PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS: UM ESTUDO TEÓRICO E EXPERIMENTAL SOBRE AS REDES SOCIAIS

GUILHERME HENRIQUE FREITAS BRANDÃO

GOIÂNIA
2021

GUILHERME HENRIQUE FREITAS BRANDÃO

SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS: UM ESTUDO TEÓRICO E EXPERIMENTAL SOBRE AS REDES SOCIAIS

Trabalho de Conclusão de Curso apresentado à Escola Politécnica, da Pontifícia Universidade Católica de Goiás, como parte de requisitos para obtenção do título de Bacharel em Engenharia de Computação.

Orientadora: Profa. Dra. Solange da Silva.

GOIÂNIA
2021

GUILHERME HENRIQUE FREITAS BRANDÃO

SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS: UM ESTUDO TEÓRICO E EXPERIMENTAL SOBRE AS REDES SOCIAIS

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Engenharia de Computação, e aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, em ____/____/_____.

_____

Profa. Ma. Ludmilla Reis Pinheiro dos Santos

Coordenadora de Trabalho de Conclusão de Curso

Banca Examinadora:

_____

Orientadora: Profa. Dra. Solange da Silva

_____

Profa. Ma. Angélica da Silva Nunes

_____

Prof. Me. Rafael Leal Martins

GOIÂNIA

2021

AGRADECIMENTOS

À Deus, em primeiro lugar, que sempre conduziu meus caminhos, me dando sabedoria, saúde, força e determinação para superar as dificuldades.

Aos meus pais, Gilson e Neila, que sempre confiaram, investiram e me motivaram nesta jornada. Por serem exemplos de pessoas de caráter e respeito, que apoiaram todas as minhas decisões e que conviveram comigo nos momentos mais difíceis e felizes da minha vida.

Aos meus irmãos, Diego, Matheus e Gabriel, por serem irmãos dedicados, inteligentes, companheiros e uma das minhas maiores alegrias.

À minha namorada, companheira e melhor amiga, Bruna, por ser meu porto seguro, que sempre deseja o meu melhor, tanto pessoal quanto profissional. Por ser uma pessoa que posso recorrer a qualquer momento, encontrar força, alegria e confiança para enfrentar quaisquer obstáculos ao decorrer de minha trajetória.

À toda minha família e amigos que colaboraram de alguma forma para ser quem eu sou hoje.

À minha prezada e querida orientadora Profa. Dra. Solange da Silva, pelos seus ensinamentos, conhecimentos, atenção e compreensão para realização deste trabalho.

Aos meus professores, que contribuíram para o meu aprendizado, repassando seus conhecimentos e experiências, durante esses cinco anos de curso.

RESUMO

Este trabalho possui o objetivo de **i**dentificar problemas e riscos existentes nas redes sociais mais utilizadas, simulando um ataque envolvendo a técnica de enviar *e-mails* utilizando táticas da engenharia social para enganar e sequestrar dados de utilizadores de redes sociais. Quantos aos aspectos metodológicos, a natureza desta pesquisa é um resumo de assunto. Quanto aos seus objetivos é uma pesquisa exploratória e descritiva. Em relação aos procedimentos técnicos, é uma pesquisa bibliográfica e experimental. O estudo realizado permitiu identificar os seguintes problemas e os riscos associados às redes sociais mais utilizadas em relação à segurança da informação, a seguir: problemas de ataques relacionados a Engenharia Social, que utilizam métodos de *phishing, spyware*, cavalo de troia, *baiting* e dentre outras. Os principais riscos relacionados ao uso de redes sociais são: o furto de identidade, a invasão de perfil, o uso indevido de informações, a invasão de privacidade, o vazamento de informações, a disponibilização de informações confidenciais, o recebimento de mensagens maliciosas, o acesso a conteúdo de mensagens maliciosas, o acesso a conteúdo impróprios ou ofensivos, danos à imagem e à reputação, o sequestro e o furto de bens. Com os resultados da implementação realizada neste trabalho foi possível concluir que os usuários são a porta de entrada para acontecer os cibercrimes. Portanto, precisam ser conscientizados e capacitados, visando ficarem mais observadores e saberem como agir ao receber os cenários dos atacantes nas redes sociais.

Palavras-chave: Redes Sociais. Engenharia Social. Segurança da Informação. Riscos. *Gophish*.

ABSTRACT

This work aims to identify existing problems and risks in the most used social networks, simulating an attack involving the technique of sending emails using social engineering tactics to deceive and hijack data from social network users. As for the methodological aspects, the nature of this research is a summary of the subject. As for its objectives, it is an exploratory and descriptive research. In relation to technical procedures, it is a bibliographical and experimental research. The study carried out allowed the identification of the following problems and risks associated with the most used social networks in relation to information security, as follows: attack problems related to Social Engineering, which use methods of phishing, spyware, trojans, baiting and among others. The main risks related to the use of social networks are: identity theft, profile invasion, misuse of information, invasion of privacy, information leakage, provision of confidential information, receiving malicious messages, access to malicious message content, access to inappropriate or offensive content, damage to image and reputation, kidnapping and theft of property. With the results of the implementation carried out in this work, it was possible to conclude that users are the gateway to cybercrimes. Therefore, they need to be made aware and trained, in order to become more observant and know how to act when receiving the attackers' scenarios on social networks.

Keywords: Social Networks. Social engineering. Information security. Scratchs. Gophish.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AES	*Advanced Encryption Standard* ou Padrão de Criptografia Avançado
AMIs	*Amazon Machine Image* ou Imagens de Máquina da *Amazon*
ARPANet	*Advanced Research Projects Agency Network* ou Agência de Projetos de Pesquisa Avançada
AWS	*Amazon Web Services* ou Serviços *Web* da *Amazon*
CD	*Compact Disc* ou Disco Compacto
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil
CPU	*Central Process Unit* ou Unidade Central de Processamento
DNS	*Domain Name System* ou Sistema de Nomes de Domínio
EBS	*Elastic Block Store*
EC2	*Elastic Compute Cloud*
GB	*Gigabyte*
GHz	*GigaHertz*
HTTP	*Hypertext Transfer Protocol* ou Protocolo de Transferência de Hipertexto
HTTPS	*Hypertext Transfer Protocol Secure* ou Protocolo de Transferência de Hipertexto Seguro
ID	*Identity* ou Identidade
IDEA	*International Data Encryption Algorithm* ou Algoritmo de Criptografia de Dados Internacional
IEC	*International Electrotechnical Commission* ou Comissão Eletrotécnica Internacional
IP	*Internet Protocol* ou Protocolo da *Internet*
IPv4	*Internet Protocol version* 4 ou Protocolo de *Internet* versão 4
ISO	*International Organization for Standardization* ou Organização Internacional de Normalização
NBR	Norma Brasileira
NCP	*Network Control Protocol* ou Programa de Controle de Rede
PEM	*Privacy Enhanced Mail*
PIN	*Personal Identification Number* ou Número de Identificação Pessoal

PPK	*PuTTY Private Key*
RAM	*Random Access Memory* ou Memória de Acesso Aleatório
RSA	*Rivest-Shamir-Adleman*
SMS	*Short Message Service* ou Serviço de Mensagens Curtas
SO	*Operational System* ou Sistema Operacional
TCC2	Trabalho de Conclusão de Curso 2
TCP	*Transmission control protocole* ou Protocolo de Controle de Transmissão
URL	*Uniform Resource Locator* ou Localizador Uniforme de Recursos
VPCs	*Virtual Private Cloud* ou Nuvem Privada Virtual
WEB	*World Wide Web* ou Rede Mundial De Computadores

SUMÁRIO

1 INTRODUÇÃO

A *Internet* surgiu no final da década de 60, no período de tensão da Guerra Fria, entre Estados Unidos e União Soviética. Pelo fato da corrida espacial e tecnológica, os norte-americanos pretendiam se alertar de qualquer ataque não identificado proveniente das forças soviéticas. Por conta disso, criaram uma maneira de comunicação segura e descentralizada, inicialmente, divididas em quatro locais distintos do país, obtendo assim a primeira rede que interligava computadores, chamada de *Advanced Research Projects Agency Network* (ARPANet), que utilizava o protocolo: *Network Control Protocol* (NCP) (LONGEN, 2019).

Em 1974 houve a necessidade de evoluir o protocolo NCP, devido a criação de novas redes de computadores fora da ARPANET. “*Vinton Cerf* e *Robert Kahn* desenvolveram os protocolos *Transmission control protocole* (TCP) e *Internet Protocol* (IP), com o objetivo de tornar a transmissão por pacotes de dados aplicável a todos os tipos de sistemas de informação”. (MOURA, 2019, p. 2).

Em razão da evolução e crescimento da *Internet*, houve a necessidade de adotar políticas, serviços, normas e técnicas buscando preservar dados e informações de usuários domésticos e corporativos contra criminosos cibernéticos. Surgiu, assim, o conceito da segurança da informação nas redes (ARGOLLO, 2017).

A segurança da informação nas redes fornece serviços fundamentais para garantir que a segurança ocorra,

> quatro deles estão relacionados com a mensagem trocada por meio da rede: confidencialidade, integridade, autenticação e não-repúdio de mensagens. O quinto serviço oferece autenticação ou identificação de entidades (FOROUZAN, 2010, p. 961).

De acordo com *Forouzan* (2010), conveniente dos fatores sobre os serviços de segurança, as informações precisam chegar no lugar certo, para a pessoa certa, no tempo certo e de maneira correta com relação ao que está sendo enviado.

A segurança da informação está fortemente ligada às práticas que buscam a proteção das informações de ameaças. Tendo a criptografia como uma prática que tem como objetivo a obtenção da confidencialidade, da integridade, da autenticação, do não-repúdio de mensagens e da autenticação de entidades (FOUROZAN, 2010).

Segundo *Stallings* (2014), a criptografia é a forma de codificar e decodificar os dados, procedimento que deve ser tratado com muita complexidade para barrar ameaças de pessoas mal-intencionadas.

> Os procedimentos usados para fornecer os serviços de segurança são muitas vezes nem um pouco intuitivos. Normalmente, um mecanismo de segurança é complexo, e não fica óbvio na definição de seus requisitos que essas medidas são necessárias (STALLINGS, 2014, p. 9).

As redes sociais digitais são “um conjunto de *websites* e portais de relacionamento existentes e disponíveis na *Internet*” (SOUZA et al., 2018, p.3).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.BR, 2012), produziu uma Cartilha de Segurança para *Internet*, apontando como um aspecto importante, a privacidade dos usuários que utilizam as redes sociais, que desejam manter as suas informações pessoais sigilosas.

> As redes sociais possuem algumas características próprias que as diferenciam de outros meios de comunicação, como a velocidade com que as informações se propagam, a grande quantidade de pessoas que elas conseguem atingir e a riqueza de informações pessoais que elas disponibilizam. Essas características, somadas ao alto grau de confiança que os usuários costumam depositar entre si, fez com que as redes sociais chamassem a atenção, também, de pessoas mal-intencionadas (CERT.BR, 2012, p. 87).

Em consequência da popularidade das redes sociais digitais, os usuários acabam se expondo as vulnerabilidades que existem no meio digital, e desta maneira, pela falta do uso responsável e consciente na *Internet*, surgem lacunas para atividades de engenheiros sociais.

Segundo Aramuni e Maia (2018), a Engenharia Social é uma técnica de manipulação, que possui a finalidade de induzir pessoas para facilitar ou passar imediatamente informações preciosas, seja elas do âmbito pessoal ou corporativo.

> Existem diversos motivos para alguém estudar e usar esses truques: espionagem industrial, obter informações confidenciais para cometer alguma fraude, roubo de identidade, interromper redes e serviços ou, simplesmente, por pura diversão, apenas para provar que nenhum sistema é seguro o suficiente (ARAMUNI; MAIA, 2018, p. 33).

Para Tieso e Santo (2020), existem técnicas de engenharia social que foram desenvolvidas para enganar pessoas, sendo que as mais recorrentes são aquelas que criam familiaridade com a vítima, abusando de sua confiança e inocência. O

principal tipo de ataque relacionado a engenharia social é o ataque de *phishing*, que possui uma forma simples com capacidade de atingir várias pessoas. Este ataque consiste no invasor se passar por uma pessoa ou organização, enviando e-mails falsos as vítimas.

Justifica-se estudar esse tema porque as redes sociais estão no meio digital da maioria das pessoas. Devido ao crescimento da utilização das redes sociais, foi acarretado o aumento de anomalias que infringem e colocam em risco a segurança da informação e de dados dos usuários existentes. “De acordo com um relatório da *Norton Cyber Security*, em 2017 o Brasil passou a ser o segundo país com maior número de casos de crimes cibernéticos, afetando cerca de 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões” (UOL, 2018). Até o ano de 2021, os custos globais do cibercrime “deve chegar a US$ 6 trilhões por ano – um valor 15 vezes maior do que o registrado em 2015, de US$ 400 bilhões” (PROOF, 2016). Segundo a empresa de segurança digital líder da América Latinha, *PSafe*, apenas em 2021, estimasse um total de vítimas do golpe de engenharia social de técnicas de *phishing* ultrapassaram 150 milhões de brasileiros (DINIZ, 2021).

Portanto, existe a necessidade de melhorar os investimentos em serviços de segurança, criando normas e técnicas buscando assim, garantir a proteção e privacidade dos ativos de informação. Sendo assim, é de grande importância informar, alertar, ensinar e conscientizar usuários, grupos e empresas sobre as situações de riscos que podem afetar a segurança da informação nesses ambientes virtuais.

Diante do contexto, este projeto visa responder à questão de pesquisa: **Quais os problemas e os riscos associados as redes sociais mais utilizadas em relação a segurança da informação?**

Este trabalho tem o objetivo geral de **i**dentificar problemas e riscos existentes nas redes sociais mais utilizadas, simulando um ataque envolvendo a técnica de enviar *e-mails* utilizando táticas da engenharia social para enganar e roubar dados de utilizadores de redes sociais.

Os objetivos específicos são:

a) Apresentar os conceitos da segurança da informação;
b) Apresentar os fundamentos da segurança e seus serviços;
c) Levantar os principais problemas e riscos associados às redes sociais mais usadas;

d) Descrever as técnicas de engenharia social utilizadas por cibercriminosos.

Espera-se que os resultados deste trabalho possam contribuir:

a) Com o aumento da segurança da informação para os usuários de redes sociais;
b) Apresentando conceitos, técnicas e normas de segurança da informação, visando assim, informar e esclarecer os riscos associados a esses ambientes virtuais;
c) Informando colaboradores da importância de se preservar a informação e a segurança nas redes sociais;
d) Conscientizar usuários que utilizam a *Internet* sobre os métodos de ataques relacionados a engenharia social;

Quantos aos aspectos metodológicos, a natureza desta pesquisa é um resumo de assunto. Quanto aos seus objetivos é uma pesquisa exploratória e descritiva. Em relação aos procedimentos técnicos, é uma pesquisa bibliográfica e experimental.

Esta monografia está organizada em 7 capítulos, sendo estruturada da seguinte forma:

O Capítulo 1 apresenta a introdução com o contexto do trabalho, a questão de pesquisa, objetivos e resultados esperados. O Capítulo 2 traz o referencial teórico com conceitos, definições e trabalhos relacionados com o tema. No Capítulo 3 estão descritos os procedimentos metodológicos, mostrando como e o que foi feito para atingir o objetivo geral. O Capítulo 4 traz as ferramentas utilizadas no ambiente de implementação, fazendo o uso do serviço de computação em nuvem da *Amazon Web Services* (AWS), da ferramenta de criação de instâncias chamado *Amazon Elastic Compute Cloud* (*Amazon EC2*), do *software PuTTY* e o *framework* do *Gophish*. No Capítulo 5 é apresentada a descrição do experimento, que trata da simulação de um ataque utilizando da engenharia social, chamada de e*-mail phishing*. O Capítulo 6 contém a análise dos resultados obtidos. Finalmente, o Capítulo 7 traz as considerações finais e sugestões de trabalhos futuros.

2 REFERENCIAL TEÓRICO

Este capítulo é formado por duas partes: uma teórica, que traz os conceitos e definições da área e uma parte prática, que apresentam alguns trabalhos relacionados ao assunto. Foi realizada uma revisão literária de trabalhos científicos e acadêmicos, abordando os principais conceitos relacionados ao tema de Segurança da Informação nas Redes Sociais.

2.1 Segurança da Informação

Informação, segundo o dicionário online da língua portuguesa (DICIO, 2021), “é a reunião dos conhecimentos, dos dados sobre um assunto ou pessoa”. A informação tem se tornado cada vez mais valioso, para as pessoas, pequenas e grandes organizações. Segundo a ABNT NBR ISO/IEC 27002 (2013),

> o valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p. 10).

Segurança, segundo o dicionário online da língua portuguesa (DICIO, 2021), é uma forma de garantir que algo esteja seguro, estando afastado do perigo. É uma forma de proteger algo ou alguém, ou pelo menos diminuir os riscos e perigos.

Segundo Silva, Carvalho e Torres (2003), a utilização do termo Segurança da Informação surgiu de técnicos de sistemas de informática no início do desenvolvimento de sistemas, por conta do crescimento da utilização de computadores e pelo interesse das empresas em redes de computadores corporativas. Os princípios para a segurança na época foram o custo/benefício, a concentração, a proteção em profundidade, a consistência do plano e a redundância.

A segurança da informação tem como o principal objetivo, fornecer proteção para um conjunto de informações de um determinado indivíduo ou organização. No

âmbito organizacional, necessita garantir a continuidade dos negócios, aumentando o retorno sobre investimentos e reduzindo os riscos (DURBANO, 2019).

A Norma ABNT NBR ISO/IEC 27002:2013, informa que

> a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013, p. 10).

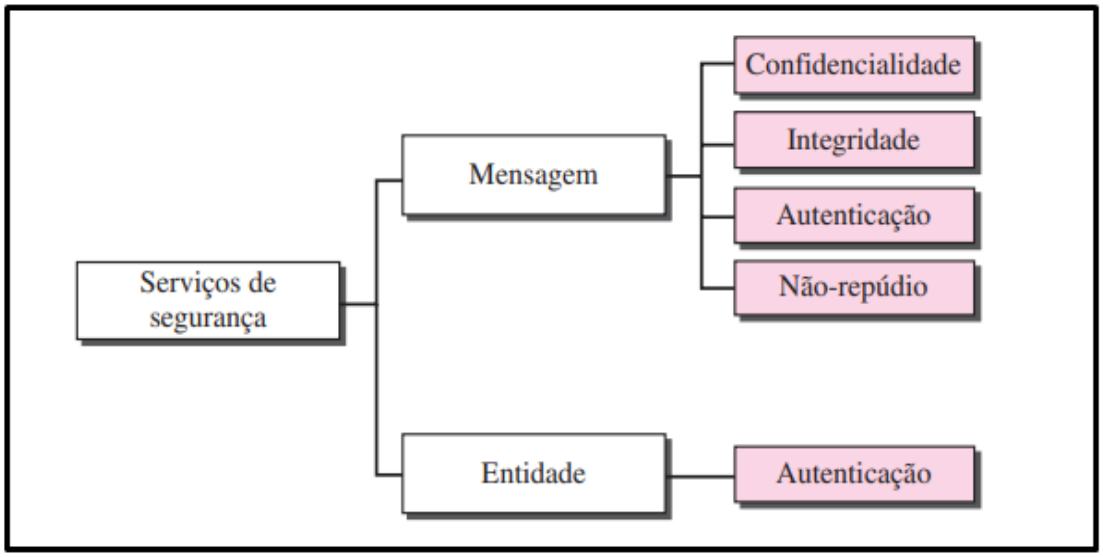
De acordo com Oliveira, Moura e Araújo (2012), existe uma hierarquia dentro da segurança, seguida da seguinte maneira: os dados, a informação e o conhecimento. Sendo assim, é necessário manter os dados protegidos, preservando toda a informação e o valor existente nos dados. O conhecimento está ligado no combate aos ataques que podem prejudicar a integridade dos dados, a confidencialidade e a disponibilidade, fazendo uma ligação com os serviços da segurança de redes e da informação.

2.2 Serviços de Segurança

Os fatores que podem prejudicar a segurança da informação, estão associadas ao usuário, ao ambiente, a infraestrutura e as pessoas mal-intencionadas que buscam roubar, alterar ou destruir estes dados. A segurança da informação tem o objetivo de manter a informação segura, de modo correto, preciso e disponível, garantindo também que a informação possa ser manipulada e compartilhada por aqueles que a detém. Por conta destes fatores, surgem as ideias e técnicas dos serviços de segurança de redes (QUEIROZ; ROSA, 2019).

Para Forouzan (2010), os serviços de segurança de redes são separados em quatro relacionados a troca de mensagens por meio da rede e um deles relacionada a autenticação de entidades, conforme ilustrado na Figura 1:

Figura 1 - Serviços de Segurança



Fonte: Forouzan (2010, p.961).

2.2.1 Confidencialidade de Mensagens

A confidencialidade está associada ao sigilo da informação, ou seja, apenas o remetente e o destinatário podem e devem entender o conteúdo das mensagens transmitidas entre eles, sendo incompreensíveis para terceiros (FOROUZAN, 2010).

Segundo a norma ABNT NBR ISO/IEC 27002 (2013), a confidencialidade é baseada em características da exclusividade e da privacidade, no qual, age de modo que a informação seja restringida, estando disponível apenas para pessoas confiáveis e autorizadas.

2.2.2 Integridade da Mensagem

A Integridade está associada a coerência dos dados, isto é, no momento da comunicação entre o remetente e o destinatário os dados devem chegar exatamente como foram enviados, sem sofrer alterações durante uma transmissão (FOROUZAN, 2010).

2.2.3 Autenticação de Mensagens

A Autenticação é um serviço que confirma a identidade dos envolvidos, isto é, o receptor precisa estar certo da identidade do emissor, tendo a certeza de que não é um impostor que está enviando uma mensagem (FOROUZAN, 2010).

2.2.4 Não-repúdio de Mensagens

Não-repúdio está associado a confiança dos dados, ou seja, o emissor não pode negar uma mensagem que ele enviou (FOROUZAN, 2010).

2.2.5 Autenticação de Entidades

Autenticação de mensagens por entidades, tem o objetivo de possibilitar que uma parte provenha a identidade de outra parte, fornecendo assim a garantia da identidade de um usuário. Sendo que uma entidade se compara a uma pessoa, processo, cliente ou servidor. (FOROUZAN, 2010).

De acordo com Forouzan (2010, p. 976), “a entidade cuja identidade precisa ser provada é denominada requerente; a parte que tenta provar a identidade do requerente é chamada de verificador”.

Segundo Forouzan (2010, p. 976), para comprovar as identidades deve ser feita uma verificação de um dos três tipos de testemunhos:

- Algo que conhecemos: Trata-se de um segredo conhecido apenas pelo requerente que pode ser checado pelo verificador. Exemplos: uma senha, um número PIN, uma chave secreta e uma chave privada.
- Algo que possuímos: Aquilo que pode provar a identidade do requerente: passaporte, carteira de motorista, carteira de identidade, cartão de crédito e *smart card*.
- Algo que somos: Trata-se de uma característica inerente do requerente. Exemplos: assinatura convencional, impressões digitais, voz, traços faciais, padrão de retina e caligrafia.

2.3 Criptografia

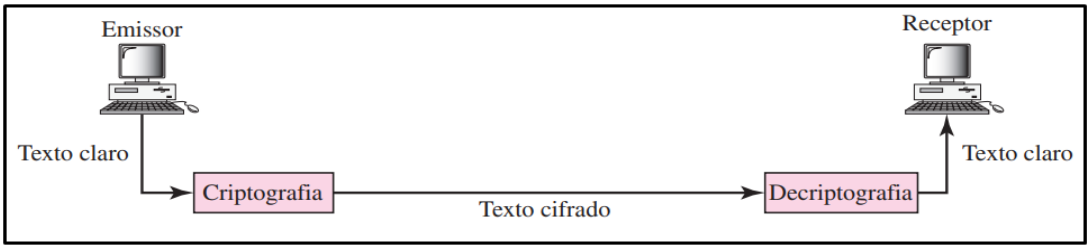
O conceito da palavra criptografia segundo Stallings (2014, p.2), “consiste no desenvolvimento de técnicas para garantir o sigilo e/ou a autenticidade de informações”. A criptografia possui origem grega e significa escrita secreta.

Segundo Vanacor (2020), “a criptografia tem dois propósitos principais: impedir que os dados armazenados sejam lidos e permitir que dados sejam transmitidos de forma segura por um canal inseguro”. Portanto, apenas as pessoas que possuem autorização para o acesso informação poderão entender o seu significado.

A Figura 2 ilustra os componentes criptográficos que segundo Forouzan (2010), podem ser classificados em:

- Emissor: Pessoa ou serviço que envia a informação;
- Receptor: Pessoa ou serviço que recebe a informação;
- Texto Claro: mensagem original, com os dados legíveis e compreendida por qualquer um que tiver acesso a ela;
- Texto Cifrado: possui a informação do texto claro criptografado, ou seja, o texto cifrado passou por algum algoritmo criptográfico, se tornando complexo e incompreensível;
- Cifra: são algoritmos de criptografia ou decriptografia;
- Chave: possui a função de trancar ou destrancar o acesso à informação, ou seja, para trancar a informação é necessário de uma cifra capaz de criptografar, da chave criptográfica e o texto claro. A junção desses elementos cria o texto cifrado. Para decriptografar é necessário a cifra e a chave decriptográfica, junto do texto cifrado, revelando a informação em texto claro novamente.

Figura 2 - Componentes da Criptografia



Fonte: FOROUZAN (2010, p. 931).

Existem duas técnicas de ataque a um esquema de encriptação convencional, chamados de criptoanálise e ataque por força bruta. Segundo Stallings (2012, p. 23):

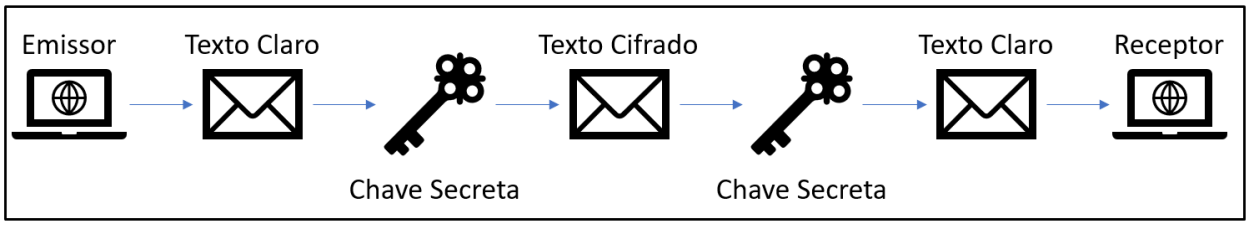
- Criptoanálise: os ataques criptoanalíticos utilizam-se da natureza do algoritmo, e talvez de mais algum conhecimento das características comuns ao texto claro, ou ainda de algumas amostras de pares de texto claro-texto cifrado. Esse tipo de ataque explora as características do algoritmo para tentar deduzir um texto claro específico ou a chave utilizada.
- Ataque por força bruta: o atacante testa todas as chaves possíveis em um trecho do texto cifrado, até obter uma tradução inteligível para o texto claro. Na média, metade de todas as chaves possíveis precisam ser experimentadas para então se obter sucesso.

De acordo com o CERT.BR (2012), a criptografia pode ser utilizada para proteger dados sigilosos, criar partições com informações criptografadas automaticamente, proteger *backups* contra invasores e proteger comunicações realizadas na *Internet*. Os métodos criptográficos se dividem em duas categorias: a criptografia de chave simétrica e a criptografia de chaves assimétricas.

2.3.1 Criptografia de chave simétrica

A criptografia de chave simétrica ou encriptação de chave secreta, faz a utilização de uma mesma chave para criptografar e decriptografar a mensagem. O emissor vai utilizar a chave secreta e um algoritmo de criptografia para criptografar o texto claro, transformando-o em texto cifrado e o receptor vai utilizar a mesma chave secreta em conjunto de um algoritmo de decriptografia para decriptografar o texto cifrado em texto claro novamente, conforme ilustrado na Figura 3. (FOROUZAN, 2010).

Figura 3 - Criptografia de chave simétrica



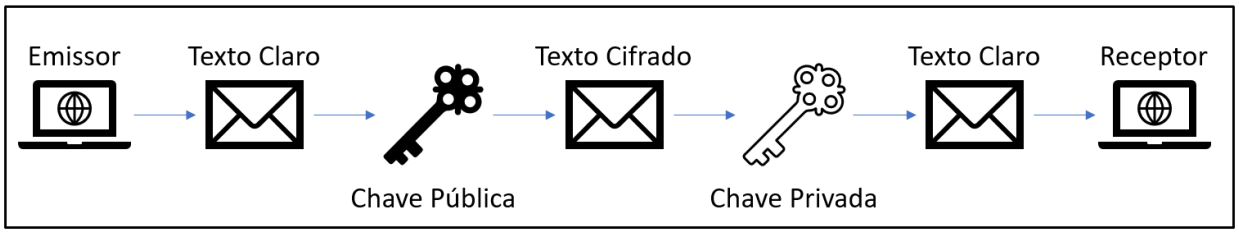
Fonte: Adaptado de Forouzan (2010, p.933).

De acordo com a MILLS (2021), o *Advanced Encryption Standard* (AES, do português: Padrão de Encriptação Avançada) e o *International Data Encryption Algorithm* (IDEA, do português: Algoritmo Internacional de Criptografia de Dados) são exemplos de métodos que utilizam criptografia de chave simétrica.

2.3.2 Criptografia de chave assimétrica

A criptografia de chave assimétrica ou encriptação de chave pública, faz a utilização de duas chaves, sendo uma pública e a outra privada. A chave privada pertence ao receptor, enquanto a chave pública fica disponível ao emissor e ao público em geral. Neste caso, a chave pública é utilizada para criptografar o texto claro em texto cifrado, utilizando um algoritmo criptográfico, enquanto apenas a chave privada tem a capacidade de decriptar o texto cifrado em claro novamente, utilizando algum algoritmo criptográfico, conforme ilustrado na Figura 4 (FOROUZAN, 2010, p. 68).

Figura 4 - Criptografia de chave assimétrica



Fonte: Adaptado de Forouzan (2010, p.933).

Segundo a CERT.BR (2010), a criptografia de chave simétrica possui processamento mais rápido que a de chave assimétrica, sendo recomendada para garantir a confidencialidade de grandes volumes de dados, porém, a criptografia de chave assimétrica

> facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves (CERT.BR, 2010, p. 69).

O *Rivest-Shamir-Adleman* (RSA) é o algoritmo mais utilizado no mundo e um dos primeiros algoritmos de chave pública, desenvolvido em 1977 por *Ron Rivest*, *Adi Shamir* e *Leonard Adlema*. O algoritmo possui finalidade de construir chaves

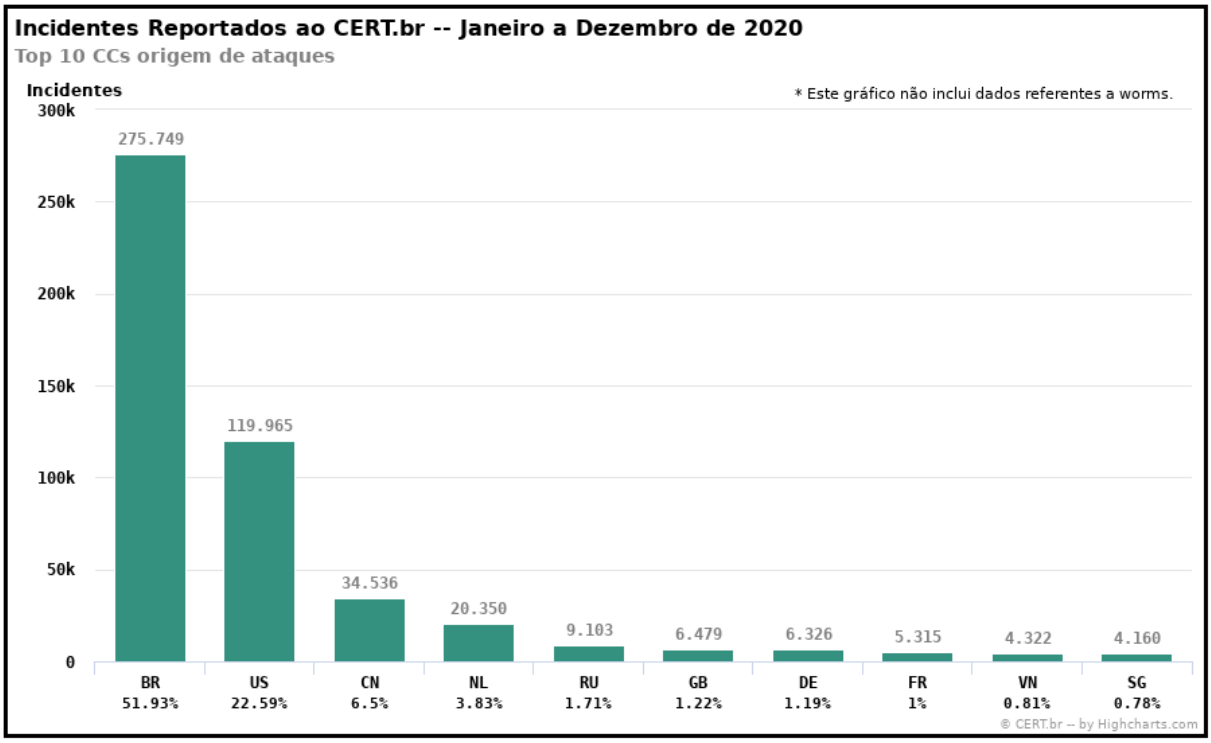
públicas e privadas utilizando números primos, sendo considerado um dos mais seguros devido à dificuldade de fatorar um número em seus componentes primos (TOTVS, 2020).

De acordo com MILLS (2021), decriptografar um texto cifrado com RSA sem possuir a chave privada é praticamente impossível, pois o comprimento da chave atinge o tamanho de pelo menos 2048 *bits*, resultando em um número de 617 dígitos.

2.4 Incidentes Relacionados à Segurança da Informação

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), entre os meses de janeiro e dezembro de 2020, 531.039 incidentes foram reportados, dos quais 275.749 (51,93% dos incidentes) tiveram origem no Brasil, conforme exibido na Figura 5.

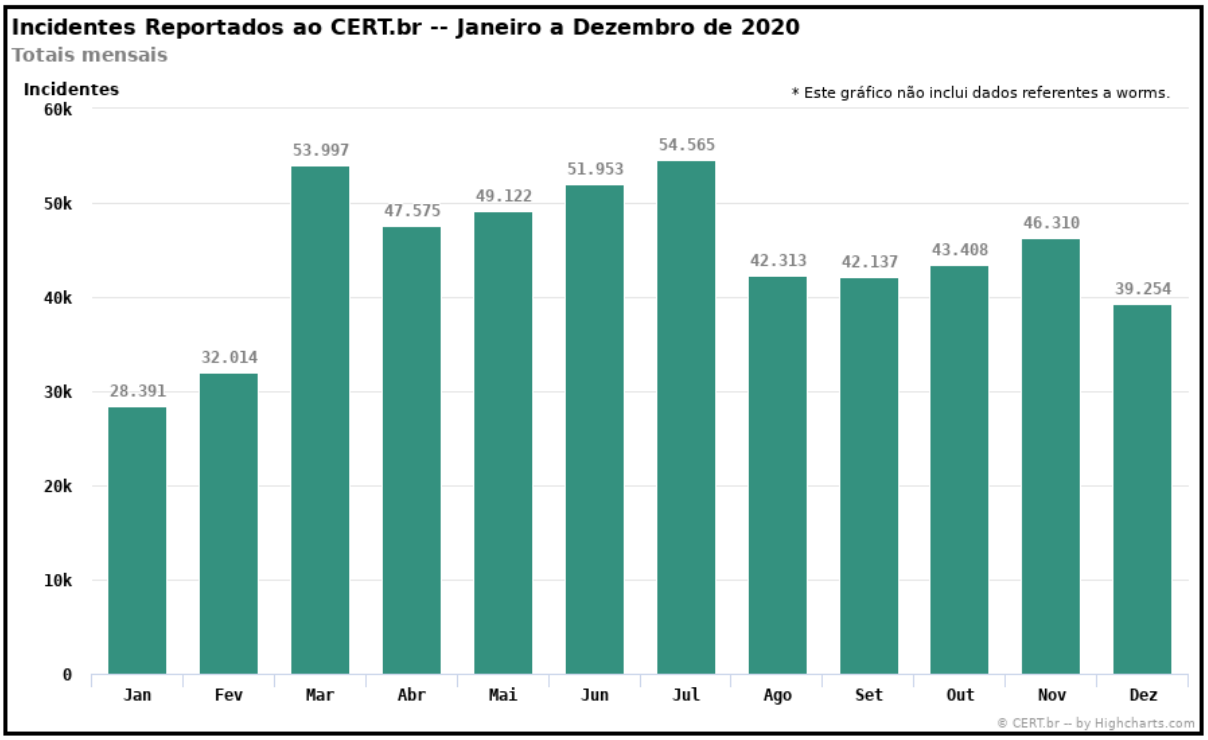
Figura 5 - Incidentes por país reportados ao CERT.BR - 2020



Fonte: CERT.BR (2021).

O pico dos casos ocorreu no mês de julho, com 54.565 (10.27%) incidentes reportados, conforme exibido na Figura 6. (CERT.BR, 2021).

Figura 6 - Incidentes totais mensais reportados ao CERT.BR - 2020



Fonte: CERT.BR (2021).

2.5 Redes Sociais

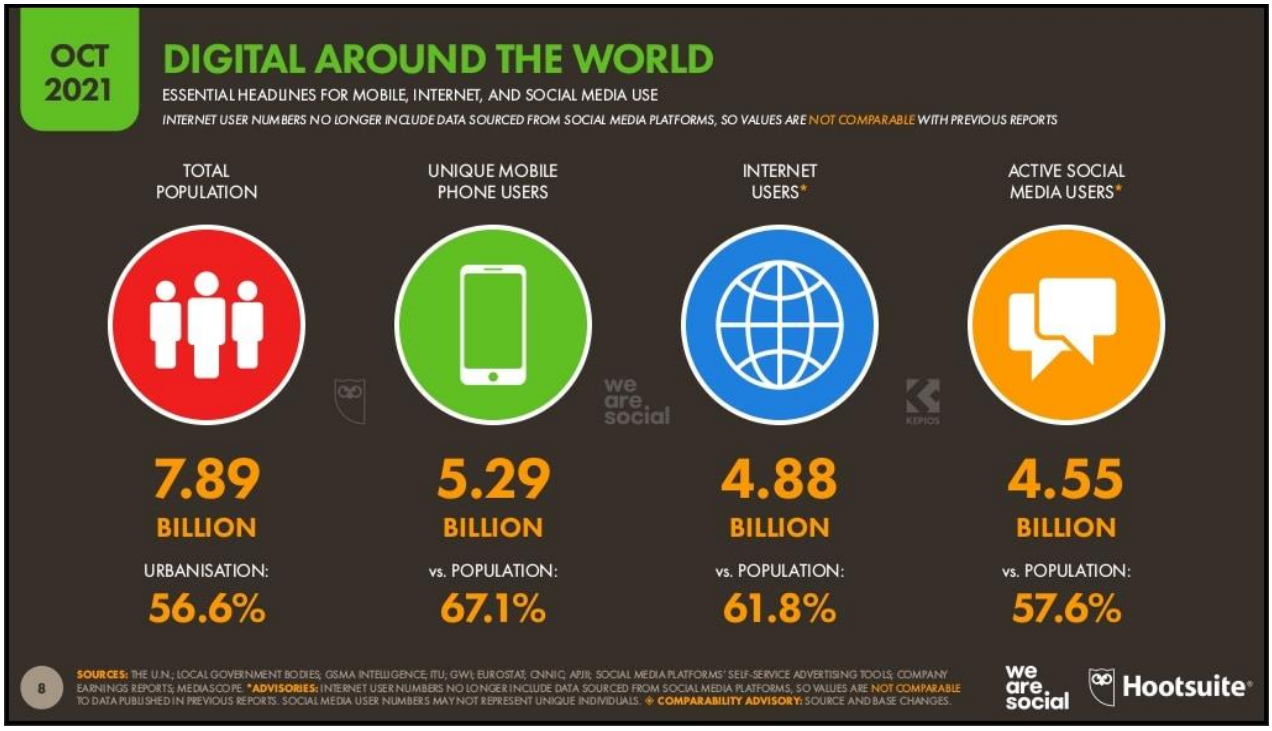
Em termos gerais, as redes sociais podem ser caracterizadas pelas relações entre pessoas ou organizações, nas quais dividem interesses e valores comuns, via *Internet*, tendo como objetivo,

> conectar pessoas, em nível mundial, através da difusão das comunicações. Em termos conceituais, as redes podem ser compreendidas como serviços materializados em páginas na WEB ou em aplicativos que, a partir de perfis pessoais, permitem uma ampla interação entre seus usuários, proporcionando e facilitando as relações e os laços sociais entre os sujeitos (pessoas, instituições, empresas ou grupos) no ambiente virtual (TEFFÉ e MORAES, 2017, p. 116-117).

Relatórios produzidos pelas agências de marketing digital *Hootsuite* e *We are social*, segundo Pareto (2019), fizeram uma parceria para a elaboração de relatórios que fornecem informações e *insights* sobre como as pessoas ao redor do mundo utilizam a *Internet*, as mídias sociais, os dispositivos móveis e o comércio eletrônico. Segundo a DataReportal (2021), essas pesquisas foram realizadas em outubro de

2021, estimando que a população mundial tenha atingido 7,89 bilhões de habitantes, no qual 4,88 bilhões dessas pessoas estão conectadas à *Internet* e 4,55 bilhões deste total mundial possui alguma mídia social ativa, equivalendo a 57,6% da população total do mundo, conforme mostrado na Figura 7.

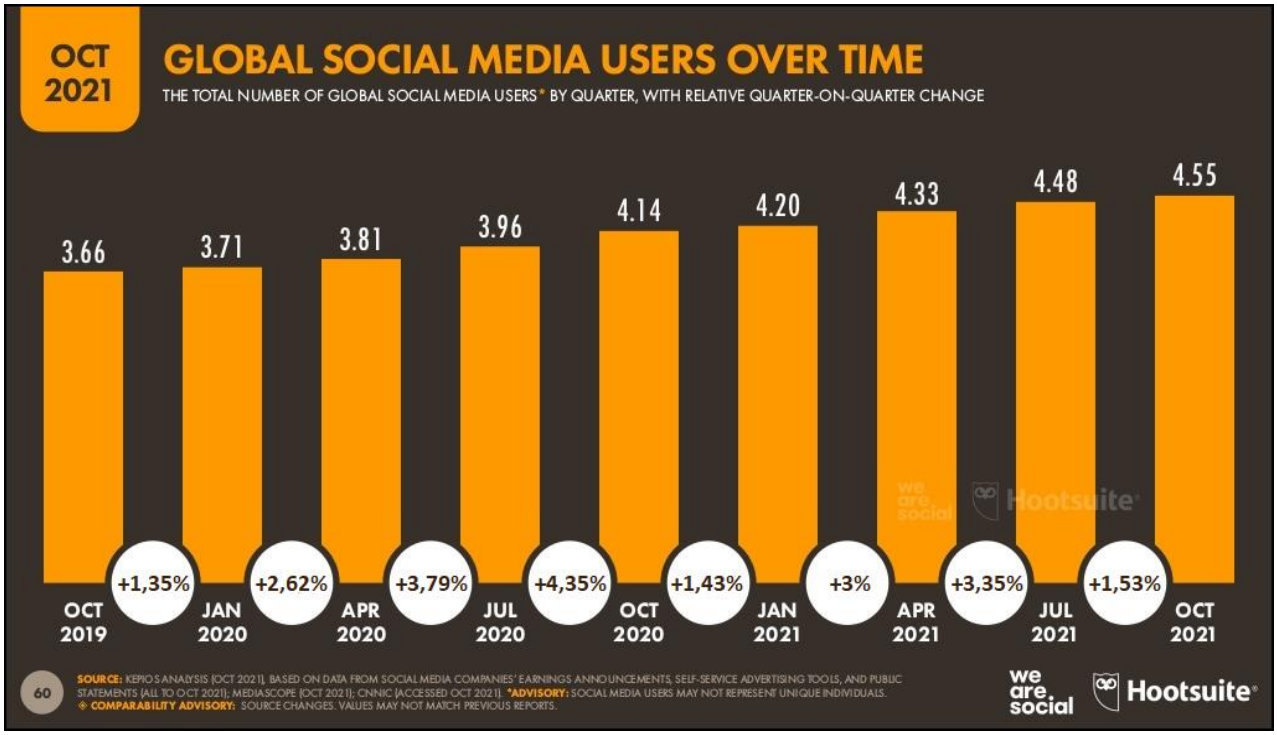
Figura 7 - Dados mundiais da população, *Internet* e mídia sociais



Fonte: DATAREPORTAL (2021, p. 8).

Em comparação ao mês de outubro de 2020, a base de usuários ativos em mídias sociais cresceu mais de 9%, conforme ilustrado na Figura 8. Enquanto a base de usuários da *Internet* cresceu 4,5% e o número global de habitantes acresceu um pouco mais de 1% em sua soma, apontando uma rápida expansão da utilização de mídias sociais ao redor do mundo (DATAREPORTAL, 2021).

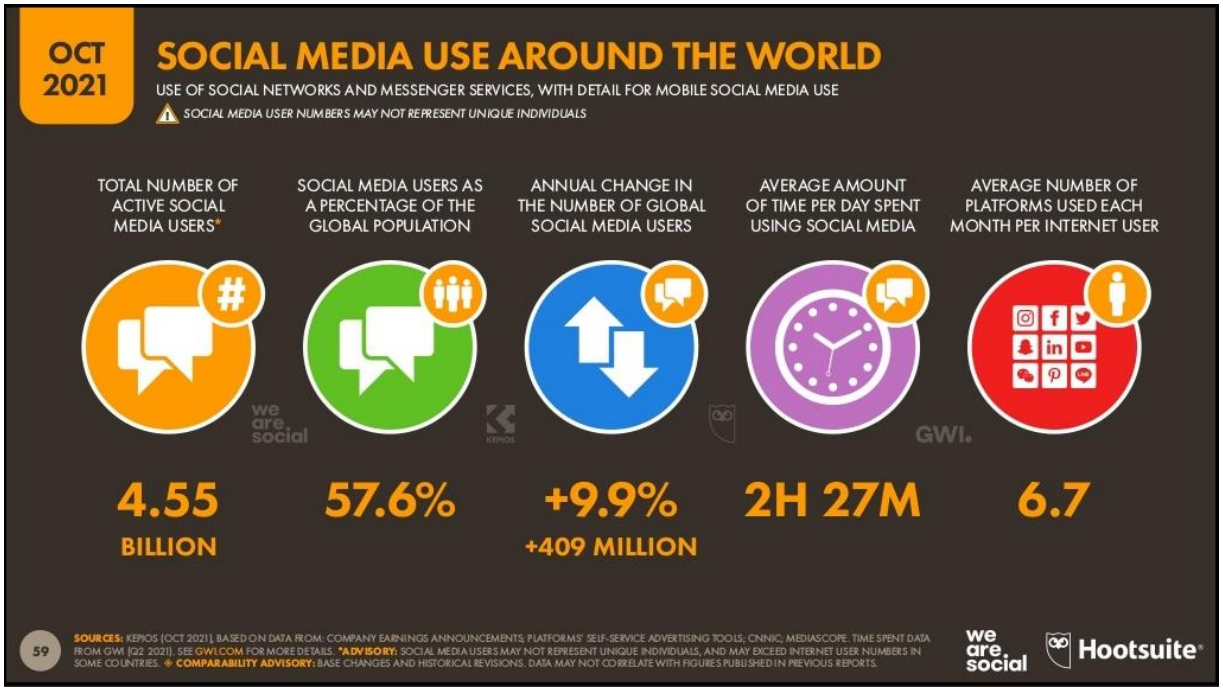
Figura 8 - Dados mundiais da utilização de mídias sociais ao longo dos anos



Fonte: Alterado do DATAREPORTAL (2021, p. 60).

Entre os meses de outubro de 2020 e outubro de 2021, quase 410 milhões de pessoas ingressaram nas mídias sociais, uma média de 1,120 milhão de pessoas ingressando em alguma mídia social todos os dias, equivalendo em 13 novos usuários a cada segundo. Além disso, o tempo médio gasto por dia utilizando alguma mídia social é de 2 horas e 27 minutos, contendo um número médio de 6.7 plataformas distintas sendo usadas a cada mês por usuários da *Internet*, conforme ilustrado na Figura 9 (DATAREPORTAL, 2021).

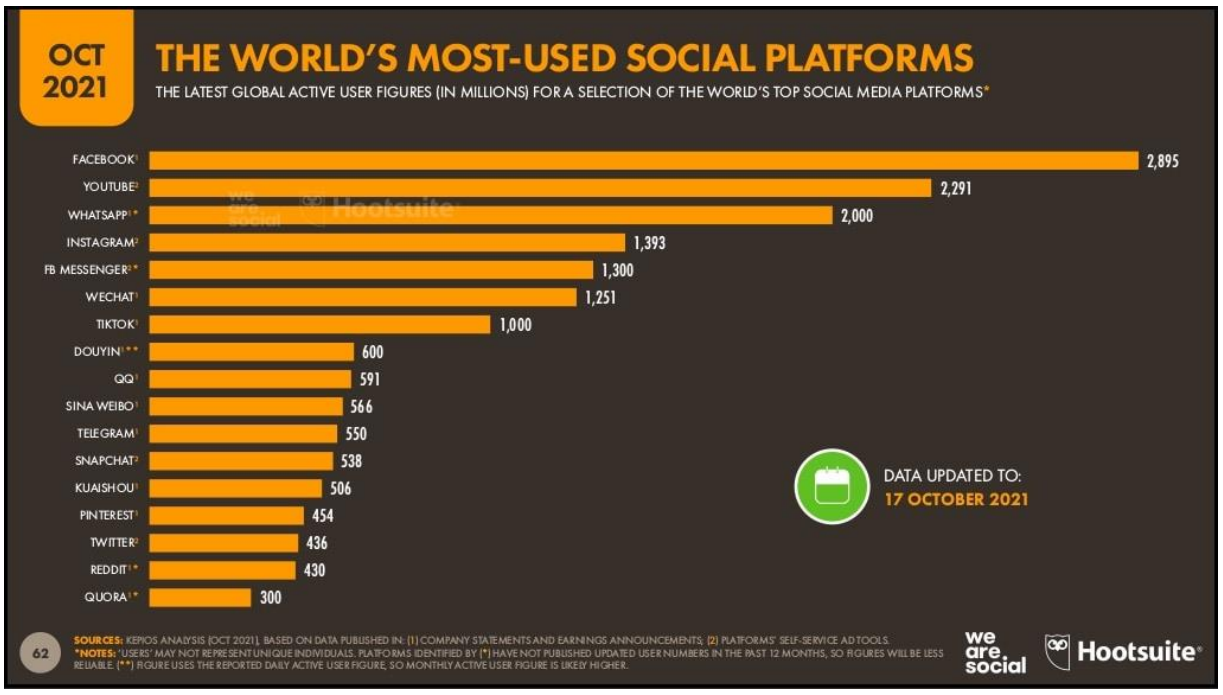
Figura 9 - Dados mundiais do comportamento dos usuários em mídias sociais



Fonte: DATAREPORTAL (2021, p. 59).

Dentre as redes sociais com mais usuários no mundo em 2021, conforme ilustrado na Figura 10, tem-se as seguintes 17 maiores redes sociais (*DATAREPORTAL,* 2021, p. 62):

Figura 10 - As redes sociais mais utilizadas do mundo



Fonte: DATAREPORTAL (2021, p. 62).

Ao observar a Figura 10, nota-se as seguintes redes sociais:

- 1° Lugar: *Facebook* – 2,895 bilhões de usuários. Para Aguiar (2016), o *Facebook* é uma mídia social e rede social virtual, que possibilita criar perfis pessoais ou empresariais, para interação entre pessoas através do compartilhamento de conteúdo e pela troca de mensagens instantâneas. Além disso, proporciona a participação de grupos sociais, partilhando de interesses e necessidades de um ou mais indivíduos pessoais ou empresariais.
- 2° Lugar: *YouTube* – 2,291 bilhões de usuários. Segundo Pin (2017), o *YouTube* é uma rede social digital que permite o compartilhamento de vídeos, hospedando vídeos caseiros de pessoas comuns até grandes produções, como filmes, documentários e videoclipes.
- 3° Lugar: *WhatsApp* – 2 bilhões de usuários. O *WhatsApp* é um aplicativo multiplataforma de troca de mensagens instantâneas e de comunicação em áudio e vídeo via *Internet*, que possui criptografia de ponto a ponto, com intuito em manter a privacidade e a segurança de pessoas e empresas. Além das mensagens de texto, a rede social possibilita o envio de emojis, figurinhas, *gifs*, fotos, vídeos, documentos e localização em tempo real (NUVENS, 2021).
- 4° Lugar: *Instagram* – 1,393 bilhão de usuários. Para Coutinho (2021), o *Instagram* é uma rede social online focada no compartilhamento de fotos e vídeos de curta duração, sendo muito conhecida pela usabilidade de suas ferramentas de edição. Além disso, o aplicativo também funciona como uma plataforma de troca de mensagens instantâneas.
- 5° Lugar: *Facebook Messenger*– 1,3 bilhão de usuários. O *Messenger* é uma rede social que funciona como mensageiro instantâneo, criada para fornecer a comunicação entre o aplicativo e a plataforma do *Facebook*, facilitando a integração entre seus usuários. O *Messenger* permite compartilhar áudios, fotos, vídeos, figurinhas, gifs, além de ganhar atualizações que permitiram “realizar ligações, chamadas de vídeos, compartilhamento de localização e até a disputa de jogos *on-line* com outra pessoa” (HOTMART, 2020).

- 6° Lugar: *WeChat* – 1,251 bilhão de usuários. Segundo Nieto (2019), o *WeChat* é um aplicativo multiplataforma de mensagens instantâneos, utilizado em sua maior parte na China. O maior diferencial do aplicativo é a comunicação entre pessoas que estão próximas umas das outras, utilizando a localização em tempo real do aparelho.
- 7° Lugar: *TikTok* – 1 bilhão de usuários. O *TikTok* é uma rede social baseada na criação e compartilhamento de vídeo curtos, sendo possível visualizar, curtir, comentar, produzir, editar, compartilhar e interagir com vídeos de outros usuários (FABRO, 2021).
- 8° Lugar: *Douyin* – 600 milhões de usuários. De acordo com Madhok (2021), a rede social *Douyin* é basicamente o aplicativo do *TikTok* separado para a região da China.
- 9° Lugar: *QQ* – 591 milhões de usuários. O *QQ Messenger* é um antigo programa de mensagens instantâneas, utilizado em sua maior parte na China. Por muito tempo a rede social foi utilizada para substituir o *e-mail* na China, pela sua facilidade e maior interação entre os usuários. (LIANG, 2020).
- 10° Lugar: *Sina Weibo* – 566 milhões de usuários. Para Velasco (2019), *Sina Weibo* é uma rede social de *microblog* chinês. O *Weibo* permite que seus usuários publiquem imagens, vídeos e links, seguidas de um número limitado de caracteres em cada postagem.
- 11° Lugar: *Telegram* – 550 milhões de usuários. Segundo Dias (2019), o *Telegram* é um mensageiro instantâneo russo baseado em nuvem, que possui criptografia de ponto a ponto, com intuito em manter a privacidade e a segurança de pessoas e empresas, além de possuir funções de *chats* secretos para envio de mensagens autodestrutivas. A rede social possibilita fazer o envio de mensagens, fotos, vídeos, figurinhas, documentos, localização em tempo real e realizar chamadas de áudio e vídeo. Os maiores diferenciais do mensageiro é a possibilidade de criar conversas em grupo com até 200 mil participantes e o envio de arquivos de tamanho ilimitado.
- 12° Lugar: *Snapchat* – 538 milhões de usuários. O *Snapchat* é um aplicativo móvel de mensagens multimídia, tendo como principal recurso a

escolha do tempo em que as fotos e vídeos publicados pelo usuário remetente fica acessível ao usuário destinatário, projetado principalmente para incentivar a troca de mensagens (TILLMAN, 2021).

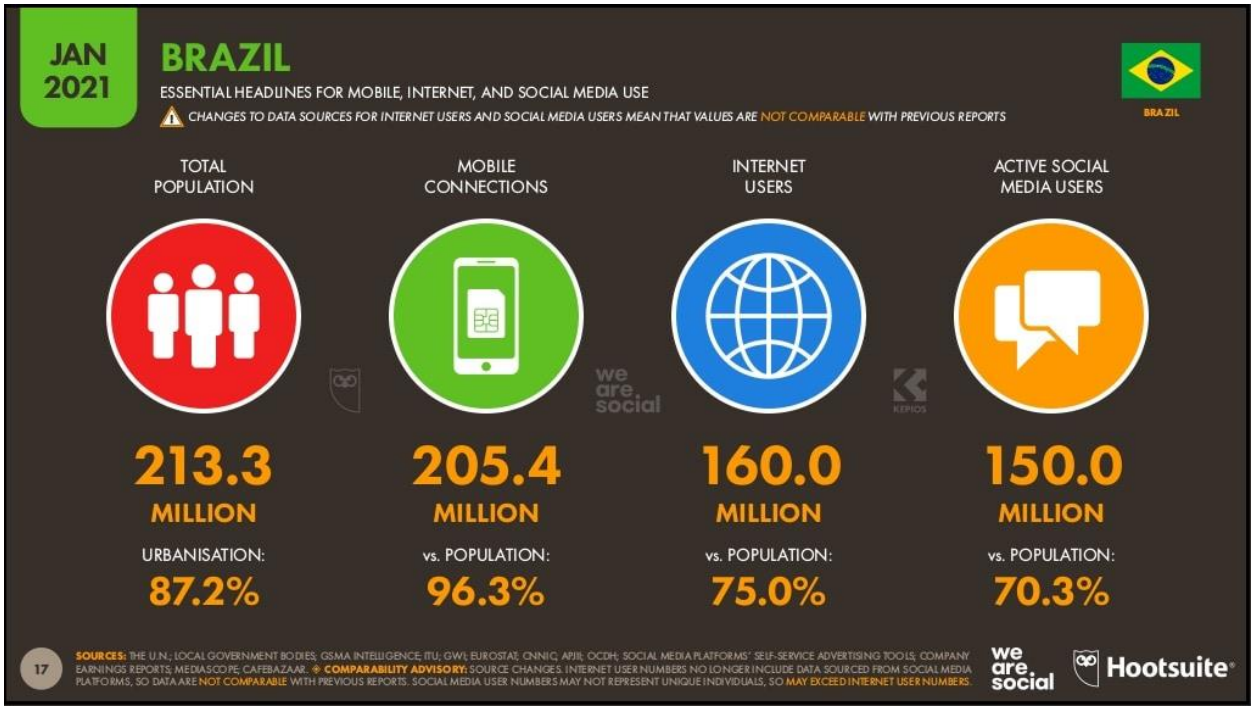
- 13° Lugar: *Kuaishou* – 506 milhões de usuários. De acordo com Batista (2021), *Kuaishou* ou *Kwai*, é uma rede social móvel baseada na criação e compartilhamento de vídeos curtos. O aplicativo foi originado na China, mas vêm ganhando espaço em todo o mundo, tendo como principal concorrente o *TikTok*, conhecido na China como *Douyin*.
- 14° Lugar: *Pinterest* – 454 milhões de usuários. *Pinterest* é uma rede social visual de compartilhamento de fotos, funcionando como álbuns de fotos para seus usuários. Ao navegar pelo aplicativo é possível buscar e descobrir imagens, criar pastas públicas para compartilhar as imagens e criar pastas privadas para armazenar imagens. Muitas empresas utilizam o *Pinterest* como uma forma de *marketing*, para expor as imagens de seus produtos ou suas campanhas (CASAROTTO, 2019).
- 15° Lugar: *Twitter* – 436 milhões de usuários. O *Twitter* é uma rede social de *microblog* que possui características de envio ou recebimento de textos com até 280 caracteres por mensagem, essas postagens são conhecidas como “*tweets*”. As interações entre os usuários acontecem de forma pública, ou seja, usuários podem ler e responder qualquer *tweet* dentro da plataforma, com exceção de usuários bloqueados (MLABS, 2021).
- 16° Lugar: *Reddit* – 430 milhões de usuários. Segundo Gaiato (2021), o *Reddit* é uma rede social de compilado de fóruns ou social *bookmarks*, no qual são organizadas por temas e reúnem pessoas para uma determinada comunidade que possui interesses em comum, chamada de “*subreddits*”.
- 17° Lugar: *Quora* – 300 milhões de usuários. Para Barbosa (2018), *Quora* é uma rede social de perguntas e respostas com objetivo em compartilhar conhecimento de pessoas que sabem para pessoas que não sabem, sobre um determinado conteúdo. A plataforma então pode ser definida da seguinte maneira: usuários encontram a dúvida e perguntam na plataforma, usuários com conhecimento visualizam a pergunta, respondem, editam e organizam as ideias sobre a aquele determinado

assunto, posta o seu entendimento e por fim, colabora no conhecimento coletivo das pessoas.

2.5.1 Redes Sociais no Brasil

A *DataReportal* (2021) possui relatórios de pesquisa separados por países, no Brasil, estima-se que no início do ano de 2021, a população do país tenha atingido 213,3 milhões de habitantes, sendo que 87,2% estão em um ambiente urbanizado. Cerca de 160 milhões dessas pessoas estão conectadas à *Internet* e aproximadamente 150 milhões de brasileiros possui alguma mídia social ativa, equivalendo a 70,3% da população total do Brasil, conforme mostrado na Figura 11.

Figura 11 - Dados da população, *Internet* e mídia sociais do Brasil



Fonte: DATAREPORTAL (2021, p. 60).

Dentre as redes sociais mais usadas por usuários da região do Brasil no mês de janeiro de 2021, é identificada as seguintes 16 mais utilizadas (*DataReportal,* 2021, p. 47):

- 1° Lugar: *YouTube;*
- 2° Lugar: *WhatsApp;*
- 3° Lugar: *Facebook;*

- 4° Lugar: *Instagram*;
- 5° Lugar: *Facebook Messenger*;
- 6° Lugar: *Twitter;*
- 7° Lugar: *TikTok*;
- 8° Lugar: *Pinterest;*
- 9° Lugar: *LinkedIn.* Segundo Barbosa (2021), é uma rede social de negócios, sendo a maior no quesito profissional. O principal objetivo da plataforma é apresentar a carreira profissional de seus usuários, promovendo a interação entre profissionais e empresas.
- 10° Lugar: *Telegram;*
- 11° Lugar: *Skype.* Para KINAST (2020), o *Skype* é um aplicativo multiplataforma de comunicação de texto, voz e vídeo. O *software* é usado principalmente para realizar chamadas entre dois usuários ou entre um grupo de usuários. As videochamadas possuem recursos de compartilhamento de tela e de gravação, além do *software* possuir um mensageiro instantâneo que permite comunicar através de textos, fotos, vídeos e arquivos.
- 12° Lugar: *Snapchat*;
- 13° Lugar: *Twitch*. De acordo com Noleto (2021), a *Twitch* é um serviço de *streaming* de vídeo ao vivo concebida inicialmente para a indústria de games, mas diversificada para qualquer tema. O diferencial da rede social é a interação entre o transmissor (*streamer*) e seus espectadores (*viewers*), que acontece através de um chat em tempo real da plataforma. Uma transmissão pode ter a duração contínua de no máximo 48 horas, após este tempo ela deve ser reiniciada.
- 14° Lugar: *Tumblr.* É uma plataforma de *microblog* para compartilhamento e interação de publicações de forma mais livre, sendo realizada por meio de textos, áudios, imagens, vídeos, *links*, gifs e citações. (CARNIEL, 2021).
- 15° Lugar: *Badoo.* Segundo Ventura (2021), o *Badoo* é uma rede social de relacionamento que possibilita a personalização do perfil, postagens de fotos, troca de mensagens instantâneas e conversas por vídeo. Possui a

ferramenta de busca tradicional e o de busca por pessoas próximas, utilizando a localização do dispositivo.

- 16° Lugar: *Reddit.*

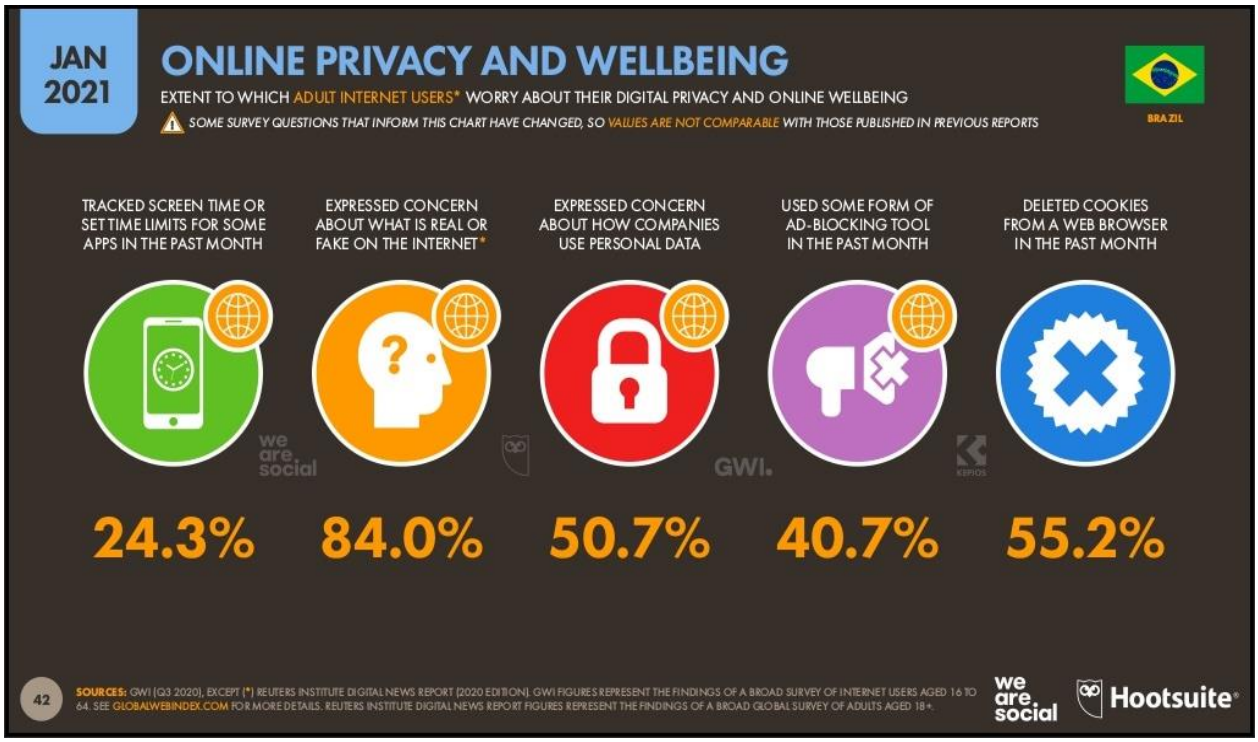
Por conta do grande crescimento de usuários nas redes sociais, houve surgimento de golpes e pessoas mal-intencionadas, que fazem de tudo para prejudicar outros usuários. Para Moraes (2011, p. 139, apud GOMES, 2017, p. 21) “da mesma forma que as redes sociais podem ser usadas para divulgação de conteúdo útil, ela também tem sido usada por criminosos, que induzem os usuários a clicarem em *links* e efetuar *download* de *malware*”. Segundo o CERT.BR (2012, p. 87-88):

> os principais riscos relacionados ao uso de redes sociais são: o contato com pessoas mal-intencionadas, o furto de identidade, a invasão de perfil, o uso indevido de informações, a invasão de privacidade, o vazamento de informações, a disponibilização de informações confidenciais, o recebimento de mensagens maliciosas, o acesso a conteúdo de mensagens maliciosas, o acesso a conteúdo impróprios ou ofensivos, danos à imagem e à reputação, o sequestro e o furto de bens.

Privacidade, segundo o dicionário online da língua portuguesa (DICIO, 2021), é a qualidade do que é privado, é referente ao particular, que busca assegurar a exposição e disponibilidade de informações acerca de uma pessoa ou empresa.

No Brasil, segundo pesquisas feitas para pessoas adultas pela *DataReportal* (2021), cerca de 84% destas pessoas estão preocupadas com o que é real ou falso na *Internet*, 50,7% deles expressa preocupação sobre como as empresas utilizam dos seus dados. No mês de dezembro de 2021, 40,7% utilizaram alguma ferramenta de bloqueio de anúncios e 55,2% se preocuparam em excluir os *cookies* de um navegador da web no mês de dezembro de 2020, conforme ilustrada na Figura 12.

Figura 12 - Dados sobre a preocupação da privacidade virtual e o bem-estar *online* dos brasileiros



Fonte: DATAREPORTAL (2021, p. 42).

Por conta de todos os riscos associados, algumas condutas podem ser tratadas para evitar, ou pelo menos dificultar, que esses ataques ocorram. Algumas das maneiras são:

a) Criar senhas com no mínimo 8 caracteres, misturando números e letras, e trocar essa senha a cada 6 meses;

b) Ao aceitar algum novo amigo nas redes sociais, conferir outros dados como foto, cidade e, se possível, por telefone. Alguém pode usar a foto de um conhecido seu para aplicar golpes;

c) Não divulgar suas informações pessoais como endereço completo, número de documentos, ou data de nascimento;

d) Refletir antes de postar uma foto em uma rede social, se ela pode te comprometer ou expor de alguma maneira. Depois de postadas, as fotos estão sujeitas a cópias e dificilmente você terá acesso a apagar todas caso se arrependa;

e) Modificar as opções de privacidade, fazendo com que só seus amigos diretos visualizem seu conteúdo;

f) Nunca avisar nas redes sociais que você passará dias fora, essa pode ser a informação que falta para alguém que está planejando roubar sua casa ou apartamento;

> g) Ao receber comentários com *links*, verifique se o *link* é válido. Se possível, digite-o no navegador em vez de clicar. (MORAES, 2011, p. 140, *apud* GOMES, 2017, p. 21).

Sousa (2021), procurou entender o comportamento e o grau de conhecimento das pessoas com relação à segurança da informação nas redes sociais, realizando uma pesquisa de opinião com 177 pessoas. Em relação aos resultados obtidos, foi observado que em 79,7% dos casos, as pessoas passaram dados pessoais via rede social, como telefone, endereço e documentos pessoais. Dos entrevistados, 81,4% afirmaram que já utilizaram ou utilizam datas comemorativas como senhas em aplicativos, 70,1% declararam ter dado permissão de acesso aos seus dados para sites e aplicativos desconhecidos pelo menos uma vez, 75,1% disseram que já adicionaram pessoas desconhecidas em suas redes sociais e 66,6% alegaram que salvam ou já salvaram senhas em seu navegador de *Internet*.

De acordo com Romero (2017), pesquisas realizas pela Universidade *Stanford*, nos Estados Unidos, cerca de 97% dos estadunidenses não leem os termos de uso e políticas de privacidade na *Internet* e pulam direto para opção “concordo”. No Reino Unido, aproximadamente 90% da população britânica aceita os termos e condições sem compreender com o que está concordando. A justificativa da falta de interesse por parte da população sob a leitura destes termos ocorre pelo fato de possuírem um conteúdo muito extenso (THINKMONEY, 2020).

Segundo a ISTOÉ (2017), a empresa britânica *Purple*, que trabalha com o fornecimento de *Wi-Fi* gratuito e *hotsposts* para lojas e áreas pública, forneceu uma ação para verificar se as pessoas realmente liam os termos de contrato antes de usufruir do serviço. Esta ação consistia em colocar uma cláusula dentro do contrato que exigia o cumprimento do usuário em trabalhar com serviços comunitários durante mil horas. Durante a campanha, aproximadamente 22 mil pessoas aceitaram os termos e acessaram os serviços que a empresa distribuía. Em contrapartida, apenas uma pessoa procurou a empresa por ter descoberto a campanha.

2.6 Engenharia Social

Engenharia Social é o conjunto de métodos e técnicas com o objetivo de obter informações sigilosas e importantes de pessoas ou organizações. Estas técnicas são utilizadas por pessoas mal-intencionadas que utilizam estratégias de persuasão, que “consiste na utilização de recursos emocionais ou simbólicos para induzir alguém a aceitar uma ideia, uma atitude, ou realizar uma ação” (MARCONDES, 2017).

> Na ausência desses protocolos de segurança, programas de treinamento e procedimentos adequados, qualquer um está exposto e arrisca-se à tornar vítima de cibercriminosos, que se utilizam da meios ardilosos e conhecimento técnico específico para aproveitarem da falta de perspicácia e proteção dos incautos que navegam através de meios eletrônicos como se a *Internet* fosse um mar tranquilo e não houvesse ali nenhum predador, esquecendo-se que o que se encontra na *Internet* é a reprodução do que há fora dela, e por isso muitas vezes haverão pessoas que pretendem obter vantagem sobre outras, furtar, extorquir e praticar todo tipo de dano e atrocidade (GUSMÃO, 2019, p. 8).

A engenharia social busca ir direto à parte mais fraca da segurança, segundo Aramuni e Maia (2018, p.32), o atacante desvia da “criptografia, segurança de computador e de redes, indo direto para o elo mais fraco de qualquer sistema de segurança: o ser humano”.

De acordo com Rocha (2018), existem dois tipos de ataques de engenharia social, os baseados em humanos e os baseados em tecnologia.

2.6.1 Ataques baseados em humanos

Segundo Rocha (2018), os ataques baseados em humanos requerem a interação pessoal sem utilizar tecnologia, utilizando técnicas de *dumpster diving, shoulder e tailgating*.

a) *Dumpster diving*: técnica que o atacante procura recuperar algo de valor para o próprio consumo, através do lixo de outra pessoa ou empresa.

   Exemplos de ativos que são roubados: Papéis com informações pessoais e/ou sigilosos, *pen-drives*, discos rígidos e cartões de memória.

Medida contra esse ataque: criar técnicas e políticas de descarte do lixo, triturando papéis e ocultando dados sensíveis. Em relação aos componentes eletrônicos, formatar e realizar a limpeza completa do dispositivo antes do descarte.

b) *Shoulder:* técnica que o atacante se aproveita da distração da vítima para espionar “sobre seus ombros”, buscando roubar informações pessoais e/ou sigilosas.

Exemplos de locais que essa técnica normalmente acontece: em bancos, através de caixas eletrônicos, e em locais públicos como aeroportos e *shoppings*, através de documentos físicos, *notebooks*, *tablets* e celulares.

Medida contra esse ataque: Procurar locais adequados para mexer em informações pessoais e/ou sigilosos, sempre olhar em sua volta procurando possíveis atacantes e utilizar películas de privacidade na tela dos dispositivos.

c) *Tailgating:* técnica no qual o atacante acessa locais não autorizados, explorando a distração ou a boa vontade da vítima, com o objetivo de obter informações confidenciais ou ativos valiosos.

Medida contra esse ataque: não emprestar *gadgets* a estranhos e utilizar chaves, senhas e/ou crachás para acesso a locais privados.

2.6.2 Ataques baseados em tecnologia

De acordo com Rocha (2018), os ataques baseados em tecnologia requerem o uso de equipamentos eletrônicos para manipular e enganar a vítima, utilizando técnicas de *phishing*, *spyware*, cavalo de troia e *baiting*.

a) *Phishing*: técnica mais comum de ataques da engenharia social, é um ataque de falsificação, que consiste no atacante utilizar um *e-mail* falso se passando ser um e-mail verdadeiro. Normalmente a mensagem do *e-mail* vem com algum arquivo anexado de teor financeiro ou uma mensagem persuadindo o usuário a acessar algum *link web* para atualização de dados. No momento do acesso ao site, a vítima se deparara com uma

página semelhante a original, mas se trata de um golpe, normalmente o atacante finge ser o website de uma organização (TIESO; SANTO, 2020).

Exemplos de situações envolvendo *phishing*: páginas falsas de redes sociais, páginas falsas de comércios eletrônicos, mensagens com *links* para códigos maliciosos e solicitações de recadastramento.

Medidas contra esse ataque, segundo Rocha (2018, p. 4):

I. Não clicar em *links* suspeitos adicionados a e-mails não solicitados ou em redes sociais;
II. Ao ler e-mails, não abra aquelas mensagens que sejam de um destinatário desconhecido;
III. Arquivos baixados automaticamente ou pedidos de downloads desnecessários devem ser evitados;
IV. Não executar arquivos não solicitados, *malwares* podem acessar suas informações e enviá-las diretamente para criminosos do outro lado da rede;
V. Sempre verificar a *Uniform Resource Locator* (URL, do português: Localizador Uniforme de Recursos) do *website*, pois em muitos casos o endereço pode parecer legítimo, mas a URL pode estar com erro de grafia ou o domínio pode ser diferente.

b) *Spyware*: técnica que utiliza um *software* de espionagem em segundo plano, no qual irá monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Exemplos de situações envolvendo *spyware*, segundo Rocha (2018): registrar os toques na tela, acompanhar atividades *online*, assumir o controle do computador e reduzir a velocidade do dispositivo.

Medidas contra esse ataque: utilizar programas *antispyware*, utilizar antivírus, colocar o nível de segurança do seu navegador no máximo e não baixar programas de origem desconhecida.

c) Cavalo de Troia: é um *malware*, que consiste na técnica de esconder um *software* malicioso dentro de arquivos de programas que parecem ser inofensivos.

Exemplos de situações envolvendo cavalo de troia, segundo Rocha (2018, p. 6):

I. Criar *backdoor*: normalmente os cavalos de Troia alteram seu sistema de segurança de forma que outros *malwares*, ou mesmo um *hacker*, consiga invadir.
II. Espionar: alguns cavalos de Troia são essencialmente *spyware* projetado para aguardar até que o usuário acesse suas contas *online* ou insira dados do seu cartão de crédito e depois enviar suas senhas e outros dados de volta ao atacante.
III. Transformar seu computador em um zumbi: as vezes os *hackers* não estão interessados somente nas informações confidenciais de um usuário, mas também querem usar o dispositivo como um escravo em uma rede sob seu controle.
IV. Enviar mensagens aleatórias: quando um dispositivo está infectado com um cavalo de Troia, este pode tornar-se um encaminhador de mensagens, seja através de *e-mail*, redes sociais ou SMS (no caso de um smartphone), espalhando conteúdo malicioso através das mensagens e infectando mais dispositivos.

Medidas contra esse ataque: evitar o acesso a sites desconhecidos, não instalar programas pirateados ou suspeitos e não acessar links suspeitos.

d) Baiting: técnica que um dispositivo infectado é deixado à disposição do usuário, com intenção de despertar a curiosidade da vítima, cometendo o erro de inserir o dispositivo infectado em algum dispositivo pessoal, infectando assim a máquina da vítima.

Exemplos de situações envolvendo baiting: infectar um CD, pen-drive, cartão de memória ou discos-rígidos com malwares.

Medidas contra esse ataque: não adicionar dispositivos desconhecidos em sua máquina pessoal.

Segundo PERCILIA (2021), os principais objetivos pelos quais as pessoas mal-intencionadas buscam ao atacar suas vítimas, são: destruição das informações, modificação e/ou falsificação das informações da vítima, roubo dos dados e a interrupção de serviços.

Existem ferramentas e boas práticas de gestão de segurança da informação que diminuem as adversidades geradas pela engenharia social, mas é imprescindível a conscientização dos usuários (ARAMUNI; MAIA, 2018).

3 PROCEDIMENTOS METODOLÓGICOS

Quanto à natureza da pesquisa, esta pesquisa é um resumo do assunto, pois, conforme *Wazlawick* (2014, p. 21), “buscam apenas sistematizar uma área de conhecimento, usualmente indicando sua evolução histórica e estado da arte”, ou seja, adequado para os cursos de graduação.

Quanto aos objetivos, esta pesquisa é exploratória. Exploratória, pois busca “examinar um conjunto de fenômenos, buscando anomalias que não sejam ainda conhecidas e que possam ser, então a base para uma pesquisa mais elaborada” (WAZLAWICK, 2014, p. 22).

Quantos aos procedimentos técnicos, esta pesquisa é bibliográfica e experimental.

> A pesquisa bibliográfica é elaborada com base em material já publicado. Tradicionalmente, esta modalidade de pesquisa inclui material impresso, como livros, revistas, jornais, teses, dissertações e anais de eventos científicos. Todavia, em virtude da disseminação de novos formatos de informação, estas pesquisas passaram a incluir outros tipos de fontes, como discos, fitas magnéticas, CDs, bem como o material disponibilizado pela *Internet*. (GIL, 2017, p. 34).

Foi realizada uma pesquisa bibliográfica sobre a segurança da informação nas redes sociais, estudando teoricamente os problemas de segurança que estão envolvidas nas redes sociais. *Wazlawick* (2014), sugere que a pesquisa bibliográfica deve seguir os seguintes passos:

a) Listar periódicos e eventos relevantes ao tema da pesquisa e periódicos gerais sobre computação verificando se existe algum artigo na área do tema a ser pesquisado.
b) Selecionar da lista, títulos relacionados ao tema a ser pesquisado.
c) Ler artigos com alta relevância e fazer resumos com os principais assuntos aprendidos sobre o tema. Anotar títulos que podem ser mencionados na bibliográfica mesmo que tenham mais de cinco anos.
d) Se necessário, ler artigos de relevância média ou baixa, porém sempre priorizar os artigos com alta relevância.
e) O aluno decide se já possui material suficiente para elaborar uma pesquisa consistente.

Segundo *Wazlawick* (2014), a pesquisa experimental se dá pela manipulação de uma parte da realidade do pesquisador. No caso, este trabalho, por exemplo, demonstra uma técnica de enviar *e-mails*, utilizando táticas da engenharia social para enganar utilizadores de redes sociais. Em específico, foi usado o exemplo do *Facebook*, roubando as suas credenciais e os seus dados. Na pesquisa experimental é necessário possuir variáveis manipuláveis pelo pesquisador e variáveis de observação. A medição dessa variável de observação que pode concluir se existe alguma dependência entre ela e alguma variável manipulável. No caso desse trabalho, as variáveis manipuláveis são os componentes da rede, ou seja, servidores em nuvem, *softwares*, *firmwares* e funções para segurança.

A pesquisa experimental, de acordo com Gil (2017, p.34) “consiste essencialmente em determinar um objeto de estudo, selecionar as variáveis capazes de influenciá-lo e definir as formas de controle e de observação dos efeitos que a variável produz no objeto”.

Gil (2017), sugere que para a realização de uma pesquisa experimental é necessário seguir os seguintes passos:

a) Formulação do problema: **Quais os problemas e os riscos associados as redes sociais mais utilizadas em relação a segurança da informação?**
b) Definição do plano experimental: foi descrito os principais ataques relacionados a engenharia social e realizado uma simulação de *penetration testing* (do português: teste de intrusão).
c) Determinação do ambiente: o ambiente foi formado basicamente por uma máquina *Windows*, um servidor virtual de nuvem da AWS e algumas ferramentas que em conjunto servem para rodar a aplicação.
    - Ferramentas utilizadas:
        i. *Amazon* EC2: serviço da AWS, baseado em computação escalável na nuvem;
        ii. PuTTY: *software* de emulação de terminal de código livre;
        iii. *Gophish: framework* de campanhas *phishing*.
    - Configuração da instância do Amazon EC2: foi utilizada uma instância do tipo *t2.micro*, possuindo 1 CPU virtual de 2.5GHz de velocidade de processamento, 1 *Gigabyte* (GB) de memória Memória de Acesso

Randômico (*RAM)* e um armazenamento da instância do tipo *Elastic Block Store* (EBS);

- Configuração da Máquina Principal: Todos estes testes foram realizados em um *notebook Lenovo*, com o Sistema Operacional (SO) do *Windows 10 Home Single Language*, versão 21H1, com arquitetura de 64 *bits*. A máquina possuía um processador i7 de 8° Geração com 1,8 *GigaHertz* (GHz) de velocidade de processamento e 20 GB de RAM.

d) Coleta de dados: Foi criado e configurado a instância no *Amazon* EC2 (mostrado no Apêndice A), instalado o software do PuTTY (apresentado no Apêndice B) e feito a instalação e configuração do Gophish (exposto no Apêndice C). Após feita as referidas instalações e configurações, foi possível executar o servidor administrador e o servidor de *phishing* do *Gophish*. O acesso a plataforma permitiu iniciar campanhas de phishing, com o objetivo de roubar as credenciais de utilizadores da rede social do *Facebook,* coletando os dados do usuário.

e) Análise e interpretação dos dados: Após a realização da simulação do experimento, foi analisado se os dados informados pela vítima eram os mesmo que os obtidos na plataforma do *framework* do *Gophish*. Com isso, conclui-se que, o *login* e senha do usuário da rede social do *Facebook* foram capturadas pela plataforma do *Gophish*, portanto, dados foram coletados com sucesso.

f) Redação do relatório: registrar a pesquisa realizada no TCC2.

4 FERRAMENTAS UTILIZADAS NO AMBIENTE DE IMPLEMENTAÇÃO

Neste capítulo estão descritas as ferramentas utilizadas no ambiente de implementação. As ferramentas em conjunto possuem o propósito de realizar a simulação do experimento.

4.1 Plataforma da Amazon Web Services (AWS)

Amazon Web Services (AWS), é uma plataforma de *cloud* (do português: nuvem), criada para ser um dos melhores ambientes de *cloud computing* (do português: computação em nuvem) do mundo. A plataforma oferece mais de 200 serviços de *datacenters* no mundo, sendo utilizada por clientes comuns, empresas e órgãos governamentais, por ser ágil, inovadora e possuir um preço acessível (AWS, 2021).

A plataforma AWS disponibiliza serviços de computação, banco de dados, armazenamento, inteligência artificial, análises, *Internet of Things* (IoT, do português: *Internet* das Coisas) e *data lakes* (do português: lago de dados). A AWS possui 81 zonas de disponibilidade, divididas em 25 regiões diferentes em todo o mundo, sendo que possui 3 zonas de disponibilidade no estado de São Paulo, no Brasil (AWS, 2021).

4.1.1 Serviço da AWS: Amazon Elastic Compute Cloud (Amazon EC2)

O *Amazon Elastic Compute Cloud* (EC2) é um produto de computação escalável na nuvem da AWS, que fornece capacidade computacional segura e redimensionável por meio de *Virtual Machines* (VM, do português: Máquinas Virtuais), também denominados de servidores virtuais ou instâncias. (AWS, 2021).

De acordo com a Amazon (2021), o *Amazon EC2* fornece vários serviços importantes que foram utilizados no desenvolvimento do experimento, sendo eles:

- Ambientes de computação virtual, conhecidos como instâncias;
- Os modelos pré-configurados para suas instâncias, conhecidos como Imagens de Máquina da *Amazon* (AMIs), que empacotam os bits de que você precisa para seu servidor (incluindo o sistema operacional e software adicional);

- Várias configurações de capacidade de CPU, memória, armazenamento e redes para suas instâncias, conhecidas como tipos de instância;
- Informações seguras de *login* para suas instâncias usando pares de chave (a AWS armazena a chave pública e você armazena a chave privada em um lugar seguro);
- Volumes de armazenamento para dados temporários que são excluídos quando você interrompe, hiberna ou encerra sua instância, conhecidos como volumes de armazenamento de instâncias;
- Volumes de armazenamento persistentes para seus dados usando o *Amazon Elastic Block Store* (*Amazon* EBS), conhecidos como volumes do *Amazon* EBS;
- Vários locais físicos para seus recursos, como instâncias e volumes do *Amazon* EBS, conhecidos como regiões e zonas de disponibilidade;
- Vários locais físicos para seus recursos, como instâncias e volumes do *Amazon* EBS, conhecidos como regiões e zonas de disponibilidade;
- Os endereços *IPv4* estáticos para computação em nuvem dinâmica, conhecidos como endereços IP elásticos;
- Metadados, conhecidos como *tags*, que você pode criar e atribuir aos recursos do *Amazon* EC2;
- Redes virtuais isoladas logicamente do restante da Nuvem AWS que você pode criar e, opcionalmente, conectar à sua própria rede, conhecida como nuvens virtuais privadas (VPCs) (AWS, 2021, p. 1).

4.2 Software - PuTTY

O *PuTTY* é um *software* escrito e mantido por *Simon Tatham*, sendo gratuito e de fácil utilização, que possui compatibilidade com os sistemas operacionais do *Windows* e *Linux* (CHIARK, 2021).

De acordo com *Hostgator* (2021), o *PuTTY* é um *software* de emulação de terminal de código livre, desenvolvido com finalidade de estabelecer conexões de acesso remoto a servidores, via *Secure Shell* (SSH, do português: Shell Seguro).

Segundo Ferreira (2019), o cliente *SSH* é uma conexão segura entre a máquina do usuário a um servidor através do protocolo *SSH*, que garante a transferência de dados de maneira segura e dinâmica, sem a perda de informação.

A ferramenta *PuTTYgen* é um dos componentes essenciais do *PuTTY*, sendo um gerador de chaves para a criação de pares de chaves *SSH* públicas e privadas para servidores, possibilitando criar vários criptossistemas de chave pública,

incluindo o *Rivest-Shamir-Adleman* (RSA), tornando-os mais seguros. Além disso, possui a função de converter as chaves de arquivos para o seu formato nativo de compreensão, denominado *Putty Private Key* (.ppk, do português: Chave Privada do *Putty*) (PUTTYGEN, 2021).

4.3 Framework - *Gophish*

O *Gophish* é um *framework* (do português: estrutura) de *phishing*, gratuito e de código aberto, desenvolvido para empresas e *penetration testers* (do português: testadores de penetração). O propósito do *software* do *Gophish* é disponibilizar ferramentas para criar campanhas em ambientes de simulação, para treinar e conscientizar usuários comuns ou de uma determinada organização de ataques de *phishing* que acontecem no mundo real (WRIGHT, 2018).

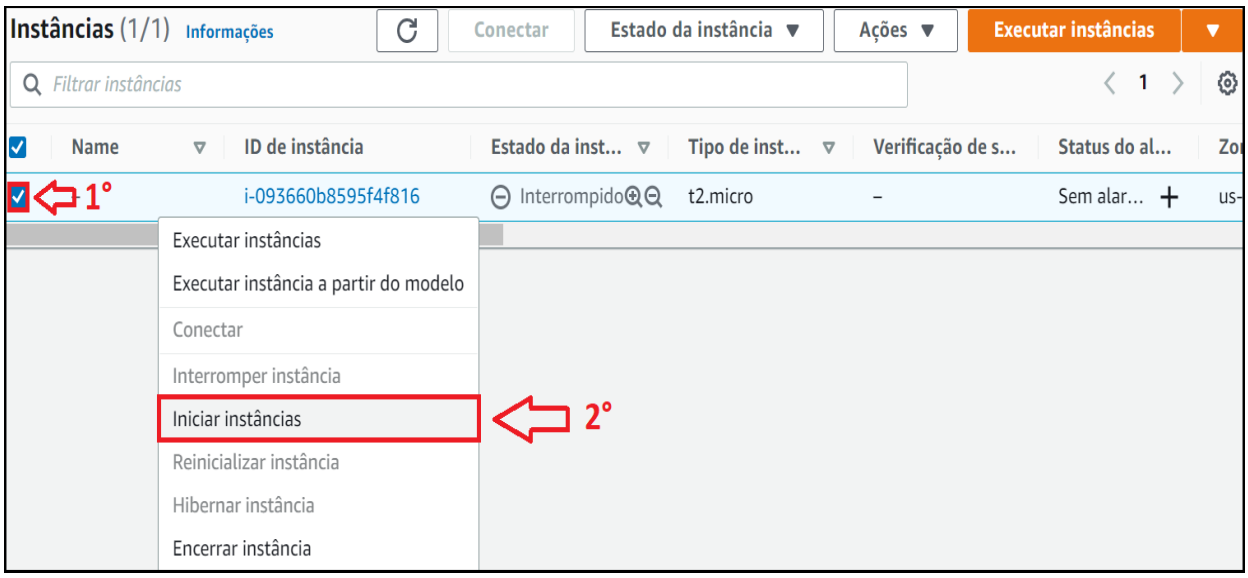
5 CONFIGURAÇÃO E UTILIZAÇÃO DO AMBIENTE

Neste capítulo é descrito a construção do ambiente de simulação, aplicando a configuração das ferramentas e *softwares* mencionados no Capítulo 4. O objetivo desta implementação é realizar uma simulação de *penetration testing*, visando demonstrar as vulnerabilidades e os riscos que os usuários podem enfrentar.

5.1 Serviços de computação em nuvem

Após realizar o processo de criação e configuração do ambiente do servidor virtual, com base na imagem do *Debian*, descrito no Apêndice A, será possível ligar a instância clicando em “Iniciar Instâncias”, conforme mostrado na Figura 14.

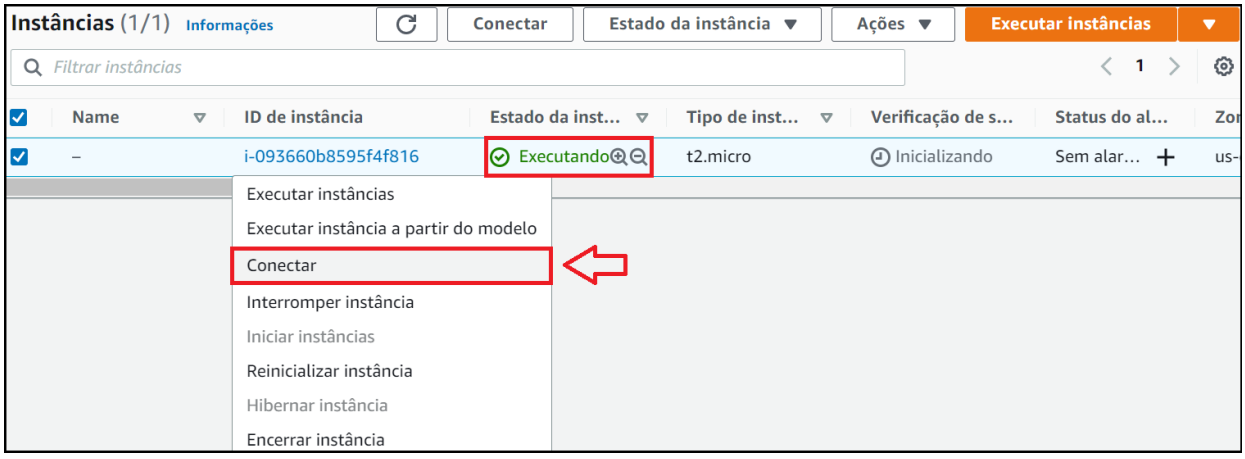
Figura 13 - Iniciar instância no *Amazon* EC2



Fonte: Tela de captura alterada do *website* da AWS (2021).

Aguardar até que o estado da instância esteja em execução, posteriormente, clique em “Conectar”, conforme exibido na Figura 15.

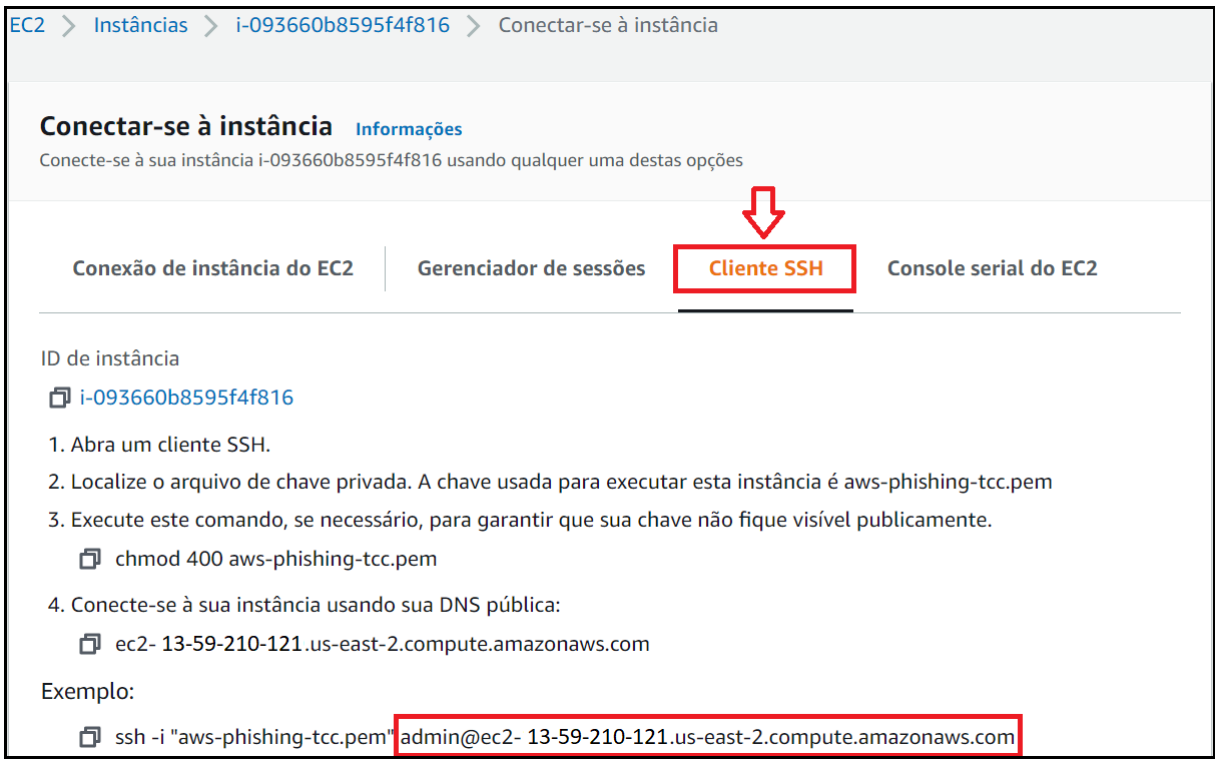
Figura 14 - Conectar ao servidor virtual do *Amazon* EC2



Fonte: Tela de captura alterada do *website* da AWS (2021).

Após a conexão da instância *Linux*, é necessário selecionar a opção “Cliente SSH”, no qual conterá o ID da instância, que é o nome do usuário (*admin@*) em conjunto do *Domain Name System* (DNS, do português: Sistema de Nomes de Domínio) público da instância (*ec-2-13-59-210-121.us-east-2.compute.amazonaws.com*), que será inserida no *Host Name* do *PuTTY*, conforme ilustrado na Figura 16.

Figura 15 - Instruções para abrir a instância no *Amazon* EC2

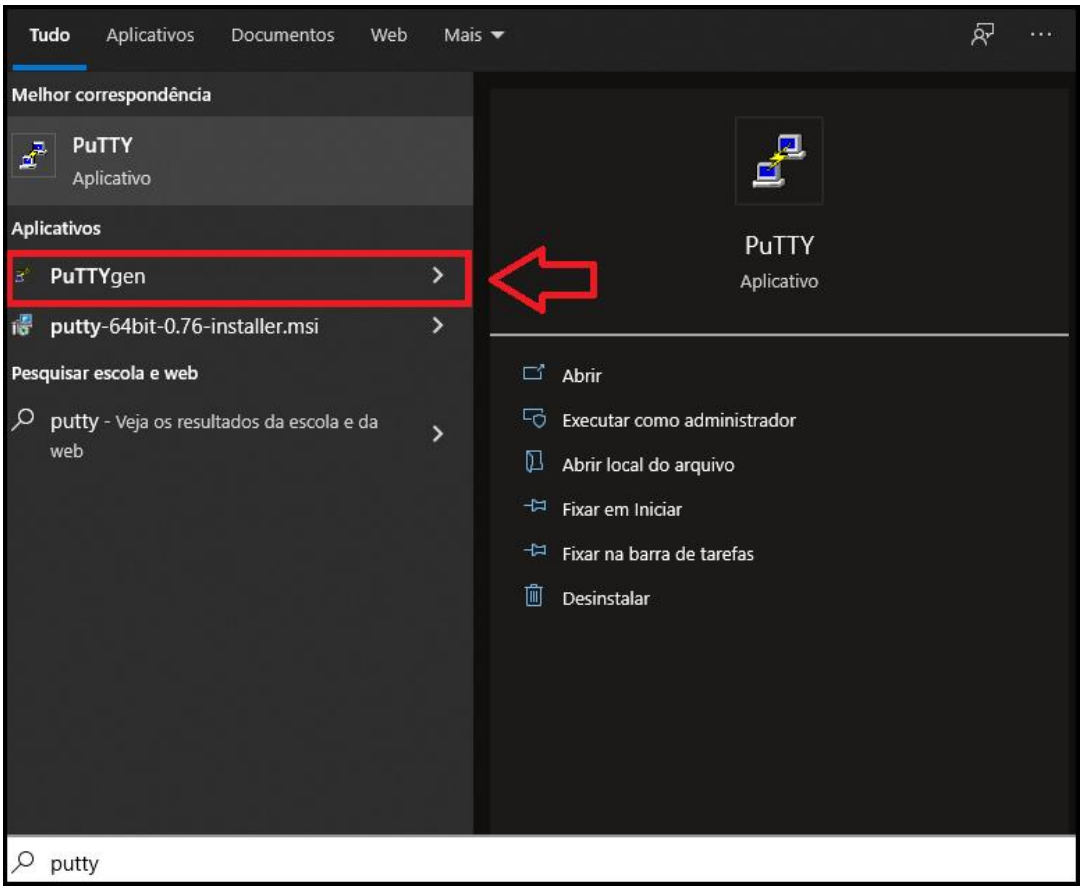


Fonte: Tela de captura alterada do *website* da AWS (2021).

5.2 PuTTY

Para se conectar a instância *Linux* com a imagem do *Debian* na AWS, é necessário utilizar o *software PuTTY*, procedendo a instalação do emulador de terminal, descrita no Apêndice B. Em conjunto ao *software PuTTY,* é instalado a ferramenta de geração de chaves, denominada *PuTTYgen*, conforme apresentado na Figura 17.

Figura 16 - Acessar a ferramenta *PuTTYgen*

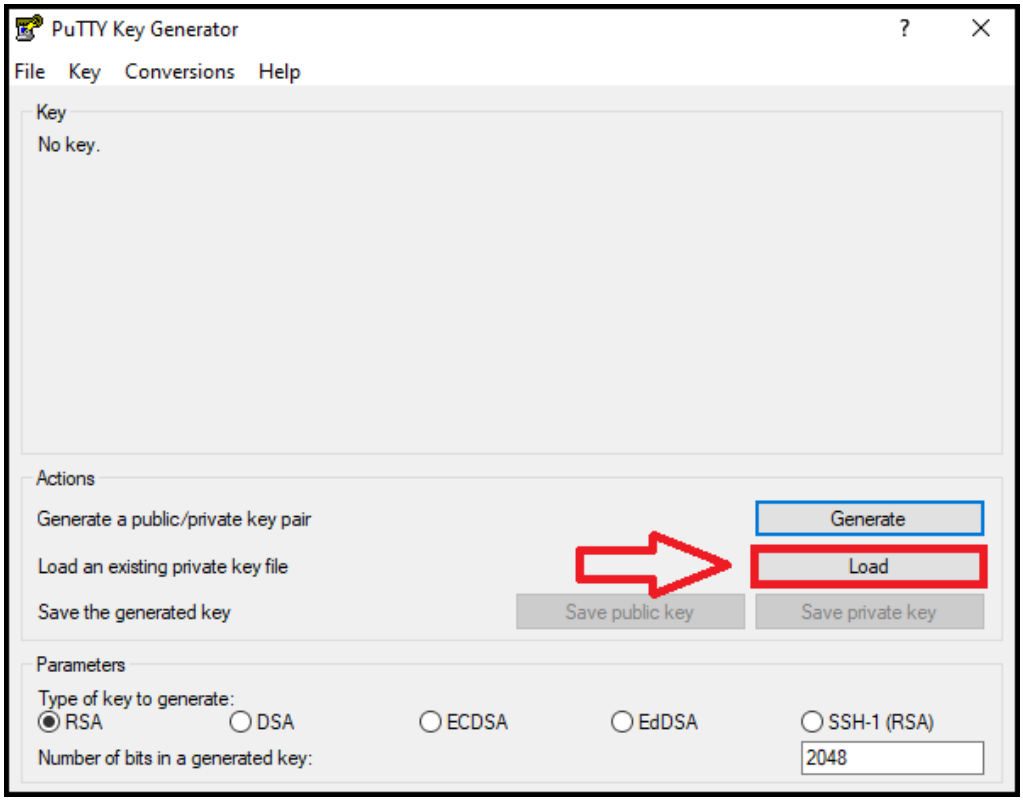


Fonte: Tela de captura alterada do *website* da AWS (2021).

A ferramenta *PuTTYgen* tem a função de converter o arquivo ".pem", gerado na conclusão da criação da instância da AWS, para o formato ideal de conectar a instância do *Amazon* EC2 no *software PuTTY*, chamado ".ppk".

Na inicialização do gerador de chaves *PuTTYgen,* foi escolhido a opção do tipo de criptografia a ser utilizada na chave, RSA com 2048 *bits*. Após o procedimento, foi selecionado a opção "*Load*" (do português: carregar), conforme ilustrado na Figura 18.

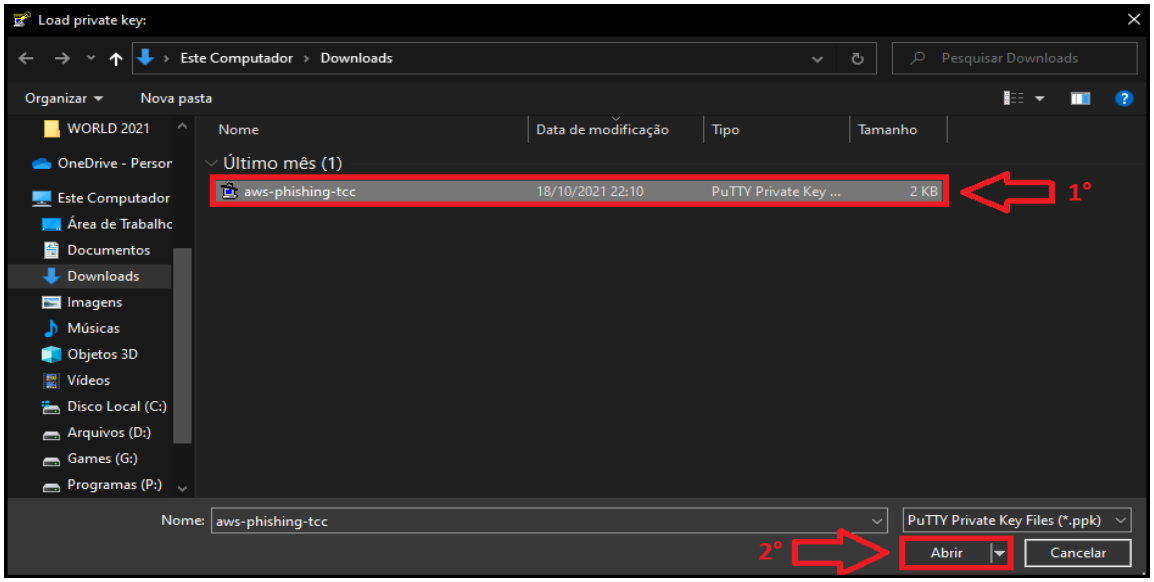
Figura 17 - Conversão da chave privada no *PuTTYgen*



Fonte: Tela de captura alterada do *website* da AWS (2021).

Posteriormente, no explorador de arquivos, foi identificada a chave obtida, baixada e salva no final do procedimento do Anexo A, denominada "*aws-phishing-tcc.pem*", conforme exibido na Figura 19.

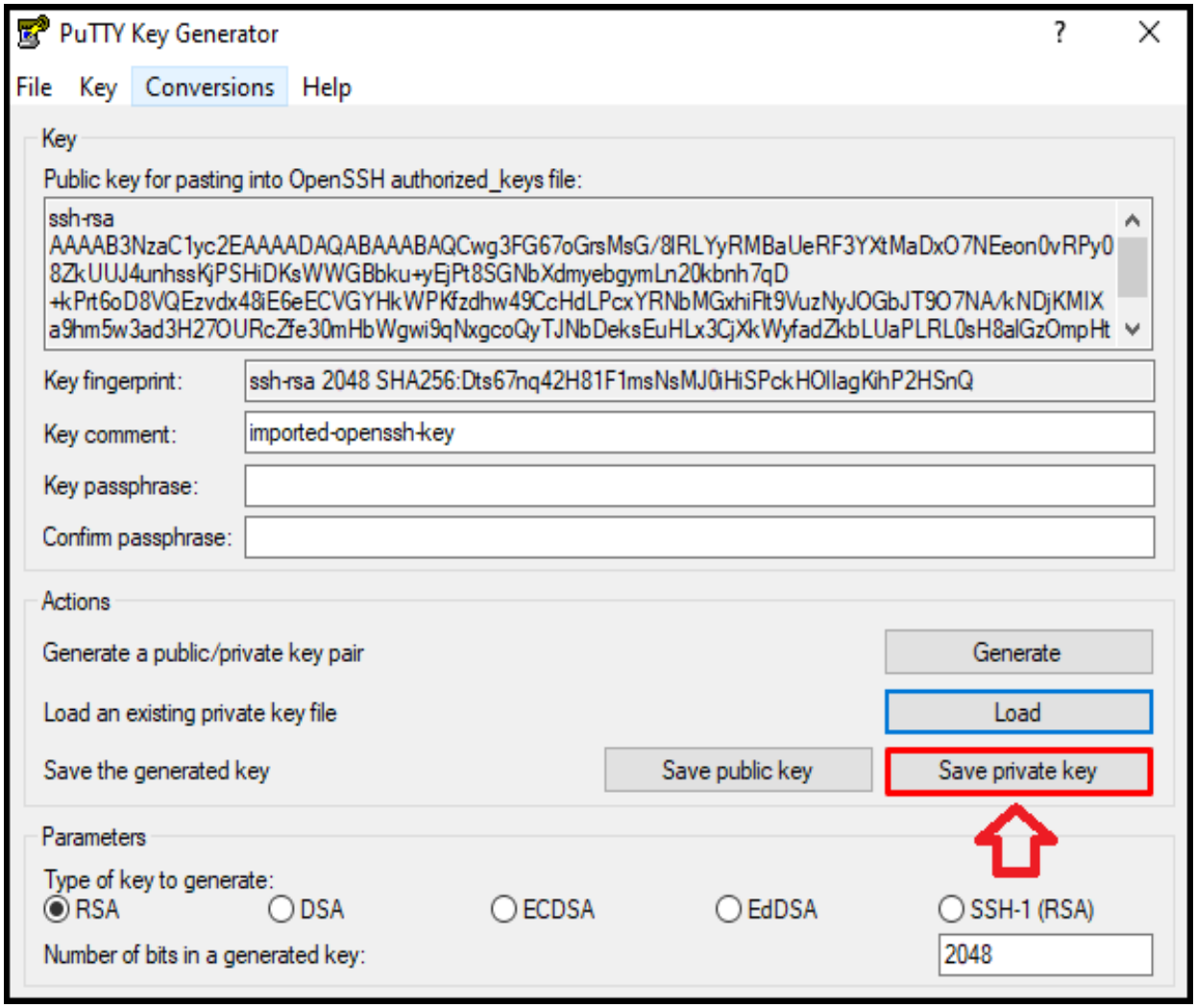
Figura 18 - Busca da chave privada no explorador de arquivos



Fonte: Tela de captura alterada do *website* do AWS (2021).

Após selecionado e aberto o arquivo, a chave foi criptografada e convertida para o formato “.ppk”. Em seguida, é feita o resgate da chave, clicando em “*Save private key*” (do português: salvar chave privada), conforme mostrado na Figura 20.

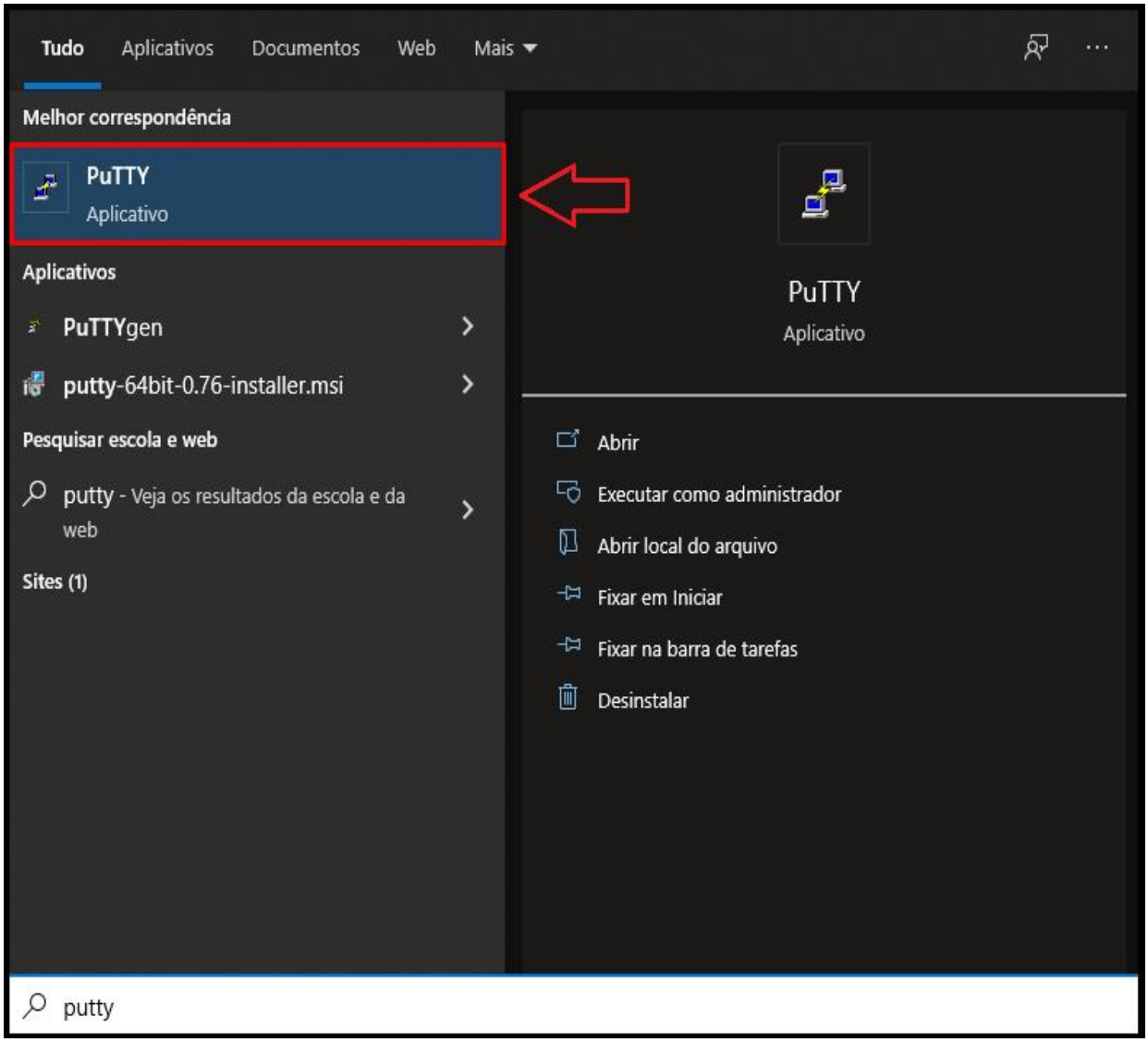
Figura 19 - Salvar a chave privada convertida



Fonte: Tela de captura alterada do *website* do AWS (2021).

Concluído o procedimento de conversão das chaves, no *PuTTYgen*. É necessário acessar o *software PuTTY*, conforme exposto na Figura 21.

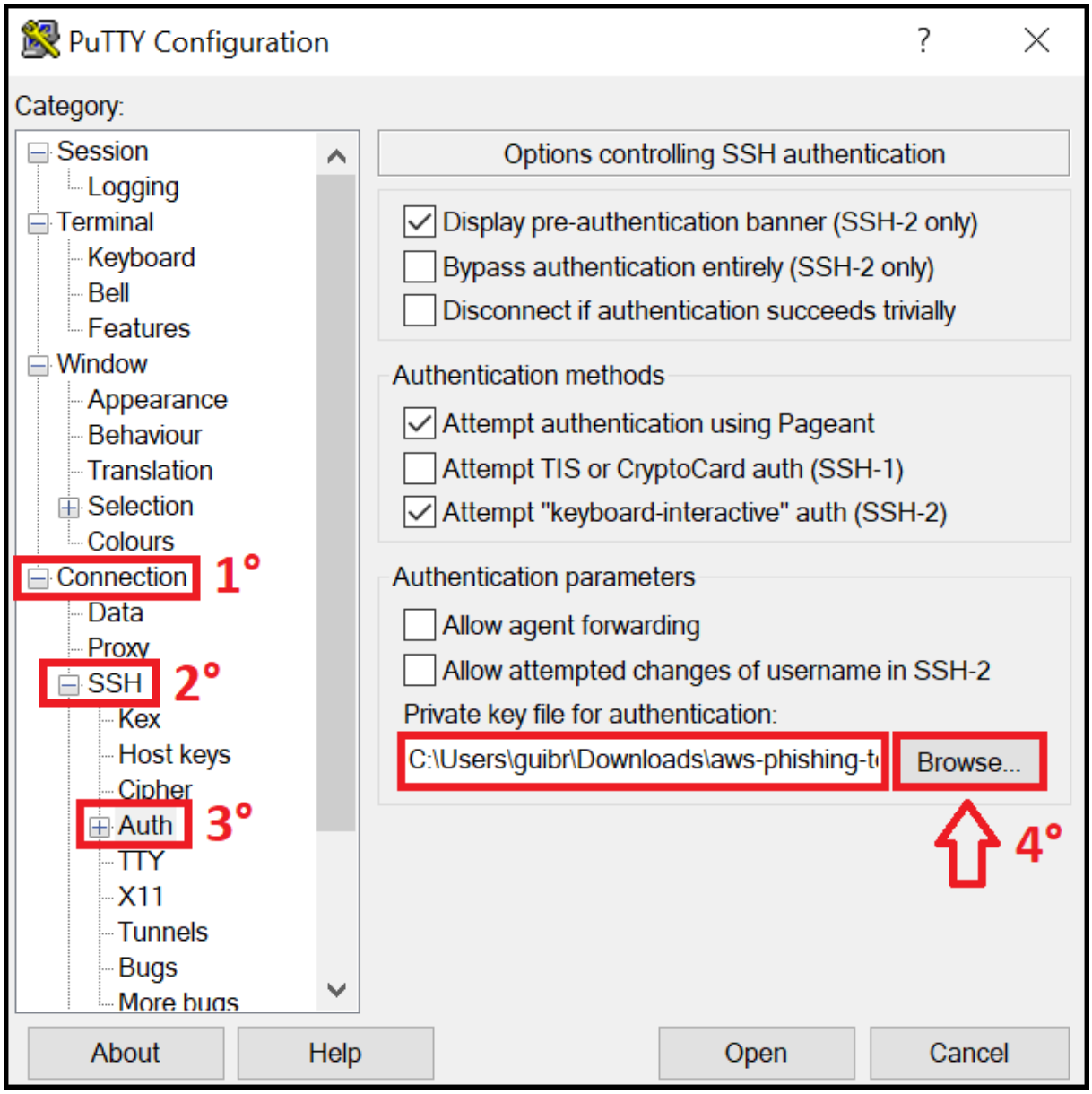
Figura 20 - Acessar o software do PuTTY



Fonte: Tela de captura alterada das configurações do PuTTY (2021).

Ao abrir a interface de configuração do *PuTTY*, é necessário expandir a categoria “*Connection*” (do português: conexões), posteriormente expandir a subcategoria localizada dentro de *Connection*, chamada “SSH”, selecionando a opção “*Auth*”. Na opção “*browser*” (do português: navegador) foi adicionado o arquivo de chave privada convertido, denominado “*aws-phishing-tcc.ppk*”, conforme exibido na Figura 22.

Figura 21 - Adicionando o arquivo de chave privada para autenticação



Fonte: Tela de captura alterada das configurações do *PuTTY* (2021).

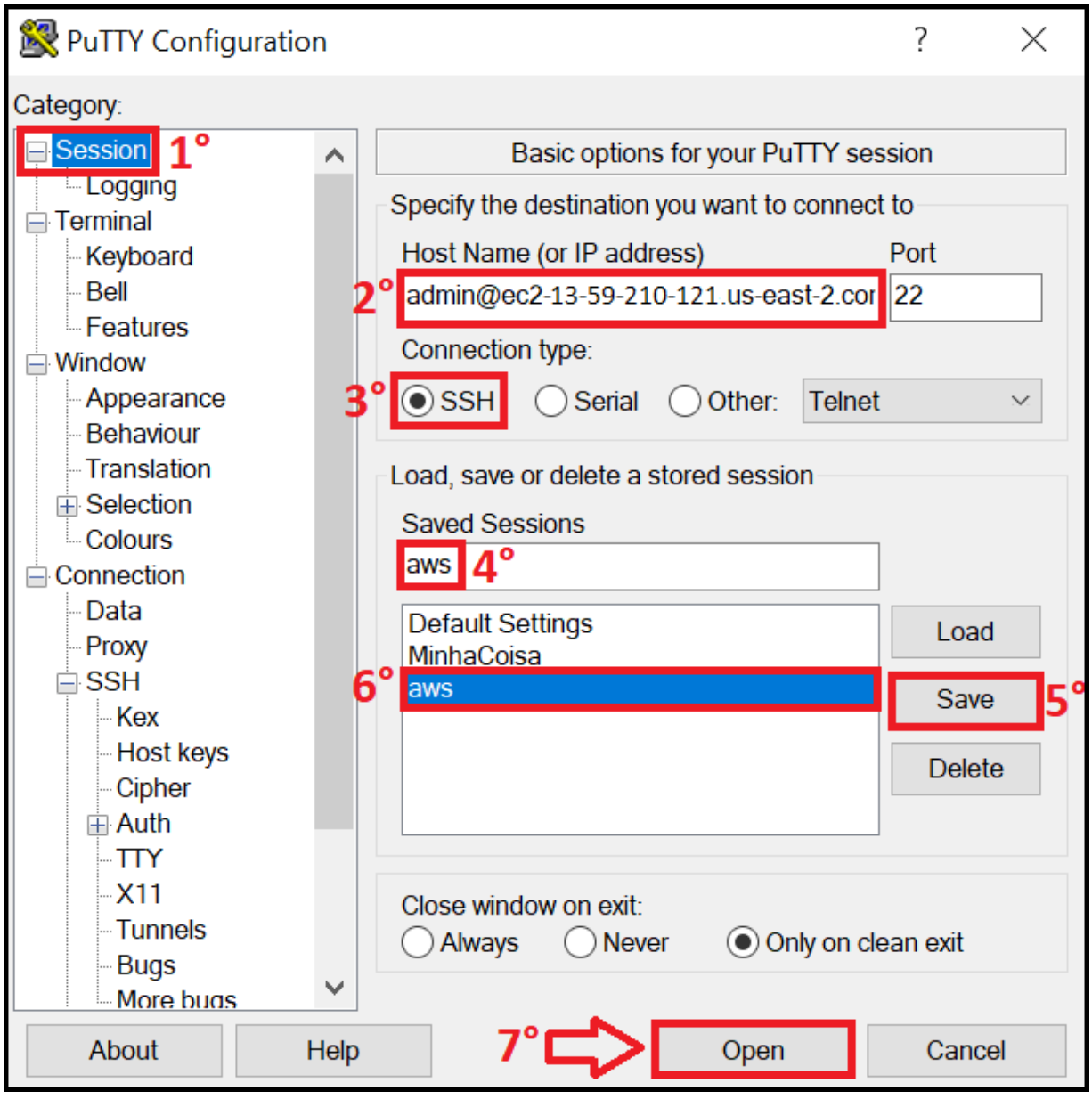
Ao incluir o arquivo de chave privada, é necessário colocar os dados da sessão da instância da AWS. Ainda dentro do *PuTTY*, clicando na categoria *Session* (do português: sessão), será aberta as opções básicas de configuração para iniciar uma sessão no *PuTTY*.

No campo "*Host Name*" (do português: nome do hospedeiro) é colado as informações do nome do usuário em conjunto do DNS da instância, que foram obtidas na página 51, conforme foi exibido na Figura 16.

Realizado este procedimento, foi selecionado o número da porta (do inglês: *port*) como padrão "22", estabelecendo a conexão ao servidor do tipo SSH. Em

seguida, foi criada e aberta a sessão, denominada de “*aws*” e, posteriormente foi acessada, clicando no botão *open* (do português: abrir), conforme mostrado na Figura 23.

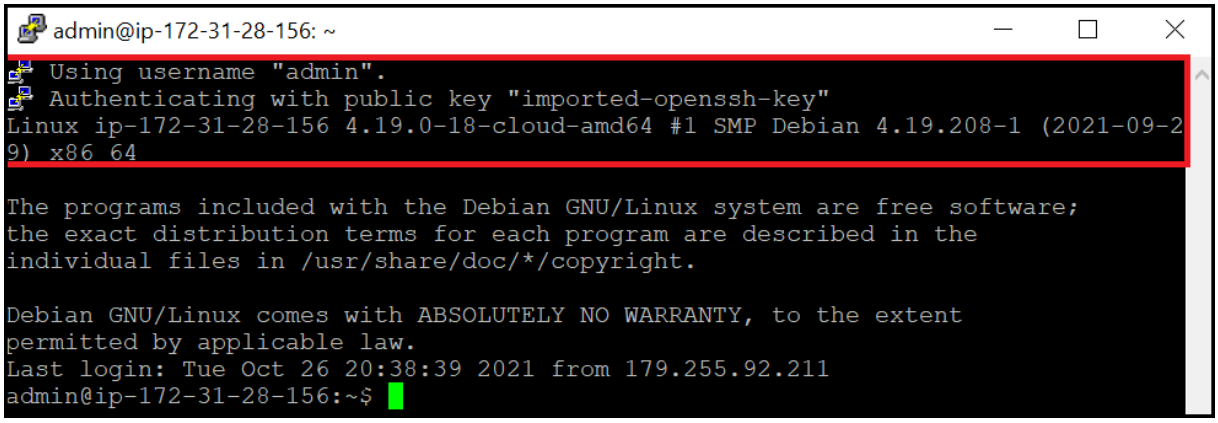
Figura 22 - Configuração da sessão no *software* do *PuTTY*



Fonte: Tela de captura alterada das configurações do *PuTTY* (2021).

Configurações finalizadas para a integração da instância *Linux* ao *PuTTY*, é aberto o terminal com a imagem do sistema operacional *Debian* na arquitetura 64 *bits*, usando o nome do usuário “*admin”* autenticado com a chave pública, conforme ilustrado na Figura 24.

Figura 23 - Acesso à instância do *Amazon* EC2 utilizando o *PuTTY*

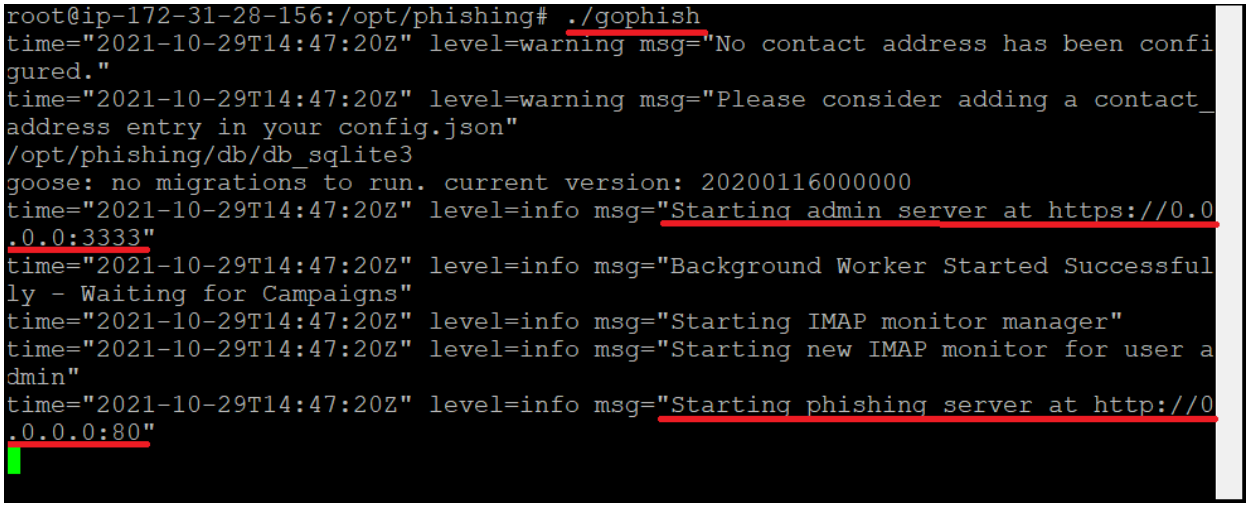


Fonte: Tela de captura alterada do *PuTTY* (2021).

5.3 *Gophish* – Passo a passo da configuração e de envio do *e-mail phishing*

Após a instalação e configuração do ambiente de simulação do *Gophish*, expostas no Apêndice C, o código "*./gophish*" foi inserido no terminal. O código permite iniciar o servidor administrador e o servidor de *phishing*, conforme exibido na Figura 25.

Figura 24 - Executando os servidores do *Gophish*



Fonte: Tela de captura alterada do terminal no *PuTTY* (2021).

O servidor administrador garante acesso à plataforma do *framework* do *Gophish* para realizar campanhas, enquanto o servidor *phishing* permite enviar *e-mails* para usuários selecionados.

Para acessar a plataforma do *Gophish*, após a execução dos servidores, foi necessário abrir o *browser* (do português: navegador) do *Google Chrome*. Posteriormente, foi acessado o servidor administrador, incorporando o endereço IP da instância do EC2, digitando *https*://<endereço IP aqui>:3333 (este endereço IP se encontra no painel do *Amazon* EC2, conforme exibido na Figura 16).

Figura 25 - Endereço de acesso ao *framework* do *Gophish* com o IP da instância do *Amazon* EC2

Fonte: Tela de captura da barra de pesquisa do *Google Chrome*

Após acessar o endereço *https://13.59.210.121:3333*, será aberto o *layout* inicial do *Gophish*, possibilitando entrar na plataforma, conforme apresentado na Figura 27.

Figura 26 - Layout de entrada do *Gophish*

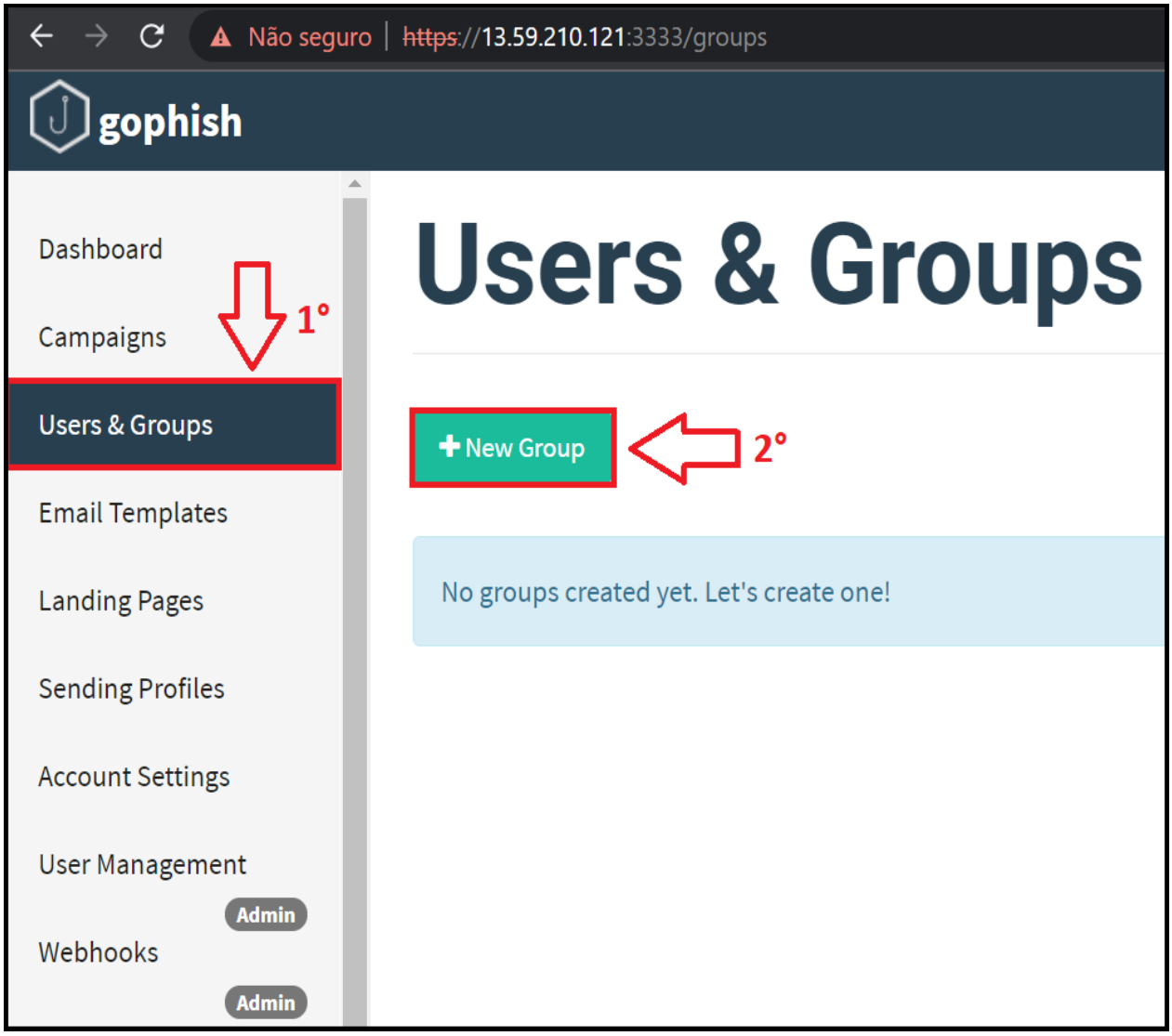
Fonte: Tela de captura alterada do *Gophish* (2021).

A credencial padrão para fazer *login* na plataforma é:

- 1° - Nome de usuário: *admin*
- 2° - Senha: *gophish*

Ao entrar com o usuário e senha na plataforma, será possível criar a campanha de *phishing*. Primeiramente, é necessário criar um grupo, ao qual será adicionado os usuários que irão receber o *e-mail* de *phishing*. No menu de navegação, em *Users & Groups* (do português: Usuários e Grupos) existe a possibilidade de criação de um *New Group* (do português: Novo Grupo), conforme mostrado na Figura 28.

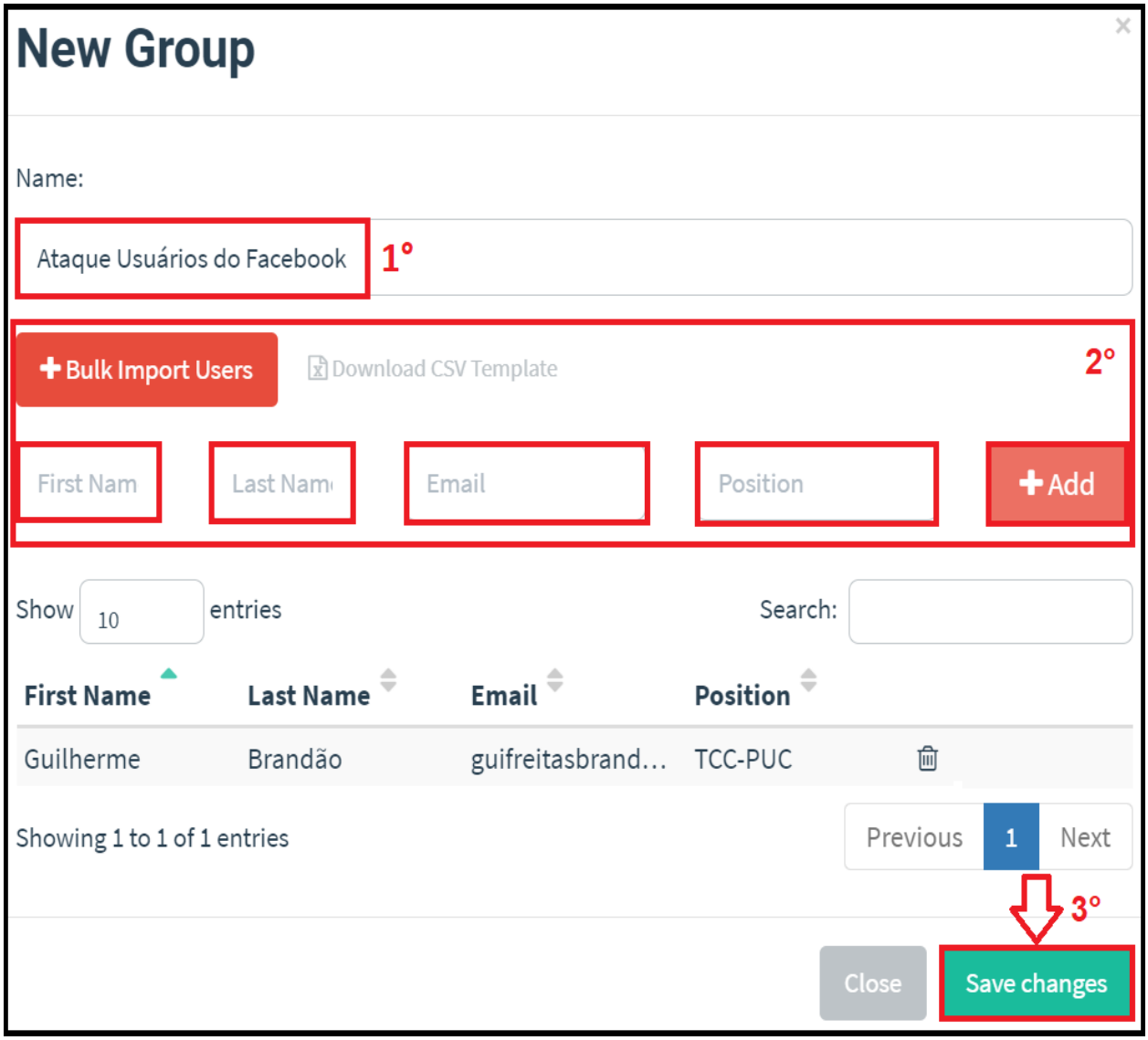
Figura 27 - Criar um grupo no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

Em seguida, será aberta a caixa de diálogo para adicionar as vítimas ao *New Group*, na qual será enviada os *e-mails*, conforme exibido na Figura 29.

Figura 28 - Configuração de grupo no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

A Figura 29 exibe os passos que devem ser realizados:

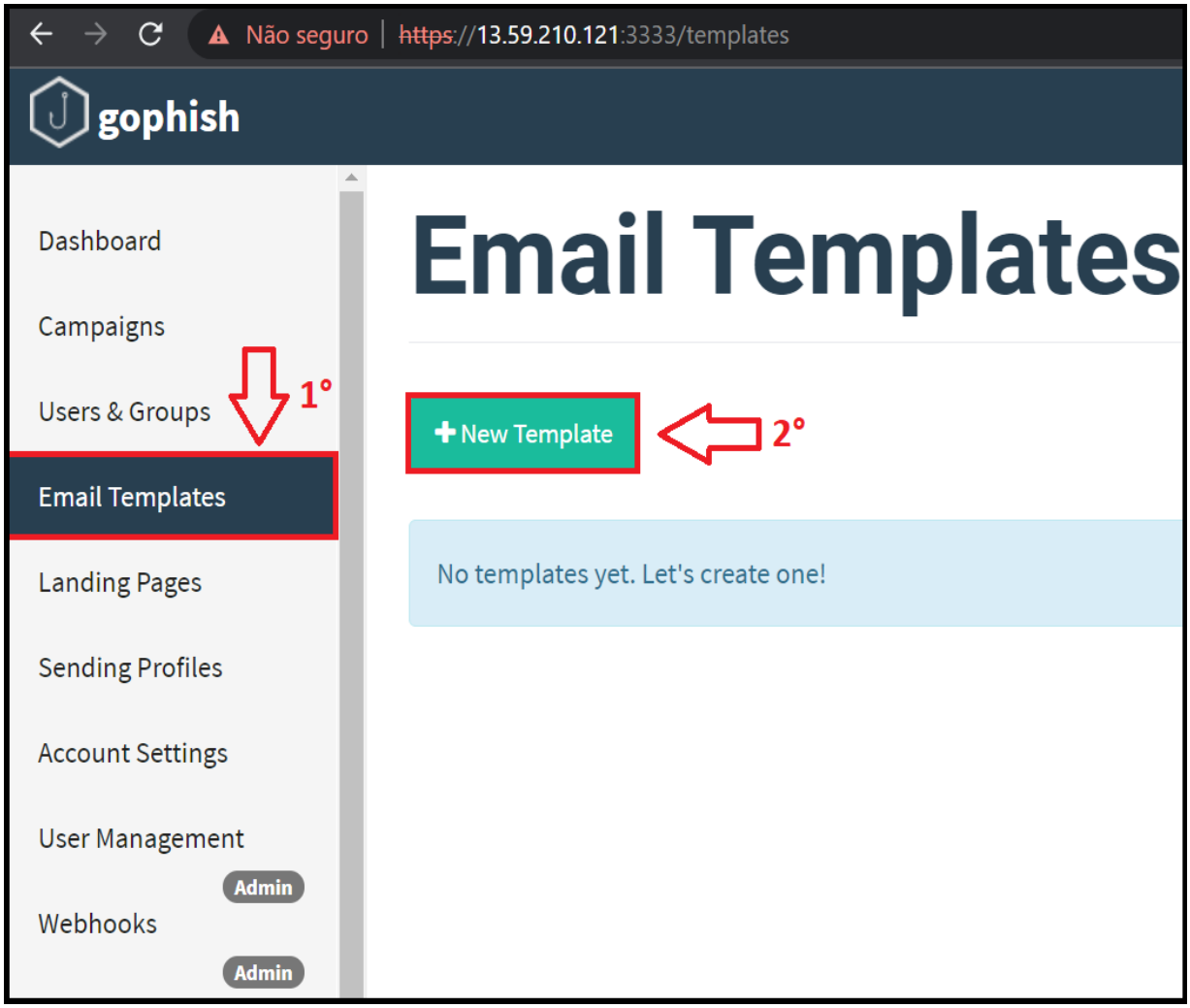
1° Passo: Especificar um nome exclusivo para o grupo, no campo *Name* (do português: Nome).

2° Passo: Adicionar os usuários ao grupo, tendo a opção de anexar um arquivo do tipo *Comma-Separated-Values* (CSV, do português: Valores Separados por Vírgulas) ou na forma manual, colocando o primeiro nome do usuário, seguido pelo último nome, *e-mail* e situação. Após colocar estes dados, conclui-se no botão *Add* (do português: adicionar).

3° Passo: Adicionado os usuários ao grupo, clique em *Save Changes* (do português: Salvar Mudanças).

Após criar o grupo, é necessário elaborar o conteúdo do *e-mail* no qual será enviado às vítimas. No menu de navegação, em *E-mail Templates* (do português: Modelos de *E-mail*), é possível criar um *New Template* (do português: Novo Modelo), conforme ilustrado na Figura 30.

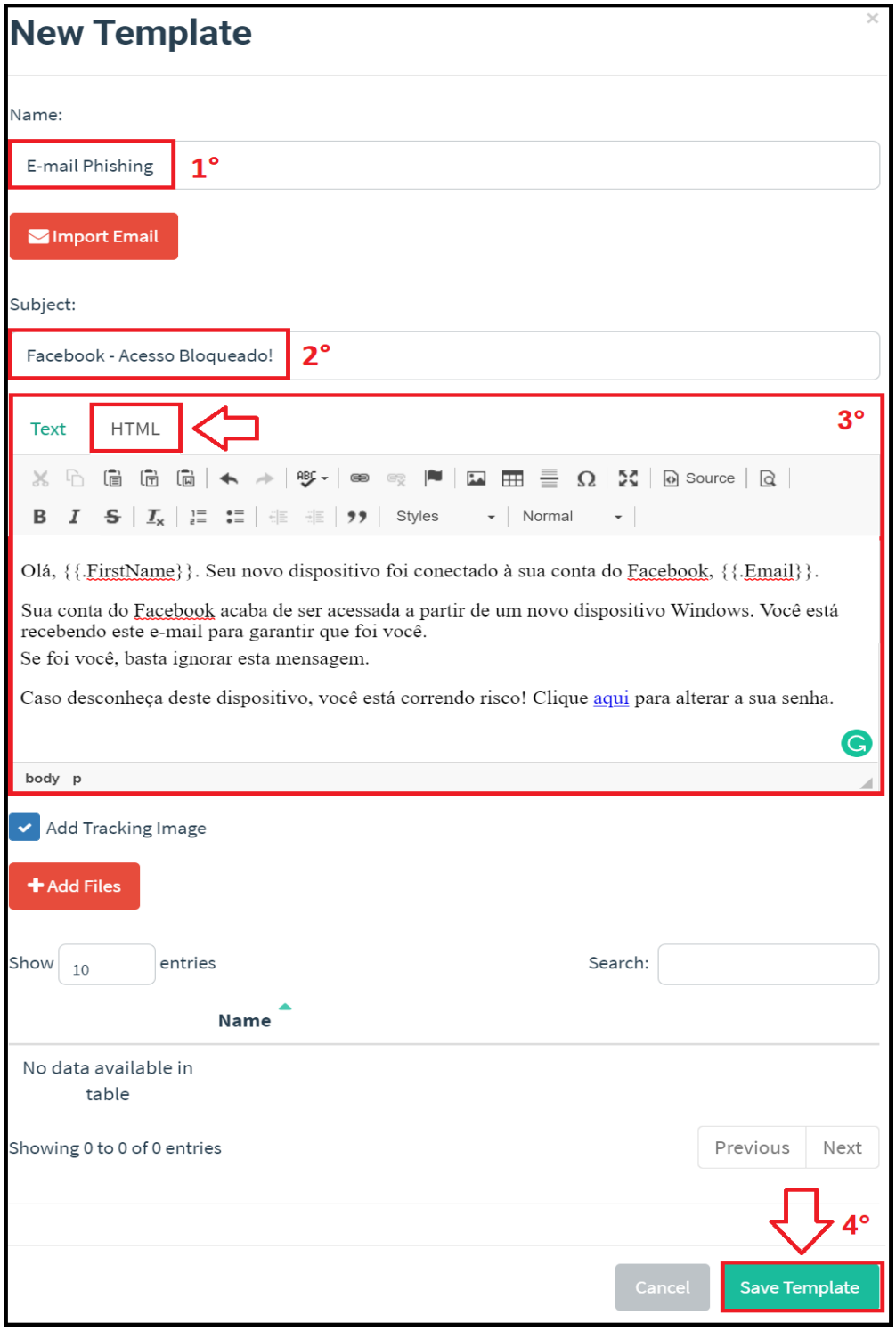
Figura 29 - Criar um modelo de *e-mail* no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

Em seguida, é aberta a caixa de diálogo para elaborar o conteúdo do *e-mail* ao *New Template*, a qual será enviada às vítimas, conforme exibido na Figura 31.

Figura 30 - Configuração do modelo de *e-mail* no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

A Figura 31 exibe os passos que devem ser realizados:

1° Passo: Especificar um nome exclusivo para o modelo, no campo *Name*.

2° Passo: Importar o conteúdo de um *e-mail* já existente na opção *Import E-mail* (do português: Importar E-mail) ou criar do zero o conteúdo de um novo *e-mail*,

sendo necessário definir o assunto do *e-mail*, no campo *Subject* (do português: o assunto).

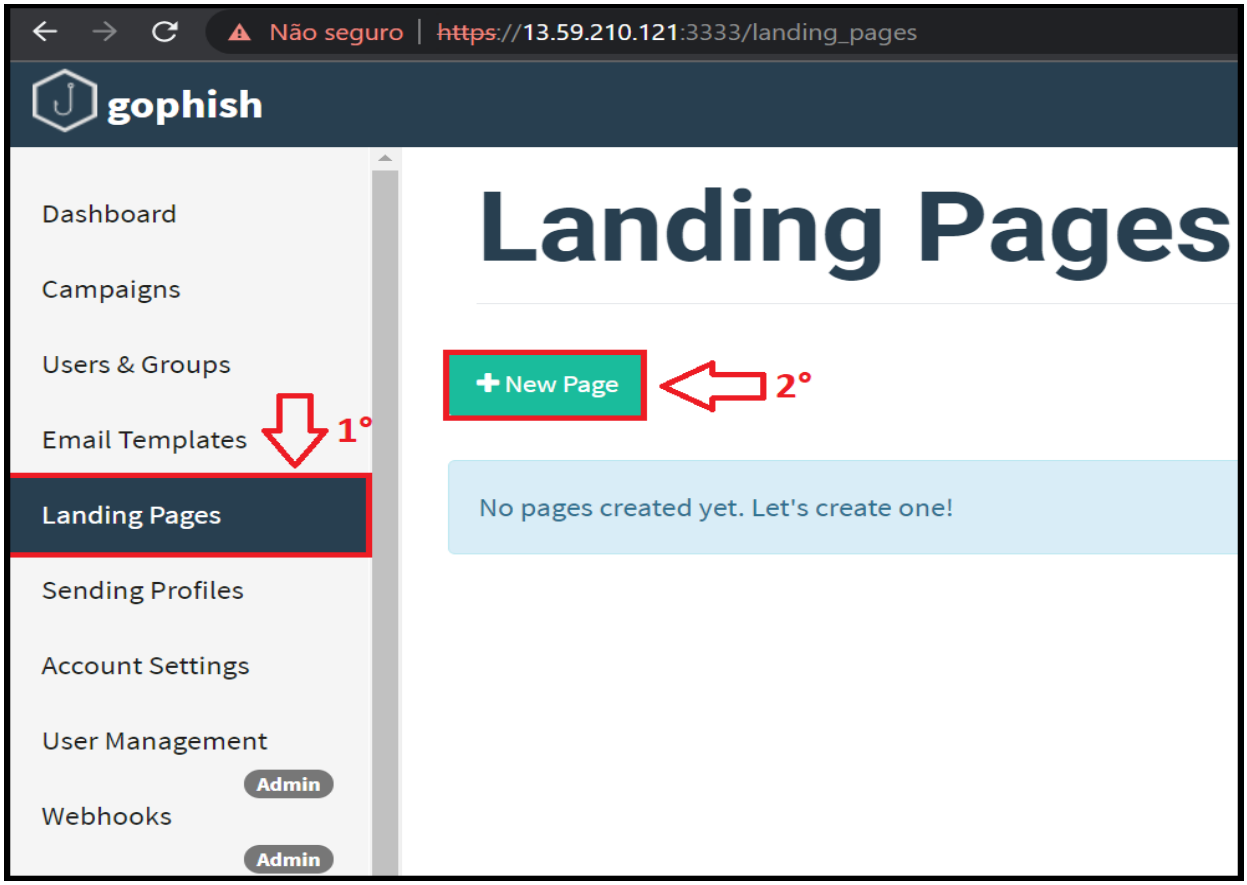
O *HyperText Markup Language* (HTML, do português: Linguagem de Marcação de Hipertexto) é uma linguagem no qual são construídas as páginas *web*. Segundo Xavier (2019), “o HTML nada mais é que uma linguagem usada para criar páginas *web* por meio de marcadores (*tags*) e atributos, que definem como o conteúdo deve ser apresentado em um navegador *web*”.

3° Passo: Elaborar o conteúdo da mensagem, utilizando a linguagem HTML.

4° Passo: Salvar o modelo, clicando em *Save Template* (do português: Salvar Modelo).

Após criar o modelo do *e-mail*, é necessário elaborar a página de destino, que são páginas em HTML reais que são retornadas aos usuários quando eles clicam nos *links* de *phishing* que eles recebem por *e-mail.* No menu de navegação, em *Landing Pages* (do português: Páginas de Destino), é possível criar uma *New Page* (do português: Nova Página), conforme apresentado na Figura 32.

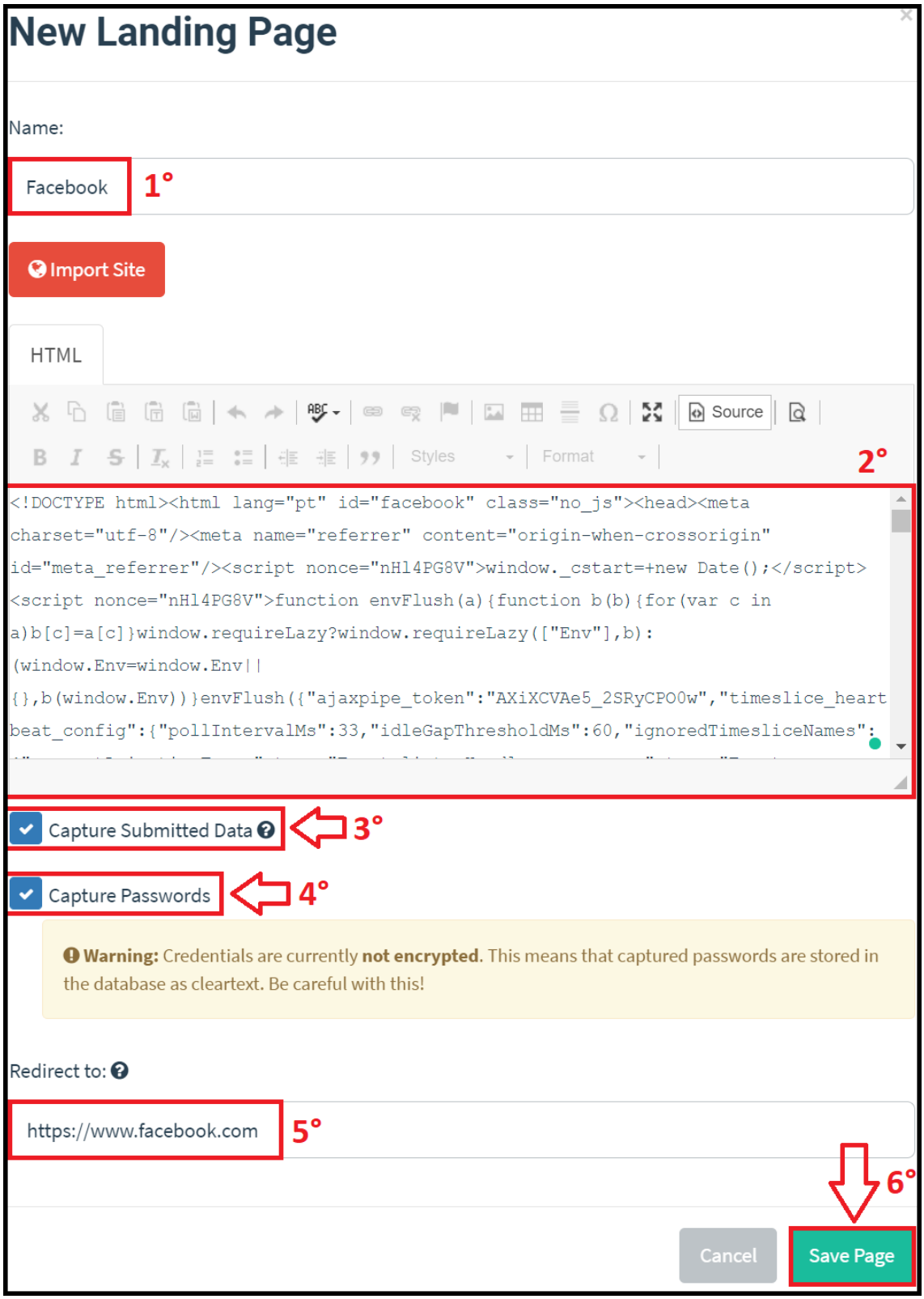
Figura 31 - Criar uma página de destino no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

Em seguida, é aberta a caixa de diálogo para elaborar uma *New Landing Page* (do português: Nova Página de Destino), conforme exibido na Figura 31.

Figura 32 - Configuração da página de destino no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

A Figura 32 exibe os passos que devem ser realizados:

1° Passo: Especificar um nome exclusivo da página de destino, no campo *Name*.

2° Passo: Importar o código fonte da página *web* original. Este campo possui a função de reproduzir as instruções da página original para uma página falsa, na linguagem HTML.

3° Passo: Marcar a caixa de seleção, *Capture Submitted Data* (do português: Captura de Dados Enviados), no qual irá capturar todos os dados visíveis colocados pela vítima na página falsa criada.

4° Passo: Marcar a caixa de seleção, *Capture Passwords* (do português: Captura de Senhas), no qual irá capturar os campos de senhas da página criada.

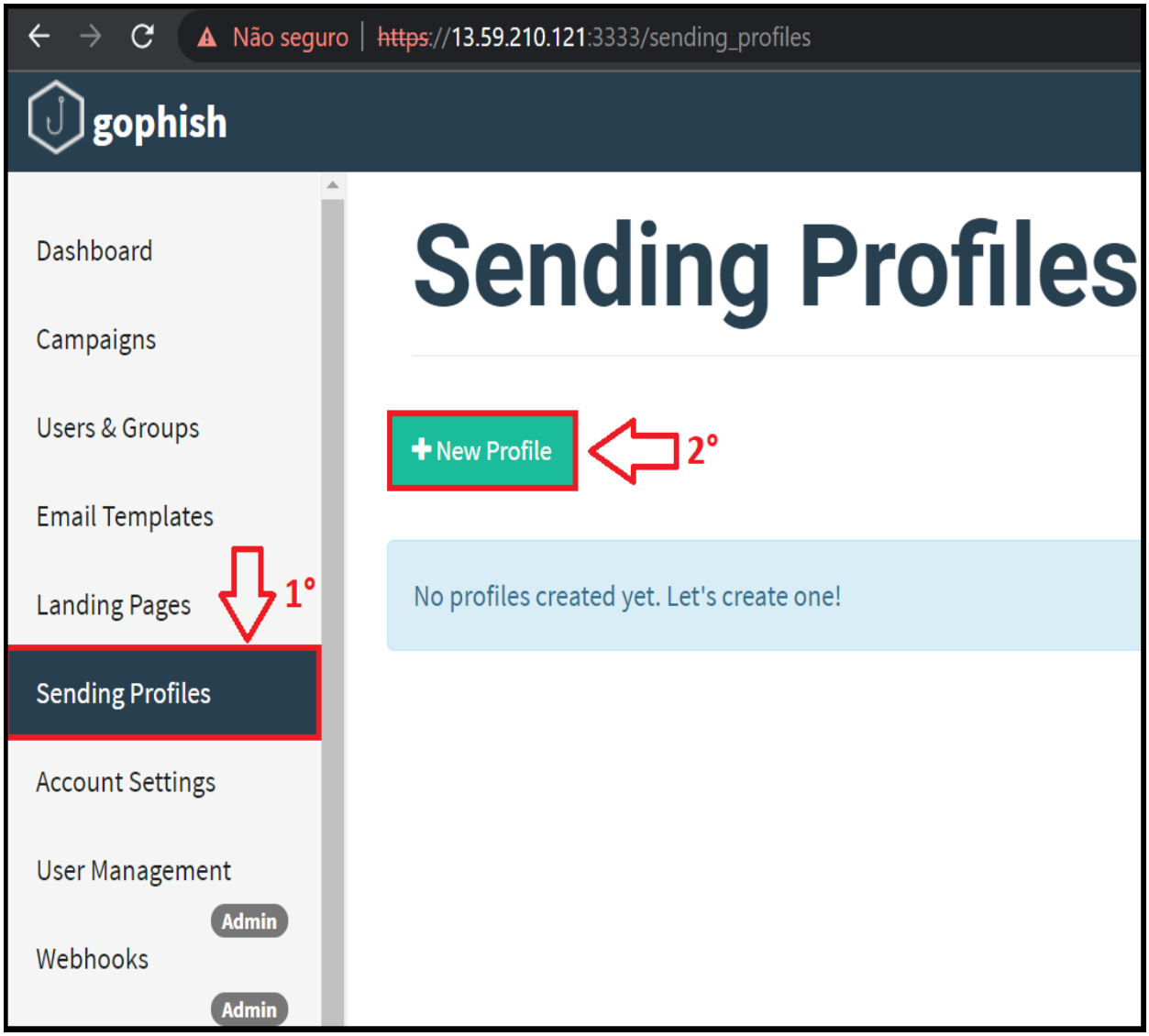
5° Passo: Definir a URL da página *web* original, no qual foi definida no 2° Passo. Este campo tem a função de redirecionar a página falsa até a página verdadeira.

6° Passo: Salvar o modelo de página de destino criada, clicando em *Save Page* (do português: Salvar Página).

Para Souza (2019), o *Simple Mail Transfer Protocol* (SMTP, do português: Protocolo de Transferência de Correio Simples) é um protocolo de envio de *e-mails*, que através da *Internet*, comunica dois dispositivos computacionais, chamados de emissor e o receptor. “Após enviar o seu *e-mail*, você conecta o seu computador ao servidor de seu provedor de *e-mails*. A partir daí o SMTP vai fazer o trabalho de se conectar com outros servidores SMTP para encaminhar o *e-mail*” (SOUZA, 2019).

Feito a criação da página de destino falsa, é preciso possuir um perfil com capacidade de enviar *e-mails*, neste caso, foi utilizado a plataforma de correio eletrônico do Gmail, que utiliza o protocolo SMTP. Desta maneira, no menu de navegação*,* em *Sending Profiles* (do português: Enviando Perfis), é possível criar uma *New Profile* (do português: Novo Perfil), conforme apresentado na Figura 33.

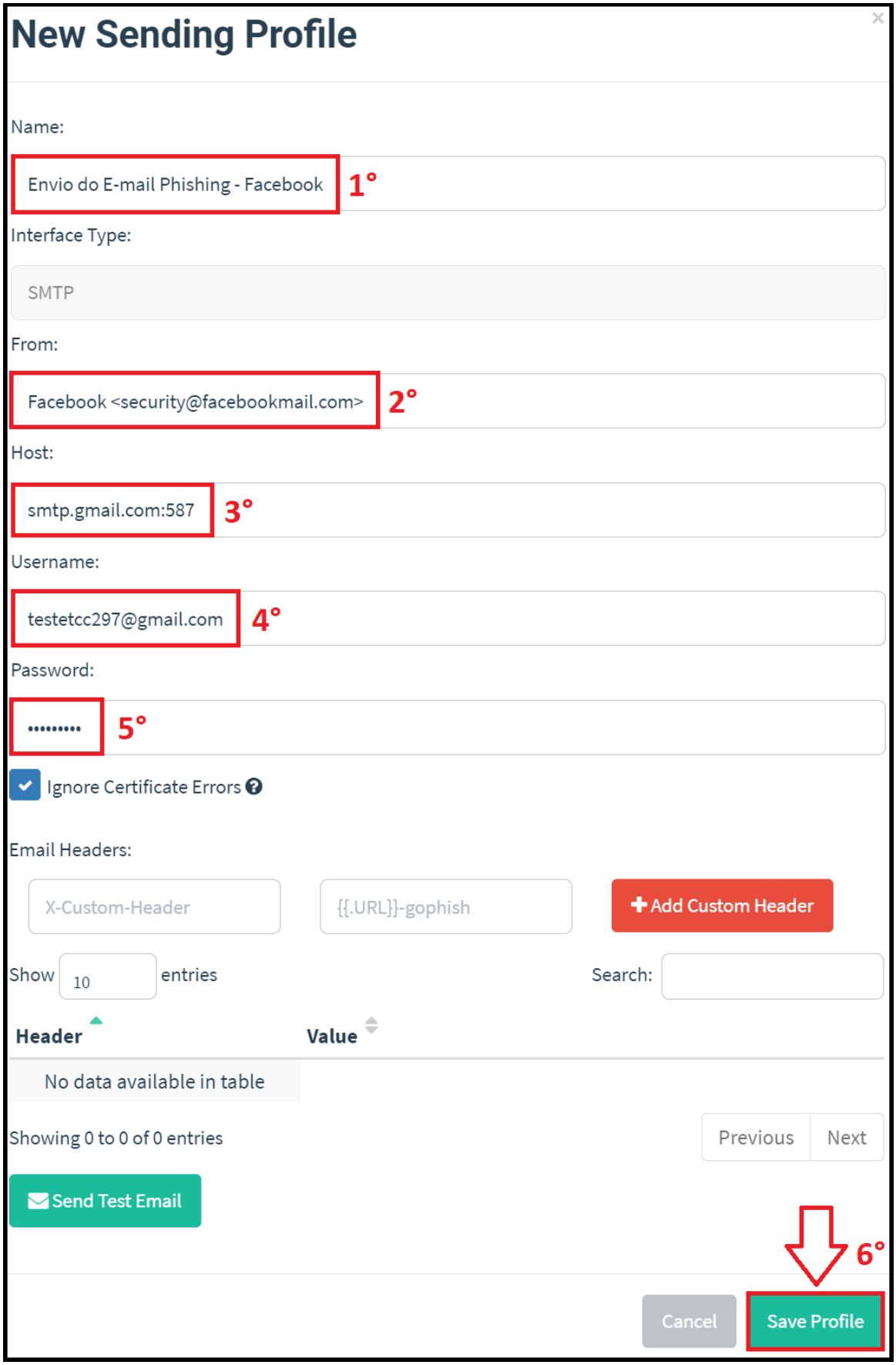
Figura 33 - Criar um perfil de envio no Gophish



Fonte: Tela de captura alterada do *Gophish* (2021).

Em seguida, é aberta a caixa de diálogo para elaborar uma *New Sending Profile* (do português: Novo Perfil de Envio), conforme exibido na Figura 34.

Figura 34 - Configuração do perfil de envio no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

A Figura 34 exibe os passos que devem ser realizados:

1° Passo: Especificar um nome exclusivo da página de destino, no campo *Name*.

2° Passo: Definir a partir de quem o *e-mail* está sendo enviado, no campo *from* (do português: a partir de).

3° Passo: Configurar um *host* (do português: hospedeiro) de *e-mail*, no qual utiliza o protocolo SMTP.

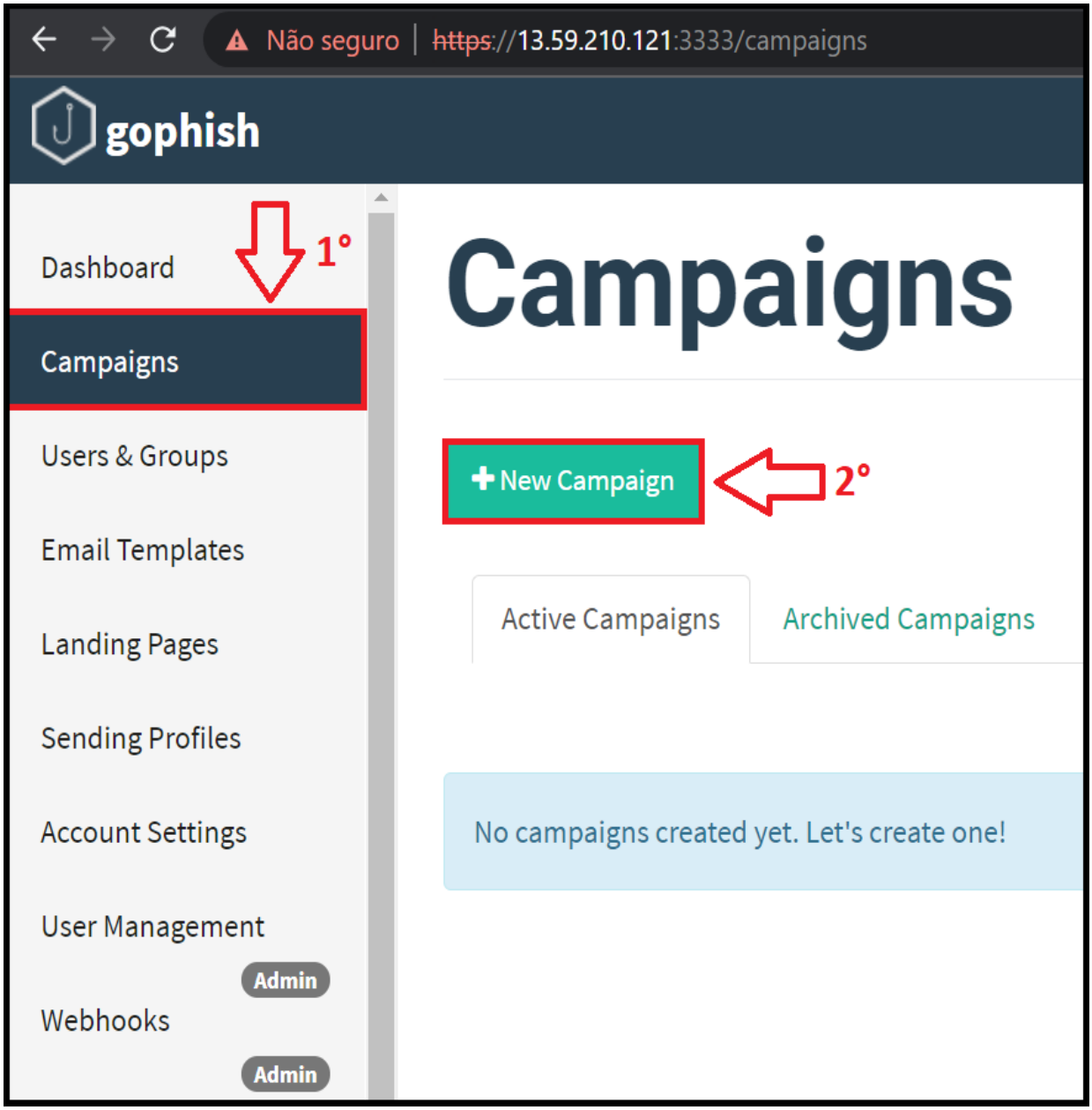
4° Passo: No campo *Username* (do português: Nome do Usuário), informar uma conta de *e-mail* existente, no qual possui acesso.

5° Passo: No campo *Password* (do português: Senha), informar a senha da sua conta de *e-mail*.

6° Passo: Salvar a configuração do perfil de envio de *e-mails*, clicando em *Save Profile* (do português: Salvar Perfil).

Finalizada todas as configurações, será possível criar a campanha que envolve o envio de *e-mails phishing* para um ou mais grupos de usuários, com intuito de roubar dados. Para criar a campanha de *phishing*, no menu de navegação, em *Campaigns* (do português: Companhas), é possível criar uma *New Campaign* (do português: Nova Campanha), conforme mostrado na Figura 35.

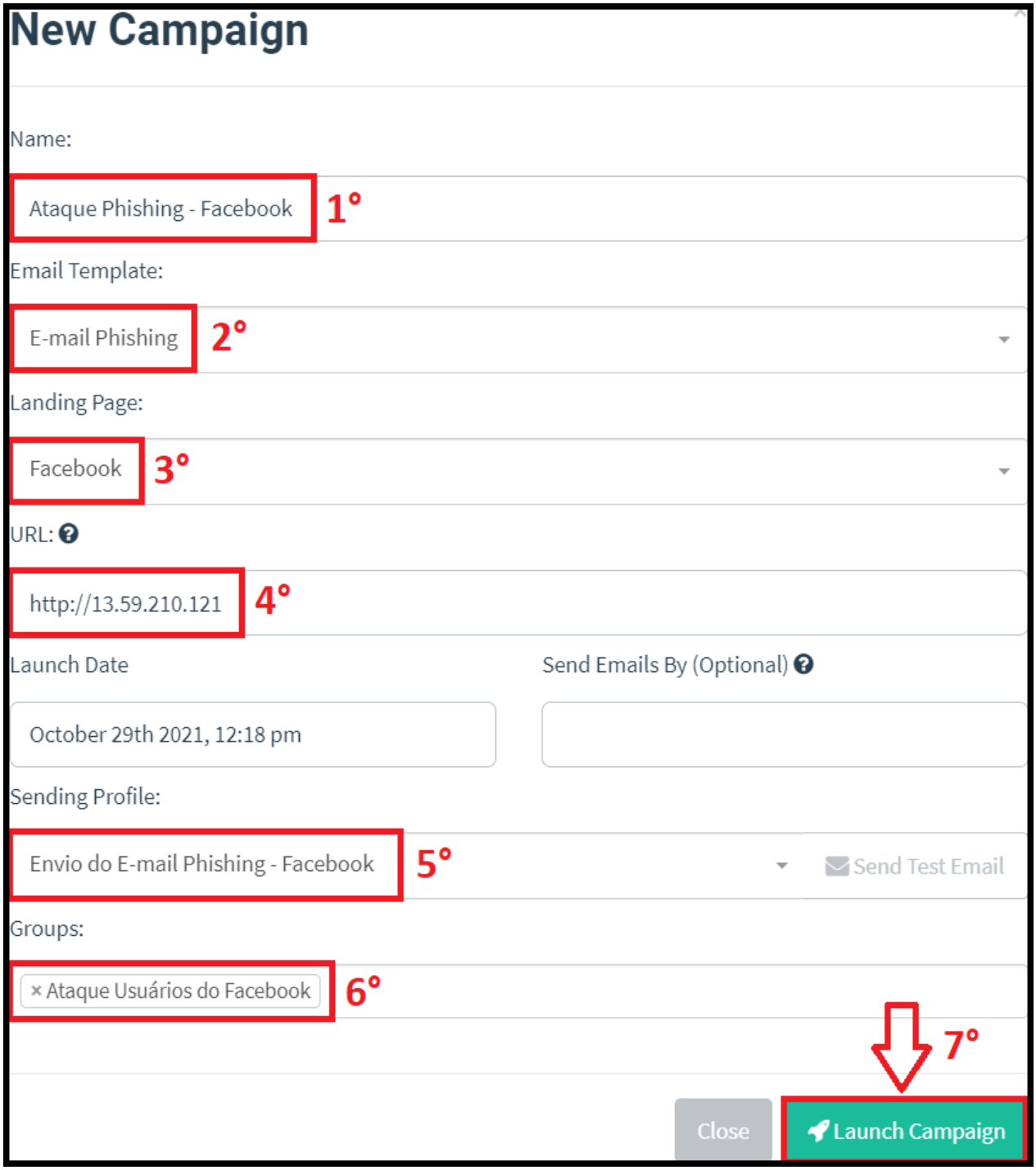
Figura 35 - Criar uma campanha no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

Em seguida, é aberta a caixa de diálogo para elaborar uma *New Campaign,* conforme exibido na Figura 36.

Figura 36 - Configuração da campanha no *Gophish*



Fonte: Tela de captura alterada do *Gophish* (2021).

A Figura 36 exibe os passos que devem ser realizados:

1° Passo: Especificar um nome exclusivo da campanha, no campo *Name*.

2° Passo: Definir o nome exclusivo que foi criada na configuração da seção *E-mail Template*.

3° Passo: Definir o nome exclusivo que foi criada na configuração da seção *Landing Page*.

4° Passo: Esta é a URL que preenche o valor do modelo {{.URL}}, comumente utilizado no modelo de *e-mail*. Deve ser um endereço IP que aponta para o servidor de *phishing Gophish* e pode ser acessado pelo destinatário. Este IP do servidor foi configurado para ser o mesmo da instância do *Amazon* EC2, da seguinte forma: *http://<endereço IP aqui>* (o endereço IP da instância neste trabalho é o 13.59.210.121).

5° Passo: Definir o nome exclusivo que foi criada na configuração da seção *Sending Profile*.

6° Passo: Definir o nome exclusivo que foi criada na configuração da seção *Groups*.

7° Passo: Para lançar a campanha de envio dos *e-mails* para os usuários vítimas, clique em *Launch Campaign* (do português: Lançar Campanha).

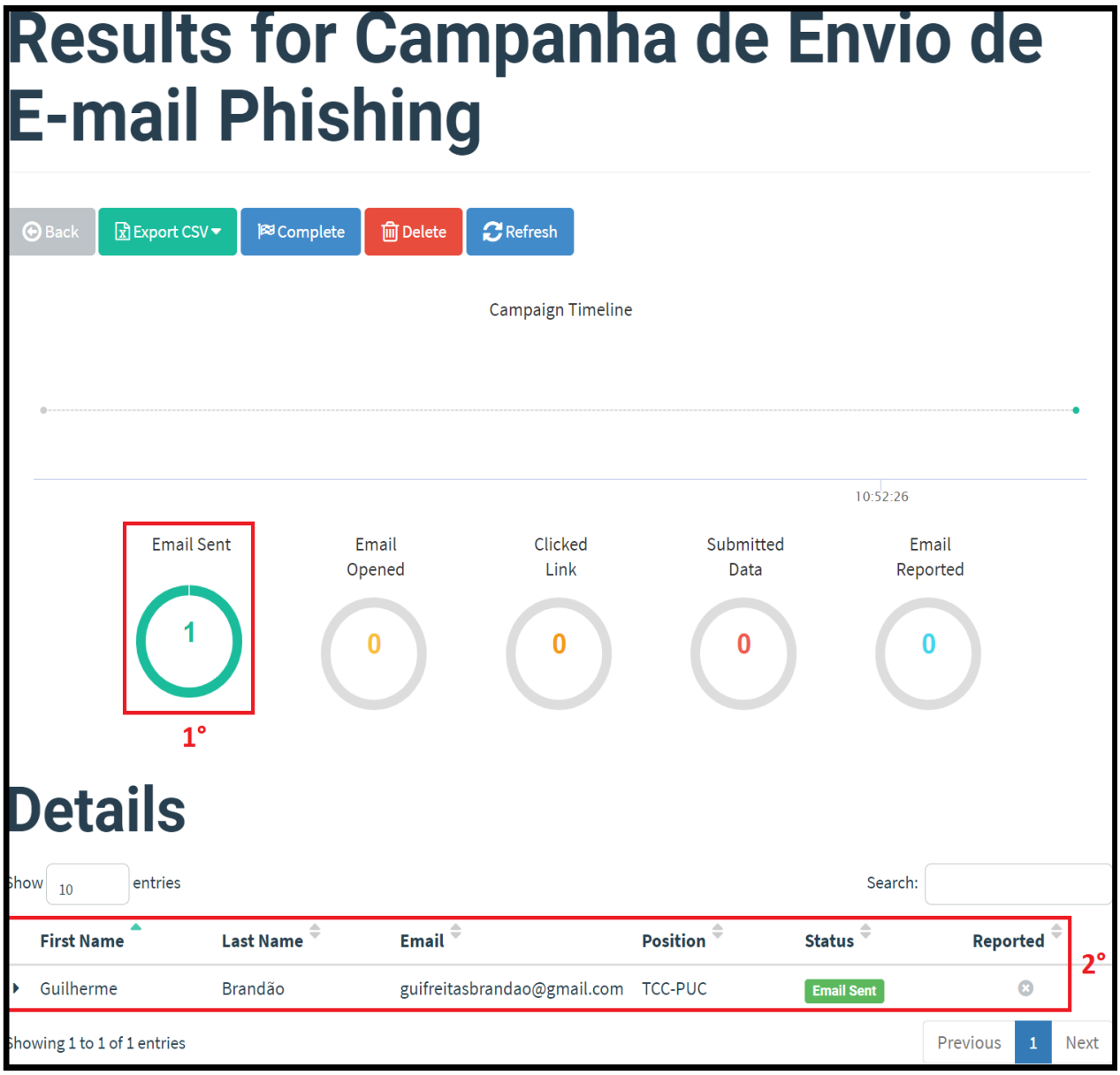
6 ANÁLISE DOS RESULTADOS OBTIDOS

Neste trabalho foi implementada uma plataforma, visando simular um ataque de *phishing*, utilizando o *framework* do *Gophish*.

Demonstração e detalhes do teste realizado:

O teste foi iniciado ao lançar a campanha de *phishing* através dos passos descritos no capítulo 5. A Figura 37 ilustra o *layout* contendo o *status* (do português: estado) da campanha de envio de *e-mail phishing*.

Figura 37 - *Layout* com o *status* da campanha – *e-mail* enviado



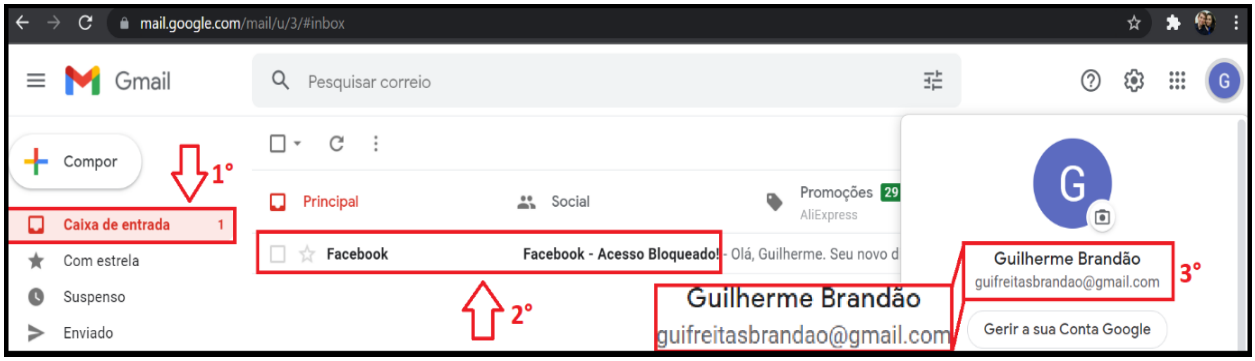
Fonte: Tela de captura alterada do *Gophish* (2021).

Detalhando a Figura 37, o *layout* é completo e informa o número de *E-mail Sent* (do português: Email Enviados), o número de *E-mail Opened* (do português: E-mail Aberto), o número de *Clicked Link* (do português: Link Clicado), o número de *Submitted Data* (do português: Dados Enviados) e o número de *E-mail Reported* (do português: E-mail Reportado). Em *details* (do português: detalhes), é possível visualizar o nome, *e-mail* e posição do usuário, no qual foi enviado o *e-mail phishing*, assim como *status* (do português: o estado) do conteúdo do *e-mail*.

O resultado deste trabalho foi obtido com base no usuário vítima possuir uma caixa de *e-mail* do *Google*, mas o mesmo ocorreria para qualquer outro provedor de *webmail* que disponibiliza caixa de *e-mail* para seus usuários.

A Figura 38 apresenta o recebimento do e-mail na caixa de entrada do alvo, sendo exatamente o *e-mail* da campanha de *phishing*.

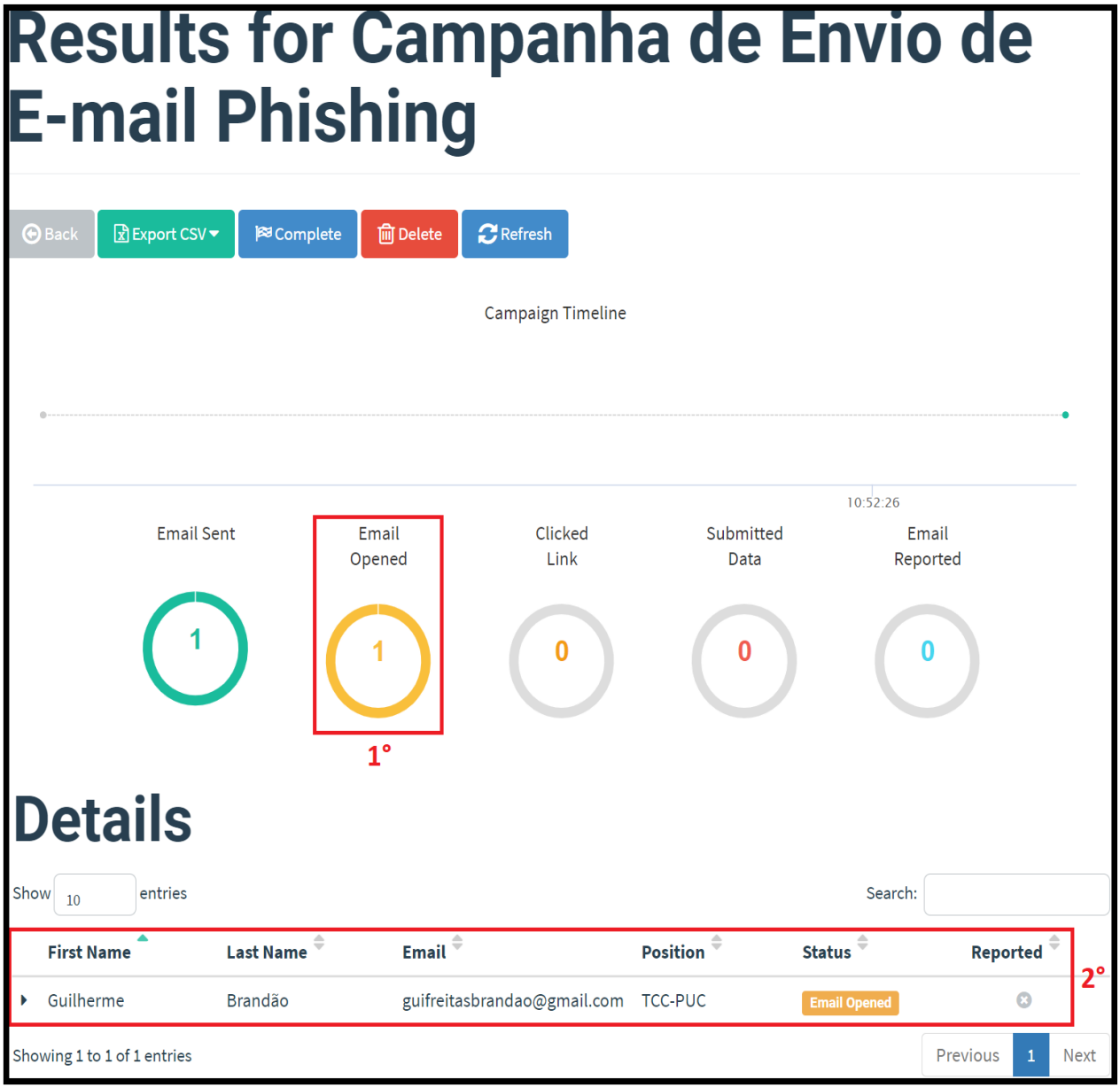
Figura 38 - Recebimento do *e-mail* no *Google Gmail*



Fonte: Tela de captura alterada do aplicativo *Gmail*.

No momento que o usuário clica no *e-mail* para ler o seu conteúdo, o *Gophish* informa em sua plataforma que ocorreu uma atualização, exatamente na parte que condiz com o clique do usuário no *e-mail*, conforme ilustrado na Figura 39.

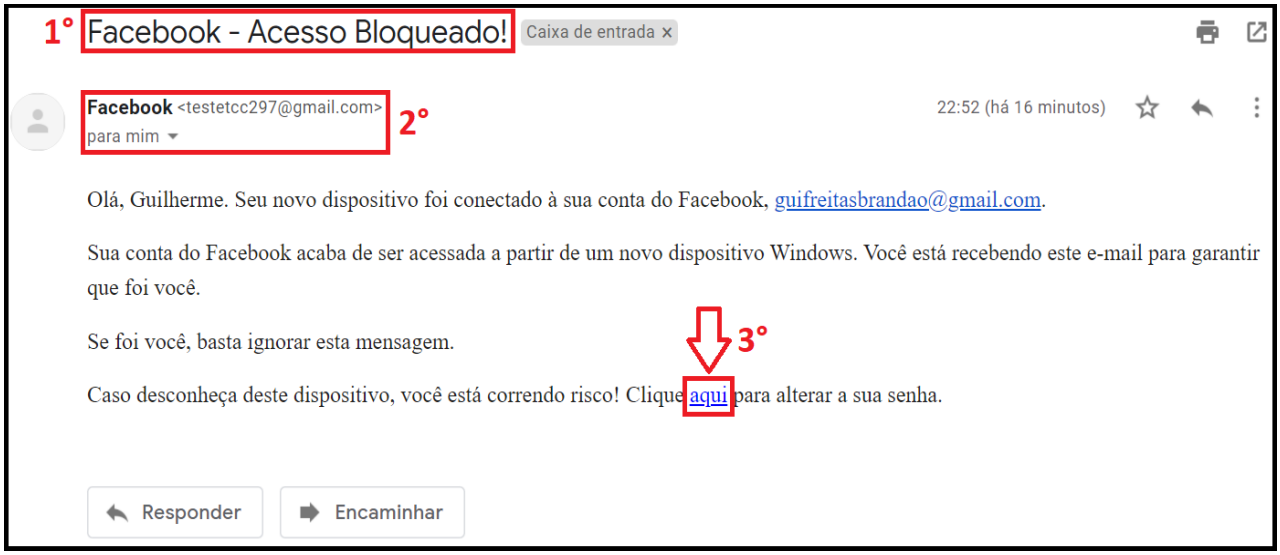
Figura 39 - *Status* da campanha – *e-mail* aberto



Fonte: Tela de captura alterada do *Gophish* (2021).

O destinatário ao clicar no *e-mail*, depara-se com a mensagem informando que sua rede social pode ter sofrido algum ataque e que é preciso modificar a senha, para a segurança do usuário, conforme mostrado na Figura 40.

Figura 40 - Conteúdo da mensagem de *e-mail* no *Google Gmail*



Fonte: Tela de captura alterada do aplicativo *Gmail.*

Junto desta mensagem, o link enviado permite que o usuário acesse a plataforma do próprio *e-mail*, apertando na opção “Clique aqui” (terceiro passo) mostrado na Figura 40.

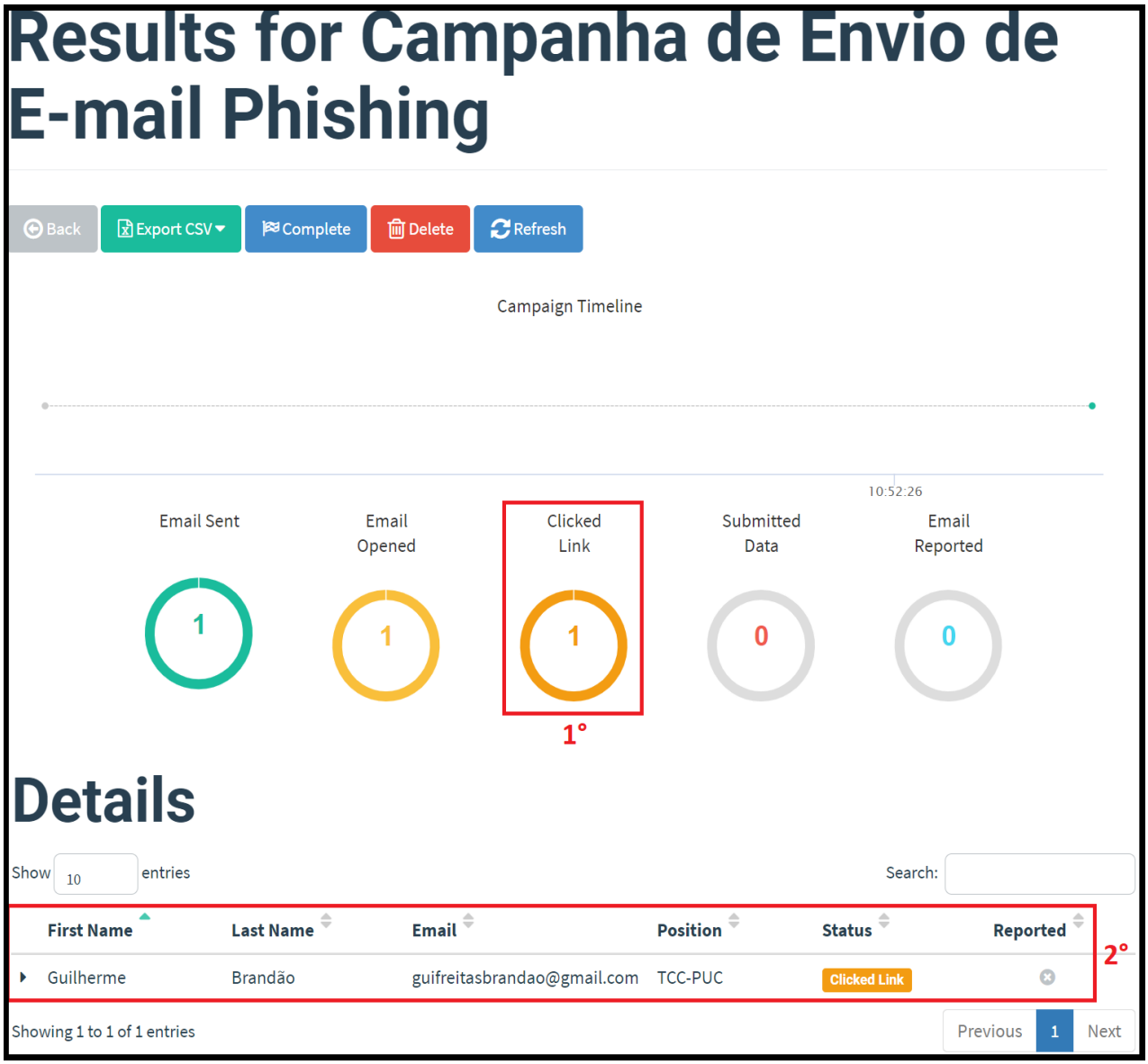
A partir disto, o usuário será redirecionado para a página falsa do *Facebook*, ocorrendo o ataque, conforme ilustrado na Figura 41.

Figura 41 - *Layout* falso simulando a página inicial do *Facebook*

Fonte: Tela de captura alterada do *Gophish* (2021).

A partir do momento que o usuário clica na opção “aqui”, mostrado na Figura 40, o *Gophish* informa em sua plataforma que obteve uma atualização, justamente na parte que condiz com o clique no *link*. Daí, acessa a falsa plataforma digital do *Facebook*, conforme ilustrado na Figura 42.

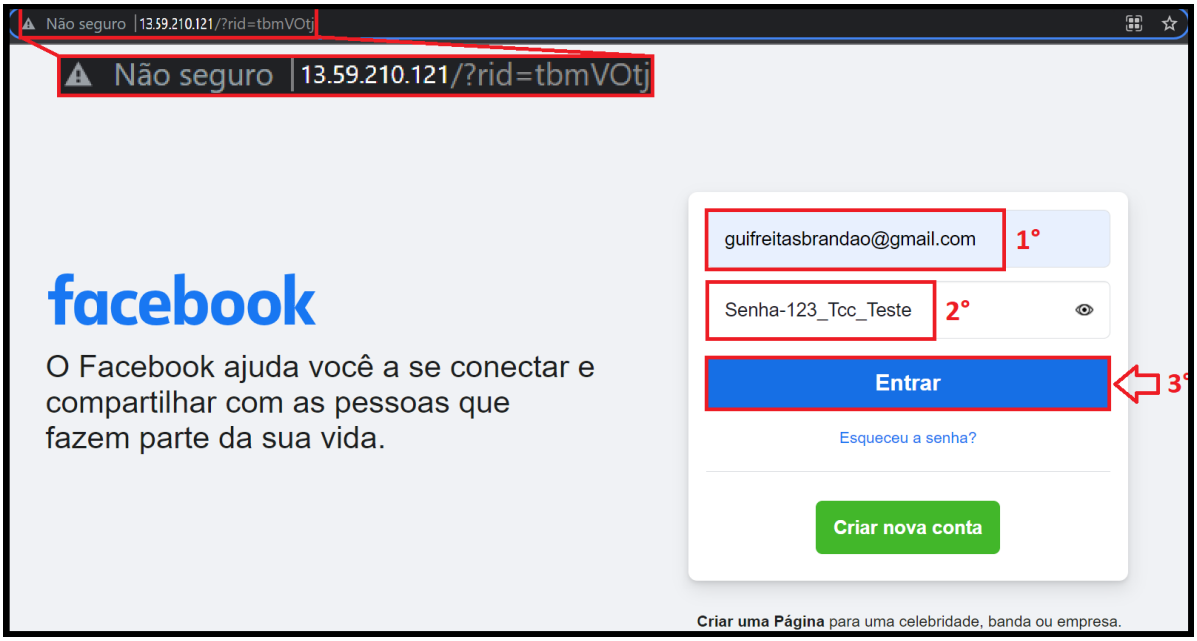
Figura 42 - *Status* da campanha – *link* clicado



Fonte: Tela de captura alterada do *Gophish* (2021).

O usuário ao ver a página do *Facebook*, possivelmente colocará seus dados pessoais de usuário e senha, buscando adentrar na plataforma digital para realização da mudança de senha, conforme ilustrado na Figura 43.

Figura 43 - *Layout* falso com os dados definidos pela vítima



Fonte: Tela de captura alterada do *Gophish* (2021).

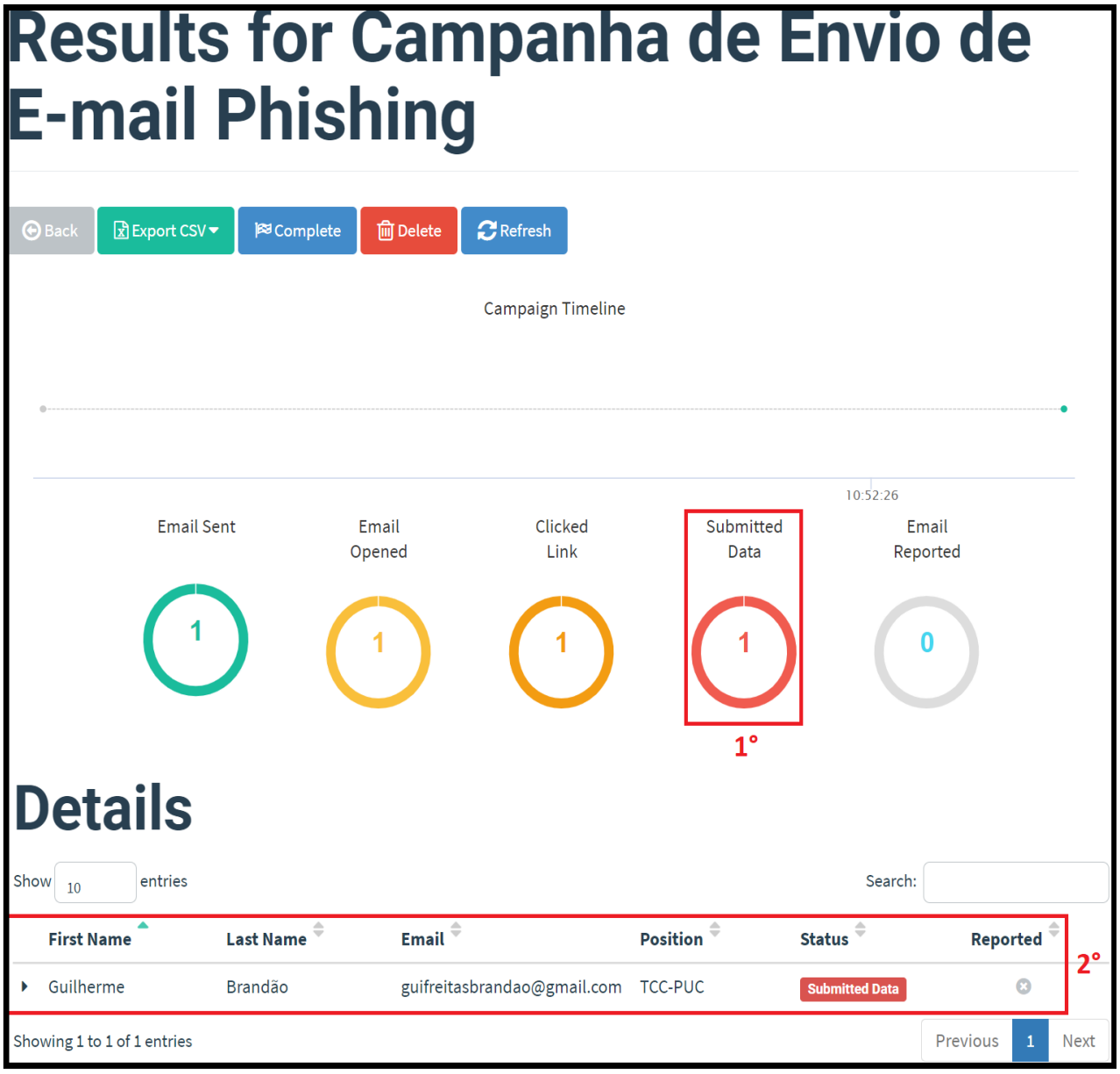
Após a vítima ter clicado em Entrar, os seus dados foram obtidos e gravados pelo *Gophish*. Assim, ocorre um redirecionamento para a página oficial do *Facebook*. Isso é feito par que a vítima pense que foi apenas um erro de digitação de seu usuário ou senha. Deste modo, o usuário entra normalmente em sua conta do *Facebook*, conforme demonstrado na Figura 44.

Figura 44 - Redirecionamento para página inicial do *Facebook*

Fonte: Tela de captura alterada do *Facebook*

No momento que o usuário clica em Entrar, o *Gophish* informa em sua plataforma que ocorreu uma atualização, condizendo com a captura de dados do usuário, através da falsa página do *Facebook*, conforme ilustrado na Figura 45.

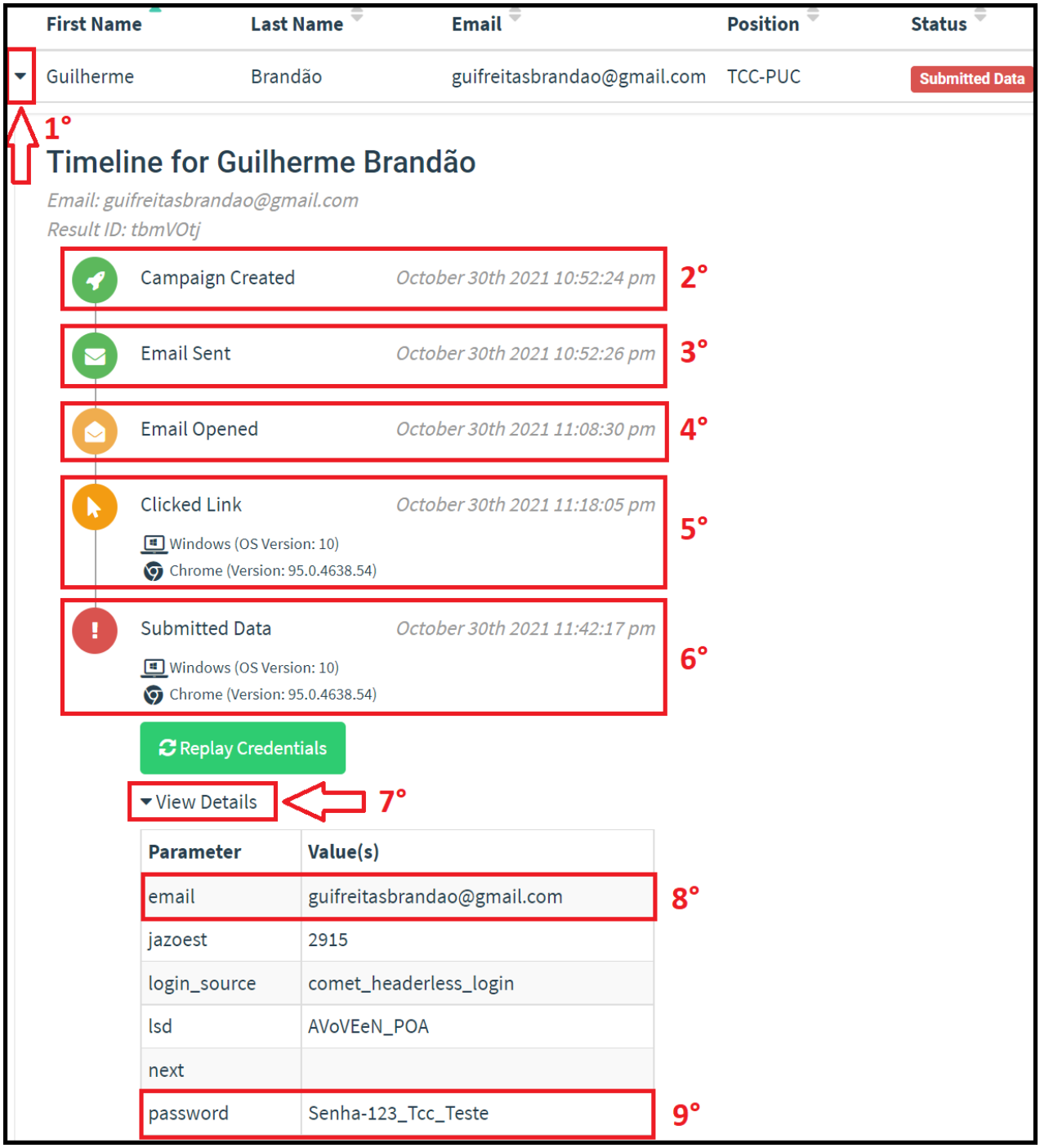
Figura 45 - *Status* da campanha – dados enviados



Fonte: Tela de captura alterada do *Gophish* (2021).

O *Gophish* proporciona uma visualização completa dos resultados da campanha em formato de linha do tempo, conforme apresentada na Figura 46.

Figura 46 - Linha do tempo da vítima com o resultado da campanha



Fonte: Tela de captura alterada do *Gophish* (2021).

Para ver a linha do tempo de cada destinatário, siga os passos de 1 a 9 mostrados na Figura 46.

1° Passo: Expanda a linha com o nome do destinatário, abrindo o painel de resultados e mostrando o que o destinatário da campanha fez até o determinado momento;

2° Passo: Mostra o dia e hora que a campanha foi criada;

3° Passo: Apresenta o dia e hora que o *e-mail* foi enviado ao seu destinatário;

4° Passo: Exibe o dia e hora que o *e-mail* foi aberto pelo destinatário;

5° Passo: Expõe o dia e hora em que o *link* dentro da mensagem do *e-mail* foi clicado pelo alvo, informando informações do sistema operacional e do navegador *web* que está sendo utilizado pela vítima;

6° Passo: Aponta o dia e hora que a vítima caiu no golpe de *phishing*, colocando os seus dados pessoais de acesso na rede social do *Facebook*;

7° Passo: Expandindo os detalhes, será possível visualizar todas as informações que foram colocadas pelo usuário, capturando as suas credenciais;

8° Passo: Exibe o *login* de acesso ao *Facebook* colocado pela vítima, neste caso o *login* era o próprio *e-mail*;

9° Passo: Expõe a senha de acesso colocado para acessar o *Facebook* informado pela própria vítima.

Análise e conclusão do experimento e os testes realizados:

Para realizar o experimento, foi necessário criar uma conta na plataforma do AWS, que disponibilizou o serviço do *Amazon* EC2, que é um produto de computação escalável da AWS, este serviço, fornece ambiente de computação virtual, denominada de instâncias. Foi muito interessante e necessária neste trabalho, pelo fato de possuir imagens de instâncias gratuitas, possuindo sistema operacional do *Debian*, que utiliza o *kernel* do *Linux* possibilitando a criação, configuração e acesso ao servidor administrador do *Gophish* e o servidor de *phishing*.

O servidor administrador foi necessário para acessar a plataforma do *Gophish*. Para criar e configurar os grupos de usuários, os modelos de *e-mails*, as páginas de destino, os perfis de envio e finalmente, a campanha de *phishing*. Já o servidor de *phishing* é essencial para enviar e capturar os dados do *e-mail* que foram enviados para os serviços de correio eletrônicos.

O *software* do *PuTTY* foi fundamental para converter as chaves do arquivo criptografado no formato .pem, para o formato .ppk, além de fazer a emulação da instância do *Amazon* EC2 para o no terminal do *PuTTY*, utilizando a imagem do *Linux*.

Portanto foi imprescindível a utilização desses serviços e ferramentas para realizar a simulação de *phishing* deste trabalho.

Na simulação de *penetration testing*, foi realizado o envio de um *e-mail* de *phishing*, utilizando a plataforma do *Gophish*. A campanha de *phishing* teve o objetivo de roubar os dados de usuário e senha de utilizadores da rede social do *Facebook*. Portanto, foi necessário criar uma página falsa, semelhante ao *Facebook*, para persuadir e enganar o usuário a colocar suas credenciais na falsa plataforma, fazendo a coleta de dados através do servidor de *phishing* do *Gophish*.

Conclui-se que, o *login* e senha do usuário da rede social do *Facebook* foram capturadas pela plataforma do *Gophish*, podendo afirmar que os dados foram coletados com sucesso.

Observou-se a necessidade de tomar as seguintes precauções em relação aos ataques de *phishing*:

I. Não clicar em *links* desconhecidos e/ou suspeitos a *e-mails* não solicitados ou em redes sociais digitais;
II. Não abrir mensagens de destinatários desconhecidos em seus *e-mails*;
III. Evitar baixar arquivos automaticamente ou pedidos de *downloads* desnecessários;
IV. Não executar arquivos não solicitados;
V. Sempre verificar a URL do *website*, pois em muitos casos o endereço parece ser legítimo, mas a URL ou domínio pode ser diferente do site original.
VI. As redes sociais digitais são locais para conectar as pessoas, em nível mundial. Sendo um fator muito importante de comunicação e serviços, que mudou totalmente o jeito de interação entre pessoas, grupos ou organizações. Mas devido a tanta interação, é uma mina de ouro para cibercriminosos, que utilizam as técnicas de engenharia social através das plataformas sociais.

7 CONSIDERAÇÕES FINAIS

Este trabalho buscou responder a seguinte questão de pesquisa: **Quais os problemas e os riscos associados as redes sociais mais utilizadas em relação a segurança da informação?**

O objetivo geral foi o de **i**dentificar problemas e riscos existentes nas redes sociais mais utilizadas, simulando um ataque envolvendo a técnica de enviar *e-mails* utilizando táticas da engenharia social para enganar e sequestrar dados de utilizadores de redes sociais.

As metodologias utilizadas no trabalho quanto à natureza é um resumo de pesquisa, quanto aos objetivos, a pesquisa é exploratória e quantos aos procedimentos técnicos a pesquisa é bibliográfica e experimental, foram suficientes para atender os objetivos estabelecidos.

Neste trabalho foram abordados conceitos de segurança da informação, segurança de redes e criptografia, no qual foi observado a partir do referencial teórico que é essencial para fornecer proteção as informações e nas conexões entre usuários que utilizam a *internet*.

Mesmo com todos os fatores de proteção, serviços, normas e técnicas que buscam assegurar usuários da rede que interliga mundialmente computadores, ainda sim, existem formas de ataques que ocorrem por pessoas mal-intencionadas.

A engenharia social tem objetivo de obter informações sigilosas e importantes de pessoas ou organizações, utilizando estratégias de persuasão. As técnicas mais utilizadas são os ataques de *phishing*, *spyware,* cavalo de troia, *baiting* e dentre outras.

A técnica de *phishing* é a mais aplicada por cibercriminosos no mundo, pois se utilizam principalmente de e-mails e mensagens instantâneas para propagar a falsificação. Além disso, possui maneira simples de ser implementada, com grande capacidade de atingir pessoas.

As redes sociais digitais são locais para conectar as pessoas, em nível mundial. Sendo um fator muito importante de comunicação e serviços, que mudou totalmente o jeito de interação entre pessoas, grupos ou organizações. Mas devido a tanta interação, é uma mina de ouro para cibercriminosos, que utilizam as técnicas de engenharia social através das plataformas sociais.

O estudo realizado permitiu identificar os seguintes problemas e os riscos associados as redes sociais mais utilizadas em relação a segurança da informação, apresentados a seguir:

- O principal problema das redes sociais são seus usuários, pela inocência e a falta de conhecimento sobre as coisas que fazem nas redes sociais, postando informações relacionadas a sua privacidade e informações pessoas.
- As técnicas mais utilizadas são os ataques relacionados a Engenharia Social, utilizando métodos de *phishing*, *spyware,* cavalo de troia, *baiting* e dentre outras. Utilizando estas técnicas, os principais riscos relacionados ao uso de redes sociais são: o furto de identidade, a invasão de perfil, o uso indevido de informações, a invasão de privacidade, o vazamento de informações, a disponibilização de informações confidenciais, o recebimento de mensagens maliciosas, o acesso a conteúdo de mensagens maliciosas, o acesso a conteúdo impróprios ou ofensivos, danos à imagem e à reputação, o sequestro e o furto de bens.

Por meio desta pesquisa teórica, a escolha de desenvolver uma simulação de *phishing* ocorreu, por ser um dos ataques mais comuns do mundo. Devido a isto, este trabalho busca conscientizar e prevenir que usuários sejam atacados, mostrando como ocorre e como é feito os procedimentos de ataque.

A implementação realizada neste trabalho permitiu concluir que os usuários são a porta de entrada para acontecer os cibercrimes. Portanto, precisam ser conscientizados e capacitados, visando ficarem mais observadores e saberem como agir ao receber os cenários dos atacantes nas redes sociais.

As principais dificuldades encontradas foram na configuração dos servidores do *Gophish*, utilizando a instância do *Amazon* EC2 e na implementação do ataque.

Para continuidade deste estudo, sugerem-se os seguintes trabalhos futuros:

- Analisar o Impacto da engenharia social na segurança da informação em ambientes corporativos;
- Aplicar os testes desenvolvidos neste trabalho em um ambiente corporativo, buscando identificar as falhas de segurança da rede empresarial e educar os funcionários para não cair em golpes *phishing*;

- Utilizar um ambiente virtual controlado para simular um Cavalo de Troia (outro ataque da engenharia social);

8 REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR, Adriana. **Facebook**: tudo sobre a rede social mais usada do mundo. [*S. l.*]: Rockcontent, 13 ago. 2016. Disponível em: https://rockcontent.com/br/blog/facebook/#facebook. Acesso em: 7 nov. 2021.

ARAMUNI, João Paulo; MAIA, Luiz Cláudio. **O impacto da Engenharia Social na Segurança da Informação:** uma abordagem orientada à Gestão Corporativa**.** Minas Gerais, p. 1-7, 2018.

ARGOLLO, Anderson Lopes. **SEGURANÇA DA INFORMAÇÃO**: O SER HUMANO COMO O ELO MAIS FRACO DA CORRENTE. Orientador: Vinícius Corrêa Ferreira. 2017. 44 p. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Computação) - Universidade Federal Fluminense, Rio de Janeiro, 2017.

AWS. **Amazon Elastic Compute Cloud:** Manual do usuário para instâncias do Windows. [*S. l.*], p. 1-1683, 28 jul. 2021. Disponível em: https://docs.aws.amazon.com/pt_br/AWSEC2/latest/WindowsGuide/ec2-windows-instances.html. Acesso em: 25 out. 2021.

AWS. **AWS:** Serviços de computação em nuvem. [S. l.], 2021. Disponível em: https://aws.amazon.com/pt/. Acesso em: 16 mar. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Rio de Janeiro, 2013.

BARBOSA, Suria. **Quora**: Como usar o Quora a favor da sua carreira. [*S. l.*], 22 mar. 2018. Disponível em: https://www.napratica.org.br/como-usar-o-quora-favor-da-carreira/. Acesso em: 7 nov. 2021.

BARBOSA, Suria. **LinkedIn**: como usar a maior rede profissional do mundo e tirar o máximo proveito. [*S. l.*]: Na Prática, 22 abr. 2021. Disponível em: https://www.napratica.org.br/como-funciona-o-linkedin/. Acesso em: 7 nov. 2021.

BATISTA, Aline. **Kwai**: como funciona e como ganhar dinheiro no app de vídeos. [*S. l.*]: Zoom, 26 jul. 2021. Disponível em: https://www.zoom.com.br/celular/deumzoom/kwai. Acesso em: 7 nov. 2021.

CARNIEL, Guadalupe. **Tumblr**: O que é e como funciona o Tumblr. [*S. l.*]: Canaltech, 26 jan. 2021. Disponível em: https://canaltech.com.br/*Internet*/tumblr-o-que-e/. Acesso em: 7 nov. 2021.

CASAROTTO, Camila. **Guia do Pinterest**: como usar um dos maiores mecanismos de busca visual do mundo. [*S. l.*]: Rockcontent, 22 jul. 2019. Disponível em: https://rockcontent.com/br/blog/pinterest/. Acesso em: 7 nov. 2021.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (org.). **Cartilha de Segurança para *Internet***: Versão 4.0. 2. ed. São Paulo: Comitê Gestor da *Internet* no Brasil, 2012. 140 p. ISBN 978-85-60062-54-6. Disponível em: https://cartilha.cert.br/livro/. Acesso em: 10 abr. 2021.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (org.). **Incidentes Reportados ao CERT.br**: Janeiro a Dezembro de 2020 – Top 10 CCs origem de ataques. [*S. l.*], 3 ago. 2021. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-dec/top-cc.html. Acesso em: 3 nov. 2021.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (org.). **Incidentes Reportados ao CERT.br**: Janeiro a Dezembro de 2020 – Totais mensais. [*S. l.*], 3 ago. 2021. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-dec/total-mensal.html. Acesso em: 3 nov. 2021.

CHIARK (Reino Unido). **PuTTY**: a free SSH and Telnet client. [*S. l.*], 15 ago. 2021. Disponível em: https://www.chiark.greenend.org.uk/~sgtatham/putty/. Acesso em: 16 nov. 2021.

COUTINHO, Thiago. **Conheça a história do Instagram e aprenda a usá-lo**: O que é o Instagram? [*S. l.*]: Voitto, 1 out. 2020. Disponível em: https://www.voitto.com.br/blog/artigo/instagram. Acesso em: 7 nov. 2021.

DATAREPORTAL. **DIGITAL 2020**: BRAZIL. [*S. l.*]: SIMON KEMP, 17 fev. 2020. Disponível em: https://datareportal.com/reports/digital-2020-brazil. Acesso em: 6 nov. 2021.

DATAREPORTAL. **DIGITAL 2021**: BRAZIL. [*S. l.*]: SIMON KEMP, 11 fev. 2021. Disponível em: https://datareportal.com/reports/digital-2021-brazil. Acesso em: 6 nov. 2021.

DATAREPORTAL. **DIGITAL 2020**: OCTOBER GLOBAL STATSHOT. [*S. l.*]: SIMON KEMP, 20 out. 2020. Disponível em: https://datareportal.com/reports/digital-2020-october-global-statshot. Acesso em: 6 nov. 2021.

DATAREPORTAL. **DIGITAL 2021:** OCTOBER GLOBAL STATSHOT REPORT. [*S. l.*]: SIMON KEMP, 21 out. 2021. Disponível em: https://datareportal.com/reports/digital-2021-october-global-statshot. Acesso em: 6 nov. 2021.

DIAS, Maria. **O que é Telegram?** Saiba tudo sobre o app russo que é rival do WhatsApp. [*S. l.*]: Techtudo, 16 mar. 2019. Disponível em: https://www.techtudo.com.br/listas/2019/03/o-que-e-telegram-4-perguntas-e-respostas-sobre-o-rival-do-whatsapp.ghtml. Acesso em: 7 nov. 2021.

DURBANO, Vinicius. **Cartilha de Segurança da informação:** Como aumentar sua proteção. [*S. l.*], 2019. Disponível em: https://blog.ecoit.com.br/cartilha-de-seguranca-da-informacao/. Acesso em: 3 nov. 2021.

FABRO, Clara. **Como funciona o TikTok?** Saiba usar o aplicativo de vídeos. [*S. l.*]: Techtudo, 25 maio 2021. Disponível em: https://www.techtudo.com.br/listas/2021/05/como-funciona-o-tiktok-saiba-usar-o-aplicativo-de-videos.ghtml. Acesso em: 7 nov. 2021.

FOROUZAN, Behrouz. **Comunicação de Dados e Redes de Computadores**. Tradução de Ariovaldo Griesi. 4° ed.: Porto Alegre: AMGH Editora Ltda., 2010. ISBN 978-85-63308-47-4.

FERREIRA, Kellison. **Saiba o que é SSH (Secure Shell)**: para que serve esse protocolo. [*S. l.*]: Rockcontent, 17 abr. 2019. Disponível em: https://rockcontent.com/br/blog/ssh/. Acesso em: 8 nov. 2021.

GAIATO, Kris. **O que é Reddit**. [*S. l.*]: Canaltech, 13 out. 2021. Disponível em: https://canaltech.com.br/redes-sociais/o-que-e-reddit/. Acesso em: 7 nov. 2021.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Editora Atlas Ltda., 2017. ISBN 978-85-97-01292-7.

GOMES, Marcelo Rodrigues. **A FORMAÇÃO PROFISSIONAL DE TI NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO**: estudo de caso em Instituições de ensino superior de Santa Catarina. Orientador: Hamilcar Boing. 2017. 67 p. Trabalho de Conclusão de Curso (TECNOLOGIA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO) - INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, FLORIANÓPOLIS, 2017.

HOSTGATOR. **PuTTY**: entenda o que é e como utilizar este software. [*S. l.*], 22 set. 2021. Disponível em: https://www.hostgator.com.br/blog/putty-entenda-o-que-e-e-como-utilizar-este-software/. Acesso em: 8 nov. 2021.

HOTMART. **Aprenda a usar o Facebook Messenger no seu negócio**: O que é o Facebook Messenger? 7 abr. 2020. Disponível em: https://blog.hotmart.com/pt-br/facebook-messenger/. Acesso em: 7 nov. 2021.

INFORMAÇÃO. In: DICIO, Dicionário Online de Português. Porto: 7Graus, 2021. Disponível em: https://www.dicio.com.br/informacao/. Acesso em: 18/09/2021.

ISTOÉ. **Sem ler contrato, mais de 20 mil pessoas se inscrevem em serviços comunitários.** 13 jul. 2017. Disponível em: https://istoe.com.br/sem-ler-contrato-

mais-de-20-mil-pessoas-se-inscrevem-em-servicos-comunitarios/. Acesso em: 8 nov. 2021.

KINAST, Priscilla. **Skype**: O que é o Skype e como ele funciona? [*S. l.*]: Oficina da Net, 6 jul. 2020. Disponível em: https://www.oficinadanet.com.br/aplicativos/31718-o-que-e-o-skype. Acesso em: 7 nov. 2021.

LIANG, Lu-Hai. **Por que uso do e-mail não se popularizou na China como no restante do mundo?** [*S. l.*]: BBC News Brasil, 22 set. 2020. Disponível em: https://www.bbc.com/portuguese/geral-54252091. Acesso em: 7 nov. 2021.

LONGEN, Andrei. **A História da *Internet***: Do Início ao Status Atual da Rede. Weblink, 8 ago. 2019. Disponível em: https://www.weblink.com.br/blog/historia-da-*Internet*/. Acesso em: 5 abr. 2021.

MARCONDES, José Sérgio. **Engenharia Social**: O que é? Conceitos, Técnicas e Como Se Proteger. [*S. l.*]: Blog Gestão de Segurança Privada, 6 fev. 2017. Disponível em: https://gestaodesegurancaprivada.com.br/engenharia-social-o-que-e-conceitos/. Acesso em: 16 nov. 2021.

MADHOK, Diksha. **Douyin**: Versão chinesa do TikTok limita uso por adolescente a 40 minutos diários. [*S. l.*]: CNN Brasil, 20 set. 2021. Disponível em: https://www.cnnbrasil.com.br/tecnologia/versao-chinesa-do-tiktok-limita-uso-por-adolescente-a-40-minutos-diarios/. Acesso em: 7 nov. 2021.

MILLS, Matt. **Criptografia**: algoritmos de chave simétrica e assimétrica explicados. [*S. l.*], 6 abr. 2021. Disponível em: https://itigic.com/pt/cryptography-symmetric-and-asymmetric-key-algorithms-explained/. Acesso em: 15 nov. 2021.

MLABS (São Paulo). **Twitter**: Tire todas suas dúvidas sobre o que é Twitter e comece a usá-lo na sua estratégia de marketing. [*S. l.*], 9 fev. 2021. Disponível em: https://www.mlabs.com.br/blog/twitter/. Acesso em: 7 nov. 2021.

MOURA, Túlio. **Um Breve Histórico da *Internet***. DialHost, 17 maio 2019. Disponível em: https://www.dialhost.com.br/blog/um-breve-historico-da-*Internet*/. Acesso em: 3 abr. 2021.

NIETO, Carlos Henrique. **WECHAT**: O QUE É? PARA QUE SERVE? [*S. l.*]: Loopa, 22 abr. 2019. Disponível em: https://agencialoopa.com.br/o-que-e-o-wechat/. Acesso em: 7 nov. 2021.

NOLETO, Cairo. **Twitch**: o que é e como fazer stream. [*S. l.*]: Trybe, 29 abr. 2021. Disponível em: https://blog.betrybe.com/tecnologia/tudo-sobre-twitch/. Acesso em: 7 nov. 2021.

NUVENS, Eduardo. **WhatsApp**: história, dicas e tudo que você precisa saber sobre o app. [*S. l.*]: Olhar Digital, 3 mar. 2021. Disponível em: https://olhardigital.com.br/2018/12/20/noticias/whatsapp-historia-dicas-e-tudo-que-voce-precisa-saber-sobre-o-app/. Acesso em: 7 nov. 2021.

OLIVEIRA, G. D.; MOURA, R. K. G.; ARAÚJO, F. A. N. G. Gestão da segurança da informação: perspectivas baseadas na tecnologia da informação (t.i.). **Múltiplos Olhares em Ciência da Informação**, v. 3, n. 2, 2013. Disponível em: http://hdl.handle.net/20.500.11959/brapci/67533. Acesso em: 10 set. 2021.

PARETO. **Tudo que você precisa saber sobre seu público digital:** Hootsuite + We are social, 3 mai. 2019. Disponível em: https://blog.pareto.io/publico-digital-hootsuite-we-are-social/. Acesso em: 24 out. 2021.

PIN, Guilherme. **Entenda o que é YouTube**: O que é YouTube? [*S. l.*]: Influu, 23 nov. 2017. Disponível em: https://influu.me/blog/entenda-o-que-e-youtube/. Acesso em: 7 nov. 2021.

PERCILIA, Eliene. "Segurança em Redes de Computadores"; *Brasil Escola*, 2021. Disponível em: https://brasilescola.uol.com.br/informatica/seguranca-redes.htm. Acesso em 19 de novembro de 2021.

PRIVACIDADE. In: DICIO, Dicionário Online de Português. Porto: 7Graus, 2021. Disponível em: https://www.dicio.com.br/privacidade/. Acesso em: 22/09/2021.

PROOF. **Custo do Cibercrime**, [*S. l.*], 23 dez. 2016. Disponível em: https://www.proof.com.br/blog/custo-do-cibercrime/. Acesso em: 17 maio 2021.

PUTTYGEN. **PuTTYgen Download Latest Version for Windows, Linux & Mac**: How to Use Puttygen on Windows. [*S. l.*], 2021. Disponível em: https://puttygen.in. Acesso em: 11 nov. 2021.

PUTTY.ORG. **Download PuTTY:** a free SSH and telnet client for Windows. [S. l.], 2021. Disponível em: https://www.putty.org/. Acesso em: 24 out. 2021.

QUEIROZ, Mariana Pessoa De; ROSA, Nícolas Domingues. **PHISHING E REDES SOCIAIS**: UM ESTUDO DE CASO. São Paulo, p. 1-88, 2019.

ROCHA, Douglas. **ENGENHARIA SOCIAL**: Compreendendo Ataques e a Importância da Conscientização. [*S. l.*], 2018. Disponível em: https://meuartigo.brasilescola.uol.com.br/atualidades/engenharia-social-compreendendo-ataques-importancia-conscientizacao.htm. Acesso em: 16 nov. 2021.

ROMERO, Luiz. **Não li e concordo**. [*S. l.*]: Super Interessante, 27 mar. 2017. Disponível em: https://super.abril.com.br/tecnologia/nao-li-e-concordo/. Acesso em: 7 nov. 2021.

SEGURANÇA. In: DICIO, Dicionário Online de Português. Porto: 7Graus, 2021. Disponível em: https://www.dicio.com.br/seguranca/. Acesso em: 18/09/2021.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. **Segurança dos Sistemas de Informação**: Gestão Estratégica da Segurança Empresarial. 1° ed.: Lisboa, Portugal: Centro Atlântico Ltda, 2003. ISBN 972-8426-66-6. Disponível em: https://docente.ifrn.edu.br/rodrigotertulino/livros/sistema-de-seguranca-da-informacao. Acesso em: 17 set. 2021.

SOUSA, Gilson Soares de. **SEGURANÇA DA INFORMAÇÃO EM APLICATIVOS MÓVEIS**: UMA ANÁLISE COMPORTAMENTAL SOBRE O WHATSAPP E INSTAGRAM. Orientador: Roitier Campos Gonçalves. 2021. 70 p. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) - Instituto Federal Goiano, Ceres - GO, 2021. Disponível em: https://repositorio.ifgoiano.edu.br/bitstream/prefix/2016/1/tcc%20_Gilson%20Soares%20de%20Sousa.pdf. Acesso em: 8 nov. 2021.

SOUZA, Dercia Antunes de *et al*. **SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS**. São Paulo, p. 1-14, 23 out. 2018.

STALLINGS, William. **Criptografia e Segurança de Redes**: Princípios e Práticas. 6° ed.: São Paulo: Pearson Education do Brasil Ltda., 2014. ISBN 978-85-430-1450-0.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes sociais virtuais: privacidade e responsabilidade civil**: Análise a partir do Marco Civil da *Internet*. Pensar: Revista de Ciências Jurídicas, Fortaleza, ano 2017, v. 22, n. 1, p. 108-146, jan./abr. 2017.

THINKMONEY. **What does your phone know about you?** 3 nov. 2020. Disponível em: https://www.thinkmoney.co.uk/blog/what-phones-know-about-you/. Acesso em: 8 nov. 2021.

TIESO, Igor Henrique de Souza; SANTO, Felipe do Espírito. **ATAQUES DE ENGENHARIA SOCIAL**. São Paulo, p. 206-218, 18 dez. 2020.

TILLMAN, Maggie. **O que é Snapchat**: como funciona e qual é o ponto? [*S. l.*]: Pocket-lint, 5 fev. 2021. Disponível em: https://www.pocket-lint.com/pt-br/aplicativos/noticias/snapchat/131313-o-que-e-o-snapchat-como-funciona-e-para-que-e-usado. Acesso em: 7 nov. 2021.

TOTVS. **RSA**: Veja quais são suas principais aplicações. [*S. l.*], 7 out. 2020. Disponível em: https://www.totvs.com/blog/negocios/rsa/. Acesso em: 15 nov. 2021.

UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**, São Paulo, 15 fev. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 17 maio 2021.

VANACOR, Vitor. **Criptografia básica**: O que é, como funciona e para o que serve? [*S. l.*]: Elos, 30 jun. 2020. Disponível em: https://blog.elos.vc/criptografia-basica-o-que-e-como-funciona-e-para-o-que-serve/. Acesso em: 9 nov. 2021.

VELASCO, Ariane. **Weibo**: conheça a principal rede social da Chin. [*S. l.*]: Canaltech, 20 dez. 2019. Disponível em: https://canaltech.com.br/redes-sociais/weibo-conheca-a-principal-rede-social-da-china-158137/. Acesso em: 7 nov. 2021.

VENTURA, Layse. **Badoo**: o guia completo sobre a rede social de relacionamentos. [*S. l.*]: Olhar Digital, 24 set. 2021. Disponível em: https://olhardigital.com.br/2021/09/24/*Internet*-e-redes-sociais/badoo/. Acesso em: 7 nov. 2021.

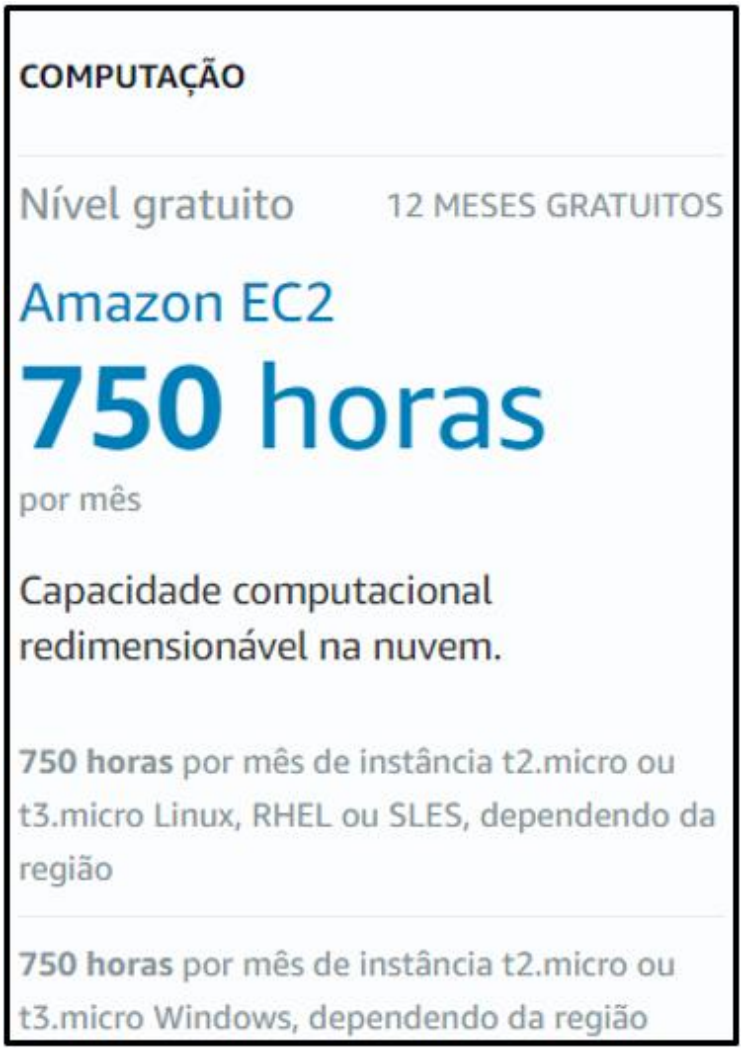
WAZLAWICK, Raul Sidnei. **Metodologia de Pesquisa para Ciência da Computação**. 2. ed. Rio de Janeiro: Elsevier Editora Ltda, 2014. ISBN 978-85-352-7782-1.

WRIGHT, Jordan. ***Gophish* User Guide**: What is *Gophish*? [*S. l.*]: *Gophish*, 2018. Disponível em: https://docs.get*Gophish*.com/user-guide/what-is-*Gophish*. Acesso em: 02 out. 2021.

APÊNDICE A – CRIAÇÃO E CONFIGURAÇÃO DA INSTÂNCIA NO *AMAZON* EC2

O cadastro de um novo usuário na *Amazon Web Services* (AWS) permite a utilização de vários produtos gratuitos de forma limitada ou ilimitada, dependendo do produto escolhido. O *Amazon Elastic Compute Cloud* (EC2) garante que novos usuários utilizem a plataforma por 12 meses gratuitos, para usufruírem das instâncias *t2.micro* ou *t3.micro*, que possui imagens de sistemas operacionais do *Windows* ou do *Linux*, conforme mostrado na Figura 47.

Figura 47 - Nível gratuito para novos usuários no *Amazon* EC2



Fonte: Tela de captura do *website* da AWS (2021).

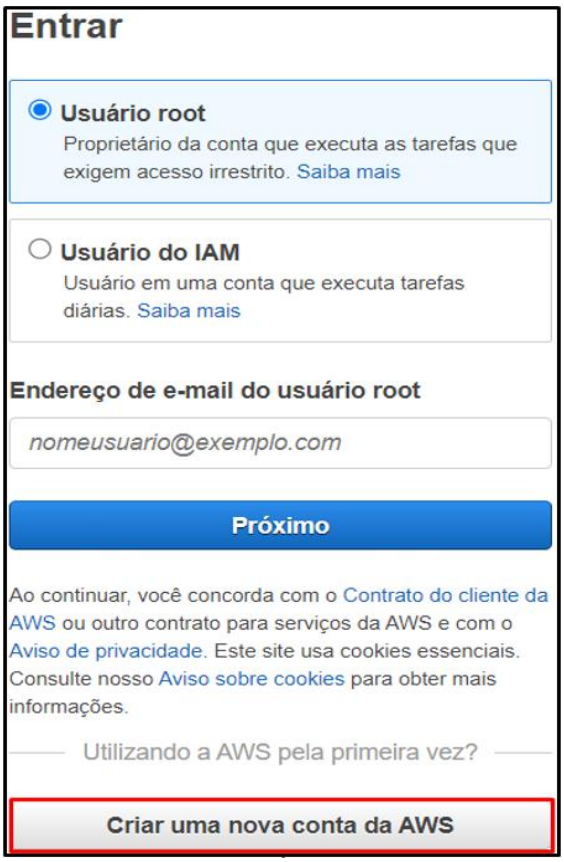
Passo 1: Acessar o site da *Amazon Web Services* (AWS) no endereço *web*: *https://aws.amazon.com/pt/console/*, conforme ilustrado na Figura 48.

Figura 48 - Página *web* oficial da AWS

Fonte: Tela de captura alterada do *website* da AWS (2021).

Após o acesso ao *site*, será necessário fazer o cadastramento na AWS, ao clicar em “fazer login novamente”, será direcionada à página para criar uma conta da AWS, conforme ilustra a Figura 49.

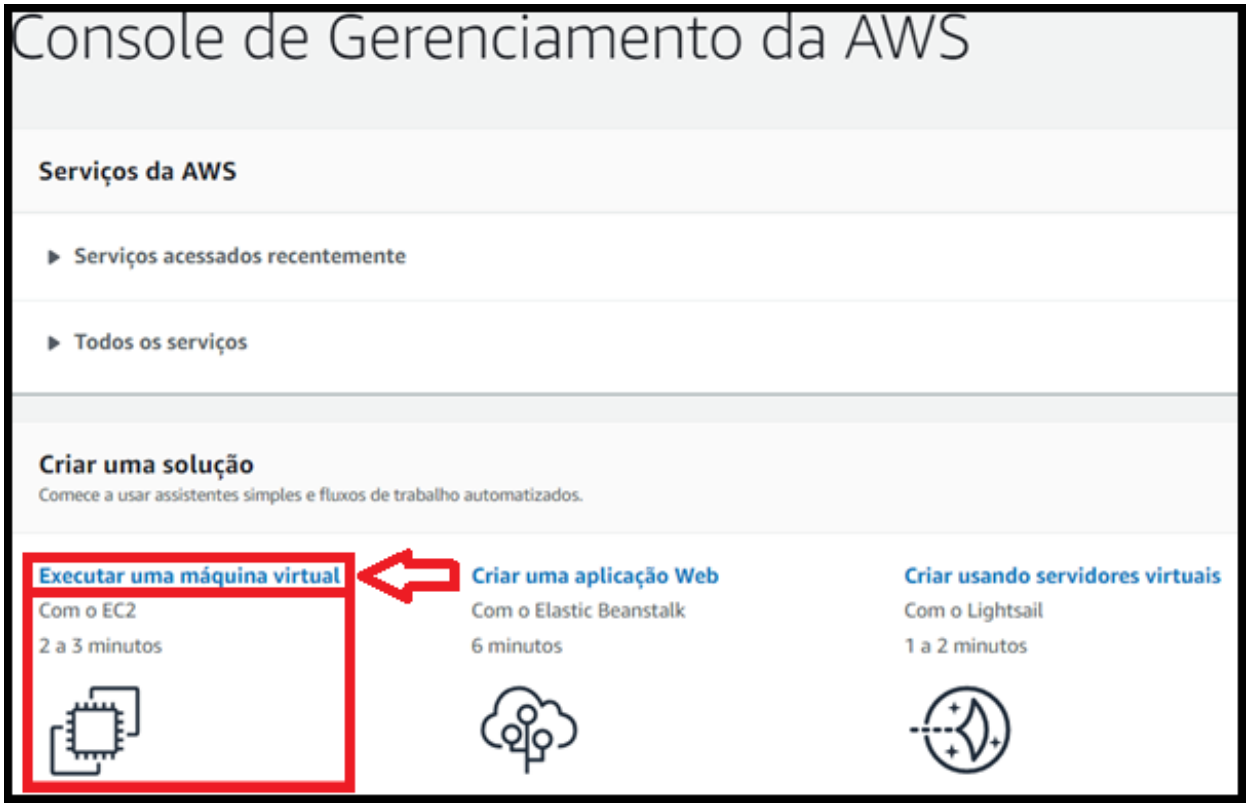
Figura 49 - Entrar ou criar uma conta na AWS



Fonte: Tela de captura alterada do *website* da AWS (2021).

Passo 2: Após criar a conta, será aberto o *layout* do Console de Gerenciamento da AWS. Para criar um servidor virtual é necessário executar a máquina virtual utilizando o *Amazon* EC2, conforme mostrado na Figura 50.

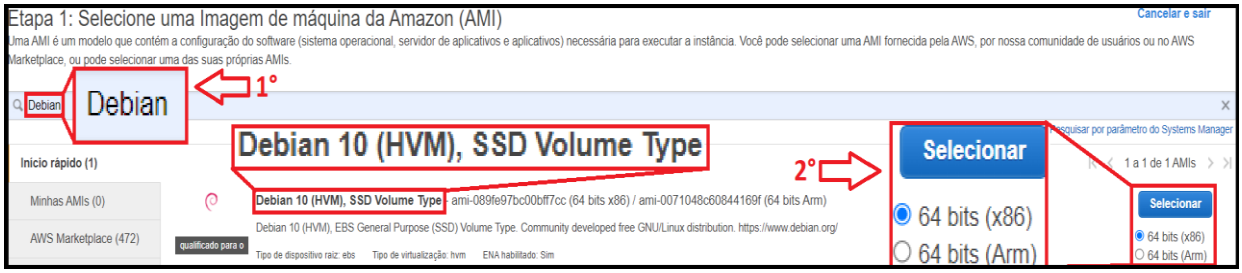
Figura 50 - Executar uma máquina virtual com o EC2



Fonte: Tela de captura alterada do *website* da AWS (2021).

Passo 3: Nesta etapa é selecionado a imagem de máquina a qual a instância irá trabalhar, no caso, foi utilizado a imagem do *Debian* 10, na arquitetura de 64 bits (x86) do sistema operacional, conforme exibido na Figura 51.

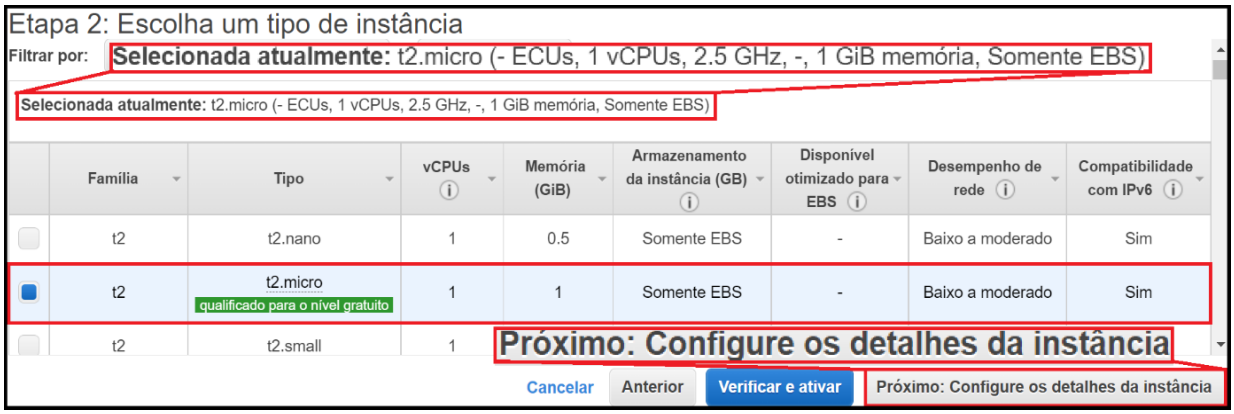
Figura 51 - Seleção da imagem de máquina



Fonte: Tela de captura alterada do *website* da AWS (2021).

Passo 4: Nesta etapa é selecionado uma instância ou servidor virtual que executa a imagem do sistema operacional. A instância selecionada foi a do tipo *t2.micro* que se qualifica nas especificações gratuitas do *Amazon* EC2, possuindo 1 CPU virtual de 2.5GHz de velocidade de processamento, 1 *Gigabyte* (GB) de memória *RAM* e um armazenamento da instância do tipo *Elastic Block Store* (EBS), que é um serviço de armazenamento em blocos fácil de utilizar, escalável e de alta performance, conforme apresentado na Figura 52.

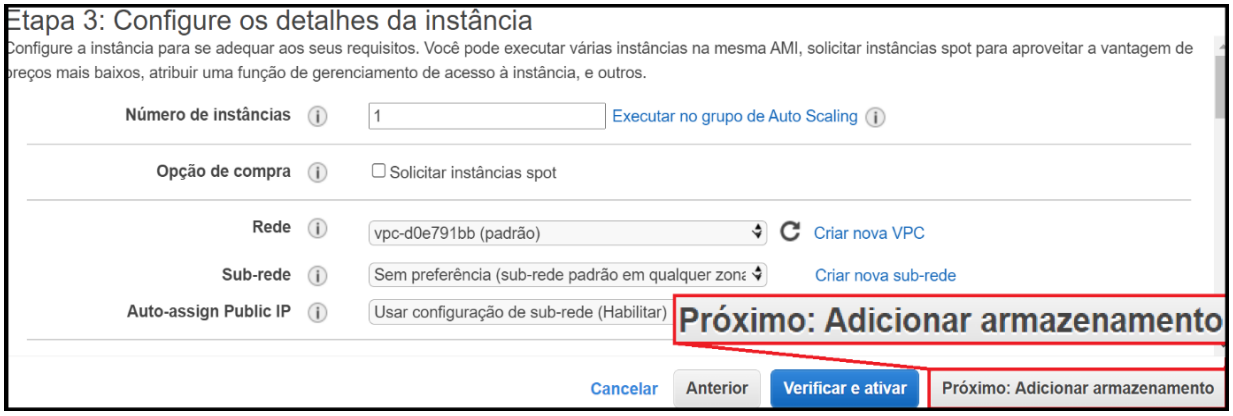
Figura 52 - Seleção da instância



Fonte: Tela de captura alterada do *website* da AWS (2021).

Passo 5: Nesta etapa, as configurações dos detalhes da instância não foram alteradas, sendo utilizada a configuração padrão, conforme mostrado na Figura 53.

Figura 53 - Configuração da instância

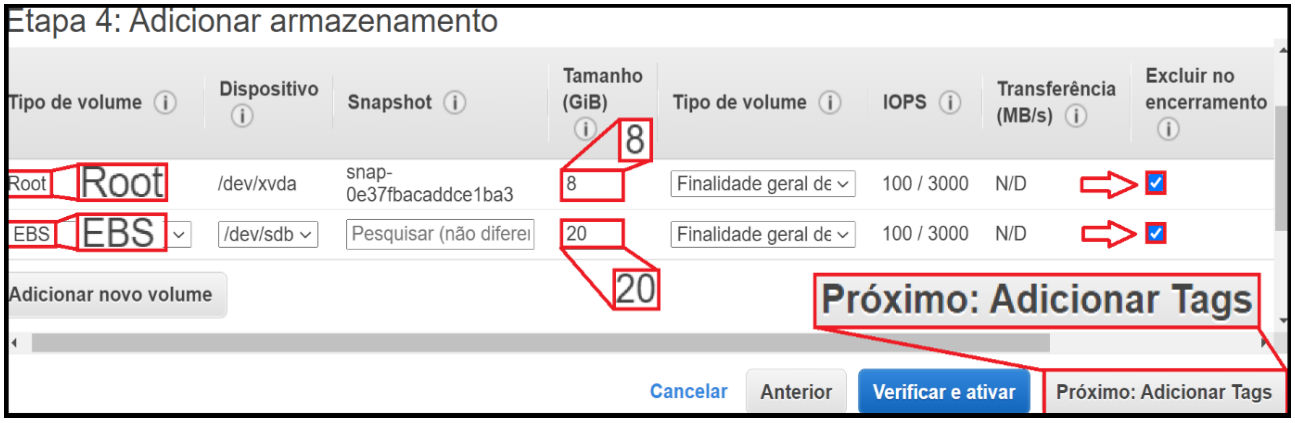


Fonte: Tela de captura alterada do *website* do AWS (2021).

Passo 6: Nesta etapa de configuração do armazenamento, foi selecionado um armazenamento do tipo *root*, possuindo 8GB de tamanho e um armazenamento

do tipo EBS de 20GB de tamanho, além disso, foi selecionada nos dois volumes a opção de excluir o armazenamento após encerrar a instância por completo, conforme exibido na Figura 54.

Figura 54 - Configurações de armazenamento



Fonte: Tela de captura alterada do *website* da AWS (2021).

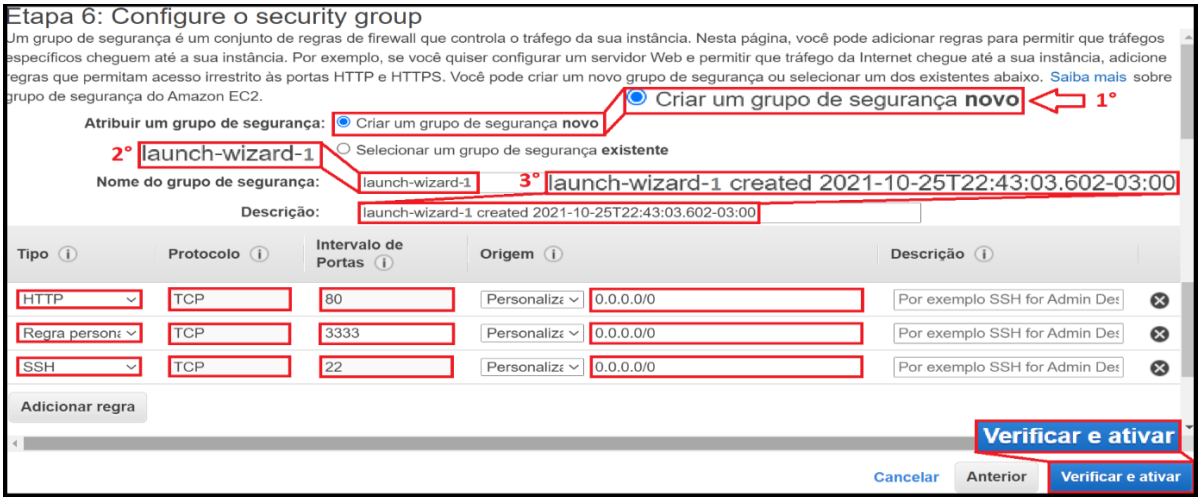
Passo 7: Nesta etapa, nenhuma *tag* ou par de chave-valor foi adicionada, sendo utilizada a configuração padrão, conforme apresentado na Figura 55.

Figura 55 - Configurações de *tags*

Fonte: Tela de captura alterada do *website* da AWS (2021).

Passo 8: Nesta etapa, é configurado um novo grupo de segurança para o controle do tráfego da instância, chamado de *launch-wizard-1*, no qual contém três regras, conforme mostrado na Figura 56.

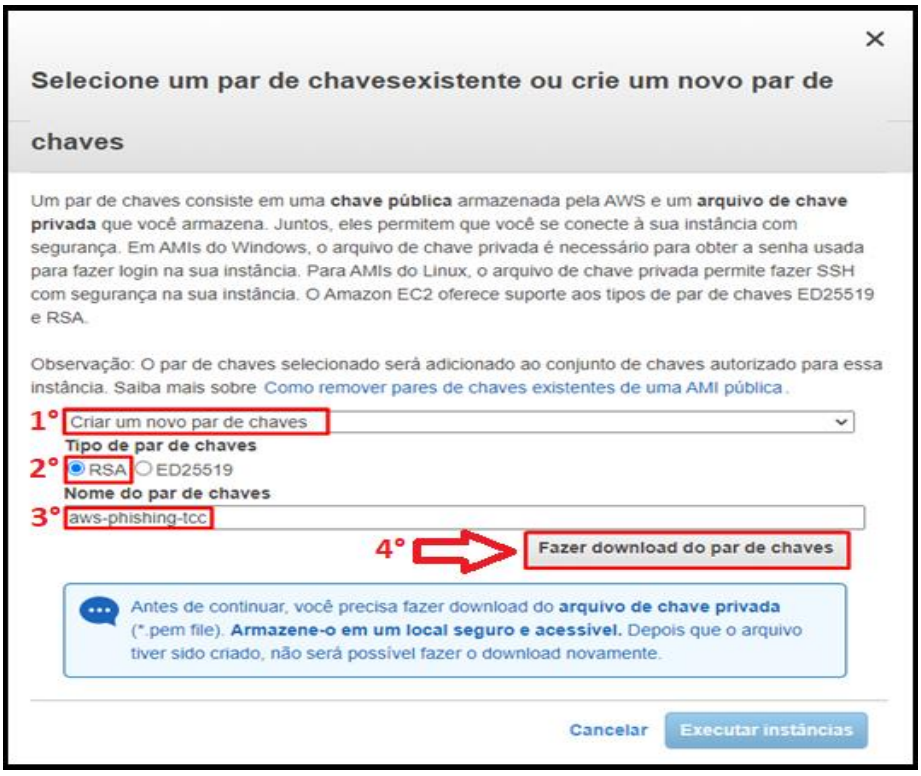
Figura 56 - Configurações de Segurança



Fonte: Tela de captura alterada do *website* da AWS (2021).

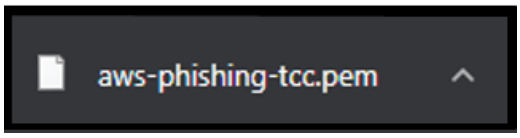
Passo 9: Nesta etapa foi criado um par de chaves do tipo *RSA* para realizar acesso via *Secure Shell* (SSH), designado de "*aws-phishing-tcc*". Após configurado, clique em "fazer download do par de chaves", conforme demonstrado na Figura 57, no qual será feito o download da chave da instância em um arquivo no formato *Privacy Enhanced Mail* (PEM), conforme exibido na Figura 58.

Figura 57 - Criação e *download* do par de chaves



Fonte: Tela de captura alterada do *website* da AWS (2021).

Figura 58 - Download do arquivo no formato PEM



Fonte: Tela de captura da barra de *Downloads* do *Google Chrome* (2021).

APÊNDICE B – INSTALAÇÃO DO *PUTTY*

Para instalar o *PuTTY* é necessário realizar o *download* no site oficial da fabricante, o acesso é gratuito e seguro.

Passo 1: Acessar o site do fabricante no endereço *web*: *https://www.putty.org/*. Após acessar o *link*, será carregado o *layout* do site, em seguida, a opção *Download PuTTY* e clique na opção "*here"* (do português: aqui), conforme mostrado na Figura 59.

Figura 59 - Página *web* oficial do *PuTTY*

Fonte: Tela de captura alterada do *website* do *PuTTY* (2021).

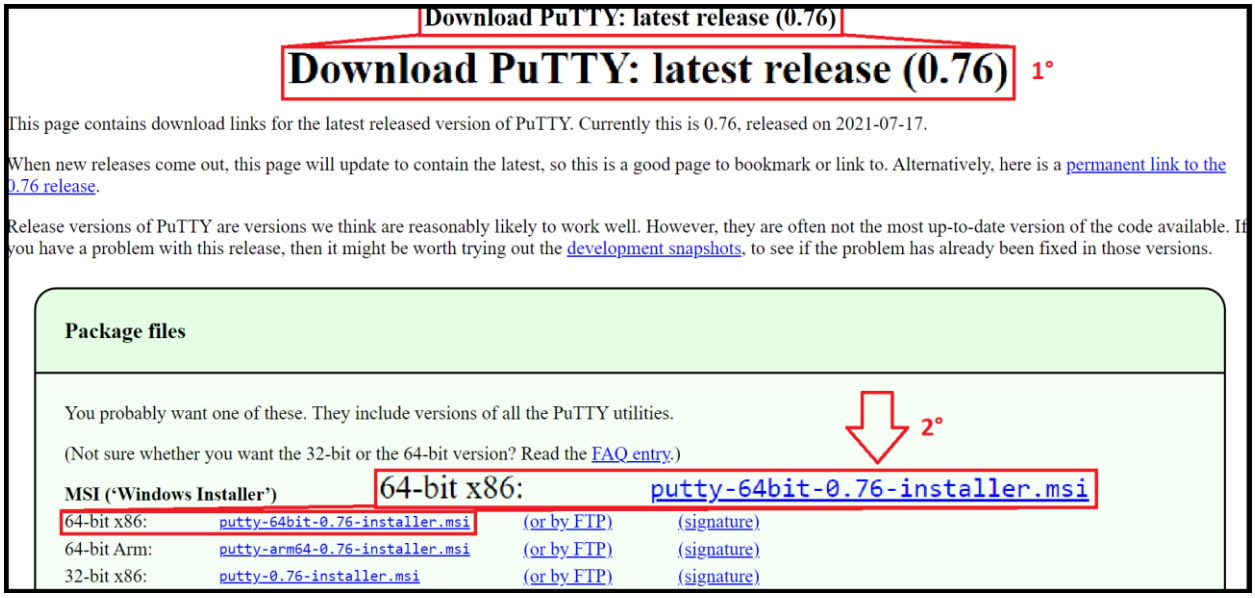
Passo 2: Ao clicar na opção "*here"*, é realizado um redirecionamento para a página que contém todas as versões existentes desenvolvidas do *PuTTY*.

É recomendado sempre escolher a versão mais recente do *software*, escolhendo, portanto, a versão 0.76, lançada no segundo semestre de 2021.

Após escolher a versão, faça o *download* do executável que será instalado em seu sistema operacional, conforme ilustrado na Figura 60.

Neste caso, foi utilizado o sistema operacional do *Windows 10 Home Single Language*, versão 21H1, baseado em uma arquitetura de 64 bits do processador e do sistema operacional, portanto o executável referente é o *putty-64bit-0.76-installer.msi*.

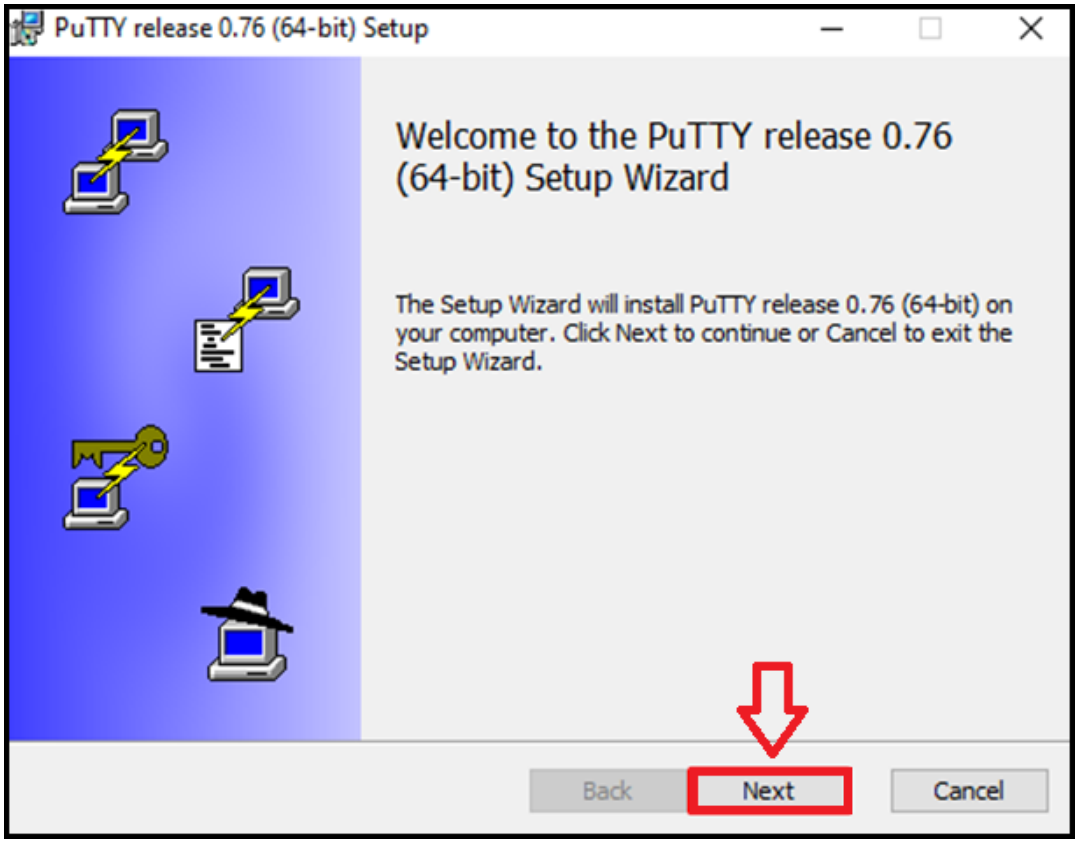
Figura 60 - *Download* da Versão 0.76 do *PuTTY*



Fonte: Tela de captura alterada do *website* do *PuTTY* (2021).

Passo 3: Execute a versão baixada do *PuTTY*, clique em *next* (do português: próximo), conforme ilustrado na Figura 61.

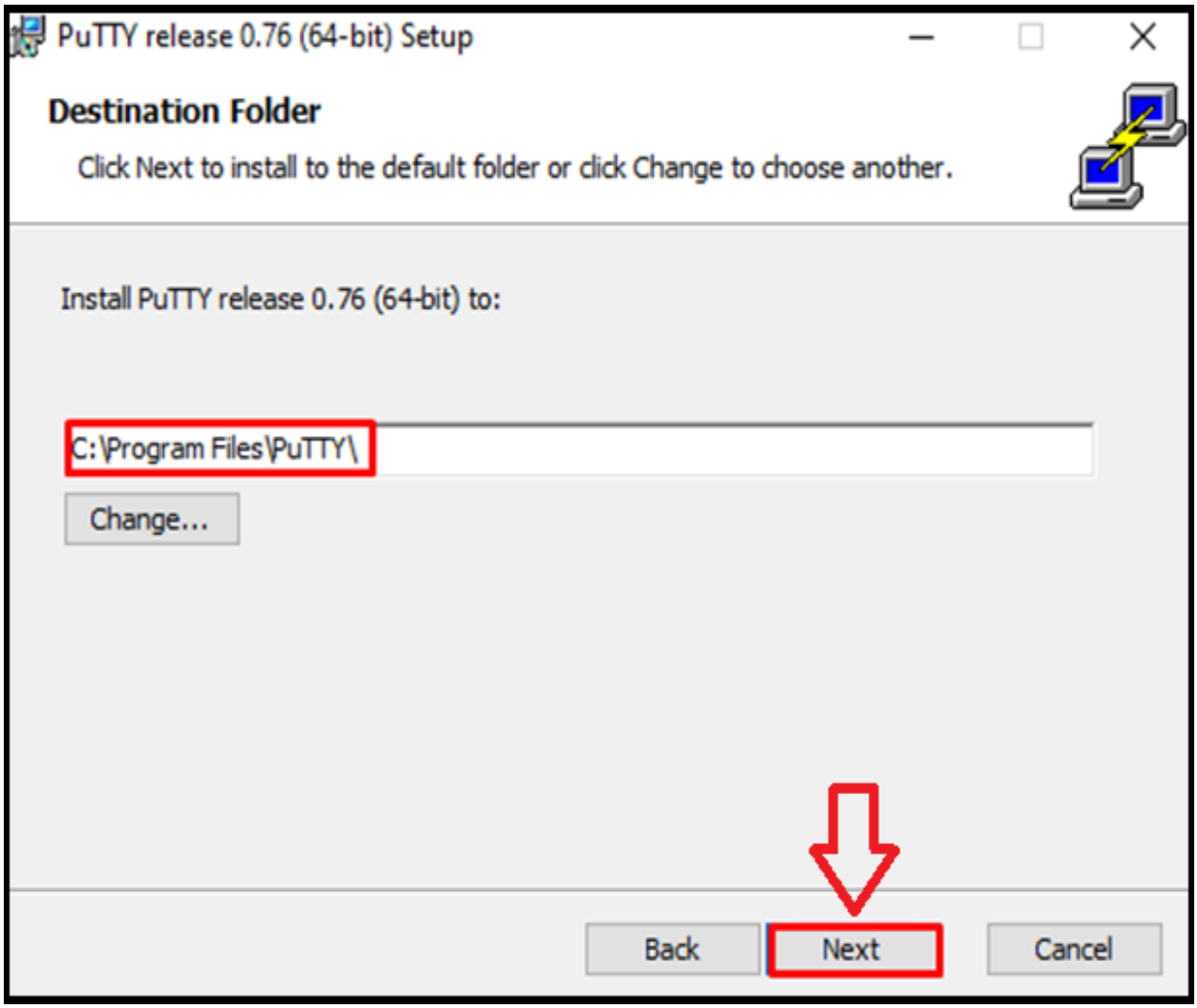
Figura 61 - Executando a Versão 0.76 do *PuTTY*



Fonte: Tela de captura alterada do processo de instalação do *PuTTY* (2021).

Passo 4: Defina o diretório no qual o *PuTTY* será instalado em sua máquina, após definir o local, clique em *next*, conforme exibido na Figura 62.

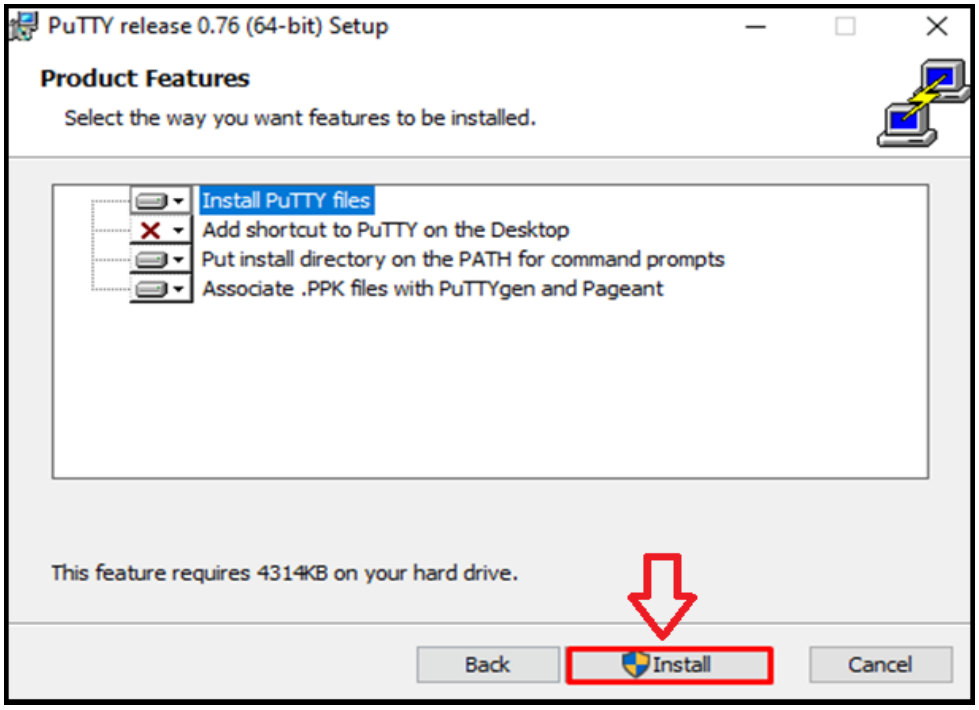
Figura 62 - Definindo o local de instalação do *PuTTY*



Fonte: Tela de captura alterada do processo de instalação do *PuTTY* (2021).

Passo 5: Deixe de forma padrão as características e os recursos do produto, clique em *install* (do português: instalar) para prosseguir, conforme apresentado na Figura 63.

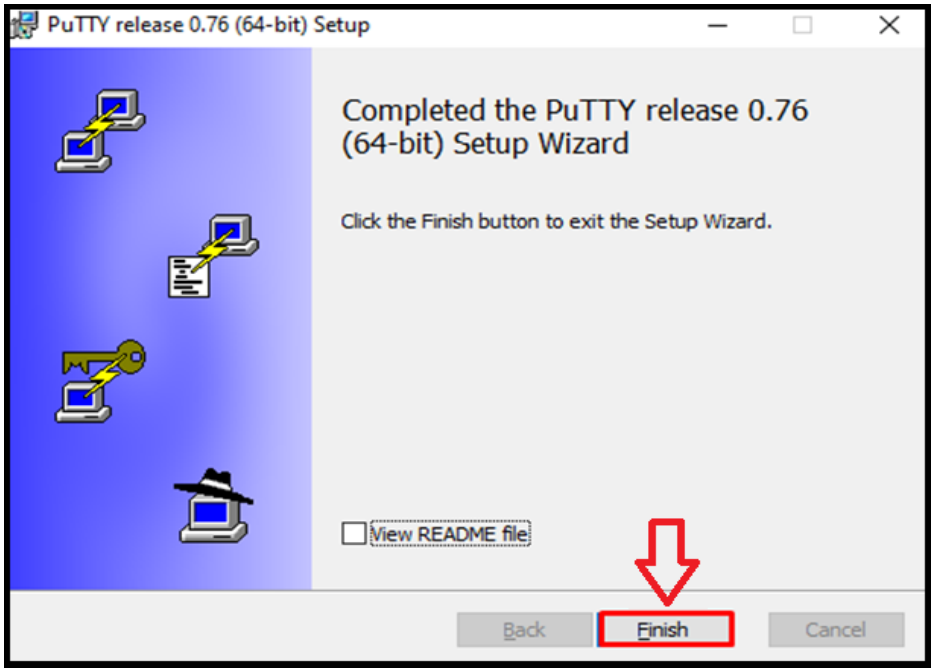
Figura 63 - Definindo os recursos do produto e instalando o *PuTTY*



Fonte: Tela de captura alterada do processo de instalação do *PuTTY* (2021).

Passo 6: Após a instalação do software, o produto estará pronto para ser utilizado, clique em *"finish"* (do português: finalizar) para concluir a etapa de instalação, conforme ilustrado na Figura 64.

Figura 64 - Finalização da instalação do *PuTTY*



Fonte: Tela de captura alterada do processo de instalação do *PuTTY* (2021).

APÊNDICE C – INSTALAÇÃO E CONFIGURAÇÃO DO *GOPHISH*

Para instalar o *Gophish* é necessário realizar o *download* no *site* oficial da fabricante, o acesso é gratuito e seguro.

Passo 1: Acessar o site do fabricante no endereço *web*: *https://getGophish.com/*. Após acessar o *link*, será carregado o *layout* do site, clique na opção "*Download*", conforme mostrado na Figura 65.

Figura 65 - Página *web* oficial do *Gophish*

Fonte: Tela de captura alterada do *website* do *Gophish* (2021).

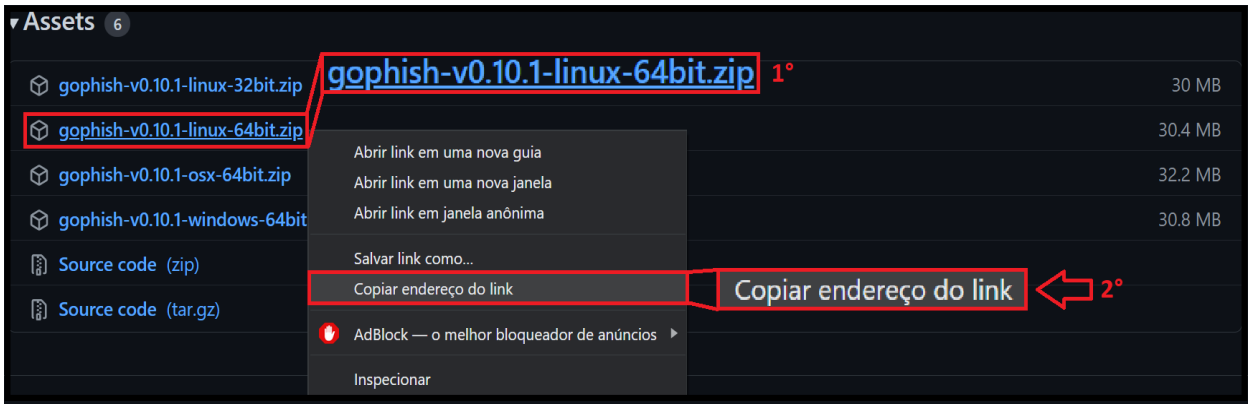
Passo 2: Ao clicar na opção "*Download*", é realizado um redirecionamento para a página que contém todas as versões existentes desenvolvidas do *Gophish*. É recomendado sempre escolher a versão mais recente do *software*, escolhendo, portanto, a versão 0.10.1, lançada no primeiro semestre de 2020, conforme exibido na Figura 66.

Figura 66 - Escolhendo a Versão 0.10.1 do *Gophish*

Fonte: Tela de captura alterada do *website* do *Gophish* (2021).

Passo 3: Após escolher a versão, clique com o botão direito no arquivo executável e selecione a opção “Copiar endereço do *link*”, isto será necessário pelo fato do *download* ter que ser feito no sistema operacional *Debian*, que utiliza o *kernel* do *Linux*, baseado em uma arquitetura de 64 bits do processador e do sistema operacional, portando o executável referente é o “*Gophish-v0.10.1-linux-64bit.zip”*, conforme apresentado na Figura 67.

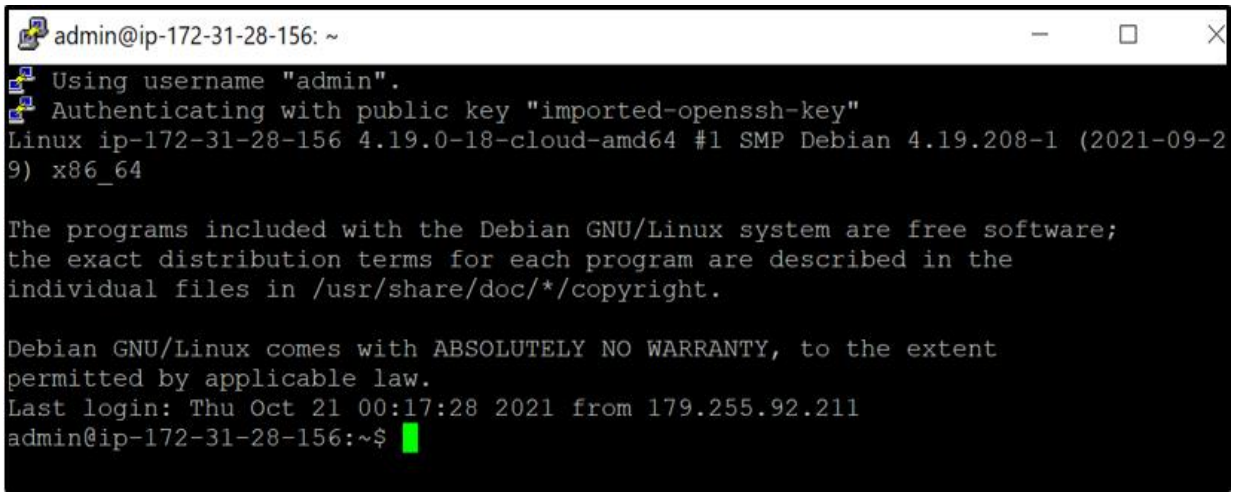
Figura 67 - Cópia do *link* do endereço da Versão 0.10.1 do *Gophish*



Fonte: Tela de captura alterada do *website* do *Gophish* (2021).

Passo 4: Após a cópia do endereço do *link* referente a versão do executável do *Gophish*, acesse o *PuTTY* com a instância criada no AWS para ingressar no sistema operacional do *Debian*, posteriormente será possível fazer a configuração dos serviços do servidor através do terminal, conforme mostrado na Figura 68. Tornando-se viável realizar o *download*, instalação e configuração do *Gophish*.

Figura 68 - Execução da instância *Linux* com imagem do *Debian* na sessão do *PuTTY*



Fonte: Tela de captura retirada do terminal no *PuTTY* (2021).

Passo 5: Acessar como usuário *root* ou administrador, para ter acesso ilimitado aos recursos do sistema, utilizando o Comando 01, conforme apresentado no Quadro 01.

Passo 6: Baixar atualizações e informações dos pacotes de todas os repositórios configurados e instalar as atualizações disponíveis dos pacotes instalados atualmente no sistema, utilizando o Comando 02, conforme exibido no Quadro 01.

Passo 7: Para descompactar pastas e arquivos, é necessário instalar o *unzip* (do português: descompactar) na linha de comando do sistema *Debian*, utilizando o Comando 03, conforme mostrado no Quadro 01.

Passo 8: Alteração do diretório padrão para o */opt/*, que é um diretório de pacotes opcionais do *Debian*, tendo a utilidade em colocar *softwares* proprietários, utilizando o Comando 04, conforme exibido no Quadro 01.

Passo 9: Criação de uma pasta chamada "*phishing*" no diretório pai */opt/*, utilizando o Comando 05, conforme apresentado no Quadro 01.

Passo 10: Alteração do diretório */opt/* para o diretório filho */opt/phishing/*, utilizando o Comando 06, conforme mostrado no Quadro 01.

Quadro 1: Preparando o ambiente para a instalação do Gophish

Comando 01	*# sudo su*
Comando 02	*# apt update && apt upgrade*
Comando 03	*# apt-get install unzip*
Comando 04	*# cd /opt/*
Comando 05	*# mkdir phishing*
Comando 06	*# cd /opt/phishing/*

Fonte: Autoria própria

Passo 12: Seguindo o Passo 3, é necessário baixar o arquivo compactado da versão 0.10.1 do *Gophish* para o sistema operacional do *Debian*. Colocar o comando "*wget*" é essencial antes de colar o endereço do *link* no terminal, pois ele permitirá baixar arquivos que utilizam protocolo HTTPS, para este passo foi utilizado o Comando 07, conforme exibido no Quadro 02.

Passo 13: Descompactar o arquivo baixado no Passo 12, utilizando o Comando 08, conforme informado no Quadro 02.

Passo 14: Após descompactar o arquivo, será possível configurar o arquivo "*config.json*", através do editor de texto "*nano*", utilizando o Comando 09, conforme apresentado no Quadro 02.

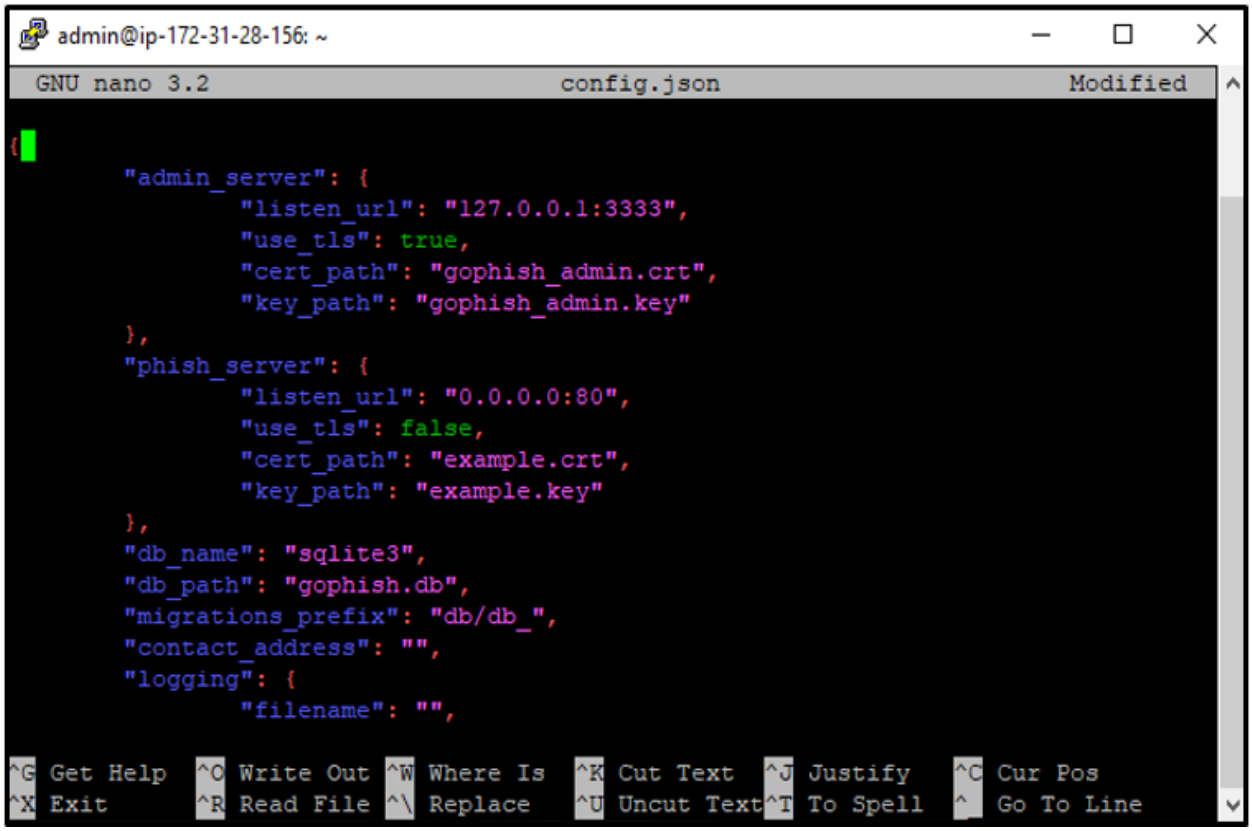
Quadro 2: Instalando e configurando o Gophish no sistema Debian

Comando 07	*# wget https://github.com/Gophish/Gophish/releases/download/v0.10.1/Gophish-v0.10.1-linux-64bit.zip*
Comando 08	*# unzip Gophish-v0.10.1-linux-64bit.zip*
Comando 09	*# nano config.json*

Fonte: Autoria própria

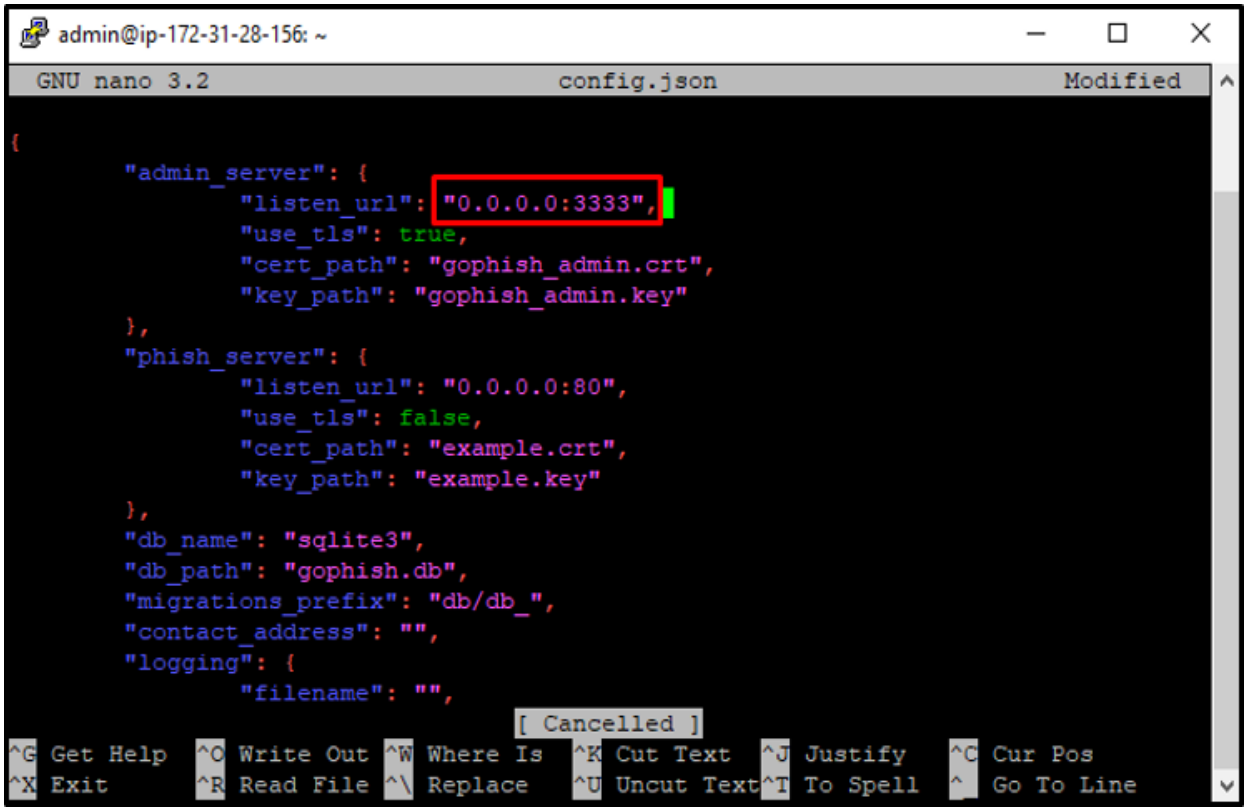
Passo 15: O editor de texto "*nano*" abrirá o arquivo "*config.json*", possibilitando o *root* alterar as configurações padrões deste arquivo de formato "*json*" que tem a função de trocar informações e dados entre o servidor do *Gophish* e o servidor do administrador, conforme ilustra a Figura 69. A única alteração será feita na URL de escuta do *admin_server*, para aceitar qualquer endereço IP do servidor local, utilizando a porta 3333 de protocolo TCP, conforme ilustrado na Figura 70.

Figura 69 - Conteúdo padrão do arquivo *config.json*



Fonte: Tela de captura do arquivo *config.json* no *PuTTY* (2021).

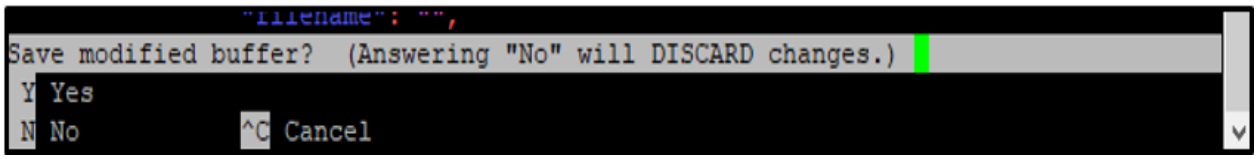
Figura 70 - Conteúdo modificado do arquivo *config.json*



Fonte: Tela de captura alterada do arquivo *config.json* no *PuTTY* (2021).

Passo 17: Após alterar as configurações da URL do *admin_server*, aperte as teclas CTRL + X, depois clique na tecla Y para salvar as alterações feitas no arquivo, conforme apresentado na Figura 71. Em seguida, saia do editor de texto "*nano*" clicando na tecla ENTER, finalizando o processo de instalação do *Gophish*.

Figura 71 - Salvando as alterações feitas no arquivo *config.json*



Fonte: Tela de captura do arquivo *config.json* no *PuTTY* (2021).

Passo 18: Parar de executar o servidor *apache2*, utilizando o Comando 10, conforme informado no Quadro 03.

Passo 19: Permitir que o arquivo *Gophish* seja executado dentro do diretório */opt/phishing/*, utilizando o Comando 11, conforme exibido no Quadro 03.

Passo 20: Executar o arquivo *Gophish* no terminal, utilizando o Comando 12, conforme informado no Quadro 03.

Quadro 3: Instalando e configurando o Gophish no sistema Debian

Comando 10	# *systemct1 stop apache2*
Comando 11	# *chmod +x Gophish*
Comando 12	# *./Gophish*

Fonte: Autoria própria