PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

ESTUDO SOBRE VULNERABILIDADES E IMPLEMENTAÇÃO DE UM CENÁRIO DE SQL INJECTION

BRUNA CARNEIRO MACHADO

GOIÂNIA
2021

BRUNA CARNEIRO MACHADO

ESTUDO SOBRE VULNERABILIDADES E IMPLEMENTAÇÃO DE UM CENÁRIO DE SQL INJECTION

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

Orientadora:

Profa. Dra. Solange Da Silva

GOIÂNIA

2021

BRUNA CARNEIRO MACHADO

ESTUDO SOBRE VULNERABILIDADES E IMPLEMENTAÇÃO DE UM CENÁRIO DE SQL INJECTION

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Ciências da 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

_____
Prof. Me. Max Gontijo De Oliveira

_____
Prof. Me. Rafael Leal Martins

GOIÂNIA

2021

Dedico este trabalho para meus pais pelo apoio e carinho que tiveram em todos os momentos da minha vida.

AGRADECIMENTOS

A Deus por ter me dado saúde e força para superar as dificuldades e me permitido ultrapassar os obstáculos encontrados.

Gostaria de agradecer a minha família, minha mãe Marina, meu pai Renato, minha irmã Carolina, minha avó Neuza e minha tia Maria Luciane, por sempre me apoiarem e me incentivarem ao longo da vida.

Em especial, gostaria de agradecer aos meus pais, por terem me proporcionado oportunidades de estudo, me apoiado e auxiliado ao longo da minha vida estudantil. Além de terem caminhado e comemorado todas as minhas conquistas junto comigo.

A minha orientadora Solange da Silva, pelo apoio, paciência e por sempre ter me ajudado a realizar cada passo dessa monografia.

RESUMO

O objetivo deste trabalho foi o de identificar e descrever algumas formas de ataques aos dados mais conhecidas, apresentando os pontos de vulnerabilidade do acesso. Em relação aos procedimentos técnicos, é uma pesquisa bibliográfica e experimental. Quantos aos resultados foram identificados os seguintes ataques: *Port Scanning Attack, Phishing, Spoofing, Sniffing* e SQL *Injection*. Os seus pontos de vulnerabilidade são: portas de rede desprotegidas, falta de conscientização dos funcionários e desenvolvedores, protocolos de segurança fracos e falta de boas práticas no desenvolvimento das aplicações. Os resultados permitiram concluir que não existe uma única solução para evitar os ataques e resolver todos os problemas de vulnerabilidades da empresa. Entretanto, existem diversas formas eficientes de proteção e boas práticas, tais como o treinamento dos funcionários e manter políticas de segurança difundidas na organização. Além disso, saber quais são os principais tipos de ataques e como os cibercriminosos agem são fatores para manter a empresa protegida contra ataques cibernéticos.

Palavras Chaves: Segurança de dados. Vulnerabilidades. Ataques. Cibercrime. Políticas de Segurança.

ABSTRACT

The objective of this work was to identify and describe some forms of attacks on the most known data, presenting the points of vulnerability of access. In relation to technical procedures, it is a bibliographic and experimental research. How many of the results were identified the following attacks: Port Scanning Attack, Phishing, Spoofing, Sniffing and SQL Injection. Its points of vulnerability are: unprotected network ports, lack of awareness of employees and developers, weak security protocols, and lack of good practices in application development. The results allowed us to conclude that there is no single solution to prevent attacks and solve all company vulnerability issues. However, there are several efficient forms of protection and good practices, such as training employees and maintaining widespread security policies in the organization. In addition, knowing what are the main types of attacks and how cybercriminals act are factors to keep the company safe from cyber attacks.

Key Words: Data security. Vulnerabilities. Attacks. Cybercrime. Security Policies.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados Pessoais
ANSI	*American National Standarts Institute*
API	*Application Programming Interface* ou Interface de Programação de Aplicativos
ARP	*Address Resolution Protocol* ou Protocolo de Resolução de Endereços
BD	Banco de Dados
CERT.br	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil
CMMI	*Capability Maturity Model Integration* ou Modelo de Capacidade e Maturidade Integrado
COBIT	*Control Objetives for Information and Related Techonology*
COPEL	Cia Paranaense de Energia
DCL	*Data Control Language* ou Linguagem de Controle de Dados
DDL	*Data Definition Language* ou Linguagem de Definição de Dados
DML	*Data Manipulation Language* ou Linguagem de Manipulação de Dados
DNS	*Domain Name System*
FBI	*Federal Bureau of Investigation* ou Departamento Federal de Investigação
FTP	*File Transfer Protocol*
GB	*GigaByte*
GDPR	*General Data Protection Regularion* ou Regulamento Geral de Proteção de Dados
GHz	*GigaHertz*
GPS	*Global Positioning System* ou Sistema de Posicionamento Global

HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
IANA	*Assigned Numbers Authority*
IBM	*International Business Machines*
ICMP	*Internet Control Message Protocol* ou Protocolo de Mensagens de Controle de Internet
ID	*Identity* ou Identidade
IDE	Ambiente de Desenvolvimento Integrado
IP	*Internet Protocol* ou Protocolo da Internet
ISP	Internet *Service Provider*
ITIL	*Information Technology Infrastructure Library* ou Biblioteca de Infraestrutura de Tecnologia da Informação
J2EE	*Java 2 Platform Enterprise Edition*
LAN	*Local Area Network* ou Rede Local
LGPD	Lei Geral de Proteção de Dados Pessoais
MPS.br	Melhoria do Processo de Software Brasileiro
NNTP	*Network News Transfer Protocol*
OWASP	*Open Web Application Security Project* ou Projeto Aberto de Segurança em Aplicações Web
RAM	R*andom Access Memory* ou Memória de Acesso Randômico
RDP	*Remote Desktop Protocol*
SFTP	*Secure File Transfer Protocol* ou Protocolo de Transferência de Arquivos Seguro
SGBD	Sistema Gerenciador de Banco de Dados
SGSI	Sistema de Gestão de Segurança da Informação

SI	Segurança da Informação
SMS	*Short Message Service* ou Serviço de Mensagens Curtas
SMTP	*Simple Mail Transfer Protocol*
SO	Sistema Operacional
SQL	*Structured Query Language* ou Linguagem de Consulta Estruturada
SQLi	SQL *Injection* ou Injeção SQL
SSH	*Secure Shell*
STI	Superintendência de Tecnologia da Informação
TCC	Trabalho de Conclusão de Curso
TCP	*Transmission Control Protocol* ou Protocolo de Controle de Transmissão
TFDV	Técnicas e Ferramentas de Detecção de Vulnerabilidades
TI	Tecnologia da Informação
UDP	*User Datagram Protocol* ou Protocolo de Datagrama do Usuário
URL	*Uniform Resource Locator* ou Localizador Uniforme de Recursos
USP	Universidade de São Paulo
VPN	Rede Privada Virtual
WCVT	*Waitsfield e Champlain Valley Telecom*

SUMÁRIO

1 INTRODUÇÃO

A facilidade do acesso à Internet mudou a forma de interação entre as pessoas no mundo, também trouxe meios para novos crimes que se tornaram possíveis com o uso da rede (CAMPELO e PIRES, 2019).

Os dados estão sendo vistos, a cada dia, como um patrimônio em razão do seu valor estratégico. A segurança dos dados é necessária para organizações porque para empresas que contém processos digitalizados é imprescindível transmitir confiança e integridade dessas informações para clientes e para o próprio local (TOTUS, 2020).

Os dados podem ser definidos como um conjunto de recursos em estado bruto, algo que ainda não possuí significado. A partir desses elementos, é possível tirar determinadas informações. Podem ser considerados dados, por exemplo, filmes, imagens, livros, entre outros (MOREIRA et al., 2020).

A segurança dos dados é a proteção dos mesmos diante de ameaças, acidentes, roubo, destruição, entre outros. Segurança de dados refere-se à preservação das informações de uma organização, sendo uma preocupação não só do departamento de Tecnologia da Informação (TI) mas de toda a empresa (LUCENA, 2017).

No Brasil, com o objetivo de proteger os dados de todo cidadão que esteja no país foi aprovada em agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) de n° 13.709, que entrou em vigor em agosto de 2020. Esta lei tem o propósito de criar condições de segurança jurídica, padronizando normas e práticas, de forma igualitária (SERPRO, 2018).

A norma ISO 27005, de técnicas de segurança e gestão de riscos de Segurança da Informação (SI), também tem como objetivo fornecer padrões e normas para as organizações, para lidar com ameaças na área da TI (CICCO, 2008).

A norma ISO 27002, tem como objetivo apresentar métodos de SI e efetivas práticas de gestão da segurança. Estabelece procedimentos e elementos gerais para iniciar, realizar, manter e aprimorar a gestão da SI em uma empresa (ABNT, 2005).

A SI é a proteção dos dados. Sendo informação o valor significativo desses dados para uma organização ou indivíduo. As ameaças à SI podem ser pessoas ou condições que causam impacto nos negócios da empresa, explorando os pontos de vulnerabilidades, ocasionando perda de integridade ou confidencialidade (RAMOS et al., 2017).

A segurança cibernética é um conjunto de ações preventivas com o objetivo de proteger sistemas, dispositivos e pessoas de ataques que utilizam das falhas dos sistemas para invadir, roubar e manipular os dados. Implica na prevenção e proteção, agindo apenas no ciberespaço (SCHULTZ, 2020).

> [...]Os acontecimentos concentrados no período que vai de junho de 2012 até junho de 2013 marcaram um “Ano Zero” para a cibersegurança, isto é, marcaram a ampliação das discussões midiáticas e governamentais sobre o tema. Em junho de 2012, uma extensa reportagem de David Sanger ao jornal *The New York Times* revelaria as origens do *Stuxnet*, o vírus de computador que danificou centrífugas nucleares na usina de Natanz, no Irã. Exatamente um ano depois, em junho de 2013, as revelações do caso *Snowden*, o maior vazamento de informações da comunidade de Inteligência na história dos EUA, abalaram relações diplomáticas e trouxeram o ciberespaço e o controle da Internet para o centro do debate (MAIER, 2019, p. 380).

O ciberespaço é o local em que as informações são armazenadas, compartilhadas e comunicadas *on-line*, em um domínio de redes de computadores. Não somente virtual, o ciberespaço, também contém computadores que armazenam dados, Internet, celulares, entre outros (GALOYAN, 2019).

A propagação da tecnologia (sendo fixa ou móvel) criou oportunidades para a criminalidade. As facilidades tecnológicas para a comunicação e informação, com a movimentação de serviços, mercadorias e diversos dados, gera possibilidades de explorar novas modalidades do crime (SOUZA, 2017).

O termo *hacker* tem como significado um indivíduo que estuda códigos de programação, realiza a procura de falhas em sistemas que não deveriam existir e realiza a tentativa de acesso aos dados. Determinados *hackers* praticam esse ato para o bem, informando as empresas sobre as falhas, às vezes, sendo pagos por isso. No entanto, outros aproveitam das falhas para obter acesso aos dados para o aproveito próprio (ANDRADE et al., 2017).

O cibercrime, também conhecido como crime de computador, é um conjunto de atividades ilegais em que criminosos, utilizando ferramentas digitais, roubam ou realizam atividades criminosas. As fraudes de credenciais seria um dos exemplos desse tipo de crime, em que para fazer isso, hackers se apropriam dos dados dos usuários (GALOYAN, 2019).

Justifica-se estudar este tema, pois a propagação da TI e das comunicações junto com o aumento da base de dados resultou em fragilidade para os países,

empresas e para os indivíduos (CORREIA et al., 2017). Além disso, a ausência de políticas de segurança numa organização expõe os seus dados aos riscos de ataques, tornando-se vulnerável (RAMOS et al., 2017).

Diante deste contexto, esse projeto visa responder a seguinte questão de pesquisa: **- Quais são as formas de ataques aos dados mais conhecidas e as correspondentes vulnerabilidades?**

O objetivo geral deste trabalho é identificar e descrever algumas formas de ataques aos dados mais conhecidas, apresentando os pontos de vulnerabilidade do acesso. Além de realizar experimentos desse ataque.

Os objetivos específicos são:

- Identificar as formas preventivas de ataques aos dados;
- Identificar exemplos de empresas que já foram alvo de ataques;
- Realizar o experimento do ataque de SQL *Injection*.

Espera-se que os resultados deste trabalho possam contribuir:

- Alertando os administradores de dados sobre as vulnerabilidades de acesso existentes;
- Informando a comunidade sobre os ataques aos dados já conhecidos;
- Mostrando a importância de se ter políticas de segurança de dados em uma empresa;
- Apresentando as normas de segurança existentes.

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 estruturada da seguinte maneira: neste Capítulo é apresentado o contexto do trabalho, a questão de pesquisa, objetivo e resultados esperados. O Capítulo 2 traz o referencial teórico com conceitos, definições, leis de proteção aos dados e trabalhos relacionados com o tema. No Capítulo 3 é descrito o método, mostrando como o trabalho foi desenvolvido e o que foi feito para atingir o objetivo geral. No Capítulo 4 é apresentado alguns dos ataques aos dados de empresas já conhecidos, identificando as vulnerabilidades que permitiram que o acesso indesejado ocorresse. Além disso, foi realizada a implementação de um dos ataques. O Capítulo 5 é apresentado a análise dos resultados obtidos. Finalmente, o Capítulo 6 traz as considerações finais do TCC e sugestões para trabalhos futuros.

2 REFERENCIAL TEÓRICO

Neste capítulo são apresentadas três partes: uma de conceitos e definições, a segunda de leis e de normas e a terceira de trabalhos relacionados.

2.1 Conceitos e Definições

A Segurança da Informação (SI) é a proteção da informação, dos dados disponíveis em uma empresa, dos vários tipos de ameaças. Sendo amplamente debatida devido ao avanço da tecnologia, tornando cada vez mais importante para as organizações (RAMOS, et al. 2017).

A SI assegura que não tenha acessos não autorizados nos computadores e aos dados, evitando que pessoas não autorizadas tenham acesso a essas informações. Além disso, impede a destruição, roubos ou que os dados sejam danificados. Dessa forma, as informações disponíveis ficam disponíveis, integras e com autenticidade (GAIDARGI, 2018).

O conjunto de ações de proteção dos dados, da SI, é formado pelos seguintes pilares: confidencialidade, integridade, disponibilidade e autenticidade. Essas bases são fundamentais para a proteção das informações da organização (DURBANO, 2018).

A segurança cibernética é a prevenção dos ataques que são realizados por sistemas maliciosos que utilizam de falhas sistêmicas para invadir dispositivos, podendo roubar, manipular ou tornar indisponíveis dados ou arquivos. Envolve ações de proteção de sistemas, pessoas e dispositivos contra esses ataques (SCHULTZ,2020).

A segurança cibernética é uma parte da SI, que abrange etapas de proteção dentro da empresa que é necessária para manter segura contra acessos indesejados devido as vulnerabilidades na rede ou dos sistemas de informação (TORRES, 2019).

O investimento na segurança cibernética se tornou necessária e um fator de sucesso para as empresas. Além desses ataques aumentarem as vulnerabilidades e colocar em risco os dados das organizações, tendem a crescer e desenvolver rapidamente, acompanhando os avanços tecnológicos (FERNANDES, 2019).

O cibercrime é a prática ilegal que utiliza o computador ou meios da TI para realizar uma ação criminosa em que os equipamentos de TI é o objeto do crime

(ALEXANDRE JUNIOR, 2019). Utilizam de vulnerabilidades da rede para roubar principalmente dados, o que pode ocasionar grandes danos a empresas (FERNANDES, 2020).

A *Symantec*, empresa que desenvolve soluções em antivírus para todo o mundo, realizou uma pesquisa informando que, no ano de 2016, os brasileiros obtiveram um prejuízo de mais ou menos R$33 milhões com cibercrimes. Ou seja, foram em torno de 42,4 milhões de cidadãos no país afetados por esses crimes (LUCENA, 2017).

O roubo de credenciais, um dos cibercrimes existentes, tem como objetivo coletar informações roubadas de empresas ou de usuários, utilizando essas informações em vários *websites*, com o propósito de conseguir acesso às contas de redes sociais, servidores de e-mail, bancos, entre outros. A empresa *Akamai*, especializada em segurança, identificou mais de 3 bilhões de tentativas de roubos de credenciais no Brasil (RIBEIRO, 2021).

A segurança dos dados é a proteção contra acessos indesejados que possam modificar, sequestrar ou roubar os dados, ou seja, previne situações que possam comprometer uma organização. A segurança nas empresas utiliza um conjunto de ações preventivas e que reagem a ataques, das quais confidencialidade, integridade, autenticidade, conformidade, entre outros, para que possam manter a disponibilização das informações de forma correta e segura (TOTUS, 2020).

Operações de empresas e as atividades profissionais estão sendo realizadas em ambientes online. Dessa forma, a segurança dos dados passou a ser ainda maior, pois essas circunstâncias fazem aumentar os riscos a integridade das informações que trafegam na rede (SANTIAGO, 2018).

A determinação de um programa de segurança dos dados fornece a melhor maneira de manter os dados da empresa seguros. Dessa forma, é avaliado os riscos que a empresa pode enfrentar e caso ocorra um ataque, como lidar com a situação para minimizar os impactos na organização. Além disso, indica com que frequência deve ser revisado e atualizado o formato das medidas de segurança (GAIDARGI, 2018).

Segundo os dados do relatório do *Cyber View* de 2019, as empresas que participaram da pesquisa, apesar de reconhecer a importância da segurança dos dados, 46,3% delas não a consideram como principal prioridade. Além disso, 44,2%

das organizações não têm planos de investir no futuro contra acessos indesejados (SANTIAGO, 2018).

As empresas, geralmente, possuem diversas informações e dados que precisam ser organizados e disponibilizados para consultas posteriores. Dessa forma, um Banco de Dados (BD) armazena, organiza e agrupa essas informações, em um domínio específico, para segurança ou para verificação futura pela organização (SOUZA, 2020).

Um BD bem estruturado, com os dados bem relacionados entre si, gera informações valiosas as empresas, que ao utilizar em um determinado contexto, se torna conhecimento que pode ser utilizado para tomar alguma decisão (GOMES, 2019).

Um Sistema Gerenciador de Banco de Dados (SGBD) é um software que permite manipular um BD. Com o SGBD é possível manusear os dados, através de uma linguagem, como *Structured Query Language* (SQL), para verificar a integridade, controlar permissões, transações, entre outros. Um exemplo é o MySQL (OLIVEIRA, 2020).

No laboratório de pesquisa da *International Business Machines* (IBM), década de 70, em San Jose, Califórnia, surgiu a linguagem SQL como resultado do desenvolvimento de uma linguagem para manipulação dos bancos de dados relacionais. Pouco tempo depois se tornou um produto comercial. Com o grande sucesso, foi necessário a padronização do uso pelo órgão regulamentador americano, *American National Standarts Institute* (ANSI) (NOLETO, 2020).

A linguagem SQL é utilizada para trabalhar com banco de dados relacionais. Para essa linguagem não é necessário grandes conhecimentos de programação, por exemplo, profissionais que utilizam planilhas para armazenar os dados, podem acabar precisando aprender a linguagem SQL para transferir as informações para um banco de dados. Alguns exemplos de bancos de dados no mercado que utilizam SQL são: *Oracle, MySQL, PostgreSQL*, entre outros (SILVEIRA, 2019).

Conforme Noleto (2020), a linguagem é dividida em 3 subconjuntos. O primeiro o *Data Manipulation Language* ou Linguagem de Manipulação de Dados (DML), utilizando comandos para operar diretamente com o conjunto de dados do banco, sendo alguns dos comandos que tornam possíveis essas ações são: *insert*, *update*, *delete* e *select*. O segundo subconjunto é o *Data Definition Language* ou Linguagem de Definição de Dados (DDL), que utiliza comandos para gerenciar a estrutura do

banco de dados, sendo possível criar, alterar e remover tabelas de registros, alguns dos comandos são: *create*, *alter* e *drop*. O último seria o *Data Control Language* ou Linguagem de Controle de Dados (DCL) que controla o acesso, manipulando informações de acordo com o usuário e permitindo ou restringindo permissões de acesso, um dos possíveis comandos seria o *grant*.

Compreender e lidar com grande quantidade de dados é essencial. Essa linguagem já é conhecida por diversos profissionais da área da tecnologia, porém, outras áreas requerem ou pode ser necessária o conhecimento SQL, como marketing, consultorias, gestão de projetos e entre outros (BACCA, 2019).

2.2 Leis e Normas

Está seção apresenta algumas leis relacionadas a segurança dos dados e algumas normas para a segurança da informação.

2.2.1 Marco Civil da Internet

O Marco Civil da Internet é uma lei de número 12.965/14, responsável por regulamentar a utilização da Internet, definindo princípios e garantias para tornar a rede democrática no Brasil. Essa lei garante direitos e deveres aos usuários e empresas que fornecem acesso e serviços online (MARTINS, 2018).

A lei surgiu devido a necessidade de proteção aos dados pessoais, usados indevidamente por terceiros, pois um dado publicado na Internet ou enviado para terceiros, não os permite utilizar ou exibir a informação de forma não autorizada (ALENCAR, 2019).

Os dados pessoais são uma mercadoria valiosa, sendo necessária a implementação de restrições legais. Dessa forma, garante aos usuários o consentimento livre e expresso sobre o uso e tratamento das informações pessoais. Porém, deve deixar claro a proteção e acesso a esses dados (FRAGOSO, 2019).

A lei também informa sobre a responsabilidade do conteúdo gerado. Conforme o artigo 19, é assegurado no meio digital a liberdade de expressão, sendo que as empresas como: Facebook ou Google, não são responsabilizadas pelo conteúdo postado por terceiros. Entretanto, caso sejam comunicadas judicialmente para retirar o conteúdo e não removerem, poderão ser penalizadas (AMADO, 2019).

2.2.2 Lei Geral de Proteção de Dados Pessoais (LGPD)

Aprovada em agosto de 2018, a LGPD, de n° 13.709, tem com o objetivo de proteger os dados de todo cidadão que esteja no Brasil. A lei tem o propósito criar condições de segurança jurídica, padronizando normas e práticas, de forma igualitária.

Esta lei informa que o cidadão precisa consentir que os dados pessoais possam ser tratados por determinada organização. Porém, existem exceções, como por exemplo, se for indispensável as informações para cumprir uma obrigação legal, executar contratos, preservação da vida, entre outros. Além disso, a pessoa pode revogar um consentimento, pedir para que os dados sejam deletados, transferir dados para outra empresa, entre outras ações (SERPRO, 2018).

O cidadão deve ter controle de suas informações, podendo modificar, transferir ou excluir quando quiser e sem impedimentos. Além do mais, as empresas têm que deixar claro como irão tratar os dados e explicar os motivos do armazenamento, evitando o uso de letras miúdas nos termos de adesão, botões pré-selecionados que induzem a aceitação automática e termos grandes sem objetividade. Dessa forma, as organizações também precisam oferecer modos de acesso e controle das informações para o titular (SCHULTZ, 2019).

Essa lei teve como influência para a criação e formação a *General Data Protection Regularion* (GDPR).

Esta é uma lei que tem como objetivo garantir aos usuários privacidade e domínio sobre os dados pessoais, para os países europeus, evitando o uso indevido por parte de terceiros (FERNANDES, 2020).

A Autoridade Nacional de Proteção de Dados Pessoais (ANPD), será necessária para que a lei seja eficaz. A entidade ficará responsável por fiscalizar a LGPD e caso for descumprida, aplicar as sanções. Além do mais, a ANPD ficará responsável por regular e orientar sobre execução da lei. Caso ocorra uma exposição dos dados, a autoridade fiscalizadora poderá aplicar uma multa de até 2% do faturamento anual da organização no Brasil, com o limite de 50 milhões por infração (SERPRO, 2018).

Na Figura 1 estão ilustrados os principais pontos dessa lei.

Figura 1 – Os principais pontos da lei LGPD

Fonte: Serpro (2018).

A norma ainda determina que não importa se a sede da organização está no Brasil ou no exterior, se as pessoas são brasileiras ou não, se estão em território nacional, a LGPD tem que ser seguida (SERPRO, 2018).

2.2.3 A norma ABNT NBR ISO 27002

A norma ABNT NBR ISO 27002 constitui-se em princípios e diretrizes para o início, implementação, melhoria da gestão de SI em uma empresa. Os objetivos desta norma têm como intuito atender e ser implementado em organizações, para auxiliar nos requisitos identificados pela análise e avaliação dos riscos (ABNT, 2005).

Também é possível utilizá-la como um guia prático para aprimorar ou desenvolver os procedimentos de SI, verificar práticas eficientes de gestão de segurança e ajudar a criar um ambiente organizacional que contém confiança em suas atividades (ABNT, 2005).

2.2.4 A norma ABNT NBR ISO 27005

A norma ABNT ISO 27005 fornece um guia para a gestão de riscos de SI em uma empresa. Dessa forma, cabe a organização definir sua abordagem, como por exemplo, no contexto de gestão de riscos e o setor de atividade econômica. Esta norma é baseada no método de identificar os riscos, ameaças e vulnerabilidades que não é mais atribuída pela ABNT NBR ISSO/IEC 27002 (ABNT, 2019).

Definir um processo que avalie os riscos e que trate com um plano de contingência, além de definir um contexto interno e externo, convém para que a gestão de riscos de segurança da informação se torne um processo contínuo. Uma sistematização de gestão de riscos de SI é importante para identificar as necessidades da empresa, referente aos requisitos e para criar um Sistema de Gestão de Segurança da Informação (SGSI) mais eficaz (ABNT, 2019).

2.2.5 A lei Carolina Dieckmann

Aprovada após o caso da atriz Carolina Dieckmann, a lei 12.737/2012 surgiu a partir do projeto de Lei nº 2.793/2011. O caso ocorreu após os dados da atriz terem sido acessados por hackers, através de um e-mail que teria acessado. Dessa forma, após terem acesso ao computador pessoal, obtiveram fotos íntimas, que foram publicadas na Internet (SILVEIRA et al., 2017).

Conforme a lei, é considerada vítima qualquer pessoa que sofra algum dano pela invasão, seja o proprietário do dispositivo eletrônico ou terceiros que também forem prejudicados pela ação (SIENA, 2013).

Antes do sancionamento dessa lei não havia como enquadrar alguém que cometia crimes de invasão em dispositivos eletrônicos. Apesar disso, já existiam vítimas desse tipo de crime registrados no Brasil. Dessa forma, é considerado crime a obtenção de informações particulares, através da invasão de aparelhos eletrônicos (SILVEIRA et al., 2017).

2.3 Trabalhos Relacionados

Esta seção apresenta alguns trabalhos relacionados ao tema em estudo.

2.3.1 Um estudo de caso de gestão da segurança da informação em uma empresa privada

Ramos et al. (2017) tiveram como objetivo apresentar um estudo de caso sobre a gestão de SI no setor da TI em uma empresa privada, na área da saúde. O trabalho foi realizado utilizando as normas ABNT NBR ISO/IEC 27000 e o *Control Objetives for Information and Related Techonology* (COBIT), que significa uma estrutura que oferece a governança de TI para as organizações.

As informações obtidas utilizando as normas e estudos da SI dentro da empresa fizeram com que os autores chegassem à conclusão de que a empresa não gerencia os riscos que estão expostos, podendo ser justificada pela falta de políticas de SI. Dessa forma, o trabalho contribuiu para conscientizar a empresa que foi o objeto do trabalho, a importância do setor de TI.

Concluíram elaborando um manual de políticas de SI utilizando a norma ISO/IEC 27001, informando as responsabilidades dos funcionários da empresa, do setor da TI e dos gerentes. Além disso, apresentou as formas de proteção contra *softwares* maliciosos, regras e orientação referente ao acesso à *Internet*.

2.3.2 Ataque *phishing* focada nas organizações de “cadeia de refrigeração” da vacina contra a Covid-19

O trabalho de Satter (2020) mostra que a empresa IBM comunicou que os *hackers* estão visando empresas críticas para a distribuição de vacinas contra a Covid-19. A tentativa global de ataques *phishing* focadas para as organizações de “cadeia de refrigeração”, responsáveis por manter as doses da vacina em temperaturas frias durante o transporte. A unidade de segurança cibernética da empresa detectou um grupo de *hackers* que tentam coletar informações de diferentes aspectos da rede. Utilizam e-mails com armadilhas eletrônicas enviadas em nome de um executivo da *Haier Biomedical*, empresa provedora chinesa especializada em transportar vacinas e armazenar amostrar biológicas. Os criminosos pesquisaram o modelo, marca e o preço de várias unidades de refrigeração da empresa alvo. Conforme informado pela IBM, os falsos e-mails da *Haier* foram enviados por cerca

de 10 organizações diferentes, até para empresas que fabricam painéis solares, para fornecer energia para refrigeradores de vacinas para países quentes (SATTER, 2020).

2.3.3 Os ataques sofridos pelas empresas de infraestrutura

Conforme explicado por Dermatini e Yuge (2021), um grupo cibercriminoso *Darkside*, foi responsável por dois ataques em duas companhias de infraestrutura no Brasil: as estatais Centrais Elétricas Brasileiras S.A (ELETROBRAS) e a Cia Paranaense de Energia (COPEL).

Esses ataques deixaram uma preocupação para o país, pois de acordo com as informações adquiridas pela empresa do Reino Unido, especializada em segurança digital, Sophos, ocorreu um número menor de ataques em empresas brasileiras no primeiro trimestre, pois em 2020 foram 67%, comparado aos 38%, que ocorreram em 2021, no mesmo período. Entretanto, aumentou a sofisticação dos golpes e suas eficácias, deixando o ambiente cibernético mais perigoso.

Uma pesquisa feita pela *Tenable,* uma empresa de segurança dos Estados Unidos, verificou que o setor de indústrias é o segundo mais atingido por ciberataques. Dessa forma, setores da infraestrutura tais como: gás, fornecimento de água e energia são os alvos maiores.

2.3.4 O aumento dos ataques virtuais promovido pela pandemia do COVID-19

Conforme informado por Maciel (2021), a empresa brasileira Axur, especializada no monitoramento de riscos digitais, realizou um levantamento informando que os ataques virtuais de *phishing* aumentaram quase 100% no ano de 2020, referente ao ano de 2019. Além disso, o Relatório Anual, do ano de 2020, de Atividade Criminosa Online no Brasil, informa que o crescimento dos ataques virtuais se dá principalmente, pela pandemia causada pelo vírus da COVID-19.

Dessa forma, como a uma parcela da população foi trabalhar em casa, ficaram expostos às ações criminosas virtualmente, pois é um ambiente menos protegido, se for comparado a um ambiente corporativo. Ainda de acordo com o relatório da Axur, alguns tipos de ataques virtuais que obtiveram maior destaque, no ano de 2020, foram: o *phishing*, *malwares* e *trojans*.

2.3.5 Exemplos de crimes digitais

Conforme apresentado por Branco e Yuge (2021), a pesquisa feita pela consultora alemã, *Roland Berger*, informa que o Brasil superou o número de ataques do ano de 2019, pois apenas no primeiro semestre de 2021, com 9,1 milhões de casos, referente à ataques de *ransomware*. O Brasil é o quinto maior alvo no mundo, referente a crimes digitais. O país fica atrás apenas dos Estados Unidos, Reino Unido, Alemanha e África do Sul. O laboratório Fleury, dentre outras empresas, sofreu um ataque e ficou vários dias sem conseguir realizar exames. A empresa de departamento Lojas Renner, apesar de não ter realizado o pagamento, ficou vários dias indisponível para vendas pelo *e-commerce.*

3 MÉTODO

Esta pesquisa, segundo sua natureza é um resumo de assunto, buscando explicar a área do conhecimento do projeto, indicando sua evolução histórica, como resultado da investigação das informações obtidas, levando ao entendimento de suas causas e explicações (WAZLAWICK, 2014).

Segundo os objetivos é uma pesquisa exploratória e descritiva. A descritiva busca dados mais consistentes sobre determinado assunto, porém, não ocorre a interferência do pesquisador, apenas expõe os fatos como realmente são (WAZLAWICK, 2014). As pesquisas descritivas descrevem as características de certo fenômeno ou população. Também pode ser elaborada com o intuito de identificar as relações entre as variáveis (GIL, 2017).

A pesquisa exploratória muitas vezes é considerada como a primeira parte do processo de pesquisa, porque não necessariamente o autor tem um objetivo ou hipótese definida (WAZLAWICK, 2014). Essa pesquisa tem como objetivo a maior familiaridade do autor com o problema, tornando mais explícito ou facilitar a construção de hipóteses. Geralmente é uma pesquisa flexível, porque considera os variados aspectos referentes aos fatos ou fenômeno estudado (GIL, 2017).

Quanto aos procedimentos técnicos, será uma pesquisa bibliográfica e experimental. A pesquisa bibliográfica requer o estudo de teses, artigos, entre outros. A pesquisa experimental é caracterizada por ter uma ou mais variáveis experimentais que podem ser coordenadas pelo pesquisador (WAZLAWICK, 2014).

A pesquisa bibliográfica, será elaborada a partir de materiais já publicados, podendo incluir livros, teses, materiais disponibilizados na Internet, revistas, entre outros. A principal vantagem é permitir uma sucessão de fenômenos maior do que seria capaz de pesquisar diretamente (GIL, 2017).

De acordo com Gil (2017), a pesquisa bibliográfica se desenvolve a partir das seguintes etapas:

a) A escolha de um tema: é necessário estar relacionada com o interesse do aluno. Além disso, possuir conhecimento prévio sobre a área de estudo para que as seguintes etapas sejam bem desenvolvidas.

b) Levantamento bibliográfico preliminar: realizar um levantamento bibliográfico para o pesquisador se habituar com a área de estudo escolhida, facilitando a definição do problema.

c) Formulação do problema: ao final da etapa b, o aluno estará em condições de definir o problema de forma clara, precisa e objetiva. O problema de pesquisa pode ser avaliado, verificando se possuí relevância teórica e prática, existe material bibliográfico suficiente para sua solução, o aluno possuí interesse no tema, entre outras questões.

d) Elaboração do plano provisório de assunto: elaboração de um plano provisório para definir a estrutura do trabalho, contendo uma apresentação organizadas de suas partes.

e) Busca das fontes: identificar as fontes bibliográficas capazes de fornecer informações para ser possível responder o problema proposto, consultando dissertações, periódicos científicos, obras de referência, entre outros.

f) Leitura do material: identificar as informações e dados constando no material adquirido estabelecendo relações com o problema proposto e analisar a coerência das informações e dados apresentados pelos autores.

g) Fichamento: possui o objetivo de identificar as obras consultadas, anotar as ideias que surgiram, identificar as informações relevantes, registrar os comentários das obras e organizar as informações adquiridas.

h) Organização lógica do assunto: organizar as ideias com o propositivo de atender os objetivos da pesquisa. A etapa g seria um dos elementos essenciais para elaboração dessa parte.

i) Redação do texto: constitui pela elaboração do relatório.

A pesquisa experimental, consiste que o pesquisador provoque mudanças no ambiente de pesquisa, observando se as alterações realizadas são de acordo com os resultados esperados (WAZLAWICK, 2014).

A pesquisa experimental consiste em estabelecer um objeto de estudo, escolher as variáveis que a influenciam e determinar as formas de controle e observar os efeitos que a variável gera no objeto. Realiza pelo menos um dos elementos que julga ser responsável pela circunstância que está sendo pesquisado (GIL, 2017).

A pesquisa experimental é composta das seguintes etapas, conforme Gil (2017):

a) Formulação do problema: **Quais são as formas de ataques aos dados mais conhecidas e as correspondentes vulnerabilidades?**

b) Definição do plano experimental: foi descrito os ataques aos dados realizados as empresas e implementado o ataque SQL *Injection*. Foi utilizado um

banco de dados fictício, sendo desenvolvido trechos de códigos para explorar as vulnerabilidades que tornaram possíveis os ataques.

c) Determinação do ambiente: foi realizado um experimento reproduzindo o ataque de SQL *Injection*, mostrando as vulnerabilidades no sistema que permitiram o acesso indesejado. Para isso foi utilizado o sistema gerenciador de banco de dados PostgreSQL, versão 13.2, usando dados fictícios. Para a publicação do site implementado, usou-se o *software wildfly,* na versão 23.0.2*.* A aplicação publicada foi escrita em *Java 2 Platform Enterprise Edition* (J2EE). O Ambiente de Desenvolvimento Integrado (IDE) utilizado foi o Eclipse, versão 2019-09. O computador utilizado foi um notebook Acer, com Sistema Operacional (SO) *Windows*, com 2,5 G*igaHertz* (GHz), 8 *GigaByte* (GB) de Memória de Acesso Randômico (RAM) e com processador Intel Core i5.

d) Coleta de dados: utilização do site https://owasp.org/, para exemplos do ataque. Realizados testes internos na aplicação desenvolvida nesta monografia, simulando um ataque real.

e) Análise e interpretação dos dados: foram analisados os resultados obtidos de acordo com os testes realizados na coleta de dados, realizando a comparação com trabalhos relacionados e a pesquisa realizada (discussão)

f) Redação do relatório: foi registrada a pesquisa na escrita desse trabalho.

4 OS TIPOS DE ATAQUES AOS DADOS DAS EMPRESAS

Este capítulo apresenta cinco (5) tipos de ataques que ocorrem nas empresas e as vulnerabilidades que permitem que eles ocorram. Além disso, será mostrado um exemplo prático do ataque de SQL *Injection*.

4.*1 Port Scanning Attack*

Port Scanning Attack ou Ataque de Varredura de Porta, é um tipo de ataque no qual o invasor verifica as portas do computador automaticamente, com outro computador que está conectado à rede, procurando detectar possíveis portas abertas e que tenham protocolos de segurança fracos. Dessa forma, quando conseguirem todas as informações possíveis, poderão detectar falhas de segurança, obtendo dados confidenciais, informações sobre o SO, entre outros (MILLS, 2020).

No Brasil ocorreu um aumento dos ataques de segurança em redes, segundo o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), entre os anos de 2013 e 2014. O aumento foi de que 200% nas notificações de incidentes. Entretanto, o número pode ter sido maior, já que as notificações são realizadas voluntariamente pelos administradores de rede (CONVISO, 2017).

As empresas de Internet *Service Provider* (ISP) são alvos constantes, pois são responsáveis pelo fornecimento de rede para os clientes. Dessa forma, os cibercriminosos aproveitam das vulnerabilidades para tentar obter os dados dos consumidores (ALOO, 2021).

Quando ocorre uma varredura de porta, é enviada uma mensagem para cada porta, separadamente. Assim, as respostas recebidas determinam se está sendo utilizada, revelando possíveis pontos fracos. A varredura de portas fornece informações aos invasores, como quais serviços estão em execução e quais requerem autenticação, quais usuários possuem os serviços e se são permitidos *logins* anônimos (MESEVAGE, 2019).

As possíveis respostas recebidas após enviar uma mensagem para cada porta, conforme ilustrado na Figura 2, são: aberto, existe um serviço funcionando nessa porta; fechada ou sem resposta, a porta pode estar em uso, indisponível no momento;

bloqueada ou derrubada, não obtém nenhuma resposta do computador, o serviço pode estar bloqueado ou com defeito (PETTERS, 2020).

Figura 2 – Respostas da varredura de porta

Fonte: modificado de Petters (2020).

A solicitação de rede, enviada por um *scanner* de porta, tenta se conectar a uma porta *Transmission Control Protocol* ou Protocolo de Controle de Transmissão (TCP) ou *User Datagram Protocol* ou Protocolo de Datagrama do Usuário (UDP). Dessa forma, enviando um pacote para o endereço de *Internet Protocol* ou Protocolo da Internet (IP) o computador irá saber para qual porta enviar o pacote com base, por exemplo, no conteúdo do pacote. Além disso, cada um dos serviços em execução em um computador “escuta” em uma porta específica (PETTERS, 2020).

Conforme Cobb e Lewis (2021), uma porta é o local final de comunicação que fluem os pacotes ou unidades de dados. As portas utilizadas por protocolos de camada de transporte TCP e UDP, estão relacionadas a serviços ou processos específicos. Os números de porta são padronizados em dispositivos que conectam a Internet, variando de 0 a 65535, cada intervalo reservado para uma função, conforme informado abaixo:

- A porta 0: reservada para a rede TCP/IP;
- As portas de 1 a 1023: conhecidas e definidas pela *Internet Assigned Numbers Authority* (IANA), como padrões para protocolos de Internet;
- As postas de 1024 a 29151: são associados a protocolos específicos, para as portas registradas com IANA;
- As portas: 49152 a 65535: utilizadas para conexões dinâmicas, que não utilizam portas específicas, escolhem qualquer uma que estiver disponível.

Conforme Haber (2021), algumas das portas mais utilizadas e seus protocolos de rede associados são:

- A porta 22: conexão criptografada até o servidor ou dispositivo, usada pelo protocolo *Secure Shell* (SSH);
- A porta 25: protocolo de e-mail *Simple Mail Transfer Protocol* (SMTP);
- A porta 53: *Domain name system* (DNS), serviço que converte endereços IP para nomes;
- A porta 80: utilizada pela Internet, sem criptografia, *Hypertext Transfer Protocol* (HTTP);
- A porta 443: utilizada pela Internet criptografada, *Hypertext Transfer Protocol Secure* (HTTPS),
- A porta 3389: utilizada para conexões à áreas de trabalho remoto.

De acordo com Avast (2021), os invasores utilizam verificações de portas para verificar os níveis de segurança das organizações, descobrindo *firewall* potentes, servidores ou redes vulneráveis. Utilizam de protocolo TCP para ocultar a localização, utilizar as verificações de porta e não revelar nenhum endereço de rede ao alvo.

Conforme Mills (2020), algumas medidas que podem ser utilizadas para evitar esse tipo de ataque de verificação de porta são:

- Não abrir mais portas que o necessário: não abrir um número maior de portas do que aquelas essenciais ao funcionamento;
- Utilizar ferramentas para verificação de portas abertas: utilizar ferramentas que façam uma análise, verificando e rastreando quais portas estão abertas. Alguns exemplos dessas ferramentas são Nmap e Zenmap;
- Utilizar o *firewall:* funciona como uma barreira, evitando a entrada de intrusos na rede;

- Manter o sistema atualizado: manter o sistema e equipamentos atualizados, estando com a versão mais recente e corrigir as possíveis vulnerabilidades existentes.

Conforme Petters (2020), existem diversas técnicas de verificação, algumas delas estão ilustradas na Figura 3 e explicadas a seguir:

Figura 3: Técnicas de verificação

Fonte: modificado de Petters (2020).

- Verificação Ping: um *ping* é utilizado para verificar se é possível distribuir um pacote de dados a um endereço IP sem falhas. São solicitações de *Internet Control Message Protocol* ou Protocolo de Mensagens de Controle de Internet

(ICMP), em que enviam solicitações para diferentes servidores, com o objetivo de obter uma resposta;

- Varredura SYN ou varredura de porta semiaberta TCP: é enviada um pacote SYN, solicitando uma resposta do computador, o pacote ACK. Se obter uma resposta SYN-ACK, pode ser uma possível porta aberta. Caso ocorra uma resposta reset, a porta está fechada, porém existe um computador ativo;
- Conexão TCP: utiliza de protocolos de conexão que qualquer usuário usa para se conectar a outros sistemas. Dessa forma, diferentemente da varredura de porta semiaberta TCP, a varredura de porta consegue completar a conexão TCP;
- Verificação UDP: pode ser utilizada para verificar se um servidor DNS está ativo, é enviado uma solicitação DNS. Dessa forma, caso a resposta seja ICMP, a porta está fechada, se o serviço estiver em execução, pode obter uma resposta UDP, significando que a porta está aberta. Outra forma de uso é enviar uma solicitação DNS para a porta UDP 53 e verificar se obtém uma resposta DNS, caso obtenha, que dizer que existe um servidor DNS no computador.

Portanto, para proteger uma rede, as equipes de segurança devem descobrir durante uma varredura de porta, quais estão abertas ou vulneráveis, verificando se estão acessíveis fora da rede coorporativa, realizando as medidas necessárias para proteção. Além disso, realizar medidas tais como: configurar *firewalls* e sistemas de detecção de intrusos são algumas formas de proteção da rede das instituições contra ataques (COBB e LEWIS, 2021).

4.2 *Phishing*

O *phishing* utiliza de fraudes por meios de telecomunicações, realizando a manipulação do usuário para obter informações sigilosas da vítima. Esse ataque possui três componentes: os invasores utilizam os meios de comunicações eletrônicas, como o e-mail, fingem ser uma empresa ou outra pessoa e por fim obtém dados confidenciais, como credenciais de login (BELCIC, 2020).

Algumas informações sobre as empresas e os seus funcionários estão disponíveis nas redes sociais, como nome, local de trabalho, hábitos, entre outras informações. Dessa forma, redes sociais como *Facebook*, *Amazon*, *Netflix*, *Apple* e

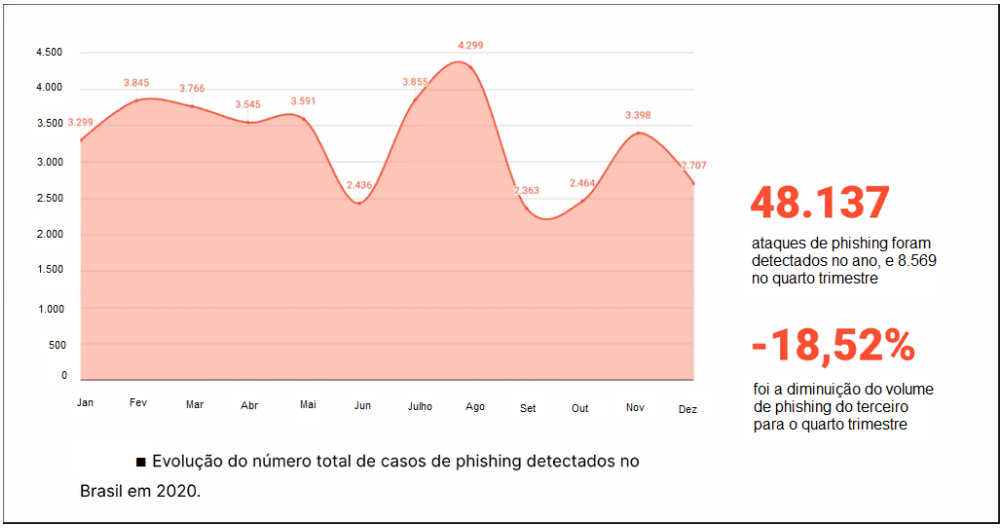
WhatsApp foram as redes que mais foram usadas em ataques de *phishing* em 2020 (ZIMMER, 2020).

Após os invasores aprenderem sobre os funcionários, podem enviar por exemplo, e-mail com um link que instale um software para obterem o controle do dispositivo. Dessa forma, o fator principal para as empresas serem o alvo é a questão financeira, por isso, a maioria das empresas realizam transações bancárias utilizando sistemas conectados com a Internet. Desse modo, os invasores falsificam boletos bancários ou simulam sites de um banco para obter os dados bancários. Além disso, podem ocorrer ataques que sequestram as informações e caso a empresa não tenha um sistema de backup, podem ter que pagar aos criminosos para obter os dados de volta (ZIMMER, 2020).

Conforme informado pelo *Federal Bureau of Investigation* ou Departamento Federal de Investigação (FBI), as empresas americanas perderam quase US$215 milhões em 2014, causada por ataques *phishing.* No ano de 2016, conforme o relatório da Verizon foram 61 ataques *phishing,* direcionados para as equipes financeiras. Em 2017, ocorreu um aumento de quase 200%, pois o número de ataques aumentou para 170 (BERTOLLI, 2018).

Conforme o relatório da empresa de monitoramento em riscos digitais, Axur, os ataques virtuais via *phishing* no Brasil, no ano de 2020, aumentaram quase 100%, se comparados com o ano de 2019. Ocorreram 48.137 casos identificados no ano de 2020, 99,23% maior se comparados com 24.161 casos do ataque no ano de 2019. A evolução do número total de casos de *phishing* está representada na Figura 4. O maior aumento desse tipo de ataque foi no setor de *e-commerce*. Como por exemplo, na *Black Friday*, que obteve 3.398 casos desse golpe, 16.82% maior comparado ao ano de 2019 (MACIEL, 2021).

Figura 4 – Evolução dos casos identificados de *phishing* no Brasil, em 2020



Fonte: modificado de Maciel (2021).

Conforme Bertolli (2018), um ataque a empresa *Snapchat*, ocasionada pelo ataque *Whailing*, um dos tipos de ataques *phishing*, fez com que um colaborador da organização, ao responder um e-mail que era supostamente do seu superior, enviou os dados da folha de pagamento da empresa para o criminoso.

Segundo Rodrigues (2020) existem medidas de segurança que as empresas podem utilizar para o seguro das redes, tais como o treinamento dos colaboradores para reconhecerem sites falsos e mensagens de *phishing*, verificando a veracidade do site e não baixar arquivos de remetentes desconhecidos e a proteção contra ameaças na rede, WEB e e-mail. Além disso, realizar uma formação básica em cibersegurança, abrangendo práticas como segurança na navegação WEB, segurança de e-mail e gestão de contas e senhas.

Sistemas de segurança, como *firewall* e antivírus podem deixar o ambiente empresarial mais seguro. Entretanto, a falta de conhecimento de cibersegurança dos funcionários deixa o ambiente das empresas expostos a esses ataques. Dessa forma, o treinamento de funcionários informando sobre as políticas de segurança e boas práticas é tão importante quanto a proteção dos sistemas (ZIMMER, 2020).

Algumas outras maneiras para evitar ataques de *phishing,* conforme Gonçalves (2021), são:

- Analisar o e-mail: verificar as informações e a intenção do e-mail recebido;
- Instalar antivírus: dentro os diversos motivos de instalar um antivírus, um deles é a proteção contra o *phishing;*

- Verificação de duas etapas: para verificar se é o usuário de fato que está acessando, é realizado uma checagem dupla;
- Instalar *plugins* anti *phishing*: são *plugins* que quando é acessado um site, verifica se há indícios do site em uma lista de não confiáveis.

Conforme Stivani (2018), conhecer os ataques de *phishing* também é uma maneira para prevenir possíveis ataques. Dessa forma, alguns desses ataques são:

- *Pharming*: responsável por atacar servidores DNS, principalmente de empresas. Os invasores instalam um cavalo de troia diretamente na rede ou em um computador host. Dessa forma, um endereço de site aparentemente seguro, pode levar a um site falso, sendo possível coletar as informações de vários usuários ao mesmo tempo;
- *Vishing:* utilizando de telefones, enviam uma mensagem automática para diversos números, se passando por empresas, para convencer as vítimas a repassarem informações pessoais.

Além disso, Porter (2020) afirma que existem outros tipos de ataques de *phishing*, conforme ilustrado na Figura 5 e exemplificado a seguir:

Figura 5 – Alguns tipos de *phishing*

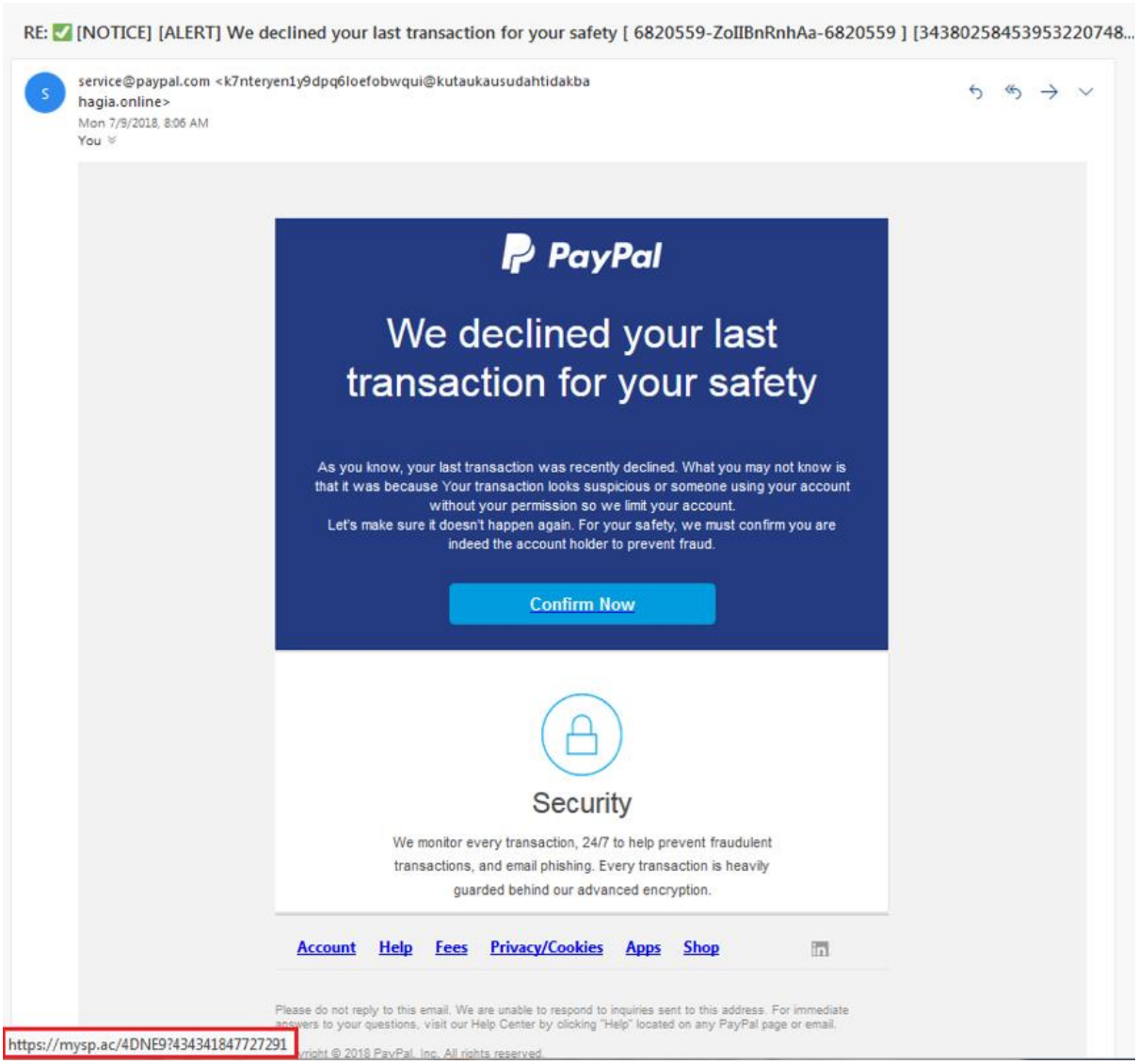
Fonte: modificado de Porter (2020).

- *Phishing* de e-mail: enviam e-mails ou mensagens que parecem ser de empresas reais. Caso a vítima não perceba que é um golpe, ao clicar no *link* e digitar os dados é possível coletar as informações.
- *Spear phising*: tipo de ataque mais personalizado, pois os golpistas ficam algum tempo pesquisando os alvos, direcionando-os a um indivíduo, empresa ou organização específica. Esses e-mails enviados aparentam ser de fontes legítimas;

- *Clone phishing*: ocorre a clonagem de um e-mail, enviando de um endereço aparentemente idêntico ao original, o corpo do e-mail também aparenta ser o mesmo, porém, o anexo ou o link da mensagem é alterado. Caso a vítima acesse, pode levar a um anexo infectado ou um site false;
- *Whaling*: geralmente utilizado para atingir empresas, procuram atingir primeiramente os funcionários que ocupam altos cargos, para conseguir acesso aos e-mails. Depois, solicitam informações aos colaboradores através das mensagens enviadas, que ao responderem aos superiores, os invasores conseguem informações confidenciais da organização;
- Pop-up *Phishing*: os anúncios *pop-up* fazem com que as vítimas instalem *malwares* em seus computadores ou as convencendo a obter uma proteção antivírus que não precisa.

Um exemplo de um ataque *phishing está* ilustrado na Figura 6, quando o remetente finge ser um aviso da empresa *PayPal*. Observa-se que no e-mail é informado que a última transação foi recusada para a segurança do usuário, pois a transação parecia suspeita ou alguém estava utilizando a conta sem permissão e pede para que o destinatário clique no botão "*Confirm Now*" e confirme os dados. Porém, ao passar o mouse sobre o botão aparece a verdadeira *Uniform Resource Locator* ou Localizador Uniforme de Recursos (URL) (MALWAREBYTES, 2021).

Figura 6 – Exemplo de um ataque *phishing*



Fonte: *Malwarebytes* (2021).

Existem formas de reconhecer *phishings* de e-mail, identificando alguns sinais, como por exemplo: bancos solicitando informações da conta ou dados financeiros pessoais, erros ortográficos, saudações genéricas, chamadas para ações imediatas, remetente que aparenta ser conhecido, *hiperlinks*, anexos, entre outros. A Figura 7, exemplifica os sinais que identificam um possível ataque de *phishing* de e-mail (PORTER, 2020).

Figura 7 – Sinais de um possível ataque de *phishing* de e-mail

Fonte: modificado de Porter (2020).

Portanto, como os cibercriminosos estão sempre aprimorando os ataques de *phishing*, é recomendável sempre ter um bom antivírus para agir em defesa nos computadores. Além disso, é de suma importância se informar sobre o *phishing*, tomando as precauções, utilizando o bom senso ao navegar online e responder mensagens (PORTER, 2020).

4.3 *Spoofing*

Spoofing significa enganar ou fingir. É um tipo de ataque de falsificação tecnológica que visa enganar uma rede ou uma pessoa, fazendo com que o invasor possa controlar e enviar e-mail, mensagens ou realizando ligações, usando o número de outras pessoas. Além disso, podem se apropriar do IP e DNS para assumir o controle da máquina, fazendo com que o usuário acesse sites falsos (RIBEIRO, 2019).

O *spoofing* ocorre quando o criminoso ganha a confiança da vítima, fingindo ser outra pessoa ou organização, as manipulam para que forneçam dados pessoais. Dessa forma, podem conseguir roubar a identidade ou os dados bancários. Nesse caso são direcionados a redes, que tem como objetivo contornar sistemas de segurança, propagar *malware*, roubar dados, entre outros (BELCIC,2020).

Existem ataques *phishing* e *spoofing* que são utilizados juntos para auxiliar a enganar as vítimas, como por exemplo, acreditarem que o e-mail enviado é legitimo. Porém, existem diferenças entre as duas. O *spoofing* cria uma aparência em que as comunicações do criminoso vêm de uma fonte confiável, já o *phishing* é iludir os usuários para revelar dados sigilosos. Existem vários tipos de *spoofing*, os de DNS e IP são mais diferentes do *phishing*, porque envolvem enganar um computador ou rede envolvendo meio técnicos (BELCIC, 2021).

O ataque de *spoofing* é um dos mais populares atualmente, muito se deve aos ataques bem sucedidos as autoridades brasileiras, entre elas, o ex-ministro da justiça e segurança pública Sérgio Moro, que ocorreu em 2019 (CONSTANCIO, 2021).

A Agência de Segurança Nacional dos Estados Unidos ou *National Securtity Agency* (NSA), em janeiro de 2020, realizou um comunicado de segurança cibernética referente ao SO *Windows* 10 da *Microsoft*. Foi identificada uma vulnerabilidade no código do *Windows*, referente às funcionalidades criptográficas, o que tornaria a verificação das conexões seguras, com a *WEB,* não confiável. Dessa forma, pediu para que todos os usuários atualizassem para a versão mais recente. A *Microsoft* também comunicou que a falha de software se chama *spoofing*. Dessa forma, com esta falha, o SO não saberia diferenciar o real da imitação, identificando que a conexão era legitima, permitindo os fraudadores invadirem. Se a falha não fosse verificada, os invasores poderiam utilizar certificados falsos, para validar softwares e aplicativos legítimos, para passar uma imagem como se fosse confiável (KLEUT, 2020).

Conforme Barbosa (2019), a proteção para esse tipo de ataque é a conscientização. Conhecer os perigos e compartilhar as informações são maneiras efetivas de evitar ser vítima dessa técnica. Existem algumas outras medidas, tais como:

- Evitar conexão em redes *Wi-fi* públicas ou desconhecidas;
- Deixar o SO e os aplicativos do dispositivo atualizado;
- Verificar as conexões de sites que utilizam de criptografia;
- Caso o aplicativo que utiliza permite o fator de dupla autenticação, habilitá-lo.

De acordo com Constancio (2021), os ataques cibernéticos ficam cada vez mais sofisticados e se manter seguro tornou-se um desafio, inclusive para os que possuem maior conhecimento ao assunto. Dessa forma, existem outras medidas preventivas que também ajudam a diminuir a probabilidade de sofrer esses ataques, como:

- Utilizar softwares antivírus: pois irá auxiliar a remover e bloquear ações maliciosas, inclusive se o usuário acessar algum conteúdo malicioso;
- Verificar a fonte: não clicar em links desconhecidos ou abrir anexos sem conhecer a sua origem;
- Entrar em contato para confirmar: se solicitado envio ou modificação dos dados, entrar em contato com o serviço que está solicitando ou acessar a URL do site oficial manualmente e verificar dados para contato no site;
- Trocar de senha regularmente: trocar periodicamente a senha, utilizando senhas fortes, utilizar um gerenciador de senhas confiável para memorizar;
- Informar as tentativas do ataque: informar o remente de um e-mail ou comunicação falsificada ajuda a impedir novos ataques.

Existem muitas formas de se proteger contra esse ataque. Conhecer as formas de *spoofing* e realizar boas práticas auxiliam na proteção e a ficar um passo na frente dos cibercriminosos (HOPKINS, 2019).

A Figura 8 traz dicas úteis do que fazer e não fazer nesse caso (HOPKINS, 2019).

Figura 8 – Como se proteger dos ataques de *spoofing*

Fonte: modificado de Hopkins (2019).

Existem vários tipos de ataque de *spoofing* como o de *Short Message Service* ou Serviço de Mensagens Curtas (SMS), em que o atacante tenta enganar a vítima enviando uma mensagem se passando por uma empresa real, fazendo com que forneça informações sigilosas (GONÇALVES, 2021).

Conforme Belcic (2021), existem outros tipos de ataque de *spoofing*, sendo alguns deles:

- *Spoofing* de e-mail: quando ocorre o envio de e-mails forjados, que as vítimas identificaram como bancos, chefes, fornecedores da empresa, entre outros. Devido o design do e-mail e por ser um sistema aberto, é relativamente desprotegido. Entretanto, existe a possibilidade de bloquear o remetente e

verificar sinais, como domínio genérico de e-mail, anexos estranhos, erros e incoerências na escrita, urgência forçada, erros de digitação de URLs, entre outros;

- *Spoofing* de IP: todo dispositivo conecta a Internet utilizando algum endereço IP. Dessa forma, quando o aparelho envia informações pela Internet, utiliza vários pacotes. Sendo assim, o cibercriminoso sobrecarrega a rede com um grande fluxo de entrada, que aparenta que o tráfego vem de várias fontes, tornando mais difícil do alvo reagir;
- *Spoofing* de ARP*:* no *spoofing* de *Address Resolution Protocol* ou Protocolo de Resolução de Endereços (ARP)*,* o atacante infiltra na *Local Area Network* ou Rede Local (LAN), disfarçando o computador como um membro da rede, conseguindo interceptar, escondido, uma conversa e fazer se passar pelas participantes, reunindo as informações;
- *Spoofing de DNS:* o criminoso modifica a um servidor DNS de uma lista do site alvo e alterna o endereço IP para outro de, redirecionando as vítimas para um falso site, coletando os dados pessoais ou fazendo com que baixam algum malware;
- *Spoofing* de *site:* realiza a réplica de um *site*, para parecer com o real, para os usuários realizarem o login e o atacante conseguir receber as credenciais;
- *Spoofing* de ID: o *spoofing* de *Identity* ou Identidade (ID) faz parecer com que as ligações ou mensagens de texto vem de um número ou região confiável, convencendo a vítima a divulgar informações sigilosas;
- *Spoofing* de GPS: falsifica as coordenadas do *Global Positioning System* ou Sistema de Posicionamento Global (GPS) para aparecer que esteja em outro local.

De acordo com a empresa de telefonia dos Estados Unidos *Waitsfield e Champlain Valley Telecom* (WCVT), os criminosos utilizam o *spoofing* de ID para falsificar as informações no identificador de chamadas. Ao se passar por uma pessoa ou empresa de confiança, obtém informações pessoais. Dessa forma, existem boas práticas que podem ser realizadas para evitar esse tipo de ataque, conforme ilustrado na Figura 9 (WCVT, 2021).

Figura 9 – *Spoofing* de ID

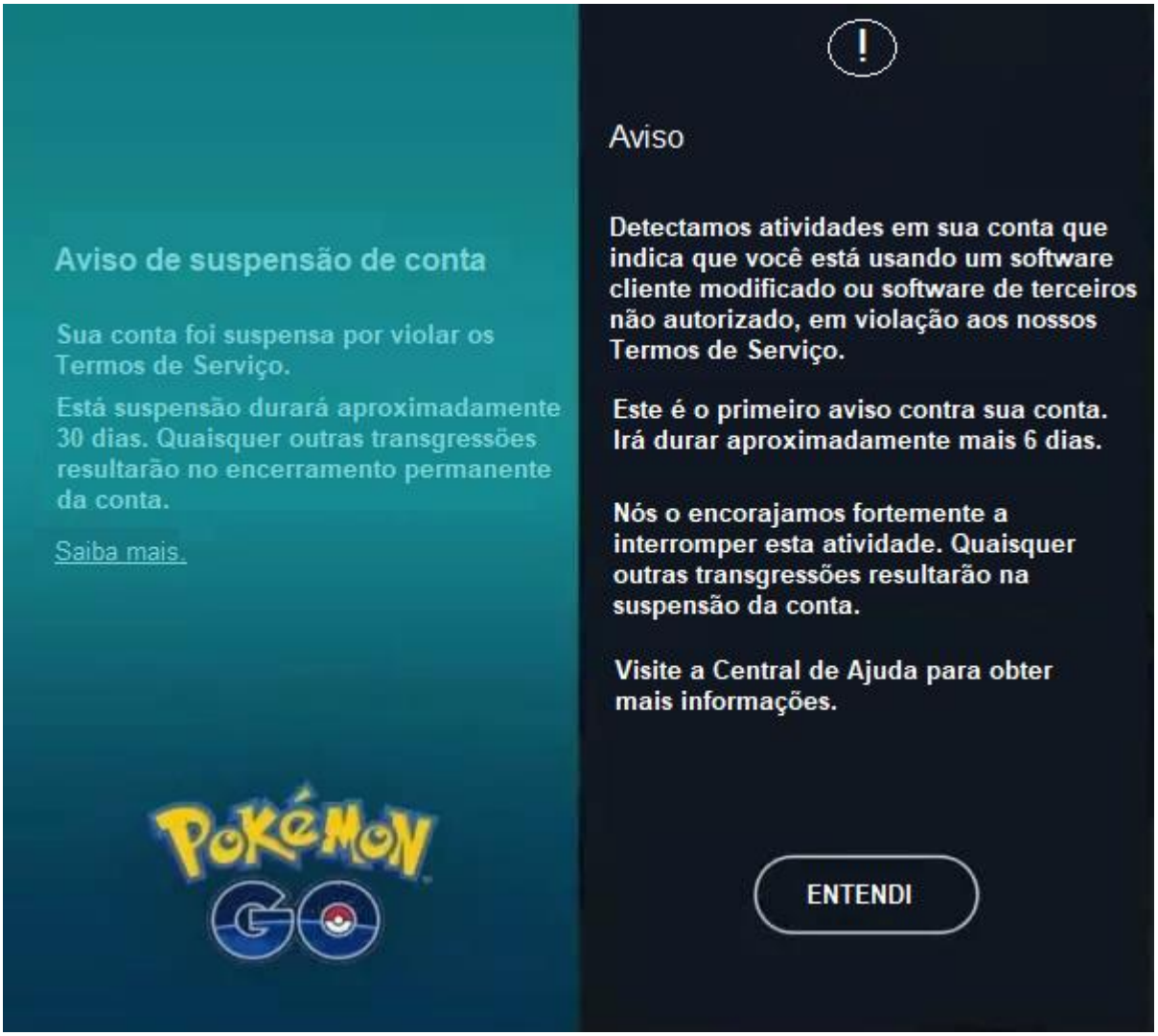
Fonte: modificado de WCVT (2021).

O *spoofing* de GPS também pode ser utilizado para falsificar a localização em jogos *mobiles*, como o Pokémon GO. Aplicativos de *spoofing* de GPS são muitas vezes utilizados pelos jogadores para adquirir maiores vantagens, por exemplo, a busca por um Pokémon raro. Alguns aplicativos populares de *spoofing* utilizados no jogo são: PokeGO++, *iSpoofer*, entre outros (MARIUS, 2021).

Conforme Marius (2021), essa prática vai contra os termos de uso da *Niantic*, empresa de desenvolvimento de *software* americana, em parceria com a Nintendo. Dessa forma, caso o uso de *spoofing* de uma conta seja detectado, a empresa utiliza algumas regras para banir o jogador de forma justa, emitindo três avisos, conforme ilustrado na Figura 10 e explicado abaixo:

- O primeiro, apenas uma mensagem de aviso é emitida;
- O segundo, não poderá jogar durante um mês;
- A terceira e última advertência, a conta é permanentemente banida.

Figura 10 – Avisos de banimento do Pokémon GO



Fonte: modificado de Marius (2021).

A Niantic está realizando medidas adicionais para que esse tipo de falsificação não ocorra, como o lançamento de *boots*, que não requerem verificação humana, deixando o processo mais direto e fácil, obtendo melhores resultados (MARIUS, 2021).

Portanto, para se proteger desse tipo de ataque o *spoofing*, o aumento das ferramentas de segurança, como antivírus para computadores e aparelhos móveis, é recomendável para evitar esse tipo de ataque. Além disso, as boas práticas do usuário também são muito importantes, como atenção para acessar os e-mails ou verificar alguma atividade estranha em algum aplicativo (RIBEIRO, 2019).

4.4 *Sniffing*

O *sniffing* de rede ou de pacotes é utilizada para capturar pacotes de dados que são transferidos através de uma rede e então os pacotes registrados e analisados. É possível monitorar todo o tráfego de uma rede utilizando ferramentas de *sniffing*. As ferramentas usadas são conhecidas como *sniffers*, responsáveis por interceptar pacotes de dados, que podem revelar os dados brutos que esses pacotes carregam (RODRIGUES, 2019).

Nas redes locais os dados trafegam de um dispositivo a outro, através do cabo, em pequenas unidades denominadas *frames*, que são divididos em seções que transportam informações. Dessa forma, os *sniffers* se instalam entre essa troca de pacotes, capturando-os. Desse modo, põe em risco a segurança devido a forma como os frames são transportados e entregues (FERNANDES, 2021).

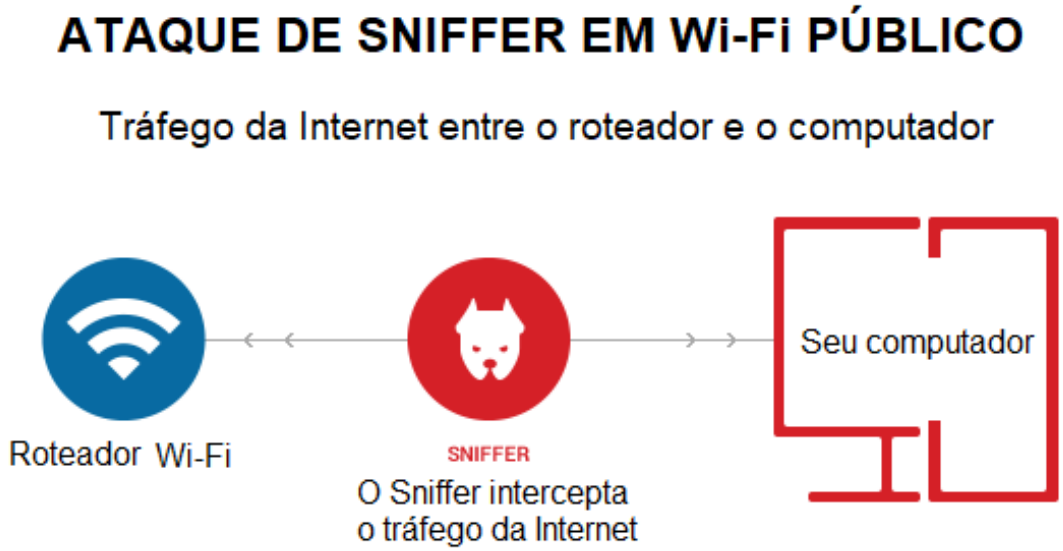
Os softwares *sniffers* ajustam as configurações do computador para verificar os pacotes enviados por ele e copia para investigá-los. Pode ser utilizado com um filtro, analisando pacotes específicos de dados ou sem filtro, verificando todo tráfego da rede (BELCIC, 2020).

Conforme Latto (2020), o *sniffer* de pacotes, conhecido também como analisador de pacote, rede, *Wi-fi* e *Ethernet*, são *softwares* ou *hardwares* de monitoramento. São ferramentas originalmente desenvolvidas para os engenheiros de rede, porém os cibercriminosos, muitas vezes, utilizam dos softwares *sniffers* para capturar as informações. Porém, também são utilizadas por:

- Engenheiros de rede: para otimizar as redes;
- Administradores de rede: para observar o tráfego, como a largura de banda disponível. Também pode ser utilizada para verificar se sistemas estão funcionando, como *firewalls*;
- Profissionais de cibersegurança: para monitorar a rede, buscando anormalidades nos sistemas, como por exemplo, diferentes tipos de tráfego podem indicar *malwares* ou um invasor no sistema;
- Corporações: para monitorar a rede dos funcionários, como por exemplo, verificando algum acesso a sites não permitidos;
- Cibercriminosos: para roubar os dados e espionar os usuários.

Os criminosos podem fazer com que os usuários acessem sites infectados que baixem automaticamente o *sniffer* ou através de e-mails, utilizando de engenharia social ou golpes de *phishing*. Além disso, redes *Wi-fi* públicas desprotegidas também são utilizadas nesse ataque, conforme ilustrado na Figura 11, pois são utilizadas para capturar o tráfego dos usuários que estão conectados. Geralmente, redes sem fio são utilizadas para ataques *spoofing* (BELCIC, 2020).

Figura 11 – *Sniffer* em Wi-Fi público



Fonte: modificado de Cucu (2017).

Os administradores de redes geralmente utilizam de *hardware sniffer*, que funciona como um adaptador que se conecta à rede existente, coletando os dados, os armazenando ou enviando para um coletor para inspeção adicional. Os cibercriminosos, geralmente utilizam os *softwares sniffers*. Em geral, os computadores desconsideram o tráfego que vai para algum local qualquer da rede, porém, esses aplicativos conseguem alterar as configurações e permissões do dispositivo. Dessa forma, permite que o invasor consiga armazenar a analisar as informações da rede quando quiser (LATTO, 2020).

Um exemplo de software que realizar a captura do tráfego de uma rede, para os usuários legítimos, é o *Wireshark,* conforme ilustrado na Figura 12. Pode ser utilizado para capturar pacotes sem fio, Ethernet, entre outros tipos de tráfego. “Sendo um analisador de protocolos de rede de forma gráfica que nos permite aprofundar em

cada pacote que se move em uma rede” (MACÊDO, 2016). Além disso, existem outros softwares, para capturar e analisar o tráfego para fins maliciosas, como o *BUTTsniffer* (LATTO, 2020).

Figura 12 – *Software Wireshark*

Fonte: modificado de Kancharla (2019).

Conforme Friedlander (2020), algumas medidas de segurança que podem ser realizadas contra o *sniffing* são:

- Evitar computadores públicos: não utilizar computadores de locais públicos, como bibliotecas;
- Verificar comunicações suspeitas: verificar o remetente dos e-mails e números de telefone;
- Utilizar o *Secure File Transfer Protocol* ou Protocolo de Transferência de Arquivos Seguro (SFTP): mais seguro que o protocolo *File Transfer Protocol* (FTP);

- Serviço de criptografia: se possível, criptografar informações importantes que são enviadas e recebidas;
- Manter o software atualizado: atualizar regularmente o SO e os dispositivos.

Conforme Latto (2020), outras medidas de segurança e prevenção que podem ser seguidas para proteger o sistema contra esse tipo de ataque são:

- Utilizar um antivírus potente: detecta e deleta o que não está no computador, como um *sniffer*;
- Evitar redes sem fio públicas, Wi-Fi: cibercriminosos utilizam a rede Wi-Fi de locais públicos para espionar toda a rede;
- Utilizar uma Rede Privada Virtual (VPN): criptografa a conexão e oculta os dados que são enviados ao computador, deixando as informações seguros;
- Evitar protocolos inseguros: procurar acessar sites com protocolo HTTPS, pois a comunicação é criptografada e evitar protocolos HTTP, porque não é uma rede segura, não há criptografia.

Conforme Macêdo (2017), o ataque *sniffing* depende da falta de segurança existentes em alguns protocolos de rede. Os protocolos TCP/IP, por exemplo, não forem projetados com a preocupação de segurança. Alguns protocolos que podem se tornar alvo desse ataque, são:

- HTTP: projetado para enviar informações, porém, sem proteção;
- SMTP: utilizado para realizar a transferência de e-mail, não possuí proteção contra *sniffing*;
- *Network News Transfer Protocol* (NNTP): as comunicações, inclusive os dados, são realizadas de forma “aberta”, por não ter nenhum tipo de criptografia;
- FTP: utilizado para receber e enviar arquivos, também são feitas sem algum tipo de criptografia ou defesa contra *sniffing*.

Conforme Belcic (2020), existem duas principais técnicas de análise realizada por *sniffers*, sendo utilizadas de acordo com a estrutura da rede que será realizada a conexão, são elas:

- *Sniffer* passivo: os dispositivos em um hub recebem todo o tráfego da rede. Os hubs são dispositivos que conectam várias máquinas em uma única rede, não existindo regulador de tráfego, todos os computadores recebem todo o fluxo e determinam o que é relevante para o usuário. Dessa forma, o *sniffer* absorve de forma passiva tudo que é recebido, devido os dispositivos receberem todo o tráfego da rede;
- *Sniffer* ativo: os comutadores enviam os dados específicos as máquinas que devem receber, sendo essa a solução quando os hubs possuem um grande fluxo de tráfego. Dessa forma, o *sniffer* ativo precisa contornar os comutadores. Existem várias formas para realizar esse processo, porém todas envolvem a injeção de tráfego adicional à rede, tornando o processo ativo.

Apesar desse ataque não ser tão comum como nos anos de 1990, ainda podem acontecer. Portanto, apesar dos softwares *sniffers* serem utilizados por qualquer equipe de segurança, os hackers também o utilizam, para desviar pacotes, podendo levar a violações de segurança. Dessa forma, para proteger a empresa contra pacotes de *sniffing* ilegais, é necessário realizar medidas de segurança, tais como: por exemplo, utilizar VPN e manter os softwares atualizados. Além disso, é importante utilizar o bom senso online (FRIEDLANDER, 2020).

4.5 SQL *Injection*

SQL *Injection* (SQLi) é o termo utilizado para falhas encontradas em uma aplicação, seja WEB ou local, que permite por meio de entradas de dados disponíveis aos usuários, a manipulação da consulta SQL utilizada internamente na aplicação para acessar os dados. Essa manipulação é chamada injeção, por isso o nome SQL *Injection* (PAYÃO, 2017).

Neste tipo de ataque, o invasor executa comandos maliciosos, explorando as consultas dinâmicas no Banco de Dados (BD), para tentar mostrar os dados sigilosos, podendo também apagar dados no servidor deste BD (RESENDE FILHO, 2019).

Falhas SQLi são um dos maiores riscos de segurança de aplicação WEB e estão na lista da OWASP *Top Ten* 2017. A fundação *Open Web Application Security Project* (OWASP) é sem fins lucrativos, que investe na melhoria da segurança do

software e dedica-se para que as organizações desenvolvam e mantenham suas aplicações e *Application Programming Interface* (API) confiáveis (OWASP, 2017).

As vulnerabilidades de injeção SQL ficaram mais difíceis de serem exploradas e detectadas, devido ao aumento da consciência da segurança de aplicações WEB. Algumas aplicações evitam esses ataques substituindo por APIs, pois são seguras contra ataques SQLi. Dessa forma, a injeção de SQL ocorre em casos pontuais, com essa tendencia, os métodos utilizados para encontrar e explorar as falhas tem evoluído, utilizando indicadores de vulnerabilidade sutis e técnicas mais poderosas (MACÊDO, 2016).

Conforme Daityari (2020), um exemplo de uma aplicação WEB vulnerável é a solicitação de um BD através de entradas do usuário, como por exemplo, a tela de *login*.

O pesquisador Giovanni Zadinello, da GZ Segurança, descobriu duas falhas de segurança na Universidade de São Paulo (USP), nos sistemas de acesso a serviços internos da faculdade. Essas falhas poderiam ter sido acessadas por atacantes a partir do ataque SQLi. A falha mais grave estava relacionada ao portal eDisciplinas, que deixou vulneráveis os dados pessoais, tais como: logins, senhas, nomes, endereços completos, IP do último acesso, entre outras informações. Dessa forma, os dados poderiam ser acessados em campos de consulta não tratados, o que acabaria retornando informações que o usuário não deveria ter acesso. De acordo com o pesquisador, 188,6 mil pessoas estavam vulneráveis. As falhas encontradas foram mitigadas, não havendo mais possibilidade de explorar as falhas descritas no ambiente online. A Superintendência de Tecnologia da Informação (STI), da USP, confirmou a brecha existente e a sua respectiva correção. Dessa forma, não há informações sobre um acesso indesejado ou vazamento do banco de dados disponível (DEMARTINI, 2021).

Arntz (2018) afirma que existem diversos objetivos possíveis que o invasor pode querer utilizar o SQLi, como por exemplo:

- Destruição: o cibercriminoso deseja encerrar o site ou aplicativo;
- Roubo de informações: roubo de dados, causando a empresa a perca de confiança dos clientes;
- Fornecimento de informações falsas: o criminoso pode fazer com que a decisão de algum negócio seja com base em informações falsa;

- Assumindo o controle: o criminoso ao ter controle do BD, pode negar acesso a funcionários da empresa, remover dados importantes ou fornecer informações falsas.

4.5.1 Implementação do SQL *Injection* (SQLi)

A realização da parte prática tornou necessária a instalação de um SGBD, sendo utilizado o PostgreSQL versão 13, através do site https://www.postgresql.org/. Configurações após a criação do BD:

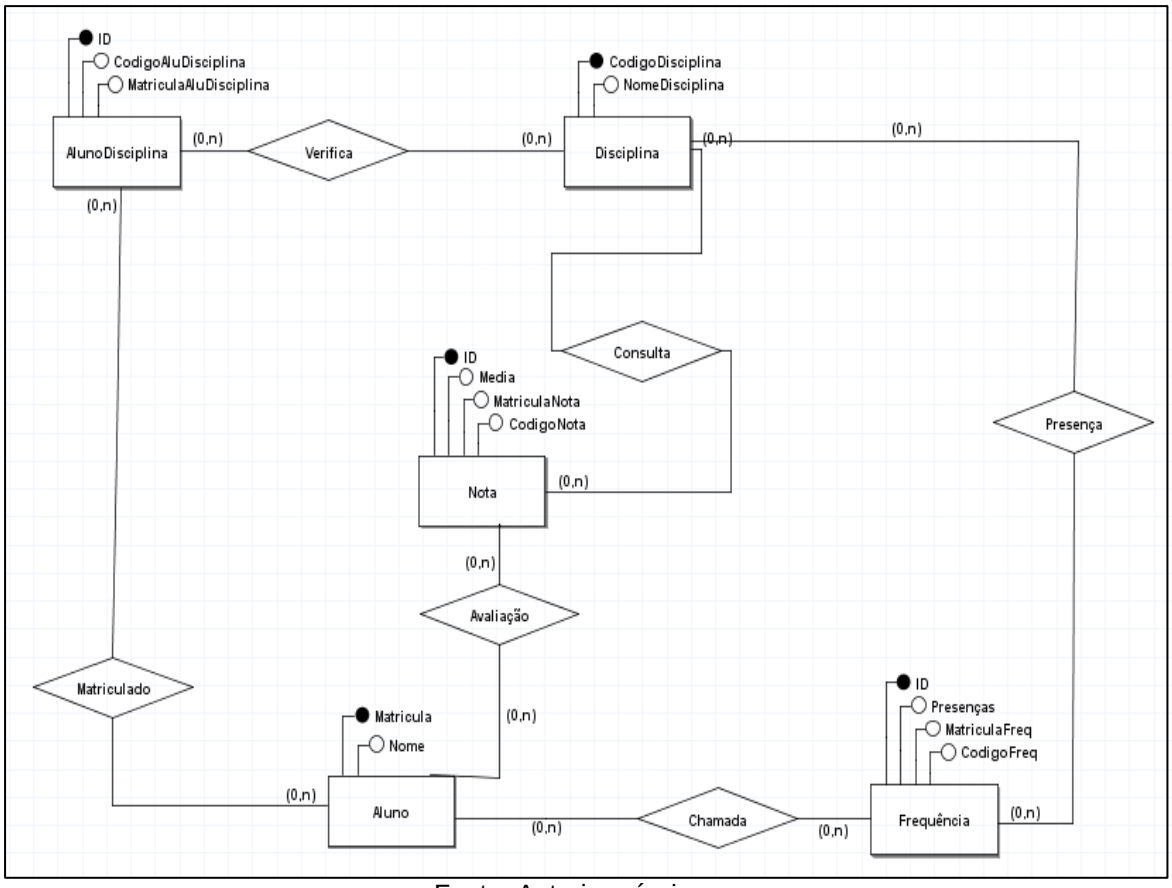
1. O acesso externo ao banco foi ativado inserindo nos arquivos:
   - No arquivo D:\postgres\pg_hba.conf: inserir a linha: “host *all all* 0.0.0.0/0 md5”, próximo à linha: “host *all all* 127.0.0.1/32 md5”;
   - No arquivo D:\postgres\postgresql.conf: inserir a linha *“listen_addresses* = '0.0.0.0' “, próximo à linha “*#listen_addresses* = 'localhost' “.
2. Foi criado uma pasta para os logs:
   - Utilizado o *prompt* de comando para criar a pasta, com o comando “mkdir D:\postgres\log”.
3. Foi estabelecida uma conexão no PGAdmin:
   - Na aba de conexões, foi inserido no host o IP 127.0.0.1, utilizando a porta 5432.

A criação dos *schemas* para as tabelas foi configurado para deixar o acesso como público, configurando a *security*:

- *Security*: *grantee*, colocado como *public*;
- *Security*: *privileges* colocado como *all*.

Para a criação do diagrama de classe do modelo do BD, foi utilizado o brModelo, versão 3.3.3, para *Windows*, instalado através do site sourceforget.net. O BD utilizado de exemplo foi o de uma universidade fictícia, incluindo as tabelas e os relacionamentos necessários para mapear as relações aluno, frequência, nota e disciplina, conforme ilustrado na Figura 13.

Figura 13 – Modelo do Banco de Dados



Fonte: Autoria própria.

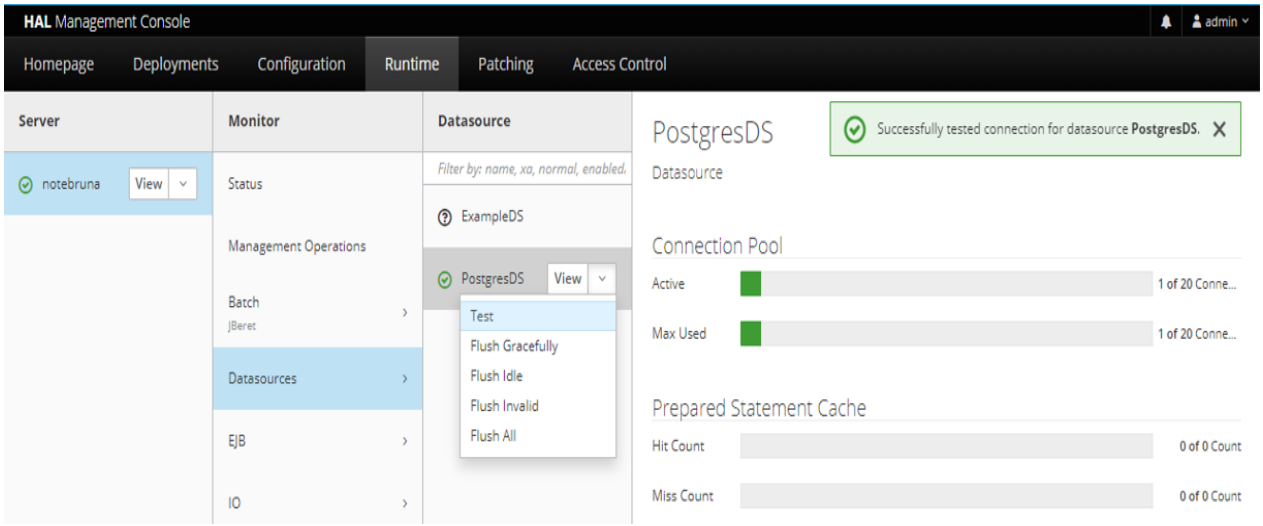
Estabelecido o funcionamento do BD, o próximo passo é criar a aplicação WEB. A plataforma WEB utilizada foi o Java EE, neste tipo de aplicação é necessário um ambiente de execução. Foi selecionado o *Wildfly, versão 23.0.2.Final*, da produtora de *software* dos Estados Unidos *Red Hat*, baixado através do site https://www.wildfly.org/.

O *Wildfly* necessita de um interpretador Java, sendo escolhida a versão Java SE *Development Kit* 11.0.13, baixado através do site https://www.oracle.com/java/technologies/. Optou-se por uma versão autônoma, sem instalador, para não interferir com outras versões existentes na máquina.

Ao preparar o ambiente, foi criado *batchfile* para ligar o *Wildfly*. Na máquina onde foi realizado o experimento, o *batchfile* incluiu manualmente o caminho das pastas onde estavam o *Wildfly* e o ambiente Java. Observou-se que os *scripts* do programa apresentam erro ao incluir pastas com espaço em branco.

A conexão ao BD foi gerenciada pelo *Wildfly,* através de um *pool* de conexões, que é uma estrutura dinâmica que cria mais conexões à medida que são requisitas pela aplicação. A Figura 14 mostra um teste do *connection pool*.

Figura 14 – *Connection Pool*



Fonte: Autoria Própria.

Utilizando o IDE Eclipse, versão 2019-09, foi criado um *workspace* separado para a aplicação, ligado diretamente ao *Wildfly,* facilitando o processo de desenvolvimento para a publicação das alterações da aplicação.

Após a preparação do ambiente, foi desenvolvida a aplicação WEB. A aplicação foi estruturada em 4 páginas WEB, sendo uma de apresentação, onde são mostrados os botões com as funções desenvolvidas e uma página correspondendo à função de cada um dos três botões.

Todas as páginas foram geradas com um cabeçalho fixo, com o nome da universidade fictícia: Universidade Formandos. Na parte de consulta, os botões ficaram dentro do cabeçalho, com o objetivo de manter os parâmetros visíveis, caso o número de resultados fique maior que a janela visível.

Além disso, foi inserido um item de acessibilidade nos botões, exemplificado na Figura 15, utilizando uma tecla de atalho de acordo com a letra destacada em cada botão. Os cabeçalhos e as listas de resultados, possuem suas larguras especificadas em porcentagem ao invés de pixels, favorecendo a responsividade das páginas.

Figura 15 – Código de inclusão da tecla de atalho

```
<td>
    <button name="listAl" type="button" onclick ="window.location.href='mostraAlunos.jsp';" autofocus accesskey="l">
    <span style="text-decoration: underline;">L</span>ista Alunos</button>
</td>
<td> </td>
<td>
    <button name="listFreq" type="button" onclick ="window.location.href='mostraFrequencia.jsp';" autofocus accesskey="f">
    Lista <span style="text-decoration: underline;">F</span>requência</button>
</td>
<td> </td>
<td>
<td>
    <button name="listNotas" type="button" onclick ="window.location.href='mostraNotas.jsp';" autofocus accesskey="f">
    Lista <span style="text-decoration: underline;">N</span>otas</button>
</td>
```

Fonte: Autoria Própria.

A aplicação acessa o BD, obtendo uma conexão do *connection pool*, criado dentro do *Wildfly*. Ele é encarregado dos detalhes da conexão, como informar o caminho do BD, usuário e senha, demonstrado na Figura 16.

Figura 16 – Obtendo conexão ao BD

```
@Resource(lookup = "java:/PostgresDS", name = "universidade")
private DataSource universidade;
```

Fonte: Autoria Própria.

O resultado de cada consulta foi armazenado em um vetor, no qual cada posição contém um objeto que representa uma linha de resultados da consulta SQL ao BD. O vetor é enviado a página WEB, mostrando os resultados em um quadro, conforme ilustrado na Figura 17.

Figura 17 – Os resultados mostrados em uma tabela

Fonte: Autoria Própria.

Na página de resultados o vetor com o resultado da consulta, é obtido através da *taglib core* que permite a comunicação entre a página WEB e a aplicação Java. As figuras 18 e 19, demonstram essa comunicação.

Figura 18 – Envia o vetor a página WEB

```
RequestDispatcher despReq = request.getRequestDispatcher("/mostraFrequencia.jsp");
request.setAttribute("resPesq", respConsulta);
despReq.forward(request, response);
```

Fonte: Autoria Própria.

Figura 19 – Recebe e mostra o vetor

```
<c:if test="${ not empty resPesq }">
    <table style="width: 80%; margin: auto; text-align: left;">
        <tbody>
            <tr>
                <th>Disciplina</th>
                <th>Matrícula</th>
                <th>Nome</th>
            </tr>
            <c:forEach items="${resPesq}" var="alunoFreq">
                <tr>
                    <td>${ alunoFreq.disciplina }</td>
                    <td>${ alunoFreq.matricula }</td>
                    <td>${ alunoFreq.nome }</td>
                    <td>${ alunoFreq.presenca }</td>
                </tr>
            </c:forEach>
        </tbody>
    </table>
</c:if>
```

Fonte: Autoria Própria.

Na interface da aplicação, o botão ListaAlunos, tem a funcionalidade de consultar todos os alunos matriculados em determinada disciplina. Dessa forma, um exemplo de SQLi é que ao invés de inserir o código da disciplina no *textbox*, seja possível colocar um código *injection*, conforme ilustrado na Figura 20.

Figura 20 – Ocorrência do SQLi

Fonte: Autoria Própria.

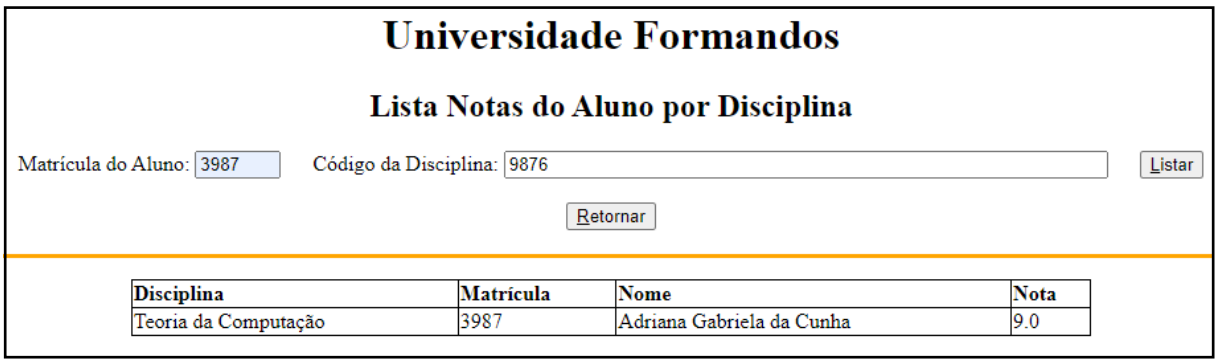
O ataque utiliza o código:

- 9876 or discip."CodigoDisciplina" = 4321

O ataque consiste em acrescentar uma condição extra, na consulta, para obter dados adicionais.

No botão ListaNotas, é possível consultar a nota do aluno em determinada disciplina, utilizando a matrícula e o código da disciplina, conforme ilustrado na Figura 21.

Figura 21 – Consulta da nota do aluno



Fonte: Autoria Própria.

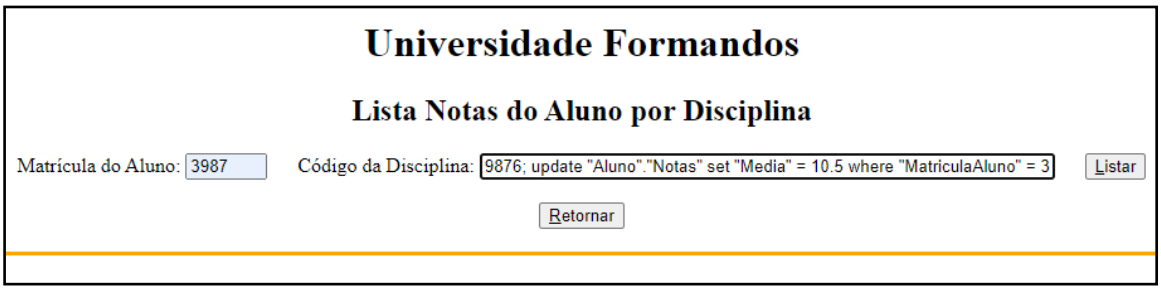
Também é possível realizar um ataque SQLi. O usuário malicioso pode inserir no *textbox* uma instrução update extra, para que seja alterada a nota de um aluno em determinada matéria, conforme mostrado na Figura 22 e Figura 23.

O ataque utiliza o código:

- 9876; update "Aluno"."Notas" set "Media" = 10.5 where "MatriculaAluno" = 3987;

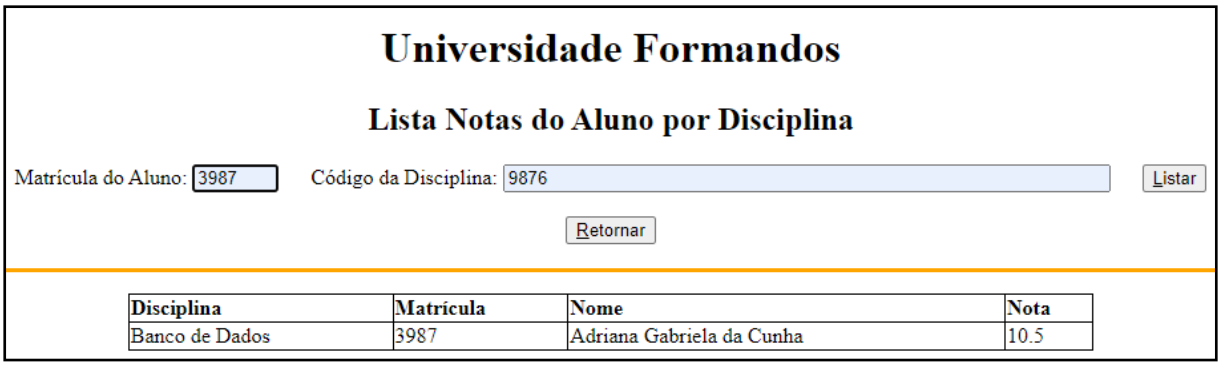
O ataque consiste em encerrar a primeira instrução com o ponto e vírgula: “9876;”, iniciando uma segunda, que é o código malicioso de atualização: “update...”.

Figura 22 – Injeção do código de alteração da nota



Fonte: Autoria Própria.

Figura 23 – Nota do aluno alterada



Fonte: Autoria Própria.

O botão ListaFrequência possuí o tratamento no código da aplicação WEB para que não ocorra um SQLi, que poderia ter sido realizado nos dois botões anteriores, ilustrado na Figura 24.

Figura 24 – Código de proteção

```
PreparedStatement consultaSql = dsConexao.prepareStatement(ConsultaSqlTxt, ResultSet.TYPE_FORWARD_ONLY, ResultSet.CONCUR_READ_ONLY);
int argAlunoInt = Integer.parseInt(argAluno);
int argDiscInt = Integer.parseInt(argDisc);
consultaSql.setInt(1, argAlunoInt);
consultaSql.setInt(2, argDiscInt);
```

Fonte: Autoria Própria.

Foi implementada uma proteção na linguagem que é o uso de *prepared statement,* onde a consulta a ser enviada ao banco, não é montada diretamente com

os dados escritos pelo usuário. Ao invés disso, os dados são parâmetros da consulta, não permitindo assim, nada além de valores, como int e *varchar*.

A aplicação pode ser protegida especificando restrições aos campos de entrada de dados, não permitindo, por exemplo, entrada de texto em campos onde se espera números. A restrição do tamanho dos campos, restringe a quantidade de código a ser injetada.

5. ANÁLISE DOS RESULTADOS OBTIDOS E DISCUSSÃO

Este capítulo apresenta uma discussão, comparando com alguns dos trabalhos relacionados com este presente estudo e uma parte prática, enfatizando como acontece um ataque.

5.1 Discussão (parte teórica)

A disseminação das tecnologias de acesso às redes de computadores, públicas ou privadas, oportunizou a propagação de uma nova criminalidade, chamada de cibercrime. O fácil acesso à tecnologia, o aumento dos dados e a sua importância, gerou atrativos para os ataques virtuais.

Os cibercriminosos aproveitam de vulnerabilidades para tentar obter o acesso a rede, detectando possíveis portas abertas ou com protocolos fracos, como é o caso do ataque *Port Scanning Attack*. Devido a pandemia do COVID-19, ocorreu um aumento dos ataques virtuais, conforme informado por Maciel (2021).

A necessidade de se utilizar conexões às áreas de trabalho remoto, utilizando VPN por exemplo, para os funcionários trabalharem em casa, ocasionou uma possível falha de segurança a rede interna das empresas. Dessa forma, os criminosos realizam uma varredura de porta, no caso pode ser realizada a tentativa na porta 3389, geralmente utilizada para conexões à área de trabalho remoto. Ao tentar conectar a uma porta TCP ou UDP, verificam as possíveis vulnerabilidades, na tentativa de obter informações confidenciais.

As fraudes e manipulações dos usuários são características dos ataques de *phishing* e *spoofing.* Existem ataques que utilizam esses dois tipos, entretanto, existem diferenças entre eles. O *phishing* ilude os usuários para conseguir que revelem dados sigilosos, já o *spoofing*, cria uma aparência que um *site* vem de uma fonte confiável, por exemplo, para que a vítima digite suas informações.

As tentativas de ataques de *phishing* ocorrem globalmente, conforme informado por Satter (2020). Os *hackers* tentam coletar os dados, utilizando armadilhas eletrônicas, por exemplo, através de e-mails e chamadas telefônicas, com o objetivo de obter informações confidências de determinada empresa. Na tentativa de enganar as vítimas, podem forjar ser um superior da empresa, por exemplo, enviando um e-mail aos colaboradores na tentativa de obter dados de acesso ao sistema ou informações da folha de pagamento da organização.

O *spoofing* é um dos ataques mais populares, de acordo com Constancio (2021). Esse tipo de invasão também pode ocorrer em empresas grandes, como por exemplo o SO *Windows* 10, da *Microsoft* que possuía uma falha de segurança, em que o sistema não saberia identificar se uma conexão era legitima ou não, permitindo os invasores se passarem por *sites* ou *softwares* legítimos.

O *phishing* também pode auxiliar em outros ataques, como por exemplo o *sniffing*. Utilizando de engenharia social, faz com que as vítimas acessem *sites* infectados e baixem automaticamente o *sniffer*. Os *softwares sniffers* verificam os pacotes enviados, copiam e analisam os pacotes de dados em busca de informações confidenciais. Apesar de serem ferramentas desenvolvidas para engenheiros de rede, a falta de segurança em protocolos de rede pode ocasionar em uma violação de segurança.

O ataque que tem como objetivo encontrar falhas em aplicações WEB, por meio da entrada de dados é chamado de SQL *Injection*. De acordo com a fundação OWASP, é um dos maiores riscos de segurança em aplicações WEB. Apesar da consciência referente a este tipo de invasão, o possível comprometimento ocasionado por esse ataque, pode levar a organização a perda de confiança dos clientes, o vazamento dos dados, comprometendo o funcionamento da empresa.

5.2 Como acontece um ataque (Parte Prática)

Ao desenvolver a parte prática do SQLi, foi criado um site fictício de uma universidade com três consultas comuns neste tipo de instituição, são elas:

- Consulta as disciplinas;
- Consultar a frequência de um determinado aluno;
- Consultar as notas de um determinado aluno.

As injeções de código foram de dois tipos:

- Obter dados não previstos pela aplicação;
- Efetuar uma alteração de dados através de uma aplicação de consulta;

Na obtenção de dados não previstos, um aluno pôde verificar a frequência e a nota de outro aluno, consistindo em uma invasão de privacidade. Além disso, a injeção

do código de alteração, permitiu que fossem falsificadas as notas no banco de dados, através da área de consulta da interface.

Os desenvolvedores devem ser treinados e alertados quanto as questões de segurança, pois a aplicação de teste foi construída com boas práticas de código e se apresenta como eficiente, apesar de conter em seu código fonte uma omissão grave de uma possibilidade de ataque.

Dessa forma, ao demonstrar o SQLi, verificou-se que ignorar a possibilidade de uso indevido da interface, pode ocasionar desde uma invasão de privacidade até a uma falsificação e alteração dos dados do BD. Em caso extremos, o atacante poderia danificar por completo a consistência dos dados e na ausência de um *backup*, comprometer o funcionamento de uma instituição.

Ao realizar a pesquisa sobre os cinco tipos de ataques que ocorrem às empresas e as vulnerabilidades exploradas pelos atacantes, foram verificados fatores comuns entre as suas vulnerabilidades:

- Desenvolvimento das aplicações com maior foco na finalização, deixando de lado o quesito da segurança;
- A falta de treinamento e conscientização dos usuários.

Portanto, para prevenir a organização de um possível ataque, é importante fazer uso das boas práticas de segurança, tais como: a conscientização dos funcionários, utilizar normas ABNT, como por exemplo, a 27001 e 27005 no setor de TI, manter políticas de SI difundidas na organização, a verificação dos protocolos de rede e atualização dos sistemas.

6 CONSIDERAÇÕES FINAIS

Este projeto teve o intuito de responder a seguinte questão de pesquisa: **- Quais são as formas de ataques aos dados mais conhecidas e as correspondentes vulnerabilidades?**

Este estudo permitiu identificar as seguintes formas de ataques: *Port Scanning Attack*, *Phishing*, *Spoofing*, *Sniffing* e *SQL Injection.*

As suas correspondentes vulnerabilidades:

- *Port Scanning Attack*: portas TCP ou UDP desprotegidas, verificando os níveis de segurança da organização, firewall, servidores ou redes vulneráveis;
- *Phishing*: manipula os funcionários das empresas, se passando por outra pessoa, seja um colega ou o supervisor, para obter dados confidenciais;
- *Spoofing*: tenta enganar a vítima imitando um site de uma empresa legitimo;
- *Sniffing*: *softwares sniffers* observam pacotes ou dados não criptografados em trânsito na rede;
- *SQL Injection*: falta da conscientização de segurança das aplicações WEB.

Os cibercriminosos utilizam falhas no sistema, descobrem informações dos funcionários e monitoram e identificam falhas na rede da empresa. Assim, com as informações necessárias, conseguem acessar o sistema da empresa e realizar o roubo ou prejudicar o acesso aos dados.

Conforme o estudo, concluiu-se que:

- Conhecer as formas de ataques e as correspondentes vulnerabilidades é uma das maneiras de prevenir as organizações desses ataques. Além disso, utilizar *firewalls* e antivírus, por exemplo, auxiliam como uma barreira deixando o ambiente empresarial mais seguro. Utilizar boas práticas de desenvolvimento das aplicações das empresas, previne ataques aos sistemas, como o SQLi;
- Os funcionários também deixam as empresas expostas a ataques, como o *spoofing e o phishing.* Esses ataques criam uma aparência em que as comunicações aparentam vir de uma fonte confiável ou manipula os

usuários para obter informações das vítimas ou das empresas. Dessa forma, o treinamento de funcionários e a constante divulgação interna na organização são ferramentas importantes para essa prevenção;

- A proteção da rede interna da empresa previne ataques como o *port scanning attack e o sniffing*. Esses ataques verificam portas abertas do computador, que possuem protocolos de segurança fracos ou captura pacotes de dados que são transferidos através de uma rede, sendo posteriormente analisados. Dessa forma, realizas técnicas de verificação, como a verificação *ping*, utilizar ferramentas que verifiquem portas abertas, utilizar VPN, antivírus, entre outras medidas de segurança, auxiliam na proteção da rede das organizações;
- Ataques cibernéticos atingem desde pequenas empresas até multinacionais, por isso, a segurança dos dados é muito importante. O conhecimento de alguns dos ataques e as vulnerabilidades que permitem o acesso indesejado pela empresa, ajudar a conscientizar seus funcionários e a prevenir o roubo de dados, pois o vazamento das informações pode gerar consequências, com altos custos e grandes prejuízos.

Portanto, não existe uma única solução para evitar os ataques e resolver todos os problemas de vulnerabilidades da empresa. Entretanto, existem diversas formas eficientes de proteção e boas práticas, tais como o treinamento dos funcionários e manter políticas de segurança difundidas na organização. Além disso, saber quais são os principais tipos de ataques e como os cibercriminosos agem são fatores para manter a empresa protegida contra ataques cibernéticos.

Para continuidade deste trabalho, sugere-se as seguintes sugestões para trabalhos futuros:

- Escrever sobre os outros ataques possíveis nas empresas;
- Escrever os ataques que podem ocorrer aos usuários comuns e realizar os respectivos exemplos práticos;
- Realizar uma pesquisa sobre as boas práticas de segurança dentro de uma empresa.

REFERÊNCIAS

ALENCAR, Morgana. **Tire as suas dúvidas sobre o Marco Civil da Internet**. Aurum. 2019. Disponível em: https://www.aurum.com.br/blog/marco-civil-da-internet/. Acesso em: 7 abr. 2021.

ALEXANDRE JÚNIOR, Júlio César. **Cibercrime: um estudo acerca do conceito de crimes informáticos**. Revista eletrônica da faculdade de direito de franca. v.14, n.1, p. 341 – 351, jun. 2019.

ALOO. **Segurança de rede: veja como proteger a sua!**. Aloo Telecom. 2021. Disponível em: https://blog.aloo.com.br/seguranca-de-rede/. Acesso em: 3 out. 2021.

AMADO, Miguel. **Marco Civil da Internet: o que é, importância e mudanças propostas**. FIA. 2019. Disponível em: https://fia.com.br/blog/marco-civil-da-internet/. Acesso em: 22 abr. 2019.

ANDRADE, M.D; BENTES, D.S; GUIMARÃES, D.F.S. **Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais**. Revista Vertentes do Direito**.** Tocantins, v. 4, n. 2, p. 191- 205, nov. 2017.

ARNTZ, Pieter. ***Explained: SQL injection****. Malwarebytes Labs*. 2019. Disponível em: https://blog.malwarebytes.com/security-world/business-security-world/2018/03/explained-sql-injection/. Acesso em: 23 set. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2005.

_____. **NBR ISO/IEC 27005:** Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio de Janeiro, ABNT, 2019.

AVAST. **O que é verificação de porta?**. Avast. 2021. Disponível em: https://www.avast.com/pt-br/business/resources/what-is-port-scanning. Acesso em: 5 maio 2021.

BACCA, Carolina Cozer. **O que é SQL e para que ele serve?.** Tecmundo. 2019. Disponível em: https://www.tecmundo.com.br/software/146482-sql-que-ele-serve.htm. Acesso em: 25 abr. 2021.

BARBOSA, Daniel Cunha. ***Spoofing*: entenda a técnica que ganhou destaque nos últimos dias**. *Welivesecurity*. 2019. Disponível em: https://www.welivesecurity.com/br/2019/07/25/spoofing-entenda-a-tecnica-que-ganhou-destaque-nos-ultimos-dias/. Acesso em: 7 maio 2021.

BELCIC, Ivan. **O guia essencial sobre *phishing*: como funciona e como se proteger**. Avast. 2020. Disponível em: https://www.avast.com/pt-br/c-phishing#topic-1. Acesso em: 7 maio 2021.

_____. **O que é *spoofing* e como posso me proteger dele?**. Avast. 2021. Disponível em: https://www.avast.com/pt-br/c-spoofing. Acesso em: 14 set. 2021.

_____. **O que é um *sniffer* e como se proteger contra ele?.** Avast. 2020. Disponível em: https://www.avast.com/pt-br/c-sniffer#topic-1. Acesso em: 12 maio 2021.

BERTOLLI, Emilia. **O que é um *Whaling Attack*?**. Varonis. 2018. Disponível em: https://blog.varonis.com.br/o-que-e-um-whaling-attack/. Acesso em: 10 maio 2021.

BRANCO, Dácio Castelo; YUGE, Claudio. **Brasil é o 5° maior alvo de crimes digitais no mundo em 2021**. Canaltech. 2021. Disponível em: https://canaltech.com.br/seguranca/brasil-e-o-5o-maior-alvo-de-crimes-digitais-no-mundo-em-2021-195628/. Acesso em: 16 set. 2021.

CAMPELO, Larissa; PIRES, Pamela de Freitas. **Crimes Virtuais**. JUS. 2019. Disponível em: https://jus.com.br/artigos/72619/crimes-virtuais. Acesso em: 25 mar. 2021.

CARDOSO, Pedro. **O que é Ransomware?**. Techtudo. 2017. Disponível em: https://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html. Acesso em: 26 abr. 2021.

CICCO, Francesco De. **A nova norma internacional ISSO 27005 de gestão de riscos de segurança da informação**. QSP. 2008. Disponível em: https://www.qsp.org.br/artigo_27005.shtml. Acesso em 9 mar. 2021.

COBB, Michael; LEWIS, Nick. ***What are port scan attacks and how can They be prevented***?. TechTarget. 2021. Disponível em: https://searchsecurity.techtarget.com/answer/What-is-a-port-scan-attack?amp=1. Acesso em: 30 set. 2021.

CONVISO. **Cuidado: os ataques a servidores crescem no Brasil**. Conviso *Application security*. 2017. Disponível em: https://blog.convisoappsec.com/ataques-a-servidores-crescem-no-brasil/. Acesso em: 3 out. 2021.

CONSTANCIO, Gabriel. **Saiba o que é *spoofing* e como se defender.** Combate a Fraude. 2021. Disponível em: https://www.combateafraude.com/post/saiba-o-que-e-spoofing-e-como-se-defender. Acesso em: 13 set. 2021.

CORREIA, P.M.A.R; SANTOS, S.I.S.; BILHIM, J.A.F. **Proposta de modelo explicativo das percepções sobre gestão e políticas públicas em matéria de cibersegurança e cibercrime**. Sociologia, Porto, v. 33, p. 95-113, 2017.

COSSETTI, Melissa Cruz. **O que é um ransomware?**. Tecnoblog. 2019. Disponível em: https://tecnoblog.net/275356/o-que-e-um-ransomware/. Acesso em: 26 abr. 2021.

CUCU, Paul. **11 *Steps to improve your public wi-fi security***. HEIMDAL *Security*. 2017. Disponível em: https://heimdalsecurity.com/blog/11-security-steps-public-wi-fi-networks/. Acesso em: 4 out. 2021.

DAITYARI, Shaumik. **Injeção de SQL: um guia para principiantes para usuários do WordPress**. Kinsta. 2020. Disponível em: https://kinsta.com/pt/blog/injecao-sql/#como-funciona-a-vulnerabilidade-da-injeo-sql. Acesso em: 3 maio 2021.

DEMARTINI, Felipe. **Universidade de São Paulo tinha falha que expôs dados de alunos e funcionários**. Canaltech. 2021. Disponível em: https://canaltech.com.br/seguranca/usp-tinha-falha-que-expos-dados-de-alunos-e-funcionarios-193007/. Acesso em: 11 set. 2021.

DEMARTINI, Felipe; YUGE, Claudio. **O Brasil está preparado para ataques contra empresas de infraestrutura?**. Canaltach. 2021. Disponível em: https://canaltech.com.br/seguranca/o-brasil-esta-preparado-para-ataques-contra-empresas-de-infraestrutura-185633/. Acessp em: 12 set. 2021.

DURBANO, Vinicius. **Segurança da Informação: o que é e 12 dicas práticas para garantir**. Ecoit. 2018. Disponível em: https://blog.ecoit.com.br/seguranca-da-informacao/. Acesso em: 28 abr. 2021.

FERNANDES, Mirian. **O que é *sniffer*? Como se proteger?**. Starti. 2021. Disponível em: https://blog.starti.com.br/sniffer/. Acesso em: 12 maio 2021.

_____. **Tudo sobre segurança cibernética**. Starti. 2020. Disponível em: https://blog.starti.com.br/tudo-sobre-seguranca-cibernetica/. Acesso em: 29 abr. 2021.

_____. **7 passos para você se tornar um especialista em segurança cibernética**. Starti. 2019. Disponível em: https://blog.starti.com.br/7-passos-para-se-tornar-um-especialista-em-seguranca-cibernetica/. Acesso em: 29 abr. 2021.

FRAGOSO, Nathalie. **O impacto do Marco Civil sobre a proteção da privacidade no Brasil**. InternetLab. 2019. Disponível em: https://www.internetlab.org.br/pt/especial/o-impacto-do-marco-civil-sobre-a-protecao-da-privacidade-no-brasil/. Acesso em: 22 abr. 2021.

FRIEDLANDER, Jamie. ***What is a sniffing attack and how to protect against sniffing***. *BeenVerified*. 2020. Disponível em: https://www.beenverified.com/crime/what-is-a-sniffing-attack/. Acesso em: 4 out. 2021.

GAIDARGI, Juliana. **Programa de segurança de dados para empresas.** Infonova. 2018. Disponível em: https://www.infonova.com.br/artigo/seguranca-de-dados-para-empresas/. Acesso em: 29 abr. 2021.

_____. **Segurança da Informação. O que faz? Para que serve?.** Infonova. 2018. Disponível em: https://www.infonova.com.br/artigo/seguranca-da-informacao-o-que-faz-para-que-serve/. Acesso em: 28 abr. 2021.

GALOYAN, Albert. **Segurança Cibernética no Âmbito das Relações Internacionais**. 2019. Trabalho de Conclusão de Curso (Bacharel em Relações Internacionais) – Universidade de Brasília, Brasília, 2019.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Editora Atlas Ltda., 2017.

GOMES, Pedro César Tebaldi. **Quais os principais banco de dados e quais duas diferenças?**. *OpServices*. 2019. Disponível em: https://www.opservices.com.br/banco-de-dados/. Acesso em: 28 abr. 2021.

GONÇALVES, Ariane. **O que é *phishing* e como se proteger de golpes na internet.** Hostinger. 2021. Disponível em: https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet#Como-se-proteger-de-ataquesphishing. Acesso em: 11 maio 2021.

GONÇALVEZ, André Luiz Dias. ***Spoofing*: técnica hacker que finge ser outra pessoa ou empresa**. Tecmundo. 2021. Disponível em: https://www.tecmundo.com.br/seguranca/215129-spoofing-tecnica-hacker-finge-outra-pessoa-empresa.htm. Acesso em: 7 maio 2021.

HABER, Lynn. ***Port Number***. *TechTarget*. 2021. Disponível em: https://www.techtarget.com/searchnetworking/definition/port-number. Acesso em: 1 out. 2021.

HOPKINS, Timothy. ***What is Spoofing and How to Prevent a Spoofing Attack***. *Rad Group*. 2019. Disponível em: https://www.rad-group.co.uk/2020/12/29/what-is-spoofing-and-how-to-prevent-a-spoofing-attack/. Acesso em: 24 set. 2021.

KANCHARLA, Ajan. ***Sniffing attack***. Slideshare. 2019. Disponível em: https://pt.slideshare.net/AjanK1/sniffing-attack-12659267/7. Acesso em: 5 out. 2021.

KLEUT, Jennifer Van Der. ***Severe Windows 10 vulnerability found by NSA – Update Windows 10 Immediately***. Norton. 2020. Disponível em: https://us.norton.com/internetsecurity-emerging-threats-severe-windows-10-vulnerability-found-by-nsa.html. Acesso em: 12 set. 2021.

LATTO, Nica. **O que é um *sniffer* e como não ser espionado?**. AVG. 2020. Disponível em: https://www.avg.com/pt/signal/what-is-sniffer. Acesso em: 12 maio 2021.

LOIK, Nayla. **Scanner de porta: o que é e por que você deveria utilizá-lo**. *Manage Engine*. 2020. Disponível em: https://blogs.manageengine.com/portugues/2020/12/29/scanner-de-porta-o-que-e-e-por-que-voce-deveria-utiliza-lo.html. Acesso em: 5 maio 2021.

LUCENA, Felipe. **Segurança de Dados: tudo que você precisa saber**. Diferencial TI. 2017. Disponível em: https://blog.diferencialti.com.br/seguranca-de-dados/. Acesso em: 21 mar. 2021.

MACÊDO, Diego. **Entendendo os *sniffers***. DiegoMacêdo. 2017. Disponível em: https://www.diegomacedo.com.br/entendendo-os-sniffers/#more-6462. Acesso em: 12 maio 2021.

_____. **Introdução ao Wireshark: Detecção e captura de tráfego em redes**. DiegoMacêdo. 2016. Disponível em: https://www.diegomacedo.com.br/introducao-ao-wireshark-deteccao-e-captura-de-trafego-em-redes/. Acesso em: 12 maio 2021.

MACIEL, Rui. **Ataques virtuais via *phishing* cresceram quase 100% no Brasil, aponta relatório**. Canaltech. 2021. Disponível em: https://canaltech.com.br/seguranca/ataques-virtuais-via-phishing-cresceram-quase-100-no-brasil-aponta-relatorio-177801/. Acesso em: 16 set. 2021.

MAIER, F. ***The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age***. Mediações, Londrina, v. 24, n. 1, p. 380-384, Jan 2019.

MALWAREBYTES. **Tudo sobre phishing**. Malwarebytes. 2021. Disponível em: https://br.malwarebytes.com/phishing/. Acesso em: 11 maio 2021.

MARIUS, Smith. ***Best 5 Pokémon Go Spoofing Apps in 2021 (iOS 15 Supported)***. *iMyFone*. 2021. Disponível em: https://www.imyfone.com/change-location/pokemon-go-spoofing-app/?gclid=CjwKCAjw7rWKBhAtEiwAJ3CWLB9M0Twb2jK4j0Ald8ob9eyaoP0nWJwUc9IyXNnnjNtwtHiAHXccRRoCFWsQAvD_BwE#2. Acesso em: 24 set. 2021.

MARTINS, Geiza. **O que é o Marco Civil da Internet?** Super Interessante. 2018. Disponível em: https://super.abril.com.br/mundo-estranho/o-que-e-o-marco-civil-da-internet/. Acesso em: 9 abr. 2021.

MESEVAGE, Tobias Geisler. **What is port scanning?**. Datto. 2019. Disponível em: https://www.datto.com/blog/what-is-port-scanning. Acesso em: 5 maio 2021.

MILLS, Matt. **O que são ataques de digitalização de portas e como evitá-los**. Itigic. 2020. Disponível em: https://itigic.com/pt/what-are-port-scan-attacks-and-how-to-avoid-them/. Acesso em: 5 maio 2021.

MOREIRA, C.; BEIRA, J.C; OLIVEIRA, M. **Um olhar dos estudantes do curso de biblioteconomia acerca do que são dados, informações e conhecimentos**. Informação & Informação. Londrina, v. 25, n. 2, p. 484 – 508, abr./jun. 2020.

NOLETO, Cairo. **SQL: o que é e quais as vantagens de utilizar essa linguagem!** Trybe. 2020. Disponível em: https://blog.betrybe.com/linguagem-de-programacao/sql/. Aceso em: 25 abr. 2021.

OLIVEIRA, Natália. **O que é um banco de dados?.** Dev. 2020. Disponível em: https://dev.to/nfo94/o-que-e-um-banco-de-dados-56fm. Acesso em: 28 abr. 2021.

OWASP. **Owasp Top Ten 2017**. OWASP. 2017. Disponível em: https://owasp.org/www-project-top-ten/2017/. Acesso em: 25 abr. 2021.

PAYÃO, Felipe. **SQL Injection: saiba tudo sobre um ataque simples que pode ser devastador**. Tecmundo. 2017. Disponível em: https://www.tecmundo.com.br/tecmundo-explica/113195-sql-injection-saiba-tudo-ataque-simples-devastador.htm. Acesso em: 23 abr. 2021.

PETTERS, Jeff. ***What is a port scanner and how does it work?***. Varonis. 2020. Disponível em: https://www.varonis.com/blog/port-scanning-techniques/. Acesso em: 5 maio 2021.

POTER, Kim. ***Wha tis phishing? How to recognize and avoid phishing scams****. NortonLifeLock.* 2020. Disponível em: https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html. Acesso em: 23 set.. 2021.

RAFTER, Dan**. *Phishing email examples to help you identify phishing scams. NortonLifeLock***. 2020. Disponível em: https://us.norton.com/internetsecurity-online-scams-phishing-email-examples.html. Acesso em: 23 set. 2021.

RAMOS, K.S.; SAPIA, H.M; ALESSI, H.C; ALESSI, R.M; RUIZ, G.A; FERRARI, D.J; PEREIRA, D.R. **Gestão de segurança da informação em uma empresa do setor de saúde: um estudo de caso**. *Colloquium Exactarum.* São Paulo, v. 9, n. 4, p. 33 – 40, out. 2017.

RESENDE FILHO, Dirceu Moraes. **SQL Server – como evitar SQL injection?.** iMasters. 2019. Disponível em: https://imasters.com.br/banco-de-dados/sql-server-como-evitar-sql-injection. Acesso em: 25 abr. 2021.

RIBEIRO, Felipe. **Brasil teve mais de 3 bilhões de roubos de credenciais em 2020**. Canaltech. 2021 .Disponível em: https://canaltech.com.br/seguranca/relatorio-aponta-mais-de-3-bilhoes-de-roubos-de-credenciais-no-brasil-em-2020-183762/. Acesso em: 29 abr. 2021.

_____. **O que é *spoofing*? Conheça a técnica hacker utilizada contra o Ségio Moro**. Canaltech. 2019. Disponível em: https://canaltech.com.br/hacker/o-que-e-spoofing-conheca-a-tecnica-hacker-utilizada-contra-sergio-moro-144951/. Acesso em: 6 maio 2021.

RODRIGUES, André. ***Sniffing* de rede**. Portal GSTI. 2019. Disponível em: https://www.portalgsti.com.br/2018/11/sniffing-de-rede.html. Acesso em: 12 maio 2021.

RODRIGUES, Renato. **Redes sociais e serviços cloud estão na mira dos hackers. Kaspersky**. 2020. Disponível em: https://www.kaspersky.com.br/blog/redes-sociais-servicos-cloud-hackers/16279/. Acesso em: 7 maio 2021.

SANTOS, L.C.M.C; PRADO, E.P.V; CHAIM, M.L. **Técnicas e ferramentas para detecção de vulnerabilidades em ambientes de desenvolvimento ágil de software**. *Brazilian Journal of Development*. Curitiba, v. 6, n.6, p. 33921-33941, jun. 2020.

SATTER, Raphael. **IBM alerta para ataques hackers visando a 'cadeia de refrigeração' de vacinas**. CNN Brasil. 2020. Disponível em: https://www.cnnbrasil.com.br/saude/2020/12/03/ibm-alerta-para-ataques-hackers-visando-a-cadeia-de-refrigeracao-de-vacinas. Acesso em: 17 maio 2021.

SCHULTZ, Felix. **LGPD: O que é, como funciona e para que serve**. Milvus. 2019. Disponível em: https://milvus.com.br/guia-lgpd-completo/. Acesso em: 22 abr. 2021.

_____. **Segurança cibernética: o que é e como ser um especialista no assunto**. Milvus. 2020. Disponível em: https://milvus.com.br/seguranca-cibernetica-o-que-e/#:~:text=%C3%89%20uma%20ramifica%C3%A7%C3%A3o%20da%20seguran%C3%A7a,e%20manipular%20dados%20ou%20arquivos. Acesso em: 5 abr. 2021.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **O que muda com a LGPD**. Serpro. 2018. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 02 mar. 2021.

SILVEIRA, Neil; SOUSA, Mirian Lima De; MELO, Antônia Morgana de Alcântara Jorge. **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann**. Jus. 2017. Disponível em: https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann. Acesso em: 7 abr. 2021.

SILVEIRA, Paulo. **O que é SQL**. Alura. 2019. Disponível em: https://www.alura.com.br/artigos/o-que-e-sql. Acesso em: 25 abr. 2021.

SANTIAGO, Christopher. **Entenda a importância da segurança de dados para empresas**. Soluti. 2018. Disponível em: https://solutiresponde.com.br/entenda-a-importancia-da-seguranca-de-dados-para-empresas/. Acesso em: 29 abr. 2021.

SIENA, David Pimentel Barbosa. **Lei Carolina Diekmann e a definição de 'crimes virtuais'**. Jus. 2013. Disponível em: https://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais. Acesso em: 3 maio 2021.

SOMBRIO, Jessica. **6 motivos (e um bônus) para você aprender SQL o quanto antes**. Kondado. 2020. Disponível em: https://kondado.com.br/blog/blog/2020/08/05/6-motivos-e-um-bonus-para-voce-aprender-sql-o-quanto-antes/. Acesso em: 25 abr. 2021.

SOUZA, J.L.C. **Crime, polícia e tecnologias da informação**. Mediações, Londrina, v. 22, n. 1, p. 301-324, Jan 2017.

SOUZA, Ivan De. **Banco de dados: saiba o que é, os tipos e a importância para o site da sua empresa**. Rockcontent. 2020. Disponível em: https://rockcontent.com/br/blog/banco-de-dados/. Acesso em: 28 abr. 2021.

STIVANI, Mirella. **Os dez tipos de phishing mais comuns**. Techtudo. 2018. Disponível em: https://www.techtudo.com.br/listas/2018/06/os-dez-tipos-de-phishing-mais-comuns.ghtml. Acesso em: 8 maio 2021.

TORRES, Fernando**. Você sabe a diferença entre cibersegurança e segurança da informação?**. Medium. 2019. Disponível em: https://medium.com/@fertorresfs/voc%C3%AA-sabe-a-diferen%C3%A7a-entre-ciberseguran%C3%A7a-e-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-19bada8d047f. Acesso em: 29 abr. 2021.

TOTUS. **Segurança de dados: por que é prioridade nas empresas?.** Totus. 2020. Disponível em: https://www.totvs.com/blog/negocios/seguranca-de-dados/. Acesso em: 21 mar. 2021.

WAZLAWICK, R. S. **Metodologia da Pesquisa para Ciência da Computação**. 2ª. ed. [S.l.]: Campus, 2014.

WCVT. ***What is Call spoofing.*** WCVT. 2021. Disponível em: https://www.wcvt.com/news/what-is-call-spoofing/. Acesso em: 24 set. 2021.

ZIMMER, Kelvin. ***Hacker* x empresas: quais os ataques cibernéticos mais comuns?.** Lumiun Blog. 2020. Disponível em: https://www.lumiun.com/blog/hackers-empresas-quais-os-ataques-ciberneticos-mais-comuns/. Acesso em: 7 maio 2021.

APÊNDICE A – *CREATE* DA TABELA ALUNO

Este Apêndice trata-se do código de criação da Tabela Aluno do Banco de Dados

```
CREATE TABLE "Aluno"."Aluno"
(
"Matricula" integer NOT NULL,
"Nome" character varying COLLATE pg_catalog."default" NOT NULL,
CONSTRAINT "Aluno_pkey" PRIMARY KEY ("Matricula")
)
TABLESPACE pg_default;

ALTER TABLE "Aluno"."Aluno"
OWNER to postgres;
```

APÊNDICE B – *CREATE* DA TABELA DISCIPLINA

Este Apêndice trata-se do código de criação da Tabela Disciplina do Banco de Dados

```
CREATE TABLE "Aluno"."Disciplinas"
(
    "CodigoDisciplina" integer NOT NULL,
    "NomeDisciplina" character varying COLLATE pg_catalog."default"
NOT NULL,
    CONSTRAINT "Disciplinas_pkey" PRIMARY KEY ("CodigoDisciplina")
)
TABLESPACE pg_default;

ALTER TABLE "Aluno"."Disciplinas"
    OWNER to postgres;
```

APÊNDICE C – CREATE DA TABELA NOTA

Este Apêndice trata-se do código de criação da Tabela Nota do Banco de Dados

```
CREATE TABLE "Aluno"."Notas"
(
    "Media" numeric(3,0),
    "id_Nota" integer NOT NULL,
    "MatriculaAluno" integer,
    "CodigoDisciplina" integer,
    CONSTRAINT "pk_Notas" PRIMARY KEY ("id_Nota"),
    CONSTRAINT "fk_Aluno" FOREIGN KEY ("MatriculaAluno")
        REFERENCES "Aluno"."Aluno" ("Matricula") MATCH SIMPLE
        ON UPDATE NO ACTION
        ON DELETE NO ACTION,
    CONSTRAINT "fk_Disciplina" FOREIGN KEY ("CodigoDisciplina")
        REFERENCES "Aluno"."Disciplinas" ("CodigoDisciplina") MATCH
SIMPLE
        ON UPDATE NO ACTION
        ON DELETE NO ACTION
)
TABLESPACE pg_default;

ALTER TABLE "Aluno"."Notas"
    OWNER to postgres;
```

APÊNDICE D - *CREATE* DA TABELA FREQUÊNCIA

Este Apêndice trata-se do código de criação da Tabela Frequência do Banco de Dados

```
CREATE TABLE "Aluno"."Frequencia"
(
    "ID" integer NOT NULL,
    "CodigoDisciplina" integer,
    "MatriculaAluno" integer,
    "Presencas" character varying COLLATE pg_catalog."default",
    CONSTRAINT "pk_Frequencia" PRIMARY KEY ("ID"),
    CONSTRAINT "fk_Aluno" FOREIGN KEY ("MatriculaAluno")
        REFERENCES "Aluno"."Aluno" ("Matricula") MATCH SIMPLE
        ON UPDATE NO ACTION
        ON DELETE NO ACTION,
    CONSTRAINT "fk_Disciplina" FOREIGN KEY ("CodigoDisciplina")
        REFERENCES "Aluno"."Disciplinas" ("CodigoDisciplina") MATCH
SIMPLE
        ON UPDATE NO ACTION
        ON DELETE NO ACTION
)

TABLESPACE pg_default;

ALTER TABLE "Aluno"."Frequencia"
    OWNER to postgres;
```

APÊNDICE E - *CREATE* DA TABELA ALUNODISCIPLINA

Este Apêndice trata-se do código de criação da Tabela AlunoDisciplina do Banco de Dados

```
CREATE TABLE "Aluno"."AlunoDisciplina"
(
    "id_AlunoDisciplina" integer NOT NULL,
    "CodigoDisciplina" integer,
    "MatriculaAluno" integer,
    CONSTRAINT "pk_AlunoDisciplina" PRIMARY KEY
("id_AlunoDisciplina"),
    CONSTRAINT "fk_Aluno" FOREIGN KEY ("MatriculaAluno")
        REFERENCES "Aluno"."Aluno" ("Matricula") MATCH SIMPLE
        ON UPDATE NO ACTION
        ON DELETE NO ACTION,
    CONSTRAINT "fk_Disciplina" FOREIGN KEY ("CodigoDisciplina")
        REFERENCES "Aluno"."Disciplinas" ("CodigoDisciplina") MATCH
SIMPLE
        ON UPDATE NO ACTION
        ON DELETE NO ACTION
)
TABLESPACE pg_default;
ALTER TABLE "Aluno"."AlunoDisciplina"
OWNER to postgres;
```

APÊNDICE F – *INSERT* UTILIZADO NA TABELA ALUNO

Este Apêndice trata-se do código de inserção de dados na Tabela Aluno do Banco de Dados

```
INSERT INTO "Aluno"."Aluno"("Matricula", "Nome")
VALUES
(1617, 'Diogo Severino da Silva'),
(5970, 'Rebeca Raimunda Lopes'),
(9053, 'Giovanni Igor Cavalcanti'),
(3987, 'Adriana Gabriela da Cunha'),
(2675, 'Benicio Heitor Ribeiro'),
(1894, 'Natalia Aparecida Ribeiro'),
(1852, 'Martin Sérgio Ribeiro'),
(9852, 'Luís Otávio da Rosa'),
(2751, 'Catarina Cavalcanti'),
(1860, 'César Diogo da Cunha'),
(6258, 'Amanda Porto'),
(7631, 'Isis Lima'),
(9218, 'Olivia Souza'),
(1575, 'André Monteiro'),
(1245, 'Lavínia da Mata'),
(5155, 'Lucas Monteiro'),
(9213, 'Vicente Cavalcanti'),
(7436, 'Milena da Cruz'),
(1216, 'Laura da Mata'),
(3912, 'Luna Moreira');
```

APÊNDICE G – *INSERT* UTILIZADO NA TABELA DISCIPLINAS

Este Apêndice trata-se do código de inserção de dados na tabela Disciplina do Banco de Dados

```
INSERT INTO "Disciplina"."Disciplinas"(
     "CodigoDisciplina", "NomeDisciplina")

     VALUES

     (4321, 'Teoria da Computação'),

     (9876, 'Banco de Dados'),

     (6541, 'Programação I');
```

APÊNDICE H – *INSERT* UTILIZADO NA TABELA NOTAS

Este Apêndice trata-se do código de inserção de dados na tabela Notas do Banco de Dados

```
INSERT INTO "Aluno"."Notas"(
     "Media", "id_Nota", "MatriculaAluno", "CodigoDisciplina")
     VALUES (8.5, 1, 1617, 4321),
     (6.0, 2, 5970, 4321),
     (9.5, 3, 9053, 4321),
     (10, 4, 3987, 4321),
     (7.8, 5, 2675, 4321),
     (6.7, 6, 1894, 4321),
     (8.7, 7, 1852, 4321),
     (10.0, 8, 9852, 4321),
     (9.3, 9, 2751, 4321),
     (5.2, 10, 1860, 4321),
     (4.7, 11, 6258, 4321),
     (8.7, 12, 7631, 4321),
     (6.1, 13, 9218, 4321),
     (7.6, 14, 1575, 4321),
     (9.5, 15, 1245, 4321),
     (5.5, 16, 5155, 4321),
     (6.7, 17, 9213, 4321),
     (8.1, 18, 7436, 4321),
     (5.9, 19, 1216, 4321),
     (10.0, 20, 3912, 4321);
     (5.7, 21, 1617, 9876),
     (8.7, 22, 5970, 9876),
     (4.9, 23, 9053, 9876),
     (6.1, 24, 3987, 9876),
     (9.2, 25, 2675, 9876),
     (10.0, 26, 1894, 9876),
     (7.5, 27, 1852, 9876),
     (5.5, 28, 9852, 9876),
```

```
(9.7, 29, 2751, 9876),
(6.9, 30, 1860, 9876),
(8.7, 31, 6258, 9876),
(9.6, 32, 7631, 9876),
(4.5, 33, 9218, 9876),
(7.9, 34, 1575, 9876),
(8.6, 35, 1245, 9876),
(6.7, 36, 5155, 9876),
(10.0, 37, 9213, 9876),
(5.9, 38, 7436, 9876),
(9.5, 39, 1216, 9876),
(7.9, 40, 3912, 9876);
(9.2, 41, 1617, 6541),
(3.2, 42, 5970, 6541),
(9.6, 43, 9053, 6541),
(5.2, 44, 3987, 6541),
(4.5, 45, 2675, 6541),
(4.7, 46, 1894, 6541),
(5.9, 47, 1852, 6541),
(6.5, 48, 9852, 6541),
(6.9, 49, 2751, 6541),
(7.3, 50, 1860, 6541),
(7.9, 51, 6258, 6541),
(8.6, 52, 7631, 6541),
(9.8, 53, 9218, 6541),
(9.0, 54, 1575, 6541),
(8.0, 55, 1245, 6541),
(10.0, 56, 5155, 6541),
(6.1, 57, 9213, 6541),
(6.3, 58, 7436, 6541),
(6.7, 59, 1216, 6541),
(6.9, 60, 3912, 6541);
```

APÊNDICE I – *INSERT* UTILIZADO NA TABELA ALUNODISCIPLINA

Este Apêndice trata-se do código de inserção de dados na tabela AlunoDisciplina do Banco de Dados

```
INSERT INTO "Aluno"."AlunoDisciplina"(
     "id_AlunoDisciplina", "CodigoDisciplina", "MatriculaAluno")
     VALUES (1, 4321, 1617),
     (2, 4321, 5970),
     (3, 4321, 9053),
     (4, 4321, 3987),
     (5, 4321, 2675),
     (6, 4321, 1894),
     (7, 4321, 1852),
     (8, 4321, 9852),
     (9, 4321, 2751),
     (10, 4321, 1860),
     (11, 4321, 6258),
     (12, 4321, 7631),
     (13, 4321, 9218),
     (14, 4321, 1575),
     (15, 4321, 1245),
     (16, 4321, 5155),
     (17, 4321, 9213),
     (18, 4321, 7436),
     (19, 4321, 1216),
     (20, 4321, 3912);
     (21, 9876, 1617),
     (22, 9876, 5970,),
     (23, 9876, 9053),
     (24, 9876, 3987),
     (25, 9876, 2675),
     (26, 9876, 1894),
     (27, 9876, 1852),
     (28, 9876, 9852),
```

```
(29, 9876, 2751),
(30, 9876, 1860),
(31, 9876, 6258),
(32, 9876, 7631),
(33, 9876, 9218),
(34, 9876, 1575),
(35, 9876, 1245),
(36, 9876, 5155),
(37, 9876, 9213),
(38, 9876, 7436),
(39, 9876, 1216),
(40, 9876, 3912);
(41, 6541, 1617),
(42, 6541, 5970),
(43, 6541, 9053),
(44, 6541, 3987),
(45, 6541, 2675),
(46, 6541, 1894),
(47, 6541, 1852),
(48, 6541, 9852),
(49, 6541, 2751),
(50, 6541, 1860),
(51, 6541, 6258),
(52, 6541, 7631),
(53, 6541, 9218),
(54, 6541, 1575),
(55, 6541, 1245),
(56, 6541, 5155),
(57, 6541, 9213),
(58, 6541, 7436),
(59, 6541, 1216),
(60, 6541, 3912);
```

APÊNDICE J –SELECT UTILIZADO PARA LISTAR ALUNOS E DISCIPLINAS

Este Apêndice trata-se do código das seleções utilizadas para listar os alunos e as disciplinas

```
select "Matricula", "Nome", discip."NomeDisciplina" as Disciplina
from "Aluno"."Aluno" aluno
left join "Aluno"."AlunoDisciplina" aldis  on aluno."Matricula" =
aldis."MatriculaAluno"
left join "Aluno"."Disciplinas"     discip on
aldis."CodigoDisciplina" = discip."CodigoDisciplina"
order by "Nome";
```

APÊNDICE K –SELECT UTILIZADO PARA LISTAR DISCIPLINAS E ALUNOS MATRICULADOS

Este Apêndice trata-se do código das seleções utilizadas para listar as disciplinas e os respectivos alunos matriculados

```
select "Matricula", "Nome", discip."NomeDisciplina" as Disciplina
from "Aluno"."Aluno" aluno
left join "Aluno"."AlunoDisciplina" aldis  on aluno."Matricula" =
aldis."MatriculaAluno"
left join "Aluno"."Disciplinas"     discip on
aldis."CodigoDisciplina" = discip."CodigoDisciplina"
order by discip."NomeDisciplina", "Nome";
```

APÊNDICE L –SELECT UTILIZADO PARA LISTAR DISCIPLINAS, ALUNOS MATRICULADOS E SUAS FREQUÊNCIAS

Este Apêndice trata-se do código das seleções utilizadas para listar as disciplinas, os alunos matriculados e as respectivas frequências

```
select "Matricula", "Nome", discip."NomeDisciplina" as Disciplina,
freq."Presencas"
from "Aluno"."Aluno" aluno
join "Aluno"."AlunoDisciplina" aldis  on aluno."Matricula" =
aldis."MatriculaAluno"
join "Aluno"."Disciplinas"     discip on aldis."CodigoDisciplina" =
discip."CodigoDisciplina"
join "Aluno"."Frequencia"      freq   on aluno."Matricula" =
freq."MatriculaAluno"
                                      and aldis."CodigoDisciplina" =
freq."CodigoDisciplina"
order by discip."NomeDisciplina", "Nome";
```

APÊNDICE M –SELECT UTILIZADO PARA LISTAR DISCIPLINAS, ALUNOS MATRICULADOS E SUAS NOTAS

Este Apêndice trata-se do código das seleções utilizadas para listar as disciplinas, os alunos matriculados e as respectivas notas

```
select "Matricula", "Nome", discip."NomeDisciplina" as Disciplina,
notas."Media"
from "Aluno"."Aluno" aluno
join "Aluno"."AlunoDisciplina" aldis  on aluno."Matricula"        =
aldis."MatriculaAluno"
join "Aluno"."Disciplinas"     discip on aldis."CodigoDisciplina" =
discip."CodigoDisciplina"
join "Aluno"."Notas"           notas  on aluno."Matricula"        =
notas."MatriculaAluno"
                                     and aldis."CodigoDisciplina" =
notas."CodigoDisciplina"
order by discip."NomeDisciplina", "Nome";
```

APÊNDICE N –SELECT UTILIZADO PARA LISTAR AS DISCIPLINAS E NOTAS DE UM ALUNO

Este Apêndice trata-se do código da seleção utilizada para listar as disciplinas e as respectivas notas dos alunos

```
select "Matricula", "Nome", discip."NomeDisciplina" as Disciplina,
notas."Media"
from "Aluno"."Aluno" aluno
join "Aluno"."AlunoDisciplina" aldis  on aluno."Matricula"        =
aldis."MatriculaAluno"
join "Aluno"."Disciplinas"     discip on aldis."CodigoDisciplina" =
discip."CodigoDisciplina"
join "Aluno"."Notas"           notas  on aluno."Matricula"        =
notas."MatriculaAluno"
                                     and aldis."CodigoDisciplina" =
notas."CodigoDisciplina"
where aluno."Matricula" = 6258
order by discip."NomeDisciplina";
```

APÊNCIDE O – CÓDIGO FONTE DA PÁGINA DE LISTAGEM DE ALUNOS

```
<%@page language="java" contentType="text/html; charset=UTF-8" pageEncoding="UTF-8"%>
<%@ taglib uri="http://java.sun.com/jsp/jstl/core" prefix= "c" %>

<!DOCTYPE html>
<html lang="pt-BR">
<head>
	<meta http-equiv="content-type" content="text/html; charset=UTF-8">
	<title>Universidade</title>

	<style>
		table, th, td {
			border: 1px solid black;
			border-collapse: collapse;
		}
	</style>
</head>
<body>
<header style="position: fixed; background: white;  width: 100%; margin-top: 0px; top:
0; left: 0; border-style: solid; border-color: orange; border-width: 0px 0px 0.1875em
0px;">
<h1 align="center">Universidade Formandos</h1>
<div style="text-align: center;">
	<h2>Lista Alunos por Disciplina</h2>
	<form action="/Universidade/listaAlunos" method="post">
		Código da Disciplina: <input type="text" name="codDis" maxlength="150"
size="50">
		    
		<button name="listAl" type="submit" autofocus accesskey="l">
		<span style="text-decoration: underline;">L</span>istar</button>
    </form>
	<br>
	<button name="listFreq" type="button" onclick
="window.location.href='index.jsp';" autofocus accesskey="r">
	<span style="text-decoration: underline;">R</span>etornar</button>
	<br>
</div>
<br>
</header>
<br><br><br><br><br><br><br><br><br><br><br><br><br>
<c:if test="${ not empty resPesq }">
	<table style="width: 80%; margin: auto; text-align: left;">
		<tbody>
			<tr style="text-align: center;">
				<th>Disciplina</th>
				<th>Matrícula</th>
				<th>Nome</th>
			</tr>
			<c:forEach items="${resPesq}" var="alunoDis">
				<tr>
					<td>${ alunoDis.disciplina }</td>
					<td>${ alunoDis.matricula }</td>
					<td>${ alunoDis.nome }</td>
				</tr>
			</c:forEach>
		</tbody>
	</table>
</c:if>
</body>
</html>
```

APENDICE P – CÓDIGO FONTE DA PROTEÇÃO DA LISTAGEM DE FREQUÊNCIA

```
package universidade;

@WebServlet("/listaFrequencia")
public class ListaFrequencia extends HttpServlet {
	private static final long serialVersionUID = 1L;

	@Resource(lookup = "java:/PostgresDS", name = "universidade")
	private DataSource universidade;

    public ListaFrequencia() {
        super();
    }

	protected void doPost(HttpServletRequest request, HttpServletResponse response)
throws ServletException, IOException {
		ArrayList<AlunosLinhaFreq> respConsulta = new
ArrayList<AlunosLinhaFreq>();

		String argDisc = request.getParameter("codDis").trim();
		String argAluno = request.getParameter("codAluno").trim();

		if(argDisc.length() < 1) {
			argDisc = "0";
		}

		if(argAluno.length() < 1) {
			argAluno = "0";
		}

		try {
			Connection dsConexao = universidade.getConnection();
			// Verifica se foi possível obter uma conexão ao postgres
			if (!dsConexao.isValid(2)) {
				System.out.println("Sem conexão ao postgres");
				return;
			}

			String ConsultaSqlTxt = "select \"Matricula\", \"Nome\",
discip.\"NomeDisciplina\" as Disciplina, freq.\"Presencas\" "
					+ "from \"Aluno\".\"Aluno\" aluno "
					+ "join \"Aluno\".\"AlunoDisciplina\" aldis  on
aluno.\"Matricula\" = aldis.\"MatriculaAluno\" "
					+ "join \"Aluno\".\"Disciplinas\"     discip on
aldis.\"CodigoDisciplina\" = discip.\"CodigoDisciplina\" "
					+ "join \"Aluno\".\"Frequencia\"      freq   on
aluno.\"Matricula\" = freq.\"MatriculaAluno\" "
					+ "                                          and
aldis.\"CodigoDisciplina\" = freq.\"CodigoDisciplina\" "
					+ "where aluno.\"Matricula\" = ? and
freq.\"CodigoDisciplina\" = ? "
					+ " order by discip.\"NomeDisciplina\", \"Nome\"";
			ResultSet res = null;

			PreparedStatement consultaSql =
dsConexao.prepareStatement(ConsultaSqlTxt, ResultSet.TYPE_FORWARD_ONLY,
ResultSet.CONCUR_READ_ONLY);
			int argAlunoInt = Integer.parseInt(argAluno);
			int argDiscInt = Integer.parseInt(argDisc);
			consultaSql.setInt(1, argAlunoInt);
```

```
                    consultaSql.setInt(2, argDiscInt);
                    res = consultaSql.executeQuery();

                    boolean lendo = res.next();
                    while (lendo) {
                           AlunosLinhaFreq linhares = new
AlunosLinhaFreq(res.getString("Matricula"), res.getString("Nome"),
res.getString("Disciplina"), res.getString("Presencas"));
                           respConsulta.add(linhares);
                           lendo = res.next();
                    }

                    res.close();
                    consultaSql.close();
                    dsConexao.close();

             } catch (SQLException  | NumberFormatException sqlEx) {
                    System.out.println("Aplicação erro sql - " +
sqlEx.getLocalizedMessage());
             }

             response.setCharacterEncoding("utf-8");
             RequestDispatcher despReq =
request.getRequestDispatcher("/mostraFrequencia.jsp");
             request.setAttribute("resPesq", respConsulta);
             despReq.forward(request, response);
       }
}
```