portanto o mais indicado é

a combinação de fatores, tornando-os um conjunto, método de autenticação multifatorial, trazendo segurança as informações dos indivíduos, tendendo ao comportamento menos seguro os usuários se mostram favoráveis a práticas que consideram mais fáceis, como PIN e senhas comuns, e na maioria das vezes não utilizando a combinação dos fatores de autenticação.

Tabela 5. Aplicativos de suporte à autenticação

Questão	5. Você utiliza aplicativo de autenticação? Ex: GoogleAuthenticator, OktaVerify, VIP Access, etc.	
	Quantidade de respostas	Representatividade (%)
Sim	73	45,6%
Não	87	54,4%
Total	160	100%

Fonte: Os autores (2021)

Segundo respostas obtidas durante a questão 5 ilustradas na **Tabela 5**, observa-se que o uso de aplicativos de autenticação é crescente pois quase metade dos respondentes já conhecem algum tipo de aplicativo de autenticação e faz uso do mesmo, o que é um ponto positivo como suporte para a segurança da informação de senhas.

Tabela 6. Utilização de dispositivos de autenticação

Questão	6. Você utiliza algum gerenciador de senhas?	
	Quantidade de respostas	Representatividade (%)
Sim	46	28,7%
Não	114	71,3%
Total	160	100%

Fonte: Os autores (2021)

Apesar da **Tabela 5** nos mostrar que a adesão a outros mecanismos de apoio à autenticação estarem em uso, observa-se que na Tabela 6 ainda é desconhecido

ou não escolhido para utilização os gerenciadores de senhas, ou popularmente conhecido como cofres de senhas, aplicativos estes que quando bem gerenciados podem aumentar o nível de composição de suas senhas e aumento da segurança por não repetir e não utilizar dados comuns (nome, data de nascimento etc) em sua composição.

Tabela 7. Senhas em mais de um dispositivo

Questão	7. Você utiliza a mesma senha em mais de um aplicativo/dispositivo?	
	Quantidade de respostas	Representatividade (%)
Sim	134	83,8%
Não	26	16,2%
Total	160	100%

Fonte: Os autores (2021)

As senhas são os meios mais comuns de autenticação, e devem seguir os mais rigorosos critérios de elaboração, como recomendam bibliografia especializada, portanto deve-se levar em consideração diversidade de caracteres, caracteres especiais, mesclar números e letras e não utilizar a mesma senha em mais de um dispositivo ou conta.

A **Tabela 7** da pesquisa demonstra que a maioria dos respondentes não possuem boas práticas de utilizar senhas distintas em dispositivos ou contas colocando em risco a integridade de suas informações, expondo em muitos casos todos usuários que mantém algum tipo de contato com o indivíduo em questão, além de se tornar uma vulnerabilidade às empresas em que possa trabalhar .

Práticas como essa podem ter seus dados vazados ou seus dispositivos infectados, podendo servir como ferramenta para criminosos em invasões e ataques em massa, e ainda como trampolim ou meio de acesso a sistemas; ter uma senha bem elaborada muitas vezes pode dificultar a utilização de métodos maliciosos e força bruta no roubo de dados, mas são práticas seguras que podem de certa maneira gerar um desconforto aos usuários, referente a memorização de todas as suas senhas em diversos dispositivos e contas que possuem.

Tabela 8. Cruzamento da tabela 7 com a Tabela 1

Utilização de mesma senha em mais de um dispositivo vs idade			
	Não	Sim	Total
16 - 24 Anos	7	36	43
24 - 38 Anos	5	58	63
38 - 55 Anos	9	31	40
Mais de 55 Anos	5	9	14
Total	26	134	160

Fonte: Os autores (2021)

Corroborando esses dados em relação à faixa etária a **tabela 8,** mostra que ao contrário do que o senso comum pensaria, onde os respondentes acima dos 38 anos que apenas utilizam a mesma senha em diversos dispositivos, evidencia-se um problema que afeta a todas as faixas etárias, e que são necessários treinamentos e conscientização sobre boas práticas de segurança, para mitigar o risco de se tornarem vítimas de ataques cibernéticos.

Tabela 9. Frequência de atualização de senhas

Questão	8. Com que frequência você atualiza suas senhas?	
	Quantidade de respostas	Representatividade (%)
Mensalmente	16	10%
Semestralmente	30	18,7%
Anualmente	30	18,8%
Nunca atualizo	84	52,5%
Total	160	100%

Fonte: Os autores (2021)

Ainda no campo das senhas, outro ponto destacado em nossos estudos, mais uma prática recomendada para uma boa administração de senhas, mantendo

assim um ambiente seguro aos dados do usuário, é a atualização de suas senhas no menor período de tempo possível, baseando-se em experiências vivenciadas pelos algumas entidades obrigam seus usuários a atualizar trimestralmente suas senhas, outras empresas tendem a diminuir esse período de valia das senhas sem atualização, podendo chegar a um período de 30 dias.

Os dados encontrados na pesquisa divergem às premissas do estudo inicial, mostrando que apesar de termos uma maioria em uma faixa etária considerada jovem, o cuidado com as senhas não ocorre de maneira ideal, tendo a maior parte 52,5% de usuários que nunca atualizam suas senhas - **Tabela 9,** e grande maioria que utilizam a mesma senha em mais de um dispositivo - **Tabela 7**, formando assim uma combinação perigosa e nem um pouco recomendada, colocando seus dados em risco; e uma somatória de 28,7% em uma frequência teoricamente satisfatória de atualização de senhas, contando em um período mensal ou semestral.

Considerando a mesma pergunta com enfoque na idade - **Tabela 10**, destaca-se que todas as faixas apresentam falhas no quesito atualização de senhas. Neste ponto podemos considerar que a análise dos resultados é ainda mais alarmante, pois a premissa de que a idade mais avançada implicaria em uma não preocupação com a segurança dos dados, não refletiu totalmente na pesquisa, mostrando que uma grande parte do que se considera público jovem e habituado com a tecnologia, ainda não se deu conta da importância das práticas seguras no referente aos nossos dados e segurança digital conforme evidenciado na **Tabela 9** onde 84 respondentes (mais de 50%) não se preocupam com o quesito atualização periódica de senhas.

Tabela 10. Cruzamento da tabela 9 com a Tabela 1

Periodicidade de atualização de senhas vs idade					
	Anualmente	Mensalmente	Nunca atualiz	Semestralmente	Total gera
16 - 24 Anos	9	5	23	6	43
24 - 38 Anos	13	3	32	15	63
38 - 55 Anos	6	6	19	9	40
Mais de 55 Anos	2	2	10	0	14
Total	30	16	84	30	160

Fonte: Os autores (2021)

Mantendo-se no tema de boas práticas, a formação de senhas no esquema de autenticação baseado em conhecimento se relaciona ao tipo de dados que você utiliza em sua senha. Na **Tabela 11**, a maioria dos respondentes demonstraram utilizar dados sensíveis ou particulares, o que não é considerado uma boa prática devido sua baixa complexidade e vulnerabilidade.

Tabela 11. Senhas em mais de um dispositivo

Questão	9. Você utiliza dados comuns em suas senhas? Nomes, datas de aniversário, animais de estimação, preferências, telefone	
	Quantidade de respostas	Representatividade (%)
Sim	86	53,8%
Não	74	46,3%
Total	160	100%

Fonte: Os autores (2021)

Buscando detalhar um pouco a faixa etária sobre os tipos de dados que compõem as senhas dos entrevistados observa-se que a faixa etária mais vulnerável é acima de 55 anos pois utiliza dados do senso comum para desenvolver seus esquemas de autenticação baseados em conhecimento - **Tabela 12**

Tabela 12. Cruzamento da Tabela 11 com a Tabela 1

Utilização de dados comuns na elaboração de senhas vs idade			
	Não	Sim	Total
16 - 24 Anos	19	24	43
24 - 38 Anos	39	24	63
38 - 55 Anos	17	23	40
Mais de 55 Anos	11	3	14
Total	74	86	160

Fonte: Os autores (2021)

Por fim, observou-se na **Tabela 13** a experiência do usuário no quesito dificuldade em elaborar uma senha evidenciou-se que não repetir senhas (50,6%) e criar senhas fáceis de serem lembradas (43,1%) são os pontos principais de atenção. O empoderamento digital somado a gerenciadores de senhas mencionados na **Tabela 5** ou os aplicativos de autenticação **Tabela 6** poderiam ser uma opção para os usuários começarem a tratar melhor de seus dados.

Tabela 13. Dificuldade na elaboração das senhas

Questão	10.Qual sua maior dificuldade ao elaborar uma senha?	
(respondentes com mais de uma opção)	Quantidade de respostas	Representatividade (%)
Não relacionar à datas	30	18,8%
Não repetir uma senha já utilizada	81	50,6%
Utilizar caracteres especiais	44	27,5%
Fazer uma senha muito elaborada	56	35%
Fazer uma senha fácil de lembrar	69	43,1%
Total	280	175%

Fonte: Os autores (2021)

(2021) CONSIDERAÇÕES FINAIS

Podemos constatar que neste cenário analisado, apesar de estarmos ainda distantes do empoderamento digital e nos faltar quesitos de inclusão digital e infraestrutura tecnológica no país, a sociedade pode ainda não estar preparada para essa ruptura de paradigmas da forte implementação cultural de segurança da informação, tendo em vista a aplicabilidade das práticas de segurança de dados em todo e qualquer indivíduo.

Apesar de parecer ainda utópico esse comportamento nos usuários, também podemos trazer a esse debate toda a carga sociocultural de desigualdade que a muito se estabelece no país, e que tem impacto direto na educação e conscientização de todos.

O contexto apresentado neste artigo, nos faz refletir quanto aos nossos privilégios de acesso à informação, e tende a nos aproximar de uma realidade ainda incomum e distante de segurança da informação, onde a cultura de segurança é aplicada por cada indivíduo envolvido em toda a rede mundial de dados.

A mudança desse paradigma parece ser um processo lento e trabalhoso, passando por etapas de empoderamento digital e conscientização de Segurança da Informação, além de investimentos educacionais e um longo período de implementação independente da faixa etária.

Podemos em uma pequena amostra constatar que o comportamento seguro não se refletiu influenciado pela a idade dos entrevistados, mostrando que mesmo em meio ao público jovem a cultura de segurança da informação ainda está muito distante do ideal, o que pode ser considerado alarmante em um quadro geral de nossa sociedade, colocando em risco os usuários, e aumentando as ameaças aos nossos dados, esta pesquisa serve de base para novos estudos sobre a maturidade de segurança da informação no meio social.

REFERÊNCIAS

ALBERTIN, Alberto Luiz; MOURA, Rosa Maria de. **Comércio eletrônico: seus aspectos de segurança e privacidade.** Revista de Administração de Empresas, [S.L.], v. 38, n. 2, p. 49-61, jun. 1998. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0034-75901998000200006. Disponível em: https://rae.fgv.br/node/46121. Acessoem: 09 nov. 2021.

ARBULU, Rafael. **Senhas mais usadas em 2020 mostram pouca preocupação com segurança em Olhar Digital, 2020.** Disponível em https://olhardigital.com.br/2020/11/18/seguranca/senhas-mais-usadas-em-2020-mos tram-que-preocupacao-com-seguranca-aind/ Acesso em 18 mai 2021.

ESTES, Adam Clark. **O cara que inventou as senhas de computador acha que elas são um pesadelo em Gizmodo Brasil**, 2014. Disponível https://gizmodo.uol.com.br/o-cara-que-inventou-as-senhas-de-computador-acha-que -elas-sao-um-pesadelo/. Acesso em 17 mai 2021.

FIORESE, Mauricio. **Uma Proposta de Autenticação de Usuários para Ensino a Distância**. 200. 90 f. Tese (Doutorado) - Curso de Programa de Pós-Graduação em Computação, Ufrgs, Porto Alegre, 2000. Disponível em: http://penta.ufrgs.br/pesquisa/fiorese/. Acessoem: 17 out. 2021.

GOGONI, Ronaldo (ed.). **2019 comprova, de novo, que nunca usaremos senhas decentes: splashdata divulga lista com as senhas mais usadas e vazadas em 2019, que traz as mesmas suspeitas de sempre entre as campeãs.** 2019. Disponível em: https://tecnoblog.net/meiobit/415518/senhas-mais-vazadas-2019-splashdata/. Acesso em: 20 ago. 2021.

GUSMÃO, Gustavo. **"123456"foi a senha mais popular de 2014 em Exame.com tecnologia**, 2015. Disponível em https://exame.com/tecnologia/noticias-seguranca-123456-foi-a-senha-mais-popularh de-2014 Acesso em 17 mai 2021.

LAUREANO, Marcos Aurelio Pchek; MORAES, Paulo Eduardo Sobreira. **Segurança como estratégia de gestão da informação**. Revista Economia & Tecnologia, Curitiba, v. 8, n. 3, p. 38-44, 2005. Trimestral. Disponível em: http://www.mlaureano.org/projects/seguranca/economia_tecnologia_seguranca.pdf. Acesso em: 29 set. 2021.

MACEDO, Diego. **Técnicas para quebrar uma senha em Diego Macedo um pouco sobre TI ,** 2017. Disponível em https://www.diegomacedo.com.br/tecnicas-para-quebrar-uma-senha/ Acesso em 17 mai 2021.

MELO, Pedro Henrique Aparecido Damaso de. **Mecanismos de autenticação e controle de acesso para uma arquitetura de Internet do Futuro**. 2017. 102 f.

Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Uberlândia, Uberlândia, 2017. Disponível em: http://doi.org/10.14393/ufu.di.2017.320. Acessoem: 28/09/2021.

OLIVEIRA, Adriana Carla Silva de; MOTTA, Daniel Beltran; MELO, Josemar Henrique de; ESTEVES, Rita de Cássia São Paio de Azeredo. **Empoderamento digital, proteção de dados e LGPD.** Revista Pesquisa Brasileira em Ciência da Informação e Biblioteconomia, [s. l], v. 15, n. 3, p. 247-261, 13 ago. 2020. Trimestral. Disponível em: https://periodicos.ufpb.br/ojs/index.php/pbcib/article/view/54698. Acesso em: 09 nov. 2021.

PILAR DA SILVA, Denise Ranghetti; STEIN, Lilian Milnitsky. **Segurança da informação: uma reflexão sobre o componente humano.** Ciênc. cogn., Rio de Janeiro , v. 10, p. 46-53, mar. 2007 . Disponível em <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1806-5821200700010 0006&lng=pt&nrm=iso>. acessos em 24 set. 2021.

SAMARATI, Pierangela; VIMERCATI, Sabrina Capitani de. **Access Control: policies, models, and mechanisms. Foundations Of Security Analysis And Design**, [S.L.], p. 137-196, 2001. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/3-540-45608-2_3. Disponível em: https://link.springer.com/chapter/10.1007/3-540-45608-2_3. Acesso em: 29 set. 2021.

SILVA, Denise Ranghetti Pilar da. **A memória humana no uso de senhas**. 2007. 105 f. Tese (Doutorado) - Curso de Programa de Pós-Graduação em Psicologia, Faculdade de Psicologia, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2007. Disponível em: http://tede2.pucrs.br/tede2/handle/tede/957. Acesso em: 27 set. 2021.

Smith, R.E. (2002). **The strong password dilemma. Authentication: From Passwords to Public Keys.** Chapter 6. Addison-Wesley.

SOUZA, Marcos Tork. **Controle de Acesso para sistemas Distribuídos**. 2010. 96 f. Tese (Doutorado) - Curso de Engenharia da Computação, Departamento de Engenharia de Computação e Sistemas Digitais, Escola Politécnica da Universidade de São Paulo, São Paulo, 2010. Cap. 3. Disponível em: https://www.teses.usp.br/teses/disponiveis/3/3141/tde-23052011-111816/publico/Dissertacao_Marcos_Tork_Souza.pdf. Acesso em: 28 set. 2021.

ZIMMERMANN, Verena; GERBER, Nina. **The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. International Journal Of Human-Computer Studies**, [S.L.], v. 133, p. 26-44, jan. 2020. Elsevier BV.http://dx.doi.org/10.1016/j.ijhcs.2019.08.006.