INSTITUTO FEDERAL GOIANO - CAMPUS CERES

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DANYELLA SOUSA SILVA

ANÁLISE SOBRE HÁBITOS DE PADRÕES EM SENHAS

CERES- GO 2022

DANYELLA SOUSA SILVA

ANÁLISE SOBRE HÁBITOS DE PADRÕES EM SENHAS

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Sistemas de Informação pelo Instituto Federal Goiano Campus-Ceres, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação sob orientação do Prof. Me. Rangel Rigo e coorientação da Prof. Dr. Regina Paiva Melo Marin.

CERES - GO 2022

Sistema desenvolvido pelo ICMC/USP
Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas - Instituto Federal Goiano

Silva, DANYELLA SOUSA SILVA
SSI586a ANÁLISE SOBRE HÁBIITOS DE PADRÕES EM SENHAS / DANYELLA SOUSA SILVA Silva; orientador RANGEL RIGO; co-orientadora REGINA PAIVA. -- Ceres, 2022.
45 p.

TCC (Graduação em SISTEMAS DE INFORMAÇÃO) -- Instituto Federal Goiano, Campus Ceres, 2022.

1. SENHAS. I. RIGO, RANGEL , orient. II. PAIVA, REGINA , co-orient. III. Título.

Responsável: Johnathan Pereira Alves Diniz - Bibliotecário-Documentalista CRB-1 n°2376

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

ATA DE DEFESA DE TRABALHO DE CURSO

Aos vinte e quatro dias do mês de Junho do ano de dois mil e vinte dois, realizou-se a defesa de Trabalho de Curso da acadêmica Danyella Sousa Silva ,do curso de Bacharelado em Sistemas de Informação, matrícula 2018103202030428, cujo título é "ANÁLISE SOBRE HÁBITOS DE PADRÕES EM SENHAS". A defesa iniciou-se às 20 horas e 18 minutos, finalizando-se às 21 horas e 40 minutos. A banca examinadora considerou o trabalho APROVADO com média 9,1 no trabalho escrito, média 9,1 no trabalho oral, apresentando assim média aritmética final de 9,1 pontos, estando a estudante APTA para fins de conclusão do Trabalho de Curso.

Após atender às considerações da banca e respeitando o prazo disposto em calendário acadêmico, a estudante deverá fazer a submissão da versão corrigida em formato digital (.pdf) no Repositório Institucional do IF Goiano – RIIF, acompanhado do Termo Ciência e Autorização Eletrônico (TCAE), devidamente assinado pelo autor e orientador.

Os integrantes da banca examinadora assinam a presente.

Prof. Rangel Rigo
Presidente da Banca Examinadora - Orientador

André Sanzone Damaceno Rosa
Membro Externo da Banca Examinadora

Prof.ª Jaqueline Alves Ribeiro
Membro Interno da Banca Examinadora

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Documentos 153/2022 - GE-CE/DE-CE/CMPCE/IFGOIANO

Repositório Institucional do IF Goiano - RIIF Goiano

Sistema Integrado de Bibliotecas

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano, a disponibilizar gratuitamente o documento no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

Identificação da Produção Técnico-Científica

[ ] Tese	**[ ] Artigo Científico**
[ ] Dissertação	**[ ] Capítulo de Livro**
[ ] Monografia – Especialização	**[ ] Livro**
[X] TCC - Graduação	**[ ] Trabalho Apresentado em Evento**

[ ] Produto Técnico e Educacional - Tipo: _____

Nome Completo do Autor: DANYELLA SOUSA SILVA

Matrícula: 2018103202030428

Título do Trabalho: ANÁLISE SOBRE HÁBITOS DE PADRÕES EM SENHAS

Restrições de Acesso ao Documento

Documento confidencial: [X] Não [ ] Sim, justifique

Informe a data que poderá ser disponibilizado no RIIF Goiano:

O documento está sujeito a registro de patente? [ ] Sim [X] Não

O documento pode vir a ser publicado como livro?	[ ] Sim	[X] Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

A referida autora declara que:

1. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
2. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
3. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Ceres, Goiás, 30/06/2022.

(Assinado eletronicamente)

Danyella Sousa Silva

Assinatura da Autora e/ou Detentora dos Direitos Autorais

Ciente e de acordo:

(Assinado eletronicamente)

Rangel Rigo

Assinatura do orientador

Documento assinado eletronicamente por:

- **Danyella Sousa Silva**, **2018103202030428 - Discente**, em 30/06/2022 21:15:53.
- **Rangel Rigo**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 30/06/2022 20:53:09.

Este documento foi emitido pelo SUAP em 30/06/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 404078
Código de Autenticação: 9862bf10bb

Dedico esse trabalho à minha mãe Hildeci Sousa e a minha avó Isabel Maria, por serem o meu porto seguro e por me derem forças para conseguir vencer os obstáculos.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por ser o meu porto seguro e por me dá forças para conseguir vencer os obstáculos. Agradeço a minha mãe Hildeci, por todo amor, carinho é incentivo durante toda a minha trajetória. Sem ela nada disso seria possível. Agradeço minhas irmãs Kathlleen e Isabella Sousa, pelo companheirismo e apoio. Direciono também meus agradecimentos aos meus colegas de graduação que sempre me ajudaram quando mais precisei em especial aos meus amigos, Gustavo Faquim, Marcos Vinícius, Neide Rodrigues, Eloisa Carvalho, Geovanna Kerolyn, Ricardo Casagrande, Igor Gabriel e Bruna Carla pelos sinceros companheirismos durante todo período da minha vida acadêmica.

Meus sinceros agradecimentos ao Instituto Federal Goiano Campus Ceres, o qual obtive a grande oportunidade de ingressar em meados de 2017 no curso técnico de Informática no qual obtive conhecimentos sobre o mundo tecnológico e suas maravilhas despertando em mim o desejo em ingressar nessa graduação. Agradeço a todos os Doutores e Mestres em especial ao meu orientador Ms. Rangel Rigo que desde o tempo do curso técnico me apoiou nessa caminhada, agradeço a ele por todos os ensinamentos, conselhos e pela inabalável paciência comigo (Risos). À minha coorientadora Dr. Regina Paiva, por acreditar em mim é tornar possível a realização desde trabalho. O seu empenho foi essencial para a minha motivação, à medida que as dificuldades iam surgindo ao longo do percurso a senhora foi o combustível para mim não desisti. Sou grata a ti pelas valiosas é inabaláveis horas dedicadas ao meu projeto sempre com a presença cheia de otimismo.

A conclusão desde trabalho resume em dedicação que vi ao longo dos anos em cada um dos professores deste curso, a quem agradeço. Sou grata ao Professor Ronneesley Teles pelo o incentivo durante toda minha graduação, sua motivação foi essencial para conclusão da minha monografia. Ao também ao Professor Marcos por partilhar seus ensinamentos é sua dedicação ao extraordinário mundo do empreendedorismo. Seus valores passados a mim foram cruciais a minha formação pessoal é profissional! Gratidão a todos os docentes do IF Goiano que influenciaram na minha trajetória em especial a Dr. Jaqueline por todo carinho é dedicação ao nosso curso. E aos professores Rafael Feitosa,

Lucas Faria, André Nascente, ao Professor Roiter pelo compartilhamento de seu conhecimento em Segurança da Informação que foi de suma importância para desenvolvimento dessa dissertação. Grata ao Ms. Adriano Braga e a nossa querida" Tia Lu" a professora Luciene Andrade, por fazerem parte da minha formação. É claro meus agradecimentos também irão para o professor Dr. Matias Nol por ter me apresentado o extraordinário mundo da Ciência. Sou eternamente grata pela motivação à pesquisa que o senhor transmitiu a mim. Agradeço do fundo meu coração ao Campus Ceres por me acolher tão bem, durante todos esses anos, por ser minha segunda casa. Agradeço em nome da minha turma ao nosso Diretor Geral Cleiton Mateus por carinho e dedicação que teve com o nosso curso, como ele mesmo apelidou "o nosso caçulinha" do IF Goiano. Restará memórias eternas, de momentos felizes, de choros no corredor, frio na barriga sempre antes da prova (risos), dos eventos incríveis do campus, das reuniões nos quiosques com os colegas, das tensões de apresentar semanários especialmente de bancos de dados. Que foram fundamentais para minha desenvoltura disciplinar, Obrigada Professor Adriano! Sentirei saudades das aulas do senhor que sempre procrastinava para fazer chamada e eu quase perdia o ônibus (Momentos inesquecíveis da vida de um estudante.) e das aulas de lógica, o que dizer?! A inabalável paciência do nosso coordenador Rangel Rigo em ensinar passo a passo cada estrutura do código ou até em explicar cada laço das estruturas de repetição (risos), as aulas de redes então... "Inesquecíveis!" Gratidão Rangel! Ficará saudades em meu coração, mas, ao mesmo tempo um sentimento enorme de gratidão ao Campus Ceres. Obrigada IF Goiano! É por fim deixo registrado meus agradecimentos à minha família por todo apoio é a todas pessoas que torceram por mim e que contribuíram para conclusão desse curso.

A todos vocês, muito obrigada!

“Desenvolver força coragem e paz interior demanda tempo. Não espere resultados rápidos e imediatos, sob o pretexto de que decidiu mudar. Cada ação que você executa permiti que essa decisão se torne efetiva dentro do seu coração” Dalai Lama.

RESUMO

A senha tem sido uma abordagem predominante na autenticação de usuário em sistemas computacionais. Para combater as fraquezas na criação de senhas fracas, administradores e organizações, instituem uma política de senha. Contudo, algumas políticas de senha, embora resultem em senhas mais fortes, podem dificultar a memorização ou a digitação dessas senhas. O objetivo deste trabalho é avançar na compreensão dos fatores adotados pelos usuários na elaboração das senhas através de uma análise qualitativa referente aos hábitos e padrões utilizados. Através da metodologia *Survey* obteve-se que as senhas apresentam estreita correlação com as principais recomendações de uso e qualidade quanto ao tamanho e complexidade das senhas.

Palavras-Chave: Padrões, Senhas; Segurança da Informação; Ataques Cibernéticos.

ABSTRACT

Password has been a main approach to user authentication in computer systems. To combat weaknesses in creating weak passwords, administrators and organizations institute a password policy. However, some password policies, while resulting in stronger passwords, can make it difficult to remember or type these passwords. The working objective of this method is based on the understanding of the factors used by the users of a qualitative analysis regarding the habits and patterns used. Through the Survey methodology that as quality confirmed passwords with proven quality as the main use and regarding the and complexity of passwords.

Keywords: Password, Patterns; Information Security; Cyber Attacks.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

UEG	Universidade Estadual de Goiás
UFG	Universidade Federal de Goiás
DAC	Discretionory Access Control
RBAC	Role Based Access Control
MAC	Mandatory Access Control

SUMÁRIO

1. INTRODUÇÃO

Recentemente, a segurança da informação se tornou de grande importância para empresas que almejam a proteção de seus dados. Para garantir a proteção de dados as organizações geram suas próprias informações, tendo a segurança da informação a função de proteger os recursos de informação que possibilitam a organização atingir os seus objetivos, institucionais e de negócios. (FONTES,2015).

Diante disso, a segurança da informação tem sido fundamental na proteção de dados contra diferentes tipos de ameaças ao sistema, como ataques Cibernéticos. Visando garantir a integridade, disponibilidade e confidencialidade, as informações os dados devem ser sob uma política de segurança, evitando vazamentos de dados e fraudes.

> Para grande parte dos usuários, e até mesmo especialistas na área de segurança digital, a utilização de senhas sempre foi um fardo e, por conseguinte, sua importância muitas vezes é dirimida, possibilitando assim a instauração de brechas de segurança. Buscando resolver este problema, novas tecnologias vêem sendo desenvolvidas com a finalidade de sobre pujar as convencionais senhas [8-10]. Alguns exemplos são as chaves eletrônicas, métodos biométricos, métodos de autenticação por dois fatores, dentre outros. Entretanto, a utilização de senhas convencionais ainda é predominante, barata, simples, ubíqua e está sempre presente com o usuário, não necessitando que este carregue algum outro objeto [8].

É necessário pontuar o escândalo ocorrido com a plataforma Facebook, como vazamento de dados pessoais de seus usuários expostos em nuvem sem qualquer tipo de senha para acesso, em que as informações foram reveladas pela Empresa de Cibersegurança UpGuard. Em nota, o Facebook realizou a retirada de dados dos usuários dos servidores em nuvem da Amazon. (G1, 2019).

Sendo assim, é necessário ter mais cuidado com o uso de senhas em sistemas de informação. Contudo, senhas simples são mais fáceis de serem lembradas, porém a possibilidade de serem invadidas são maiores (CRANOR, 2014). Desta forma, para prevenir a divulgação de dados na Internet, é recomendável optar pelo uso de senhas digitais com criptografia de ponta a ponta, assim os ataques Cibernéticos possivelmente serão menos suscetíveis.

Atualmente com base em dados o Brasil tornou-se um alvo considerável na questão de crimes cibernéticos. Como por exemplo a violação de dados de sistemas de Órgãos Públicos nacionais como Tribunal da Justiça tiveram seus sistemas invadidos. Segundo alguns especialistas de Segurança Cibernéticas o vazamento de dados pode ser considerado o maior da história. Recorrentemente temos: “Mais de 8,4 bilhões de senhas foram espalhados na internet. Ao que tudo indica, um arquivo de texto de 100 GB foi compartilhado em fórum de hackers.” diz Alves (2021).

O caso foi chamado de Rock You 2021. Em referência ao incidente ocorrido em 2009 chamado Rock You, que expôs 32 milhões de senhas de acordo com site Cyber News, especializado em Cibe segurança. Inicialmente a pessoa que disponibilizou o documento no fórum informou que 82 bilhões de acessos constavam na base de dados, porém foram fixados 8,4 bilhões de dados, de acordo com o site a combinações de senhas tem entre seis e 20 caracteres sem espaço em branco e com exceção de ASCII (tipo de linguagem unificada para computadores. Os códigos de segurança teriam sido reunidos ao longo de anos combinado dados de vazamentos anteriores.

É de grande importância que esse trabalho seja utilizado como base de alerta contra os riscos que cibercriminosos causam a sociedade, uma vez que os mesmos conseguem construir uma espécie de “dicionário” de acessos com ajuda dos cruzamentos de informações a partir de outros bancos de dados vazados anteriormente. É notável que diversos usuários utilizam a mesma senha para acessar diversos serviços online. Se em algum momento essa cobrança ser espalhada pela internet com dados pessoais, abre se caminho para futuros golpes. Portanto, é fundamental alertar a sociedade que ao criar senhas sejam utilizadas combinações com números, caracteres, letras maiúsculas e minúsculas.

> “Segredos e códigos secretos existem desde os primórdios da humanidade. Há registros de escrita codificada já no Egito Antigo, datando de aproximadamente 1900 a.C. (Aranha, n.d.). Da mesma forma, as tentativas de decifrar tais códigos são provavelmente tão antigas quanto eles. Pode-se então dizer que, de certa forma, a SI sempre existiu, embora sua relevância tenha crescido ao longo do tempo, especialmente nos últimos anos. Hoje a Segurança da Informação se tornou um problema importante da sociedade moderna. Desde grandes empresas a indivíduos comuns, todos têm o direito de esperar que seus dados privados sejam mantidos intactos e disponibilizados apenas a pessoas autorizadas.”

O presente trabalho possui o objetivo de realizar pesquisas através de questionários para analisar a principal razão de pessoas se acomodarem a utilizar senhas fáceis e quais os princípios que as levam a utilizarem determinadas senhas e, o que pode ser feito e, as medidas necessárias para manter a segurança de seus dados. Portanto, neste trabalho iremos apresentar diversas soluções para proteger os usuários de ataques Cibernéticos pensando nisso, de acordo com o artigo publicado pela Revista Brasileira de Ensino de Física (2016):

> "A lei de Zipl é observada nas línguas naturais e por conseguinte, a entropia é reduzida quando as utilizamos ao criar uma senha. Muitas empresas utilizam a política de restringir o número de caracteres de uma senha." (ARAÚJO, SANSÃO, YEHIA 2015, p.1).

Em retorno algumas empresas de informática como Google, Microsoft, Facebook e Apple sucederam a flexibilidade mais acessível a criptografia de dados no armazenamento e transmissão. Esses sistemas aprovados são classificados como sistemas de criptografia civil amparado pela concepção de Kerchhofls em que a segurança necessita plenamente pela dimensão de espaço de carácteres o que é de suma importância para preservar a entropia e manter o sistema preservado. Em consideração os usuários são considerados a ligação fraca, pois os mesmos definir senhas simples e acessíveis. Portanto, é indispensável que os usuários sabiam elaborar senhas inacessíveis, robóticas para dificultar o acesso de ataques que buscam rompe-las. (ARAÚJO,

SANSÃO, YEHIA 2015).

Em uma entrevista Edward Snowden (2021) informa que ao contrário de empregar combinações de palavras, números e anagramas é preferível alterar o paradigma e passar utilizar passphrases, isto é, criar uma frase para ser utilizada como senha. Snowden disponibiliza como exemplo a Passphrase 'Margaret Thatcheris 100% SEXY'. Em outros termos, isto significa um prosseguimento de palavras gerando uma frase, porém não há a intenção que a senha seja formada por muitos caracteres visto que, haverá mais dificuldades em tempo gasto para digita-la a cada instante que for aplicada. Vários servidores estabelece um limite superior aos números de caráteres para uma senha ser utilizada.

No primeiro Dia Global da Criptografia realizado pela Global Encryption em 2021 Edward Snowden saí em defesa sobre o fortalecimento da criptografia e alerta para ameaças à essa tecnologia. E afirma que se a criptografia for enfraquecida pessoas morrerão.” O ex agente da (NSA) ressalta a importância da criptografia na sociedade garantindo a privacidade de bilhões de pessoas pelo o mundo.

Snowden destacou, o intuito para iluminar operações ilegais que acabam ocasionando empresas, governos e entidades mais vulneráveis a ataques cibernéticos. Presentemente o uso da criptografia que está sendo empregada em diversas áreas com o propósito de manter informações inumeráveis. Assim como, autoridades policiais que inclusive desfrutam do uso dessa inteligência para certificar que organizações criminosas tenham acesso a averiguações. Esse sistema de privacidade é adotado em atividades bancárias, rede sociais como, WhatsApp, Instagram, Facebook e Telegram garantido a preservação e segurança de todos os dados. (TERRA, 2021 online).

Em seu livro “Design of Everday Things" Donald (Normam 1990) relata o bloqueio da maior parte dos indivíduos em memorizar, senhas e códigos secretos. Entretanto nesse período tecnológico em que vivemos em abundância extensão de informações, essa solicitação por segurança digital tem se desenvolvido ao grande encargo de atribuições da utilidade de informações sigilosas não autorizadas. Desta forma, o uso de senhas habitual de restringir informações favoráveis contém, o duplo mundo oposto; tecnológico e humano que necessitam relacionar- se um com o outro. Da qual a comunicação tem concebido atrito. (SILVA; STEIN, p.47).

Nesse requisito, há apontamentos de registros da escrita codificada já no Egito Antigo datando sensivelmente, 1900 a.c. (Aranha, n.d). Por conseguintes tentativas de descodificar tais códigos são eventualmente provectos quando eles. Portanto, códigos secretos encontram-se a primícias da raça humana. Em vista disso, expõe dizer que a SI a todo momento esteve presente, mesmo que sua pertinência tenha se destacado nos últimos tempos.

1.1 OBETIVO GERAL

Este trabalho de conclusão de curso tem como objetivo geral a realização de um levantamento sobre os hábitos e padrões encontrados em senhas.

1.2 OBEETIVOS ESPECIFICOS

- Pesquisa bibliográfica da revisão da Literatura sobre o uso de senhas.
- Elaborar um questionário sobre padrões e hábitos identificados nas senhas.

2. REVISÃO DE LITERATURA

Em concordância com Manzeiro, 2019 a autenticação representa a identificação de inúmeras entidades de uma organização tecnológica, durante a autenticação o indivíduo empenha-se em obter acesso ao sistema e evidência que o próprio é de fato quem realmente declara ser. Para a autenticação são estabelecidas diversas técnicas que serão concedidas nesse tratado acadêmico. A autenticação é um método de averiguação de autenticidade de um indivíduo no sistema computacional. Em outros termos a autenticação é a verificação de informações relacionadas a entidade que sejam verídicas "Correspondem as informações do mundo real que elas representam, como a identidade de um usuário o construtor de um usuário de software a origem dos dados de uma página web" (Manzeiro, 2019, p.371).

A autenticação propõe-se em constatar o usuário para certificar que apenas o usuário registrado se usufruírem ao acesso do sistema. Em abundantes situações é indispensável constatar o sistema para o usuário especialmente em redes. Podemos considerar serviços bancários no qual, usuários obtém acessos ao sistema e deseja certifica se de fato e o estimado. Para evitar que seus dados bancários sejam despojados.

A autenticação por senha é algo acessível e vulnerável a ataques, resulta em armazenamento de senhas, "Pérvios" em bases de dados ou em arquivos no sistema. Eventualmente caso ocorra algum incidente com a base de dados ou arquivo, integralmente todas as senhas serão expostas. Para deter esse tipo de ameaça são utilizadas funções unidirecionais para armazenamento. A pluralidade dos sistemas operacionais emprega a técnica de autenticação SYK esteada em login/ senha.

"Na autenticação por senha o usuário informa ao sistema seu identificador de usuário (nome de login) e sua senha, que normalmente é uma sequência de caracteres memorizada por ele" (Manzeiro, 2019, p.373). Portanto, logo o sistema associa a senha alegada pelo usuário. Consequentemente confere com a senha previamente registrada no sistema. Afins, forem idênticos o acesso será autorizado. De fato, uma oposição marcante

pertinente a autenticação por senhas consiste, na ameaça de furtos a senhas. Em função disso, em uma contingência o repasse será capaz de manipular durante o tempo em que a furta. Por consequência disso, o criminoso terá posse dessa informação e substituí-la essa mesma senha.

> Para evitar esse problema, são propostas técnicas de senhas descartáveis (OTP- One- Time Passwords). Como o nome diz, uma senha descartável só pode ser usada a uma única vez, perdendo sua validade após o uso. O usuário deve então ter em maior uma lista de senhas predefinidas, ou uma forma de gera-las quando for necessário. (MANZEIRO, 2019, p.374).

As estratégias de autenticação estão divididas em três categorias: mecanismos que utilizam o que usuário sabe, que utilizam o que usuário possui e que utilizam o que o usuário é. Os mecanismos que utilizam o que usuário sabe é uma técnica de autenticação que se refere a algo conhecido como o próprio nome diz, a mesma é baseada em informações; como por exemplo, nome, login e senha. Nesse contexto as técnicas de autenticação são enfraquecidas. Visto que as averiguações básicas para o uso da autenticação podem ser informadas por qualquer outro indivíduo. (MANZEIRO, 2019).

A segunda técnica de autenticação utiliza mecanismos que utilizam o que usuário possui. Estas táticas são fundadas por meio de retenção de posse de uma determinada informação, tendo como por exemplo; uma chave criptográfica ou até mesmo um certificado digital, entre outros meios de autenticação apesar, de serem mais resistentes essas técnicas apresentam suas imperfeições, pois dispositivos matérias podem serem furtados.

É por fim temos a técnica que utilizam o que o usuário é. Nesse processo concentra as características relacionadas aos indivíduos, entre esses atributos expomo-nos dados biométricos, padrões de ires, impressões digitais...entre outras talantes do usuário. Consequentemente são consideradas técnicas melindrosas com extrema complexidade para o uso de implementação tendo em vista, de serem eventualmente mais resistentes que seus antecedentes. Portanto, diversos sistemas constituem apenas a autenticação por login/ senha.

Diante disso, sistemas mais vigentes obtém amparos a técnicas SYK por meio de Smartcards ou técnicas com o uso da SYA utilizando sensores para acionar impressão

digital, biometria ou HTTP e SSH respectivos serviços de redes. Por esse motivo Sistemas Tecnológicos com vigorosos quesitos de preservação de dados obtém alto escalão, sua segurança devido ao uso de diversas técnicas de autenticação preservando assim, sua integridade. Perante à isso, é possível acionar o uso de autenticação por meio de certificados digitais ou por intermédio de endereços IPS de usuários.

Para Manzeiro (2019) O Multifator tal como o sistema militar podem reivindicar o acesso aos seus indivíduos através de senhas e reconhecimento de ires imposto por eles. Em contrapartida um sistema Bancário solicita, a senha e o cartão remetido pelo o mesmo. Além disso, essas técnicas são operadas de forma sucessiva. Dessa forma a autenticação básica é gerada para o indivíduo obter acesso ao sistema e realizar todas atividades do sistema, como visualizar o saldo bancário de sua conta. Entretanto, se houver solicitações de outros serviços bancários pelo usuário o sistema requeri o uso de demais autenticações, empregando outras técnicas para realização de diversas atividades exigidas pelo o usuário, como transferência bancária.

Segundo Roccia (2021) autenticadores possuem sistemas normalmente apresentam contas divergentes com antelações e favorecimentos. O admins contará com o acesso excessivo aos dados que serão associados à um usuário habitual. Algumas informações serão limitadas ao titular da conta. Dessa forma, os dados não serão expostos com finalidade para que essas anelações se tornem superiores em um sistema, é indispensável um ou mais autenticadores com o destino ao reconhecimento do usuário com o intuito de aprovação do sistema para indicar suas autenticações. Perante ao exposto o” Segredo Memorizável “um método frequente de autenticação que coagir o usuário a intimar um segredo, um caminho chave utilizado para sua identificação.

> Mais amplamente utilizado a senha ou palavra-chave consiste num identificador composto por uma sequência de carácteres levando em conta letras minúsculas, minúsculas e dígitos por existem 56.800.235.584 possibilidades para uma senha padrão de 6 carácteres. Esse número aumenta para 735.091. 890.625. se contar com todos os 95 carácteres imprevisíveis ASCII. Apesar do grande número de combinações possíveis senhas são os maiores alvos de ataques, dificultando a criação de uma senha realmente segura. (ROCCIA, 2021, p.03).

Há possibilidades de a autenticação ser realizada através de um objeto ou instrumento que o usuário apresenta como uma declaração de identificação, empregando diversos recursos para serem manuseados como cartões, dispositivos de memória externa e até mesmo utilitários que possam restabelecer-se um token em virtude de armazenar determinada informação que reconheça em constante o usuário por procedimentos de palavras chaves ou dados biométricos do indivíduo.

Entre eles o Token é um procedimento frequente em gerar chaves temporárias com o intuito de substituição de senhas habituais de seus usuários. Esse processo impede ataques Cibernéticos em virtude que os tokens se esgotam previamente de serem decifrados. Apesar disso o dispositivo token pode ser furtado mesmo sendo um sistema resguardando. Um valoroso método de autenticação e o armazenamento em senhas, que corresponde armazenar senhas em formas de texto, inserido em bases de dados. Entretanto, se qualquer indivíduo obter acesso a essas informações e todas senhas serão a teorizadas, danificado a privacidade de seus usuários. (ROCCIA,2021).

Melo (2017) Diversos problemas de segurança vêm surgindo após a ubriquidade dos sistemas computacionais, iniciando como furtos de senhas e até mesmo identidades, no qual assaltantes se apresentam como usuários autênticos, ponderando- se de seus atributos de acessos. Por consequência dessas interrupções de serviços, houve a inevitabilidade de mecanismo de autenticação para verificação de autenticidade de usuários, sistemas e processos. Esses mecanismos de autenticação são classificados em três paradigmas: Conhecimento, Propriedades e Características.

O Conhecimento ampara pela individualidade que a entidade possui sobre determinado domínio de patente. Já as Propriedades de autenticação são as posses exclusivas sobre algo. E por fim temos, as Características de autenticação que são características comportamentais próprias, físicas humanas. Portanto, autenticar é estabelecer que uma entidade seja a mesma. (BURROWS; ABADI; NEEDHAM, 1989).

Diante das contribuições de Lamport (1981) Um dos mecanismos mais empreguem são as senhas, baseando em um dos exemplos de autenticação, esteado por conhecimento esses mecanismos, dispõe certas imperfeições, como furtos de senhas ou até serem esquecidas ou adivinhas. Para alguns exemplos de autenticação podemos mencionar, Smartcard que são cartões inteligentes, chaves e até mesmo o Token que é

um modelo de autenticação concentrados em propriedade, apresentando- se desvantagens e contingências de perca e furto de um dispositivo. (HWANG; LJ, 2000).

Para um excelente exemplo de autenticação podemos ilustrar a biometria em uma característica física, na qual o usuário esteja presente no local de autenticação. (WAYMAN et.., 2005). Já a autenticação de um processo, usuário ou sistema uma função crucial para o mecanismo de controle, em razão as suas execuções serem executadas nas entidades autênticas. Para o gerenciamento de informações é necessário um sistema de controle de acesso que mantém requisitos notórios, para a proteção de dados, no qual obtém mecanismo com finalidade em objeções a divulgações não autorizadas, em luta com as modificações não conceituadas. Por efeito dessas ameaças surgiu, uma grande necessidade da existência de um mecanismo de segurança, para garantir a aplicação do controle de acesso. De uma forma conceituada, assegurando apenas acessos autorizados. (SANDHU; SAMARATI, 1994).

Em vista disso, o Controle de Acesso é o mecanismo executor, responsável por todas as ações que asseguram penosamente apenas, identidades habilitadas e empreguem aos seus recursos favorecidos. Portanto, o controle de acesso mantém esse processo de autorização para avaliar as entidades cabíveis ao sistema, ou seja, entidades que possuem autorizações para acesso de informações, recursos e dados do sistema. Com ausência dessas ações não seria possível a existência dessas entidades. Desta forma, não haveria nenhum tipo de privacidade, sendo possível o acesso de qualquer tipo de informações. (SANDHU; SAMARATI, 1994). É necessário ressaltar a autenticação com o objetivo de certificar as entidades que se identificam, dispondo assim acessos locais Informações, entre outros recursos que se disponibilizam. Dando importância a mais um adicional, atribuindo ao Controle de Acesso, dessa maneira nem todos os usuários autenticados terão autorização para o acesso.

> Mesmo com a definição de políticas de controle de acesso, implementar tal mecanismo está longe de ser um processo trivial. Uma das grandes dificuldades está na interpretação de políticas de segurança do mundo real, muitas vezes complexas e ambíguas, e na sua tradução em regras bem definidas, claras e não ambíguas que possam ser aplicadas em um sistema distribuído, muitas situações do mundo real tem políticas complexas, onde as decisões de acesso dependem da aplicação de diferentes regras que vêm, por

> exemplo, de leis, práticas e regulamentos organizacionais. (MELO, 2017, p.31).

As políticas de controle podem ser classificadas em 3 três categorias entre elas as políticas DAC. Essa política de DAC efetua o comando de acesso, manuseado pelas entidades da entidade e determinações de acesso, com essa categoria é possível identificar se as entidades obtêm autorizações estipuladas para o uso de determinados recursos. A política MAC determina e induz o acesso por regulamentos impostos por superioridades, centrais. A política de RBAC determina o acesso de determinadas funções do sistema. As quais os usuários possuem credibilidade no sistema. Desta forma, é possível perceber quais autorizações que os usuários obtêm diante das regras do sistema e quais ações são permitidas aos usuários. (SAMARATI; VIMERCATI, 2000). Por conseguinte, essas três políticas são incorporadas dessa maneira, DAC (Discretionory Access Control), MAC (Mandatory Access Control), e a RBAC (Role-Based Access Control.) (SAMARATI; VIMERCATI, 2000).

De acordo com Melo (2017, p.31). “Tanto a autenticação quanto o controle de acesso foram adicionados como uma sobreposição na arquitetura atual, em vez de ser uma parte intrínseca da arquitetura. Sendo assim esse é um dos objetivos a serem alcançados dá por novas arquiteturas de internet do Futuro.”

Julio (2021) “Todos os anos, a desenvolvedora de softwares de segurança Nord Pass divulga as senhas mais utilizadas pelos usuários em todo o mundo” No ano de 2021 o índice apontou mais de 200 senhas triviais que empregaram com sequências maus notórias possíveis nos últimos tempos, como senhas fáceis, simples e fracas, que utilizam com a grande facilidade de serem descobertas, pelo simples fato de serem óbvias. Sucedendo grandes possibilidades de seres violadas. “A lista global incluí variação de sequências numéricas mais comuns, assim como a famosa “qwerty" (nada, mais do que a sequência da primeira linha do teclado)” (JULIO, 2021). A seguir temos a Tabela 01 representando “As 10 senhas mais utilizadas no mundo em 2021”. E a segunda tabela representando, “As 10 senhas mais utilizadas no Brasil no ano de 2021”. Os dados de ambas as tabelas foram obtidos no site Nord Pass (2021).

Tabela 01. AS 10 Senhas mais utilizadas no mundo (2021)

As 10 senhas mais utilizadas no mundo (2021)	
1	123456
2	123456789
3	12345
4	qwerty
5	Password
6	12345678
7	111111
8	123123
9	1234567890
10	1234567

Fonte: Própria

Tabela 02. As 10 Senhas mais utilizadas no Brasil (2021)

As 10 senhas mais utilizadas Brasil (2021)	
1	123456
2	123456789
3	Brasil
4	12345
5	102030
6	Senha
7	12345678
8	1234
9	10203
10	123123

Fonte: Própria.

Em tese, a desenvolvedora de softwares de segurança NordPass ressalta, o grande risco de usar nomes pessoais, como senhas, login ou até mesmo nomes de time de futebol, como o famoso time Liverpool o mais empregue segundo o estudo. O alerta é válido também, para os usuários que utilizam nomes de veículos em suas senhas como o estiloso Porsche e a belíssima Ferrari. Até mesmo, nomes de bandas músicas são utilizados como senhas como o grupo musical OneDirection o mais aplicado. (JULIO, 2021).

Por ser tratar de um campo de estudo em desenvolvimento, em referência a uma avaliação efetuada pela equipe de pesquisa Scfety Detectives constituiu à posse de mais de 18 milhões de senhas para à análise das 20 senhas mais utilizadas e hackeadas, e presumíveis do mundo. Ao longo desse estudo foi apurado e averiguado mais de 18 milhões de senhas, cessando assim o resultado de 18.419.945 senhas, logo consequentemente 9 milhões de senhas resultaram, da comunidade mundial. Cerca de 9.056.593 senhas foram coletadas por diversos bancos de dados ao redor do mundo.

Esses excedentes nove milhões de senhas são peculiares à países como: EUA, Espanha, França, Rússia, Alemanha e Itália. Foram tratados de diversas perspectivas distintas para a análise e identificação de senhas mais e menos segura para cada nação. Para cada cada nação foi identificado, específicas referências culturais, os padrões de senhas mais utilizados e as vinte senhas mais empregues entre as trintas mais utilizadas. Na Tabela 03 é possível visualizar o “Top 30 MOST Used".

Tabela 03. As 30 senhas mais utilizadas mundialmente.

AS 30 senhas mais utilizadas mundialmente					
1	123456	**11**	abc123	**21**	princess
2	Password	**12**	1234	**22**	letmein
3	123456789	**13**	password 1	**23**	65432
4	12345	**14**	Iloveyou	**24**	monkey
5	12345678	**15**	1q2w3e4r	**25**	27653
6	Qwerty	**16**	000000	**26**	1qaz2wsx
7	1234567	**17**	qwerty123	**27**	12321
8	111111	**18**	3aq12wsx	**28**	qwertyuiop
9	1234567890	**19**	Dragon	**29**	Superman
10	123123	**20**	Sunshine	**30**	asdfghjkl

Fonte: Própria (2022), com dados de <https://pt.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world-pt/>

“Os dados usados neste relatório foram de reunidos de vários vazamentos encontrados de fóruns de hacking, marketplaces e sites da dark web geralmente vendidos com baús do tesouro cheios de informações sensíveis par criminosos” (MARIANO, 2021).

Portanto, é frisado nessa pesquisa os padrões de senhas mais comuns, o qual se destaca são os padrões numéricos, que são os prediletos mundialmente. Possuindo uma concepção memorável, tornando assim uma senha fácil de ser violada, dessa forma podemos mencionar os padrões numéricos crescentes como exemplo 123456, ou constantes, como: 111 111 que foram avaliados em 8 das dominantes e 13 das 30 senhas mais aplicadas no mundo segunda a pesquisa.

Desde de 1997, o Centro de Estudo CERT.br realizou a íntegra de Cartilha de Segurança para internet com o intuito de promover recomendações aos usuários de internet, com o objetivo de aumentar a segurança e proteção dos indivíduos a possíveis ameaças aos seus sistemas. Através de contas e senhas os sistemas são capazes de identificar quem é o usuário, compreendo assim a identidade do usuário. É definindo as ações que o mesmo será autorizado a realizar. (CERT.br,2020).

> A sua conta de usuário em um determinado sistema normalmente é de conhecimento público, já que é por meio delas que as pessoas e serviços conseguem identificar quem você é desta forma, proteger sua senha é essencial para se prevenir dos riscos envolvidos no uso da internet, pois o segredo dela que garante a sua identidade, ou seja que você é o dono da sua conta de usuário. (CERT.br,2020).

Se por aventura outro indivíduo obter acesso a sua conta usuário, e apossa-se de sua identidade será possível realizar ações em seu nome, via internet. Desta forma, podemos informar algumas ações que poderia ocorrer nesse tipo de situação, entra são:

- Quando são empregues em sites falsos (phishing).
- Quando são empregues em dispositivos infectados.
- Quando são empregues em computadores violados.

- Quando são capturados em quanto trafegam em rede.
- Quando são por tentativas de adivinha mento.
- Quando há acesso de arquivos os quais foram armazenados.
- Quando há o uso de técnicas de Engenharia Social.
- Quando há a observação dos cliques do mause nos teclados virtuais ou movimentação dos dedos no teclado. (CERT.br,2020).

Além disso, o estudo ainda ressalta a sensatez para práticas em elaboração de senhas, como:

- Empregue números aleatórios.
- Apodere-se uma grande quantidade de caracteres.
- Recorra diferentes tipos de caracteres.

Sejam sempre prudentes ao uso de senhas:

- Não evidencie suas senhas em hipótese alguma.
- Detenha armazenar senhas em
- navegadores web.
- Verifique as conexões empreguem em suas senhas, ateste que sejam seguras.
- Poupe utilizar senhas em dispositivos de terceiros.

Obtenha o armazenamento de suas senhas desta maneira:

- Sempre armazene senhas em arquivos criptografados.
- Senhas grave senhas em locais persistentes. (CERT.br, 2020).

Para a elaboração de senhas é aconselhado, “A frase “O cravo brigou com a Rosa debaixo de uma sacada" você pode gerar a senha “? OCbcaRddus”. Entre inúmeras orientações para a formação de senhas, seja sempre criativo. (CERT.br,2020).

A seguir temos disponível a Tabela 04 que ressalta os principais riscos que o usuário poderá debilitar em suas senhas com dados do centro de pesquisa, CERT.br (2020).

Tabela 04. Preservação de Identidade do Usuário.

PRESERVAÇÃO DE IDENTIDADE DO USUÁRIO				
Acessar sua conta de correio Eletrônico.	**Acessar o seu Computador.**	**Acessar redes sociais.**	**Acessar sua conta bancária.**	**Acessar seu site de comércio eletrônico.**
Ler (ou apagar seus e-mails.)	Apagar seus arquivos e obter informações sensíveis, inclusive outras senhas	Denegrir a sua imagem e explorar a confiança de seus amigos/ seguidores	Verificar seu extrato e seu saldo bancário.	Alterar informações de cadastro.
Furtar sua lista de contatos e enviar e-mails em seu nome.	Instalar códigos e serviços maliciosos.	Enviar mensagens de spam, contendo boatos ou códigos maliciosos.		Fazer compras em seu nome e verificar informações sobre suas compras anteriores
Enviar mensagens d spam e (conter o phishing u códigos maliciosos. e	Usá-lo para desferir ataques contra outros computadores.	Alterar as configurações feita por você tornando públicas informações que eram privadas		
Pedir o reenvio de senhas de outras contas (e assim, conseguir o acesso a elas.)		Trocar sua senha dificultando que você acesse novamente.		
Trocar sua senha dificultando, que você acesse sua conta.				

Fonte: Própria (2022)

Pensando nisso, foi criado um dia especialmente para a comemoração de senhas, segundo site Rio Preto News:

> O dia 5 de maio é comemorado o Dia Mundial da senha. A data foi criada para colocar em discussão a segurança de contas, perfis e cadastros virtuais. Um dos problemas mais decorrentes relacionados com a segurança na internet é o vazamento de dados e, com a adesão do trabalho híbrido, o assunto se torna ainda mais relevante para a população. De com relatório divulgado pela NordPass, um dos principais serviços para gerenciamento de senhas, mais de 125 milhões de senhas credenciais de cidadãos brasileiros foram vazadas somente em 2021. (RIO PRETO NEWES,2022).

Para contribuir com soluções para a sociedade, em parceria com o Docente Cristian Souza e o Consultor em Cyber Security, ambos da mesma instituição DARYUS de Ensino Superior Paulista relataram algumas sugestões para manter senhas seguras como: Ativar verificação em duas etapas, evitar salvamento em navegadores, Utilizar UPN ao se conectar em redes públicas ou desconhecidas, Ter cuidados com sites phishing, Evitar envios de senhas por e-mail ou massagens , Utilizar gerenciamento credenciais por meio de cofres de senhas, Verificação de informações que já apareceram em vazamentos de dados, Ter uma boa política de senhas, Empregar o uso de diferentes senhas para cada serviço, Não utilizar informações pessoais para gerar senhas. (RIO PRETO NEWES, 2022).

3 MATERIAIS E MÉTODOS

Após o levantamento bibliográfico, foi realizada uma pesquisa online, utilizou meto- dologia *Survey*. A ferramenta gratuita Google *Forms*, foi escolhida, pois se mostrou ser de fácil uso para criar pesquisas através do uso de formulários e se mostrou eficiente por permitir através de um link, uma divulgação rápida da pesquisa em vários meios de co- municação. Elaborou-se um questionário composto de 18 perguntas, as quais foram or- ganizadas em três grupos:

Quanto ao perfil – Caracterizar o perfil dos participantes;

Quanto a elaboração da senha - Estabelece as preferências dos participantes quanto as regras de criação de senhas;

Quanto aos Hábitos e Padrões em Senhas - Estabelece alguns padrões observados nas senhas

A realização desse levantamento será de forma qualitativa, através de repostas obtidas nos questionários realizados por acadêmicos do Instituto Federal Goiano Campus Ceres e seu corpo docente e demais indivíduos que se disponibilizaram a participar desse estudo. Para atingir os objetivos propostos, no dia 15 de fevereiro de 2022 foi expandido para demais universitários do estado de Goiás, o questionário de Análise Sobre Hábitos de Padrões em Senhas, para ingressos do curso de Direto da Faculdade Uni Evangélica campus Ceres e Rubiataba e para graduação de Engenharia Civil da mesma instituição campus Goianésia. No decorrer do mês de março foi ampliado para os estudantes(a) de Enfermagem da Universidade Estadual de Goiás, Polo Ceres. E para os discentes do Programa de Pós-graduação em Agronomia pela Universidade Federal de Goiás (UFG) Campus Samambaia. Com o intuito de obter feedbacks de indivíduos leigos como, universitários, docentes e demais civis, para a análises mais concretas em relação ao uso de Padrões em Senhas na sociedade brasileira e mundial. Para a divulgação desse instrumento de pesquisa foi indispensável, o uso de Mídias Sociais como, Facebook, Instagram, Whatzapp, LinkedIn e Telegram; para compor esse time de divulgação, empregamos correios eletrônicos (e-mails) acadêmicos e pessoais para maior exposição da tese. Esse instrumento foi primordial para exação dos dados e para acepção e perspectiva dos mesmos. Por meio deles, foi possível obter uma avalição vicinal a realidade que se estava explorada. Foram atribuídas 18 questões indagações ao

questionário, a seguir temos a visibilidade da amostra do inquérito da Análise e hábitos em senhas.

3.1. QUESTIONÁRIO DE ANÁLISE E HÁBITOS DE PADRÕES EM SENHAS

Você concorda em particular com esta pesquisa?

( ) Sim

( ) Não

1) Qual a sua faixa etária?

( ) 10 a 15 anos

( ) 15 a 20 anos

( ) 20 a 25 anos

( ) 25 a 30 anos

( ) 30 a 40 anos

( ) 40 a 50 anos

( ) Prefiro não responder

2) Você considera sua senha fácil de lembrar?

( ) Muito fácil

( ) Fácil

( ) Difícil

( ) Muito difícil

( ) Nunca me lembro

( ) Prefiro não responder

3) Sua senha se enquadra em alguma destas categorias?

( ) Esportes

( ) Sentimentos

( ) Família

( ) Animais de estimação

( ) Datas

( ) Prefiro não responder

4) Quantos caracteres você usa em senhas?

( ) 6 ou menos

( ) 7

( ) 8

( ) 9

( ) 10 ou mais

( ) Prefiro não responder

5) Sua senha possui caracteres especiais? Caso sim, quais?

( ) 1 caracteres

( ) 2 caracteres

( ) 3caracteres

Outros_____

6) Quantas letras maiúsculas existem na sua senha?

( ) 1

( ) 2

( ) 3

Outros_____

7) Quantas letras minúsculas existem na sua senha?

( ) 1letra minúscula

( ) 2 letra minúscula

( ) 3 letra minúscula

Outros_____

8) Quantos números existem na sua senha?

( ) 1

( ) 2

( ) 3

( ) 4

Outro_____

9) Você reutiliza a mesma senha em vários sites?

( ) Sim

( ) Não

10) Quantas senhas diferentes você utiliza?

( ) 2

( ) 3

( ) 4

( ) 5 ou mais

( ) Prefiro não responder

11) Você já teve alguma conta comprometida?

( ) Sim

( ) Não

( ) Prefiro não responder

12) Você usa datas comemorativas em suas senhas

( ) Sim

( ) Não

( ) Prefiro não responder

13) Você se preocupa com o quão forte ela será?

( ) Não me preocupo

( ) Não me preocupo, porém considero importante

( ) Me preocupo, porém não utilizo regras de criação de senhas

( ) Me preocupo e utilizo poucas regras de criação de senhas

( ) Me preocupo e utilizo várias regras de criação de senhas

( ) Prefiro não responder

14) Você se preocupa em criar uma senha fácil de memorizar e relembrar?

( ) Sim

( ) Não

( ) Prefiro não responder

15) Com qual periodicidade você altera sua(s) senha(s)?

( ) Nunca

( ) Semanalmente

( ) Mensalmente

( ) Semestralmente

( ) Anualmente

( ) Quando o sistema me obriga

16) Você se sente seguro(a) com a sua senha?

( ) Sim

( ) Não

( ) Prefiro não responder

17) Você possuiu facilidade em lembrar sua senha?

( ) Sim

( ) Não

( ) Prefiro não responder

18) Você ativa autenticação de dois ou mais fatores para proteger suas senhas?

( ) Sim

( ) Não

Com essas averiguações foi possível uma análise concreta dos dados através de ilustrações gráficas que foram geradas no decorrer do inquérito, tranando-se executável a visibilidade de inúmeras falhas cometidas por usuários colaboradores dessa pesquisa. Segundo Zimmer (2020) 90% das senhas são suscetíveis e podem ser exploradas tranquilamente, e para a preservação contra hackers é essencial não empregar a mesma senha em todas atividades possíveis do usuário o usuário deve verificar se todas senhas usadas no passado, foram senhas opostas das quais são usadas no momento.

> Considerando que a senha é o principal recurso para comprovar a autenticidade de um usuário é protegê-lo do acesso indevido em sistemas de bancos, perfis em redes sociais, contas de e-mails e tantos outros sistemas, é muito importante seguir algumas dicas e recomendações na criação e gerenciamento, a fim de criar senhas fortes e seguras e que não são descobertas tão facilmente. (ZIMMER,2020).

Zimmer (2020) Essas operações são capazes de ampliar a preservação das contas e sustentar a defesa de serem descobertas por hackers. Que infelizmente passam a se beneficiar desses dados.

4. RESULTADOS E DISCUSSÃO

Como resultado, foram obtidas mais de 113 respostas, sendo o período da coleta de dados realizada O período de coletas de dados foi realizado em fevereiro de 2022 até o início de abril de 2022 por acadêmicos, docentes federais, estaduais e de redes privadas nessa interpelação. É importante ressaltar que todos os participantes desta pesquisa cientificam aceitaram responder ao questionário.

4.1. QUANTO AO PERFIL DO PÚBLICO PARTICIPANTE

A primeira análise foi referente a faixa etária dos usuários colaboradores do questionário na qual 54% dos usuários possuem a faixa etária de 20 a 25 anos de idade e

27, 4% possuem de 15 a 25 anos de idade e 8% dos usuários possuem 25 a 30 anos de idade. Concluindo assim, que a maioria do público correspondente é de maioria jovem, 54% tem entre 20 a 25 anos.

4.2. QUANTO A FORMAÇÃO DAS SENHAS

Sobre ao uso de caracteres em senhas - 42, 5% dos usuários utilizam mais de 10 caracteres e 11, 5% utilizam 6 ou menos caracteres e 9,7% dos usuários afirmaram 9 caracteres e 33,6% dos usuários utilizam 8 caracteres em suas senhas. Concluindo que, a maioria dos respondentes usam mais de 8 caracteres na elaboração de senhas.

Sobre o uso de caracteres especiais - a maioria dos usuários utilizam o número "1" em senhas (40,2%) seguidos do número "2" com (19,6%) dos dados coletados e o número "3" com (11,6%). Já os sinais de pontuações como # (1,8%), @ (1,8%)! (1,8%), e * (1,8%) totalizam somente 7,2%. Portanto, os caracteres especiais mais usados são os números 1,2,3 em senhas.

Sobre quantidade em letras maiúsculas - 9,7% dos usuários possuem mais de 3 letras maiúsculas em suas senhas e 10,6% dos usuários possuem somente 2 letras maiúsculas em suas senhas. 63,7% dos usuários possuem somente 1 letra minúscula em senhas. Portanto, a maioria utiliza somente 1 letra maiúscula em senhas**.**

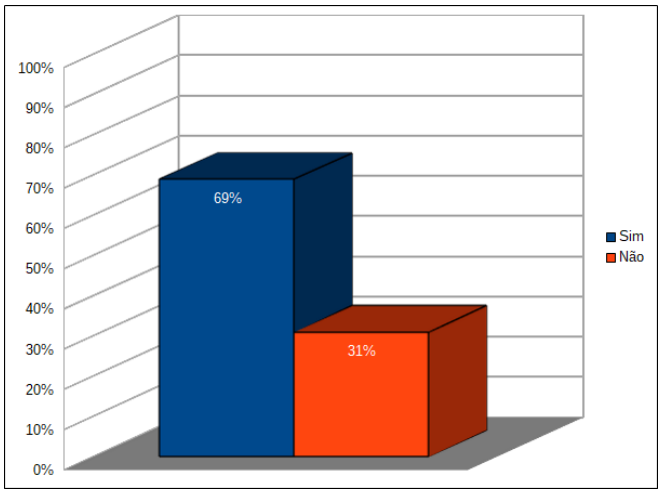
Sobre a quantidade de letras minúsculas - 11,7% dos usuários possuem 3 letras maiúsculas em senhas. Já 18,9% dos usuários preferiram não responder, 99% dos usuários possuem somente 1 letra e 33,3% dos usuários possuem mais de 3 letras minúsculas e 9% possuem uma quantidade maior de letras minúsculas. Portanto, a maioria usa 1 letras minúsculas nas senhas.

Sobre a quantidade de números - 9,9% dos usurários utilizam somente 1 número em suas senhas. E 33,3%dos usuários utilizam mais de 4 números em suas senhas e 11,7% dos usuários utilizam 3 números em senhas. 9% dos usuários usam mais 14 números em suas senhas. Cerca de 52,2% usam entre 2 a 3 números em senhas.

4.3 QUANTO AOS HÁBITOS E PADRÕES EM SENHAS

Sobre o reuso de senhas em sites diferentes - A figura 1 relata os gráficos com 69% dos usurários utilizam a mesma senha em diversos sites e 31% dos usuários não utilizam a mesma senha. Como relata o gráfico a seguir:

Figura 1- Sobre o reuso de senhas em sites diferentes



Fonte: Produzida pelo autor (2022).

Sobre a quantidade de senhas diferentes por usuário- 33,7% dos usuários utilizam 3 senhas diferentes. 31% utilizam 5 ou mais senhas diferentes. 17,7% dos usuários empregam 4 senhas diferentes e 15% dos usuários somente 2 senhas diferentes.

Sobre as contas comprometidas - Cerca de 24,8% dos usuários infelizmente relataram que sofreram com o comprometimento de suas contas. 70,8% dos usuários não houve nenhum comprometimento em suas contas.

Sobre o uso de datas comemorativas - 70,8% dos usuários não utilizam datas comemorativas em suas senhas, já 24,8% dos usuários empregam datas comemorativas em suas senhas.

Sobre a categoria das senhas - 9,7% dos usuários afirmaram que suas senhas se enquadram em relação à sentimentos. 29,2% dos usuários relataram que suas senhas pertencem ao grupo de dadas especiais. Por fim, 15% dos usuários marcaram a opção família.

DATAS > FAMÍLIA > SENTIMENTOS > ESPORTES

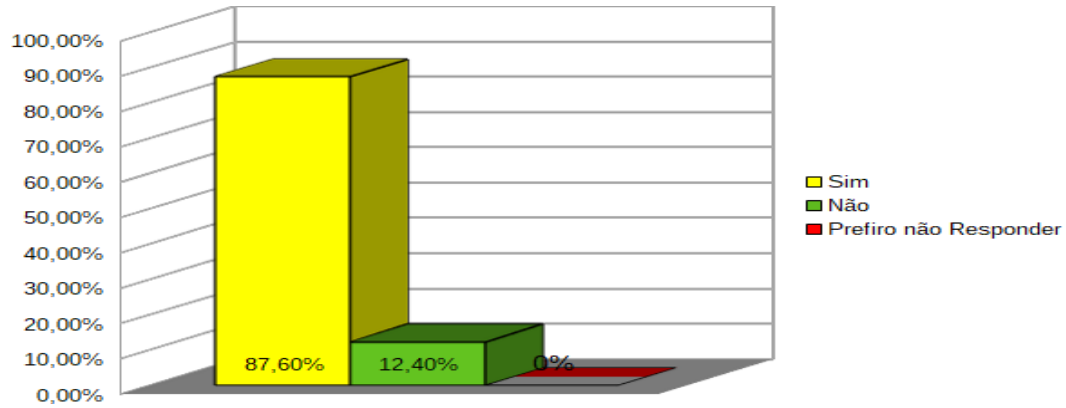
29,2% 15% 9,7% 5,3%

Sobre a preocupação dos usuários em relação à força de suas senhas - 30,1% dos usuários se preocupam e utilizam várias regras de criação de senhas e 8% dos usuários não se preocupam que as senhas sejam fortes. Por fim, 14,2% se preocupam, porém não utilizam regras de criação de senhas.

Sobre a memorização de senhas - 65, 5% dos usuários afirmaram que suas senhas são fáceis de memorizar, 13,3% dos usuários consideram muito fácil e somente 15 % dos usuários consideraram suas senhas difícil de lembrar.

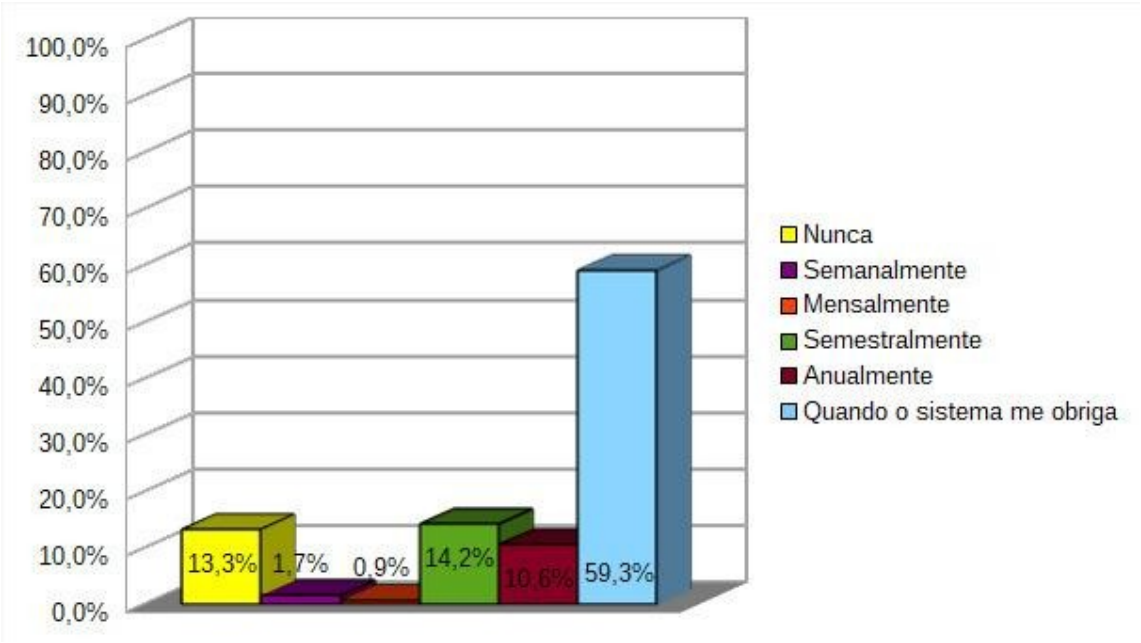
Sobre a preocupação de elaboração de senhas fáceis - 87,60% dos usuários se preocupam em criar senhas fáceis para memorizar e 12,40% não se preocupam em criar senhas fáceis, como relata a figura 2.

Figura 2 – Sobre a preocupação de elaboração de senhas fáceis.



Fonte: Produzida pelo autor (2022)

Figura 3 - Sobre a periodicidade de alteração de senhas



Fonte: Produzida pelo autor (2022).

Na figura 3 podemos observar, 59,3% dos usuários alteram suas senhas quando o sistema a obrigam. Porém, 13,3% dos usuários nunca trocaram de senhas. 14,2% dos usuários semestralmente trocam suas senhas. 0,9% dos usuários trocam mensalmente e 17% semanalmente e por fim 10,6% dos usuários trocam anualmente suas senhas.

Sobre a sensação de segurança do usuário referente à própria senha

79,6% dos usuários se sentem seguros com suas senhas e 16,8% não se sentem seguros com suas senhas

Sobre a Facilidades em lembrar senhas

68, 1% dos usuários relataram que utilizam autenticação de 2 fatores e 30,1% dos usuários colaboradores da pesquisa relataram que não utilizam esse sistema de segurança.

Sobre a Autenticação em dois fatores

68, 1 % dos usuários relataram que utilizam autenticação de 2 fatores e 30,1% dos usuários colaboradores da pesquisa relataram que não utilizam esse sistema de segurança.

5. CONSIDERAÇÕES FINAIS

O estudo constata à importância da análise e padrões de senhas em nosso cotidiano. Em conclusão, foi preconizado inúmeras maneiras de efetuar padrões em senhas, proposto em especial, à importância da privacidade.

A análise mostrou que as pessoas usam uma grande quantidade de caracteres sendo constituídos por diferentes tipos de caracteres tipos na elaboração de senhas, tais como números, e letras maiúsculas e minúsculas. Contudo, observou-se que o uso de sinais de pontuação quase não é usado, o poderia dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

Em virtude a grande falha cometida por inúmeros cidadãos que possuem hábitos de empregarem à exata senha em todos os serviços como, redes sociais, contas bancárias entre outros. Ocasionando conveniência e utilidade em reter memorização de sua senha. Porém, esse ato simboliza ameaça à segurança de seus dados, tornado possível ataques virtuais em seu meio. Desta forma, a avalição desse tratado propõe a conscientização para todos os usuários que almejam custódia aos seus dados.

6. REFERÊNCIAS

Araújo, Leonardo Carneiro de Sansão, João Pedro Hallack e Yehia, Hani Camille Influência da lei de Zipf na escolha de senhas. Revista Brasileira de Ensino de Física [online]. 2016, v. 38, n. 1 [Acessado 4 Agosto 2021] , 1313. Disponível em: <https://doi.org/10.1590/S1806-11173812125>. Epub 05 Abr 2016. ISSN

1806-9126. https://doi.org/10.1590/S1806-11173812125.

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=S1806-58212007000100006&lng=pt&nrm=iso>. acessos em 04 ago. 2021.

Ricardo, Rafaela. **3 dicas da Segurança** da **Informação para proteger seus dados**. Privacy Tech,2020 Disponível em< https://www.privacytech.com.br/destaque/3-dicas-de-seguranca-da-informacao-para-proteger-seus-dados.,378176.jhtml> Acesso em 04 de Agosto de 2021.

Inlearn. **4 Pilares da Segurança da Informação em empresas**. Inlearn Developin People, 2019. Disponível em<https://www.inlearn.com.br/seguranca-da-informacao-pilares/> Acesso em 01 de agosto de 2021.

Zeferino, Denis**. O que é informação e qual sua importância?** 2020. Disponível em <https://www.certifiquei.com.br/seguranca-informacao/> **Acesso** em 01 de agosto de 2021.

540 milhões de dados de usuários do Facebook ficam expostos em servidores da Amazon. G1, 2019.Disponível em<https://g1.globo.com/google/amp/economia/tecnologia/noticia/2019/04/04/dados-de-540-milhoes-de-usuarios-do-facebook-ficam-expostos-em-servidor.ghtml> Acesso em 01 de Agosto de 2021.

Cranor, lorrie. **Ted, 2014.** Disponível em<https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_w0rd/transcript> Acesso em 01 de Agosto de 2021.

Edison Fontes. **Segurança da Informação**. SCRIBD, 2015. Disponível em:https://pt.scribd.com/doc/271548416/Politicas-de-Seguranca-da-Informacao > Acessado em 30 de julho de 2021.

IGNACIO, Bruno Ignacio. **Edward Snowden alerta para ameaças a criptografia: "Pessoas morrerão ".** Terra, 2021. Disponível em:< https:// www. Terra.com.br/ Edward-Snowden-alerta-para-ameaças-a-criptografia-pessoas-morrerão > Acesso em 26 de outubro de 2021.

MANZEIRO, Sistemas Operacionais: **Conceitos e mecanismo. DINF-UFPR.** Curitiba, p.371,373, 2019. Disponível em: **http://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=socm:socm-livro.pdf**. Acesso em 23 de novembro de 2021

SILVA, D.; STEIN, l. M. **Segurança da Informação:** Uma reflexão sobre o componente humano. Ciências e Cognição, Rio Grande do Sul, vol. 10: 46-53, p. 52, 2007. Aceso em 07 de janeiro 2022.

ROCCIA, R. D. **Usuários respeitam as normas de criação de senhas seguras? Uma análise de data sites de senhas vazadas.** São Paulo, p. 2021. Acesso em 26 de janeiro 2022.

MELLO, P. H. **Mecanismos de autenticação e controle de acesso para uma arquitetura de acesso de Internet do Futuro.** Uberlândia, 2017. Acesso em 02 de fevereiro de 2022.

MARIANO, Michael. **A 20 senhas mais hackeadas do mundo: A sua está aqui?** SafetyDectives, c,2022. Disponível em: <pt.safetydetectives.com>. Acesso em 25, de março de 2022.

SAMARATI, P.; VIMERCATI, S. C. d. Acces Control: Policies, Modeles, and Mrchanisms. In: **Foundations of Security Analysis and Desig.** Springer, Berlin, Heidelberg, 2000. p.137-196. DOI: 10

1007/ 3-540-45608-2-3. Disponível em http://link.springer.com/artcle/10.1007/ s1224.3-009-0109-y.

SANDHU. R. S.; SAMARATI, P. Access control: principle and practice.. **IEEE communications magazine,** IEEE v.32, n.9, p.40-48, 1994.

JULIO, Clara. **Conheça as senhas mais usadas (e mais inseguras) de 2021.** Backup Garantido Proteção em Nuvem, 2021. Disponível em:<backupgarantindo.com.br> Acesso em: 04 de abril de 2021.

LAMPORT, L. Password authentication with insecure communication. **Communications of the ACM,** ACM, v.24, n.11, p.770-772, 1981.

CER.br. **Cartilha de Segurança para Internet.** FASCÍCULO SENHAS. Creative Commons 2020. Disponível em< cartilha.cert.br> Acesso em: 15 de abril de 2022.

WAYMAN, J. et al. Na introduction to biometria authentication systems [. S.I): Springer, 2005.

DIA MUNDIAL DA SENHA: 10 DICAS PARA CRIAR E MANTER A SENHA SEGURA. Rio Preto Newes, 2022. Disponível em<https://rpnews.com.br/noticia/22887/dia-mundial-da-senha-10-dicas-para-criar-e-manter-uma-senha-segura>. Acesso em 29 de abril de 2022.

ZIMMER, Kelvin. **Recomendações e dicas para criar senhas fortes e seguras.** Luniun Blog. 2020. Disponível em:< https://www.lumiun.com/blog/recomendacoes-e-dicas-para-criar-senhas-fortes-e-seguras/> Acesso em 28 de abril de 2022.

BURROWS, M.; ABADI, M.; NEE DHAM, R.M. A logic of authentication. In: THE ROYALSOCIETY. **Proceedings of the Royal Society of Lodon A: Mathematical, Physical and Engineering Sciences.**

[S.I], 1989.v.426, n.1871, p.233-271