ISSN: 2358-8829

IMPLEMENTAÇÃO DE CAMADAS DE SEGURANÇA NA PLATAFORMA DIGITAL ARTE DE CADERNO[1]

Cristhian Cintra Barbosa [2]
Douglas F. S. Nunes [3]
Giselle Cristina Cardoso [4]
Márcio Luis Bess[5]

RESUMO

Em um mundo digitalmente interconectado, é essencial assegurar a proteção das plataformas digitais. Nesse contexto, o estudo foca em proteger os dados críticos na plataforma web Arte de Caderno, seguindo as diretrizes da Lei Geral de Proteção dos Dados (LGPD). O projeto, desenvolvido no IFSULDEMINAS câmpus Poços de Caldas, foi criado para promover a manifestação artística dos alunos da rede pública de ensino, visando evitar a depredação de patrimônio público. Para tanto, promove concursos artísticos regularmente, recebendo, ao longo dos anos, centenas de desenhos de todas as localidades do país. A plataforma web veio para auxiliar com as dificuldades da gestão manual dos dados, surgindo, com ela, a necessidade de melhorar a segurança das suas informações. Foram adotadas várias medidas de segurança. O banco de dados, que anteriormente não apresentava criptografia ao armazenar senhas, agora conta com senhas dos usuários utilizando hash. Foi implementada a autenticação de dois fatores por código de e-mail, realizada no processo de login, além da implantação de tokens de acesso ao navegar pela plataforma, garantindo a maior autenticidade. Foram apresentadas orientações sobre como criar senhas mais seguras, a fim de evitar o acesso indevido a informações sensíveis. Ao adotar tais medidas, além de cumprir as orientações da LGPD, que informam sobre medidas de segurança técnicas e administrativas para proteger os dados pessoais de acessos não autorizados, foi possível aumentar a confiança do usuário. Este estudo destaca a importância de investir em segurança digital para proteger a privacidade dos usuários em plataformas digitais. Ele traz contribuições para tornar o projeto mais sólido, embasado em boas práticas de segurança. Isso assegura que o Arte de Caderno seja sempre um ambiente seguro para todos os artistas e usuários.

Palavras-chave: Segurança digital, Proteção de dados, Criptografia de senha.

---

[1] Projeto fomentado pelo EDITAL PROEX 22/2023 - APOIO A PROJETOS DE ARTE E CULTURA do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais - IFSULDEMINAS e realizado pelo Laboratório de Criatividade VOA IFSULDEMINAS campus Poços de Caldas.

[2]Bacharel em Engenharia de Computação pelo Instituto Federal do Sul de Minas Gerais, IFSULDEMINAS *campus* Poços de Caldas. Pós-graduando em Cibersegurança e Governança de Dados pela Pontifícia Universidade Católica de Minas Gerais, PUC Minas. cristhiancintra.profissional@gmail.com;

[3]Doutor em Ciências da Computação e Matemática Computacional pela Universidade de São Paulo, USP. douglas.nunes@ifsuldeminas.edu.br;

[4]Mestre em Engenharia Elétrica pela Universidade Estadual de Campinas, UNICAMP. giselle.cardoso@ifsuldeminas.edu.br;

[5]Doutor em Desenvolvimento Humano e Tecnologias pela Universidade Estadual Paulista Júlio de Mesquita Filho, UNESP. marcio.bess@ifsuldeminas.edu.br;

ISSN: 2358-8829

INTRODUÇÃO

A plataforma Arte de Caderno tem como objetivo modernizar e simplificar o processo de catalogar as manifestações artísticas de alunos da rede pública do país. O projeto, que foi idealizado pelo professor Márcio Luiz Bess[6], com apoio do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais, *campus* Poços de Caldas, consiste em evitar a vandalização de patrimônio público, sem coibir expressões artísticas. O projeto promove concursos artísticos e vem recebendo, ao longo dos anos, centenas de desenhos, de todas as localidades do país. As obras são submetidas a uma banca avaliadora, que classifica um quantitativo de artes que, então, seguem para votação popular. Ao final, as obras melhores classificadas são premiadas.

Os métodos de envio, recebimento, catalogação e julgamento das obras sempre foram realizados manualmente, com grande carga de trabalho aos envolvidos. Neste sentido, para aprimorar todos esses processos, surgiu a proposição de uma plataforma digital, que foi nomeada de Arte de Caderno.

Trazendo a essência do Arte de Caderno para o meio digital, foram acrescentadas novas responsabilidades, como a segurança e cuidado com os dados dos usuários mantidos pela plataforma. De acordo com a lei geral de proteção dos dados nº 13.709, de 14 de agosto de 2018, é de responsabilidade do controlador e operador de dados garantir a segurança de informações sensíveis provenientes dos usuários. Neste sentido, tornou-se fundamental o desenvolvimento do projeto retratado neste trabalho.

METODOLOGIA

Com base nos estudos e na compreensão da literatura, na Lei Geral de Proteção de Dados (LGPD) e nas cartilhas informativas do Governo Federal, mostrou-se necessária uma intervenção na plataforma digital Arte de Caderno, objetivando incorporar técnicas apropriadas para barrar e dificultar eventuais ações criminosas de acesso indevido aos dados pessoais armazenados nela.

A partir das etapas de elaboração, foi realizado o desenvolvimento do trabalho, para isso foi essencial seguir os procedimentos:

- Implementação da criptografia: nesta etapa, foi desenvolvido o algoritmo responsável pela criptografia das senhas cadastradas no banco, utilizando a

[6] Lattes: http://lattes.cnpq.br/2142214809343643

ISSN: 2358-8829

biblioteca crypto do Node.js. Este algoritmo é encarregado de criar a chave criptografada que foi utilizada para realizar a comparação da senha no processo de *login*, salvando-a junto com a senha, separadas pelo caractere ":" (dois pontos).

- Autenticação de dois fatores e recuperação de senha: com o auxílio da biblioteca nodemailer[7], responsável por enviar o e-mail para o usuário final mediante configuração, foi possível combinar essa biblioteca com a crypto para gerar uma sequência de caracteres que foi utilizada para a verificação da autenticidade do usuário ao efetuar uma tentativa de *login*. O mesmo princípio foi utilizado na criação da rota de troca de senhas, tornando possível gerar um novo código aleatório que é salvo para cada usuário ao solicitar a troca de senha. Mediante a resposta correta do código, é liberada ao usuário a opção de cadastrar uma nova senha na plataforma.

  Token de acesso: através da biblioteca jsonwebtoken[8], foi possível criar uma assinatura digital contendo os dados (ID, nome de usuário, e-mail e tipo de acesso) para cada usuário ao realizar o *login*. Essa assinatura é verificada pelo servidor a cada interação do usuário ao navegar pela plataforma, garantindo assim mais uma camada de verificação.

- Modelo de senha seguro: por meio da linguagem JavaScript e expressões regulares (um método para definir padrões de caracteres), foram estabelecidas barreiras para impedir que o usuário cadastre senhas consideradas fáceis de adivinhar. Ao modelar a quantidade de caracteres, símbolos e números, foi possível estabelecer um padrão de qualidade para as senhas geradas, dificultando assim a criação de palavras-chave comuns, curtas e de baixa complexidade.
- Conscientização do usuário final: conforme observado na literatura, a parte humana é considerada um dos pontos-chave ao tratar de segurança. Tendo em vista essa grande vulnerabilidade, foram desenvolvidas uma série de regras para facilitar ao usuário a gestão de suas informações sigilosas, desde a criação de palavras-chave de acesso até a forma como ele armazena esses dados e os

[7] ferramenta construída em TypeScript que roda com o NodeJS e permite o envio de e-mail com facilidade.
[8] É um padrão da Internet para a criação de dados com assinatura opcional e/ou criptografia cujo payload contém o JSON que afirma algum número de declarações.

ISSN: 2358-8829

compartilha com outras pessoas. Isso torna o usuário mais consciente de suas responsabilidades em relação à proteção de seus dados críticos.

REFERENCIAL TEÓRICO

Em um mundo conectado, a segurança da informação vem se tornando cada vez mais essencial para a garantia da privacidade e proteção dos dados de quem utiliza a internet. Os desafios aumentam a cada dia com novas tecnologias, surgindo novos métodos de burlar a segurança.

> A área de segurança de rede e de Internet consiste de medidas para desviar, prevenir, detectar e corrigir violações de segurança que envolvam a transmissão de informações. Essa é uma definição abrangente que envolve várias possibilidades.(STALLINGS, 2015, p.6)

Portanto, é de total importância uma plataforma digital, que possui dados críticos dos usuários, aplicar barreiras para que possam impedir e dificultar o acesso a essas informações por terceiros mal intencionados, assim como mostra a Lei Geral de Proteção de Dados Pessoais (LGPD):

> A LGPD introduz em seu art. 6o , VII, o Princípio da Segurança, que consiste na utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.(BRASIL,2018)

Visando manter o acesso restrito apenas a usuários credenciados, uma medida de autenticação aplicada diretamente à plataforma seria a autenticação de dois fatores, via SMS[9] ou e-mail como medida de proteção. Conforme recomendado no guia orientativo do governo federal, os usuários do sistema terão nível mínimo de acesso necessário para realizar suas atividades.

> A premissa que deve ser aplicada é a do princípio do menos privilégio (need to know), ou seja, os usuários de um sistema terão o menor nível de acesso necessário para a realização de suas atividades. Funções de alto nível, tais como as de administrador de sistema, devem ser restringidas apenas àqueles funcionários que necessitem exercer esse papel e sejam capazes de assumir essa responsabilidade (ANPD, 2021).

[9] *Short Message Service* – ou Serviço de Mensagens Curtas, em português.

ISSN: 2358-8829

Outra abordagem de segurança bastante comum para a proteção de senhas é por meio da tecnologia *hash*[10]. Com ela, as senhas dos usuários nunca são armazenadas no modo texto aberto[11], mas sim uma sequência de caracteres ininteligível gerados por essa tecnologia. Essa abordagem agrega uma camada de proteção, tendo em vista que, se o banco de dados por algum motivo for violado e seu conteúdo exposto na internet, os criminosos terão dificuldades em conseguir acesso aos dados abertos[12]. Stallings diz que:

> Funções de hash normalmente são usadas para criar um arquivo de senha de mão única. (...). Desse modo, a senha real não pode ser recuperada pelo hacker que conseguir acesso ao arquivo de senhas. De uma forma simples, quando o usuário informa uma senha, por verificação, o hash dela é comparado com o valor do hash armazenado. Esse método de proteção de senha é usado na maioria dos sistemas operacionais.(STALLINGS, 2015, p.251).

Buscando manter a integridade do sistema que trabalha com banco de dados, tem-se a necessidade de investir em medidas contra injeções SQL[13], pois, ao se perder controle do banco de dados, uma enorme quantidade de informações será exposta.

> O criminoso virtual explora uma vulnerabilidade, inserindo uma instrução SQL mal-intencionada em um campo de entrada. Mais uma vez, o sistema não filtra a entrada do usuário corretamente para os caracteres em uma instrução SQL. Os criminosos usam a injeção de SQL em sites ou qualquer banco SQL. As falhas de injeção, em banco de dados como SQL, OQ e LDAP, ocorrem quando dados não confiáveis são enviados para um intérprete como parte de um comando ou consulta. Os criminosos podem falsificar uma identidade, modificar os dados existentes, destruir os dados ou se tornar administradores do servidor do banco de dados.(SILVA, Michael Bernardo Fernandes, 2023, p.123).

Tratando-se de redes de computadores, os primeiros e principais alvos dos ataques de terceiros são os roteadores de borda, pois os mesmos atuam como controladores do fluxo de tráfego, tanto para dentro quanto para fora da rede. Estão no limite da rede interna, que podemos controlar, e a internet. Como diz Silva (2023).

Para realizar a proteção da rede, uma das mais eficazes e consolidadas técnicas é por meio do uso de *firewalls*, pois ajuda a impedir tráfego não autorizado para dentro de uma rede, evitando, assim, exposição a possíveis ataques. Rohling afirma:

---

[10] Algoritmo que mapeia dados de qualquer tamanho para dados de tamanho fixo. Aplicado para comparar dados secretos.

[11] Dados que são mantidos sem nenhuma forma de criptografia.

[12] Dados que em algum momento foram disponibilizados na internet sem autorização ou consentimento do proprietário.

[13] Tipo de ameaça de segurança que se aproveita de vulnerabilidades em sistemas que trabalham com bases de dados realizando ataques com comandos SQL.

ISSN: 2358-8829

> Além dos sistemas de IDS[14] e IPS[15], outro dispositivo amplamente utilizado na implementação das medidas de segurança de rede são os firewalls, cuja função básica é bloquear todo o tipo de tráfego que venha da rede externa (WAN) em direção à rede interna (LAN) e que não tenha sido solicitado por um dispositivo que esteja na rede interna. Portanto, o firewall deve estar posicionado na entrada da rede, entre a rede WAN e a rede LAN, de modo que todo o tráfego externo passe através dele.(ROHLING, Luis José, 2020, p.101).

Tendo em vista a importância de um *firewall*[16] bem configurado, Silva nos diz que:

> Existem vários benefícios do uso de um firewall em uma rede como impedir a exposição de hosts, recursos e aplicações sensíveis a usuários não confiáveis, pois o firewall bloqueia o recebimento de dados maliciosos em servidores e usuários da rede. Outra vantagem do firewall é a redução da complexidade do gerenciamento de segurança descarregando a maior parte do controle de acesso à rede para alguns firewalls na rede. Adicionalmente, eles sanitizam o fluxo do protocolo, o que impede a exploração de falhas no protocolo.(SILVA, Michael Bernardo Fernandes, 2023, p.147).

Mesmo com fortes camadas de proteção em um sistema, muitas vezes um invasor não precisa encontrar falhas no sistema. Apenas conseguir extrair informações críticas de um administrador de sistema já é suficiente para obter acesso indevido, como menciona Mann (2011), mostrando assim a relevância de uma boa instrução aos usuários de um sistema.

> Reunir um grupo de funcionários para uma sessão de treinamento presencial e interativa é uma das maneiras mais eficazes de desenvolver sua segurança da informação.(MANN, Ian, 2011, p.195).

Portanto, é importante o treinamento adequado para que os administradores de um sistema não favoreçam as técnicas de engenharia social, fornecendo a estranhos informações via telefone ou internet. Informações essas que irão colocar em risco a integridade de todo um sistema ou empresa, como aponta Galvão (2015).

Para desenvolver e aplicar as medidas necessárias vistas, fez-se uma codificação no *backend,* o qual foi desenvolvido em Node.js[17] e Express[18]. Visando testar a confiabilidade do sistema.

---

[14] Sistema que detecta e registra atividades suspeitas ou maliciosas na rede.
[15] Tem a capacidade de bloquear tráfego malicioso ou suspeito em tempo real. Ele monitora o tráfego de rede, assim como um IDS, mas também tem a capacidade de interromper a comunicação entre a fonte do ataque e o destino.
[16] Dispositivo de uma rede de computadores, na forma de um programa ou de equipamento físico, que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
[17] Node.js é uma plataforma de código aberto que irá permitir que o código JavaScript seja executado em várias plataformas usando o interpretador V8 do Google. Sua arquitetura é assíncrona e orientada a eventos.
[18] É uma estrutura de aplicativo da web minimalista e flexível do Node.js, oferece um conjunto sólido de recursos para o desenvolvimento de aplicativos web.

ISSN: 2358-8829

RESULTADOS E DISCUSSÃO

A partir das soluções apresentadas, foi possível chegar a uma aplicação com diversas camadas de segurança para garantir uma melhor proteção dos dados. De imediato, foi necessário partir para um *login* de 2 fatores na plataforma. O usuário informa o seu CPF e senha, e é verificado o tipo de acesso (aluno, professor ou avaliador). Então, uma função cria um código aleatório e envia para o e-mail do usuário.

Em paralelo, no banco de dados, são salvas 2 informações (*code2factor*, *createdAt*), sendo respectivamente o código de 2 fatores e a data em que foi criado, tendo em vista que o mesmo tem validade de 10 minutos (Figura 1).

Figura 1 - Dados do login no banco


```
_id: ObjectId('64dd5aef1159eb7cd5e0c472')
username: "33382727820"
password: "4dc3b7ad93239df857dd30154dcfd13e:86d4ac3b3471b170e3f622b0d5d3ba7612808…"
accessType: "professor"
code2factor: "B37ECDF1"
createdAt: 2023-09-08T20:53:44.862+00:00
email: "2testeartedecaderno@gmail.com"
```


Fonte: criada pelo autor

Para efetuar o *login*, o usuário precisa informar o código recebido dentro do prazo de validade e terá acesso autorizado à plataforma, recebendo um *token JWT* válido. O *token* opera como uma assinatura, contendo alguns dados criptografados do usuário, e atua como uma autorização para o mesmo poder navegar na plataforma.

Posteriormente, foi realizada a implementação da criptografia das senhas coletadas dos usuários, tendo em vista que as mesmas estavam sendo salvas no banco de dados de forma simples, sem nenhuma criptografia, criando uma brecha de segurança neste ponto. A técnica empregada foi o *hash com sal*[19], a qual envolve a geração de um código aleatório para ser usado na criptografia da senha fornecida pelo usuário. Este código é como uma chave de acesso, pois somente com ele é possível chegar ao mesmo resultado de criptografia utilizando a senha inicial. Logo após a criptografia da senha, esta é armazenada no banco de dados,

[19] O sal é uma string aleatória que é gerada e anexada à senha do usuário antes de passar pela função de hash. Tornando a hash de cada senha única.

ISSN: 2358-8829

juntamente com o código gerado, separados pelo caractere dois-pontos (:).O exemplo abaixo mostra uma palavra simples, somente com 9 caracteres, depois de passar pelo procedimento de criptografia.

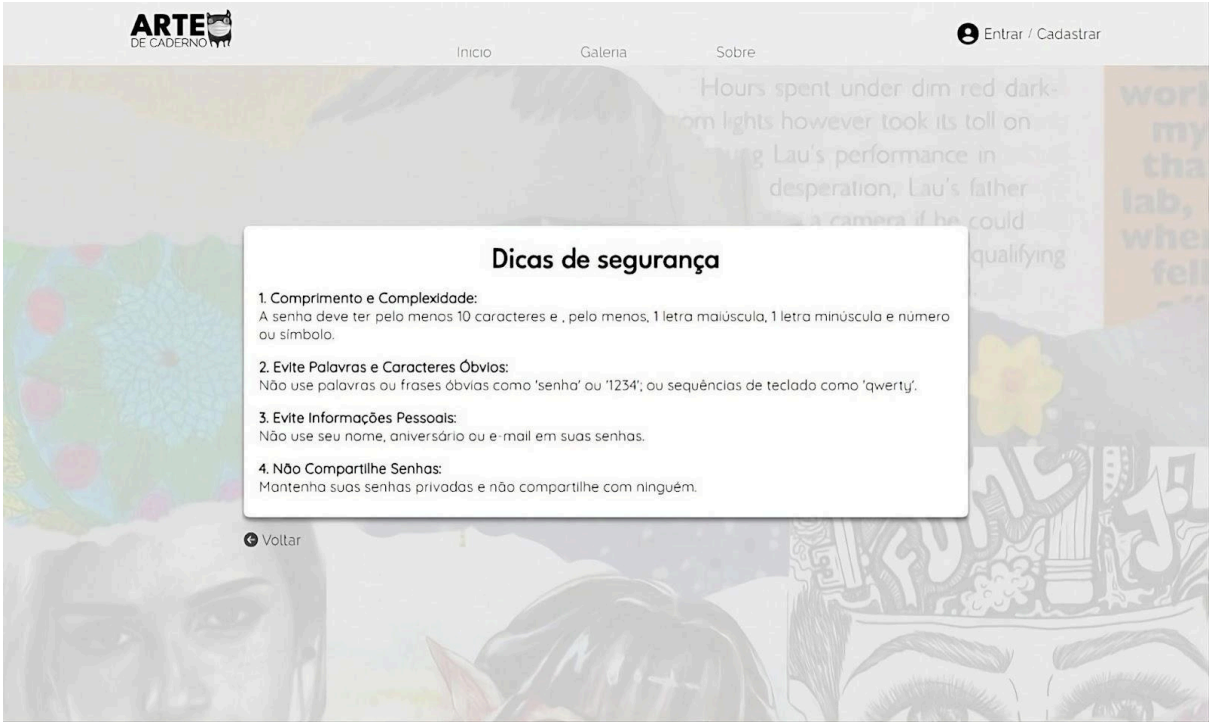
PASSWORD:"787ed87fb7db6e2f7fff263c9583c47d:c9ee1524ff941421d2826042da5b3808db45a961c257040f2da3779a62903e6a02a19e9e157a1fb98e389ddf5b4ae507561db999bf417d3d0bd3d389c27af52b"

Após a realização da criptografia e o armazenamento da senha no banco de dados, tornou-se necessário comparar a senha armazenada no banco, separando-a do código aleatório, e verificar se a senha fornecida durante a tentativa de *login* correspondia à mesma sequência de caracteres cadastrada na base de dados.

O usuário tem a possibilidade de efetuar a troca de sua senha, sendo necessário o seu CPF. Depois de solicitar a troca de senha, um código de 40 caracteres com validade de 1 hora é enviado para o *e-mail* do mesmo. Assim que fornecer o código, será solicitada a nova senha, como mostra.

Foi realizada uma validação no momento do cadastro das senhas dos usuários, visando obrigar o mesmo a utilizar senhas consideradas complexas de serem descobertas. Junto a isso, recomendações foram passadas aos usuários no momento de criação da senha, sendo elas (Figura 2):

Figura 2 - Dicas para o usuário sobre segurança



Fonte: criada pelo autor

ISSN: 2358-8829

CONSIDERAÇÕES FINAIS

Este projeto teve como objetivo a implementação de técnicas visando o aumento da segurança da plataforma digital Arte de Caderno. Foram adicionadas técnicas como criptografia de senhas, *token* para validação do tráfego da plataforma, navegação segura via *token* de acesso e para a troca de senha, filtro por formulário na criação de senha e recomendações para a criação de senhas mais complexas por parte dos usuários finais.

Tendo em vista todas essas camadas de proteção adicionadas, a plataforma atinge um grau de maturidade no cuidado e proteção dos dados nela contidos. Com o advento de novas tecnologias, tanto para proteção quanto para ataque, a plataforma está munida de qualidades que possuem maleabilidade para ampliação de novos métodos, tanto de *login* para novas redes sociais, como de criptografias mais resistentes, garantindo assim a longevidade da plataforma no que se refere à proteção.

De modo geral, a elaboração desta plataforma tem como meta primordial promover a expressão artística de maneira organizada e inclusiva, contribuindo diretamente para os objetivos centrais estabelecidos pelo Projeto Arte de Caderno. A plataforma se destaca como uma ferramenta sólida e adaptável, ideal para a submissão de desenhos de escolas públicas nos concursos promovidos pelo Projeto Arte de Caderno. Além disso, suas capacidades de aprimoramento contínuo prometem ampliar significativamente sua funcionalidade e eficiência, abrindo caminho para uma base sólida de futuras modificações impulsionadas por novas tecnologias, além de fomentar uma cultura administrativa focada na implementação de métodos de segurança inovadores, como planos de ação para invasões, controle de qualidade de backups, e planejamento e proteção contra causas naturais que possam danificar os backups.

REFERÊNCIAS

SILVA, Michael Bernardo Fernandes da. Cibersegurança: uma visão panorâmica sobre a segurança da informação na internet. Rio de Janeiro: Freitas Bastos, 2023.

ROHLING, Luis José. Segurança de redes de computadores. Curitiba: Contentus, 2020.

STALLINGS, William. Criptografia e segurança de redes: princípios e práticas.6ª ed. São Paulo: Pearson Education do Brasil, 2015.

ISSN: 2358-8829

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018.

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. 1. ed. Brasília, DF: ANPD, 2021.

MANN, Ian. Engenharia Social. São Paulo: Blucher, 2011.

GALVÃO, Michele da Costa. Fundamentos em segurança da informação. São Paulo: Pearson Education do Brasil, 2015.

GOOGLE. Recuperar sua Conta do Google ou senha do Gmail. Disponível em: https://support.google.com/accounts/answer/32040?hl=pt. Acesso em: 09 de março de 2024.

Microsoft. Como criar uma senha forte para sua conta Microsoft. Disponível em: https://support.microsoft.com/pt-br/account-billing/como-criar-uma-senha-forte-para-sua-conta-microsoft-f67e4ddd-0dbe-cd75-cebe-0cfda3cf7386#:~:text=Senhas%20fortes%20ajudam%20a%20impedir,nem%20o%20nome%20da%20empresa. Acesso em: 09 de março de 2024.

Kaspersky. How to create a strong password. Disponível em: https://www.kaspersky.com.br/resource-center/threats/how-to-create-a-strong-password. Acesso em: 09 de março de 2024.