INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CAMPUS MACAPÁ
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

LUIS ABDON ALMEIDA DE LIMA
ORLANDO NAZARÉ TÔRRES NETO

ANÁLISE DAS VULNERABILIDADES CONTRA ATAQUES NOS LABORATÓRIOS DE INFORMÁTICA DO IFAP CAMPUS MACAPÁ

MACAPÁ
2022

LUIS ABDON ALMEIDA DE LIMA
ORLANDO NAZARÉ TÔRRES NETO

ANÁLISE DAS VULNERABILIDADES CONTRA ATAQUES NOS LABORATÓRIOS DE INFORMÁTICA DO IFAP CAMPUS MACAPÁ

Trabalho de Conclusão de Curso apresentado ao Curso de Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá, em cumprimento às exigências legais como requisito à obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Me. Andrew Hemerson Galeno Rodrigues

MACAPÁ
2022

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

L732a Lima, Luis Abdon Almeida de
Análise das vulnerabilidades contra ataques nos laboratórios de informática do Ifap campus Macapá / Luis Abdon Almeida de Lima, Orlando Nazaré TÔRRES NETO. - Macapá, 2022.
87 f.: il.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2022.

Orientador: Andrew Hemerson Galeno Rodrigues.

1. ataques. 2. vulnerabilidades. 3. laboratórios de informática. I. TÔRRES NETO, Orlando Nazaré . I. Rodrigues, Andrew Hemerson Galeno, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

LUIS ABDON ALMEIDA DE LIMA
ORLANDO NAZARÉ TÔRRES NETO

ANÁLISE DAS VULNERABILIDADES CONTRA ATAQUES NOS LABORATÓRIOS DE INFORMÁTICA DO IFAP CAMPUS MACAPÁ

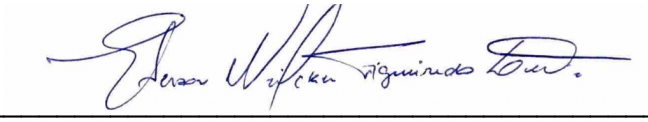
Trabalho de Conclusão de Curso apresentado ao Curso de Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá, em cumprimento às exigências legais como requisito à obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Me. Andrew Hemerson Galeno Rodrigues

BANCA EXAMINADORA

Orientador: Prof. Me. Andrew Hemerson Galeno Rodrigues
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Examinador 1: Prof. Me. Allan Meira De Medeiros
Instituto Federal de Educação, Ciência e Tecnologia do Amapá



Examinador 2: Prof. Me. Ederson Wilcker Figueiredo Leite
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Aprovado em: 07/12/2022

Conceito/Nota: 9,6

AGRADECIMENTOS

No decorrer desses 03 anos e 6 meses nunca pensei que seria tão difícil a jornada acadêmica no IFAP, confesso que foram vários obstáculos a minha frente que tive que vencer, vi colegas abandonarem o curso com o objetivo de conseguir uma vida melhor e estudar em outros estados com mais oportunidades.

Mas continuei em frente batalhando todos os dias para alcançar meus objetivos de ter um diploma de nível superior e agradecer primeiramente a Deus por ter me sustentado até aqui e permitido que tendo fé podemos fazer nossos sonhos virar realidade.

Agradecemos às nossas famílias que sempre nos apoiaram com amor, incentivo, ao nosso orientador professor Andrew Hemerson Galeno Rodrigues que sempre esteve conosco nessa caminhada nos ajudando e a todas as pessoas que direta ou indiretamente fizeram parte da nossa formação incentivando a prosseguir apesar de todos os obstáculos pela frente.

“Consagre ao Senhor tudo o que você faz,
e os seus planos serão bem-sucedidos”.
PROVÉRBIOS 16:3

RESUMO

A segurança em redes de computadores é um elemento fundamental para a proteção de usuários que utilizam os meios de comunicação da *Internet* para fazer *login* em várias plataformas da *web*. Este trabalho foi desenvolvido com a finalidade de manifestar a importância da segurança da informação no Instituto Federal do Amapá *Campus* Macapá, onde foi demonstrado as principais ameaças, vulnerabilidades e riscos que a instituição e os discentes podem estar sofrendo, com a perda de integridade e confidencialidade dos dados nos laboratórios de informática. Este trabalho tem como objetivo analisar as vulnerabilidades contra ataques virtuais nos laboratórios de informática do IFAP *Campus* Macapá. A metodologia utilizada foi a pesquisa bibliográfica com base em livros, artigos, dissertações sobre a segurança da informação e o estudo de caso sobre os principais problemas de segurança nos laboratórios de informática do IFAP. Portanto, os resultados obtidos foram a cartilha sobre as boas práticas de segurança da informação para os estudantes da instituição e o gerador de senhas seguras para proteger os dados pessoais dos alunos do IFAP.

Palavras-chave: ataques; vulnerabilidades; laboratórios de informática.

ABSTRACT

The security in computer networks is a fundamental element for the protection of users who use the Internet media to log into various web platforms. This work was developed with the purpose of manifesting the importance of information security in the Federal Institute of Amapá Campus Macapá, where it was demonstrated the main threats, vulnerabilities and risks that the institution and the students may be suffering, with the loss of integrity and confidentiality of the data in the computer labs. This work aims to analyze the vulnerabilities against virtual attacks in the computer labs of the IFAP Macapá Campus. The methodology used was the bibliographic research based on books, articles, and dissertations about information security and the case study about the main security problems in the computer labs of IFAP. Therefore, the results obtained were the primer on good information security practices for the institution's students and the generator of secure passwords to protect the personal data of IFAP's students.

Keywords: attacks; vulnerabilities; computer labs.

LISTA DE FIGURAS

Figura 1 - Propriedades mais valorosas da segurança da Informação……24
Figura 2 - O ciclo de vida dos dados conforme a LGPD…… 27
Figura 3 - O que são *Cookies*……..47
Figura 4 - Dados expostos no navegador…….53
Figura 5 - Controle de acesso dos laboratórios……54
Figura 6 - Sistemas de proteção dos laboratórios……..55
Figura 7 - Planos de contingência……..56

LISTA DE GRÁFICOS

Gráfico 1 - Relatório sobre Segurança da Informação……19
Gráfico 2 - Estatísticas sobre segurança da Informação……20

LISTA DE ABREVIATURAS E SIGLAS

DOS	Denial of Service
DMZ	Demilitarized Zone
ESR	Escola Superior de Redes
HIDS	Host - Based Intrusion Detection System
IFAP	Instituto Federal do Amapá
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
PIDS	Protocol - Based Intrusion Detection System
RNP	Rede Nacional de Ensino e Pesquisa
SSL	Secure Socket Layer
TI	Tecnologia da Informação
TLS	Transport Layer Security
VPN	Virtual Private Network

SUMÁRIO

1	**INTRODUÇÃO**	14
2	**JUSTIFICATIVA**	16
3	**OBJETIVOS**	17
3.1	**Objetivo Geral**	17
3.2	**Objetivos Específicos**	17
4	**REFERENCIAL TEÓRICO**	18
4.1	**Conceitos básicos da segurança da informação**	18
4.2	**Cenário da segurança da informação**	18
4.3	**Segurança de informação**	21
4.3.1	Importância da segurança em redes	21
4.3.2	Perigos e algumas considerações sobre Segurança	21
4.4	**Propriedades da segurança da informação**	23
4.4.1	Políticas e normas sobre segurança da informação	25
4.4.2	LGPD - Lei geral de proteção de dados	26
4.4.3	ISO/IEC 27001 - Gestão de segurança da informação	28
4.4.4	ISO/IEC 27002 - Controles de segurança da informação	28
4.4.5	Marco civil da Internet	29
4.5	**Vazamentos de dados em órgãos públicos**	30
4.6	**Tipos de ameaças em redes de computadores**	31
4.6.1	Vírus	31
4.6.2	Spam	31
4.6.3	Spyware	32
4.6.4	Adware	32
4.6.5	Worms	33
4.6.6	Trojan	33
4.6.7	Ransomware	34
4.6.8	DOS - Ataque de negação de serviço	34

4.6.9 DDoS - Ataque de negação de serviço distribuído 35
4.6.10 Rootkit 35
4.7 Tecnologias e Técnicas de Defesa 36
4.7.1 Firewall 36
4.7.2 DMZ - Zona desmilitarizada 37
4.7.3 Sistema de detecção de intrusos - IDS 37
4.7.4 Sistema de prevenção de intrusos - IPS 38
4.8 Criptografia 39
4.8.1 Assinatura digital 40
4.8.2 Email seguro 40
4.8.3 Antivírus 41
4.8.4 Plano de contingência 41
4.8.5 Backup 42
4.8.5.1 Backup completo 42
4.8.5.2 Backup incremental 43
4.8.5.3 Backup diferencial 43
4.8.6 Protocolos de segurança da informação 44
4.8.6.1 SSL - Secure sockets layer 44
4.8.6.2 TLS - Transport layer security 44
4.8.6.3 VPN - Virtual private network 45
4.9 Profissionais de segurança da informação 45
4.10 Dados pessoais 46
4.10.1 Cookies 47
4.11 Instituto Federal do Amapá 47
5 METODOLOGIA 50
6 RESULTADOS E DISCUSSÃO 52
6.1 Laboratórios de informática - Campus macapá 52
6.2 Controle dos laboratórios 54
6.3 Ferramentas de proteção e planos de contingência 55

6.4 Análise dos fatores de riscos 57
6.5 Soluções para o problema 57
6.5.1 Cartilha sobre boas práticas em segurança da informação 58
6.5.2 Resumo dos tópicos da cartilha 58
6.5.3 Gerador de senhas seguras 59
7 CONSIDERAÇÕES FINAIS 60
REFERÊNCIAS 61
APÊNDICE A - Laboratórios de informática do IFAP 64
APÊNDICE B - Cartilha de boas práticas em segurança 66
APÊNDICE C - Gerador de senhas seguras 86

1 INTRODUÇÃO

A segurança da informação é algo de extrema importância quando se trata do armazenamento de dados que tendem a ser protegidos de indivíduos maliciosos nas redes virtuais, tendo em sua propriedade a confiabilidade das informações como pilar de sua estrutura para organizações públicas brasileiras.

Mesmo a tecnologia em plena evolução no mundo contemporâneo, os conjuntos de proteção cibernética tem-se mostrados eficazes contra ataques virtuais nas redes de computadores, mas indivíduos mal-intencionados vem atacando seus sistemas de segurança e mostrando que mesmo tendo toda uma estrutura tecnológica avançada, sempre há uma falha de segurança que possibilita a invasão deles nos servidores ou aplicações usadas por várias instituições públicas.

Tendo em vista que a proteção de dados em qualquer instituição passa por um profissional de tecnologia da informação (TI) capacitado para desempenhar seu papel sem margens de erros visando proteger o bem mais precioso dentro da organização que são as informações. É importante destacar que a informação deve ser usada de maneira inteligente estando disponível em tempo hábil e protegida de acordo com seu nível de privacidade.

Este trabalho de pesquisa tem como objetivo elaborar um manual de boas práticas em segurança em redes de computadores para o uso dos Laboratórios de Informática pelos estudantes do Instituto Federal do Amapá *Campus* Macapá (IFAP) e um gerador de senha aleatórios com capacidade de segurança para a conta de usuários dos estudantes.

Para o desenvolvimento deste trabalho foram realizadas pesquisas bibliográficas em livros, artigos e dissertações sobre a segurança da informação e o estudo de caso para analisar os principais fenômenos sobre a segurança dos estudantes nos laboratórios de informática do IFAP. Para a conscientização dos estudantes sobre as boas práticas de segurança da informação foi desenvolvido uma cartilha e um gerador de senhas seguras para a proteção dos dados de usuários dos estudantes da instituição.

Neste sentido, observa-se que a estruturação do presente trabalho é composta por 7 capítulos, sendo o primeiro a introdução.

O segundo capítulo, apresenta a justificativa e a lacuna a ser preenchida pelo Trabalho de Conclusão de Curso (TCC). O terceiro capítulo, apresenta os objetivos da pesquisa científica. O quarto capítulo, apresenta o referencial teórico, onde permite verificar o estado do problema a ser pesquisado, sob o aspecto teórico e de outros estudos e pesquisas já realizadas.

O quinto capítulo apresenta os procedimentos metodológicos para se atingir o objetivo deste estudo. O sexto capítulo apresenta os resultados e discussão.

Para o fechamento do trabalho, no sétimo capítulo, foram feitas as conclusões decorrentes do estudo.

2 JUSTIFICATIVA

A segurança da informação tornou-se algo bastante discutido durante a pandemia de COVID-19, pois proteger informações para uma instituição pode garantir o sucesso ou, por outro lado o fracasso dela, entretanto, faz-se necessário ter bastante prudência em relação de como são tratados, processados e disponibilizados estes dados e o que viabilizam para a sua proteção contra ataques virtuais nos meios de comunicação.

O ensino nos Institutos Federais proporcionam uma maneira importante de aprendizado dos alunos, mas é importante dizer que a tecnologia requer um cuidado especial quando se trata de navegar na *Internet*, pois é muito comum alguns alunos sem o conhecimento sobre as boas práticas de segurança da informação deixarem seus dados salvos no navegador tornando assim uma porta de entrada para indivíduos mal-intencionados que poderão roubar ou manipular dados desses usuários.

3 OBJETIVOS

3.1 Objetivo Geral

Analisar as vulnerabilidades contra ataques nos laboratórios de informática do IFAP Campus Macapá.

3.2 Objetivos Específicos

- ➢ Identificar as vulnerabilidades presentes e como elas contribuem para deixar os dados dos usuários suscetíveis a ataques nos laboratórios do IFAP.
- ➢ Propor uma cartilha de proteção fundamentada em documentos, protocolos, ferramentas, *softwares* disponíveis que devem ser utilizadas para evitar problemas futuros.
- ➢ Sugerir um gerador de senhas seguras para proteger os dados pessoais dos alunos do IFAP.

4 REFERENCIAL TEÓRICO

4.1 Conceitos básicos da segurança da informação

A informação é o pilar de toda estrutura de uma instituição pública, pois primordialmente deve ser protegida para resguardar todos os dados da organização, utilizando recursos tecnológicos para distribuição e controle das mensagens dos usuários e do receptor.

Para Nakamura e Geus (2002, p.9):

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. Pode existir em diversos meios, ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio por meios eletrônicos e apresentada em filmes ou dita em conversas (ABNT NBR ISO/IEC 27002, 2013).

A segurança da informação está focada na proteção de um agrupamento de dados, que estão em ambientes domésticos e corporativos, esta requer uma atenção especial, pois quando se trata de informações sensíveis deve-se dar uma maior atenção a problemas relacionados à invasão de privacidade e vazamento de dados.

De acordo com a ESR(2021), a importância da segurança em redes tem como benefício implementar boas práticas dentro da instituição contra ataques cibernéticos, sendo monitoradas, protegidas contra acessos não autorizados que possam roubar dados desta ou prejudicar suas atividades.

Outrossim, a segurança da informação representa a preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações e dados importantes para uma organização ou indivíduo, passando por ambientes físicos e tecnológico com pessoas que viabilizem recursos e estruturas para sua proteção e que se importam com a qualidade e continuação dos seus serviços dentro de uma instituição pública.

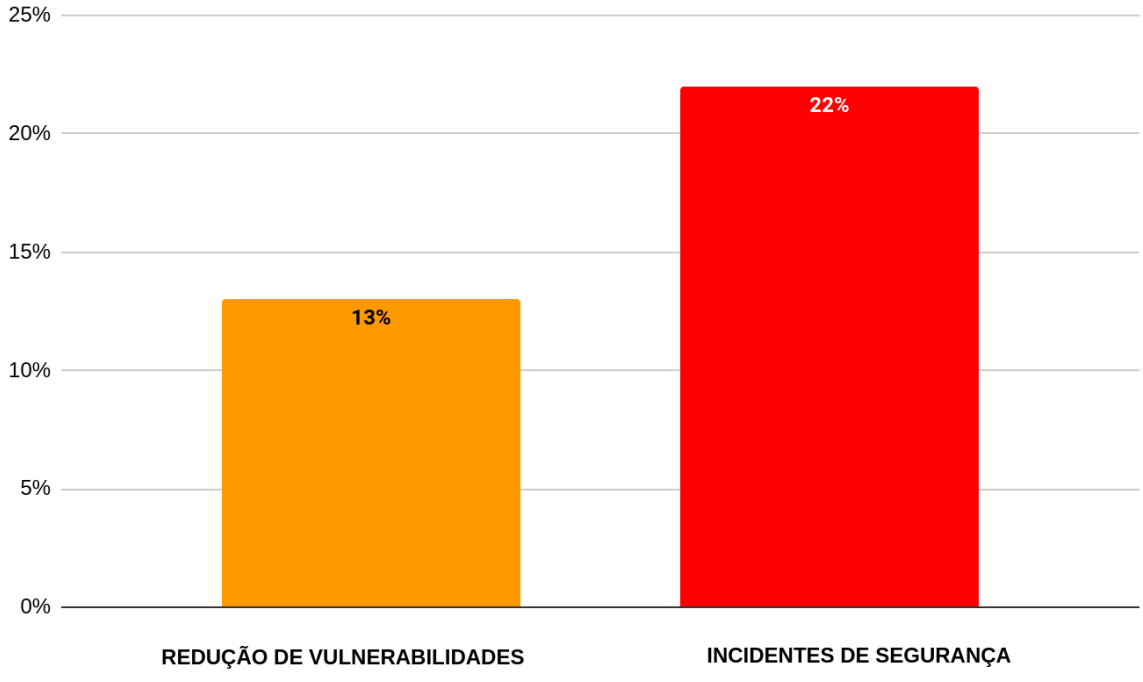
De acordo com Kurose e Ross (2013) ele descreve a rede de computadores como a conexão entre dois ou mais dispositivos que permitem o compartilhamento de recursos e troca de informações entre si.

Deste modo, a segurança da instituição é de suma importância, mas deve se levar em consideração os fatores internos desta, pois os aspectos humanos podem ser uma porta de entrada para indivíduos mal-intencionados atacarem esta por meio de falhas que podem ocorrer dentro do seu ambiente de trabalho. Portanto, a segurança em redes pode providenciar políticas que garantem as propriedades em que a segurança da informação está fundamentada e sendo implementada para inibir ataques *hackers* contra os sistemas de armazenamento e processamento de dados da instituição ou contra maus funcionários, ou *softwares* maliciosos que podem acarretar um grande problema no futuro.

4.2 Cenário da segurança da informação

O gráfico 1 apresenta o relatório sobre segurança da informação elaborado pela rede nacional de ensino e pesquisa sobre os incidentes e problemas de segurança da informação no ano de 2020.

Gráfico 1 - Relatório sobre Segurança da Informação



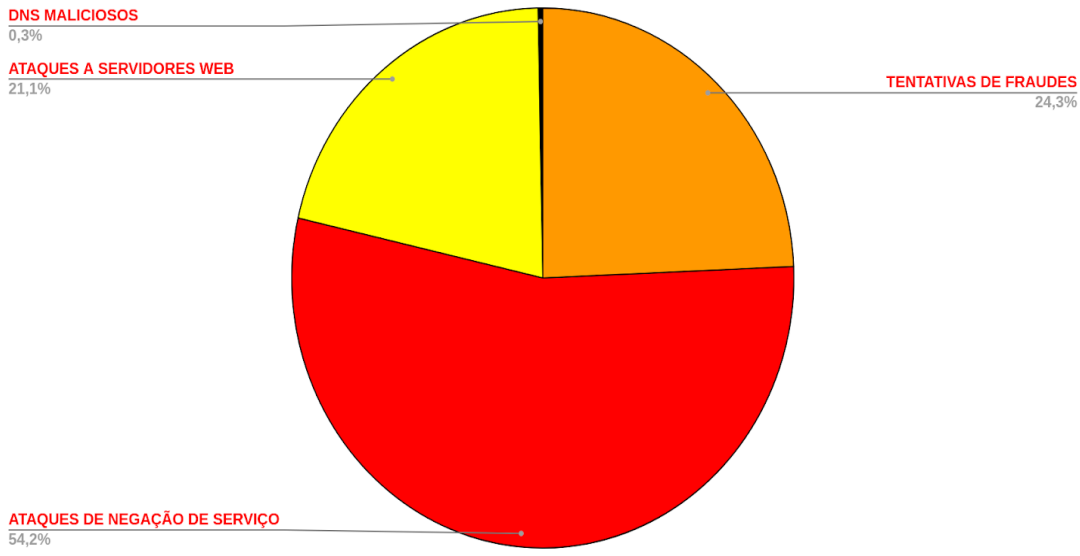
Fonte: RNP(2020)

Conforme apresentado no gráfico 1 diversos casos envolvendo vazamento de dados e invasão de sistemas no Brasil e no mundo. No entanto, por conta do isolamento social e do aumento do trabalho e ensino remoto, foi um ano em que houve redução de 13% no número de vulnerabilidades de segurança detectadas e de 22% de incidentes de segurança reportados no Sistema RNP em comparação ao ano anterior (RNP, 2020).

Embora à segurança da informação esteja atrelada a importância da proteção de dados para instituições e usuários, existem falhas externas e internas dentro dos equipamentos, servidores, serviços e criptografia vem ocasionando uma grande preocupação em relação às grandes quantidades de ataques, vazamentos e roubo de dados causando perdas financeiras, morais e a reputação de indivíduos no Brasil.

O gráfico 2, apresenta as estatísticas do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil - cert.br.

Gráfico 2 - Estatísticas sobre segurança da Informação



Fonte: CERT.BR(2020)

De acordo com o gráfico 2, às notificações de tentativas de fraude que totalizaram 24,3% em 2020, correspondendo a uma queda de 22% em relação a 2019. Em 2020 foram notificadas 68.200 informações sobre dispositivos que participaram de ataques de negação de serviço (DOS). Ataques a servidores *Web* totalizaram 26.567 em 2020, um aumento de 19% em relação ao ano de 2019; No

ano de 2020, receberam 1.212 notificações de máquinas comprometidas. Este total foi 130% maior do que o número de notificações recebidas em 2019; contabilizaram 378 notificações de servidores DNS maliciosos, utilizados como parte da infraestrutura para realização de fraudes financeiras (CERT.br, 2020).

Diante disso, os sistemas de segurança da informação dentro das instituições públicas quase não estão suprindo a necessidade existentes e aquelas que podem surgir ao longo do tempo, mas que devido à grande repercussão dos ataques em instituições públicas tem gerado uma grande insatisfação dos usuários que utilizam serviços em plataformas que deveriam dar o máximo rigor em relação ao armazenamento e processamento dos dados sensíveis destes indivíduos.

4.3 Segurança da informação

4.3.1 Importância da segurança em redes

A necessidade de segurança em redes de computadores tem se tornado de grande importância para as instituições que fazem das informações um meio para desenvolver suas atividades e políticas para seus negócios, garantindo a confiança com aqueles que acessam seus serviços ou plataformas.

Assim sendo, a segurança em redes é um conjunto de fatores utilizados para monitorar o acesso de indivíduos não autorizados à rede de computadores ou serviços acessados por estes, garantindo a integridade dos dados e o seu sigilo (ESR, 2020).

Para o meio virtual é de suma importância garantir que o sistema da rede seja da instituição ou pessoa estejam seguros contra diversas ameaças que possam surgir é um princípio primordial para a sua proteção.

4.3.2 Perigos e algumas considerações sobre Segurança

A *Internet* surgiu para revolucionar a comunicação com várias pessoas no mundo, mas devido esta ser usada publicamente por vários indivíduos permitindo o compartilhamento ao mesmo tempo de diversos dispositivos, não há uma proteção efetiva contra ataques virtuais, em vista disso podendo algumas pessoas

manipularem informações sigilosas na rede usada por instituições públicas nos meios de transmissão dos dados.

Segundo Kurose Ross (2010, p.492):

> Hoje quase todas as organizações (empresas, universidades etc.) possuem redes conectadas à internet pública. Essas redes podem ser comprometidas potencialmente por atacantes que ganham acesso a essas redes por meio da internet pública. Os atacantes podem tentar colocar *worms* nos hospedeiros na rede, adquirir segredos corporativos, mapear as configurações da rede interna e lançar ataques Dos.

Os riscos associados ao trabalhar com informações sensíveis pela instituição deve ser considerada a hipótese de que caso estes dados sejam roubados causará um grande impacto sobre a imagem e serviços desta. Para uma instituição que visa a proteção de suas operações é importante prevenir os riscos que poderão surgir, fazendo com que esta tome precauções e ações para amenizar e resolver problemas que irão surgir com o tempo sobre a segurança da informação interna ou externa.

Segundo Dantas (2011, p. 41):

> Em um cenário de incertezas, as ameaças e oportunidades têm o potencial de produzir perdas ou aumentar os ganhos. Os resultados positivos são alcançados com uma boa gestão das incertezas e de seus riscos, gerando valor ao otimizar as suas oportunidades, e ao estabelecerem estratégias para os objetivos de crescimento, na busca da maximização de seus resultados. Os resultados negativos são oriundos da ausência e/ou da fragilidade dessa gestão, em que os seus resultados podem produzir danos e perdas de grandes proporções.

A área de segurança da informação abrange a análise e proteção contra diversos tipos de riscos que deve passar por um profissional capacitado para identificar e tomar algumas decisões como:

Quadro 1 - principais riscos envolvendo a perda das informações

Principais riscos envolvendo a Segurança da Informação	Tipos
Risco Alto	Caso o risco seja extremamente alto para empresa ou órgão, este deve tomar certas ações para mitigar o efeito que certas pragas virtuais tendem a atacá-los diminuindo as vulnerabilidades existentes na sua rede de computadores e sistemas de informação.
Risco Médio	Caso o risco não seja tão grave, a organização deixa de tomar medidas graves, ou seja, esta segue suas atividades sem nenhuma precaução a tomar.
Risco Leve	Caso não o risco de segurança esteja em um nível muito baixo a instituição não tomará nenhuma medida contra ameaças que não podem causar nenhum dano.

Fonte: Elaborado pelos autores (2022)

Conforme o quadro 1, apresenta os principais riscos relacionados à perda de informações, caso o risco seja extremamente alto a empresa tem que se focar em resolver o problema focado nas vulnerabilidades da rede e do sistema. Se o risco não for tão grave a empresa não se esforçará em tomar decisões seguindo as atividades sem se preocupar. O caminho percorrido pelos dados no sistema de segurança deve ser vigiado do começo ao fim por estar suscetível a erros e falhas tanto internas quanto externas.

4.4 Propriedades da segurança da informação

A informação é o bem mais precioso de uma organização pública, nela estarão todos os dados tanto da instituição quanto do usuário, sendo assim esta deve proteger com soluções que sejam eficazes e rápidas, garantindo os direitos estabelecidos nas propriedades básicas da segurança da informação.

Segundo Fontes (2012, p.106):

> A informação utilizada pela organização é um bem que tem valor. A informação deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

A segurança da informação tem em sua estrutura propriedades que todos devem seguir como princípios fundamentais para uma boa proteção com políticas a serem seguidas por instituições e profissionais que trabalhem com dados sensíveis.

A figura 1 apresenta as principais propriedades em que a segurança da informação está fundamentada como pilar para a proteção dos dados nas instituições e organizações.

Figura 1 - Propriedades mais valorosas da segurança da Informação

Fonte: Os autores(2022)

De acordo com a figura 1**,** confidencialidade tem a função de garantir que a informação esteja acessível apenas para indivíduos autorizados. Já para Integridade na segurança da informação deve ter a disponibilidade de dados confiáveis e verdadeiros em uma formatação compatível com a mandada para seu destinatário, pois deve ter-se a certeza de que não foi manipulada por indivíduos não autorizados.

Além disso, a disponibilidade deve estar disponível a todo tempo para usuários, ou seja, o sistema utilizado para armazenar as informações e processar os dados tem que deixar acessível para todos. Autenticidade é a garantia de que o autor da mensagem é o verdadeiro dono, ou seja, a informação é proveniente de fonte segura. Dessa maneira, a legalidade da informação deve estar respaldada na legislação, evitando possíveis auditorias, garantindo a sua preservação e o respeito às normas vigentes.

4.4.1 Políticas e normas sobre segurança da informação

A segurança da informação está relacionada a um conjunto de medidas estabelecidas pela organização que visa adotar procedimentos tecnológicos de hardware e software que fazem a proteção e monitoramento de todos os dados trafegados pela rede de comunicação desta.

De acordo com Hintzbergen et al.(2018):

> A segurança da informação é alcançada através da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, revisados e melhorados, onde necessário, para assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos.

Além disso, a política de segurança da informação define como as empresas implementam um conjunto de normas e regras sobre o armazenamento, transporte e proteção das informações, sendo esta uma forma de prevenção contra manipulação de dados por indivíduos não autorizados. Definir um sistema de segurança dentro da instituição pode variar por conta que cada organização tem seus meios e normas

internas diferentes de implementar recursos para proteger dados e informações que necessitam serem armazenados e processados de forma eficiente e segura.

Portanto, essa política tem como principal objetivo gerenciar toda a segurança da organização implementando regras e padrões estabelecidos pelos órgãos responsáveis.

4.4.2 LGPD - Lei geral de proteção de dados

A Lei Geral de Proteção de Dados(LGPD) nº 13.709/2018 foi criada para assegurar os direitos à privacidade, liberdade e proteção das informações dos indivíduos residentes no Brasil por pessoas físicas ou jurídicas que fazem o tratamento e processamento de dados pessoais.

A Lei Geral de Proteção de Dados(LGPD):

> Foi Originada do conselho da União Europeia de 27 de abril de 2016, também conhecido como: Regulamento Geral sobre Proteção de Dados(RGPD), fazendo com que empresas e organizações deem uma atenção em relação à proteção de informações dos usuários (ASSIS; MENDES, 2020).

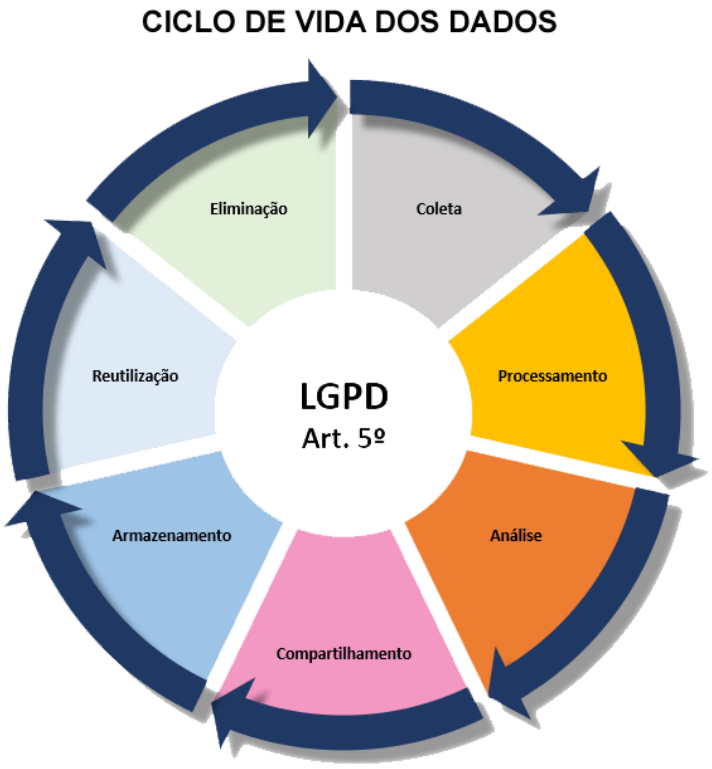
Esta Lei regula como empresas e órgãos públicos e privados tendem a proteger informações sigilosas protegendo os direitos fundamentais de liberdade e de privacidade, caso algumas organizações descumpram medidas estabelecidas nesta legislação estarão sujeitas a penalização, pois ambas devem evitar ao máximo o roubo de dados implementando sistemas de proteção mais eficazes com tecnologias e protocolos existentes no século XXI e tem como fundamentos:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - à inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A figura 2, apresenta os principais ciclos de vida dos dados dentro das instituições, desde sua coleta com autorização baseada na Lei até o arquivamento ou eliminação deste.

Figura 2 - O ciclo de vida dos dados conforme a LGPD



Fonte: XPOSITUM(2022)

Conforme a Figura 2, os dados passam por um longo tratamento, desde a coleta dos dados pessoais do indivíduo, processamento, análise do perfil da pessoa, compartilhamento das informações com autorização das pessoas, armazenamento por prazo determinado por parte da organização, reutilização como consentimento dos titulares e a eliminação deste após o término do tratamento conforme prevê a LGPD.

4.4.3 ISO/IEC 27001 - Gestão de segurança da informação

A *International Organization for Standardization*(ISO) é uma instituição que oferece padrões e normas que podem ter grande eficiência nas atividades de instituições com estrutura para gerenciar e proteger seus ativos de informações.

> A ISO/IEC 27001 é uma certificação muito importante para instituições que querem implementar um padrão com as melhores práticas sobre segurança da informação, melhorando o desempenho das suas atividades e relação com os usuários (ISO/IEC, 2018).

É a norma internacional de gestão de segurança de dados. Nesta mostra, as organizações e empresas devem implementar um sistema de gestão de segurança da informação, organizando e controlando o acesso a dados financeiros e confidenciais de maneira eficiente, diminuindo a probabilidade de serem acessados por indivíduos não autorizados.

4.4.4 ISO/IEC 27002 - Controles de segurança da informação

A ISO/IEC 27001 apresenta os principais controles de segurança da informação que uma instituição deve ter ao gerenciar as informações trabalhadas com melhores práticas para implementar, melhorar e manter seu sistema de gestão de segurança da informação com os riscos previstos na organização.

De acordo com a ISO/IEC 27002(2022):

> A norma ajuda as organizações a aprimorar seu sistema de segurança da informação com conscientização, maior controle dos ativos, políticas de controle de dados, redução dos riscos dentro da instituição e estar conforme a legislação vigente, garantindo o princípio da legalidade das informações dos seus usuários.

Assim sendo, a norma de controle de segurança da informação garante que as instituições que trabalham com ativos e informações sensíveis garantem um sistema capaz de gerenciar os riscos e oferecer maior confiança para seus usuários com as políticas de segurança da informação.

4.4.5 Marco civil da Internet

O Marco Civil da Internet Lei nº 12.965 de 2014 estabelece princípios, garantias, direitos e deveres quanto ao uso da *Internet* no Brasil. Esta norma regula como indivíduos devem usar a *internet* sabendo que mesmo sendo um meio digital não se pode cometer crimes, pois a rede mundial de computadores não é uma terra sem lei.

Esta Lei define princípios, garantias e direitos para pessoas no Brasil, através de normas que protegem a privacidade de indivíduos atacados na *internet*, garantindo direitos e deveres dos usuários dos meios de comunicação (TOMASEVICIUS, 2016)

Esta Lei estabelece princípios, garantias à privacidade e proteção de dados pessoais para indivíduos na *internet*, entretanto, há algumas exceções, pois mediante ordem judicial autoridades de segurança competentes podem ter acessos a informações do usuário desde que cumpram os requisitos estabelecidos por esta legislação.

O uso da *internet* por pessoas em ambientes virtuais é assegurado por disciplinas que todos devem seguir disposto na Lei nº 12.965 artº 3 que tem como disposto:

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

4.5 Vazamentos de dados em órgãos públicos

Tendo em vista que os dados pessoais dos indivíduos estão sendo cadastrados em diversas plataformas do governo para acessar serviços de suma importância, tem-se discutido como são tratados essas informações e quais os meios de assegurar a proteção estão sendo empregados nos meios de comunicação.

De acordo com G1 Globo (2021):

> Durante a pandemia de covid-19, muitos indivíduos usam os serviços digitais para trabalhar e estudar, grande parte da população brasileira tem seus dados cadastrados em diversos sistemas do governo federal, dentre eles temos: cadastro de pessoas físicas(CPF), cadastro nacional de pessoas jurídicas(CNPJ), Endereços, dados cadastrais de serviços de telefonia.

Esses dados foram vazados por *hackers*, que roubam as informações de diversas instituições através dos meios de comunicação, geralmente isso acontece por falha no sistema de computação, permitindo que esses indivíduos mal-intencionados tenham acesso a dados sigilosos.

> A *Deep Web* ou também chamada de *internet* profunda, é uma área da rede mundial de computadores, que está escondida na camada mais baixa da internet, não tendo nenhuma regulamentação, pois não seria possível acessar pelos navegadores padrões conhecidos como o: Google e Bing, dentre outros (GARRETT, 2019).

Essa parte da *Internet* é usada para compartilhar conteúdos ilegais dos mais diversos segmentos, geralmente *hackers* divulgam dados sigilosos nessa área, mantendo seu anonimato e dificultando a identificação pelos órgãos de inteligência, pois não seria possível saber o seu endereço de identificação ou também chamado de IP(internet Protocol), aqui vários usuários do mundo todo tem acesso por meio de um navegador privado chamado Tor que esconde os dados dos usuários.

4.6 Tipos de ameaças em redes de computadores

4.6.1 Vírus

O vírus de computador é um código malicioso que se multiplica através de modificação de outros arquivos e programas baixados para a máquina do usuário, inserindo códigos que se replicaram infectando o *host* da vítima.

De acordo com CERT.br(2020):

> Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para poder se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado, seja executado.

O vírus geralmente chega sem ser convidado na máquina do usuário através de mensagens recebidas no correio eletrônico, em arquivos da web e começando a infectar a máquina da vítima nos programas executáveis no disco rígido.

4.6.2 *Spam*

É um conteúdo disseminado em massa via *e-mail* sem prévio aviso ao indivíduo, neste tipo de ataque é mais comum mandarem anúncios e propagandas, mas também podem ocorrer tentativas de execução de fraudes, phishing usadas por criminosos nos meios virtuais para obter dados ou acesso não autorizado ao dispositivo da vítima.

Phishing é um tipo de ataque usado para enganar indivíduos que compartilham dados confidenciais como números de cartões de crédito e senhas.

De acordo com Filipe Garrett(2022):

> *Spams* são mensagens enviadas pelo emissor sem o consentimento do receptor que estão associadas principalmente pelo correio eletrônico visando divulgar informações em massa contendo propagandas, anúncios e golpes nos meios de comunicação.

Dessa forma, *spam* se tornou algo bastante preocupante, pois não só tem o intuito de divulgar informações em massa, mas também aplicar golpes através de propagandas e anúncios enganosos usados por criminosos virtuais.

4.6.3 *Spyware*

Também chamado de programa espião, este *software* foi projetado para ser invisível tornando-o um malware muito perigoso e invade a privacidade do indivíduo sem a sua permissão, em grande parte está relacionada a programas que permanecem em execução em segundo plano.

Segundo o CERT.br(2020) “O *spyware* é um programa malicioso projetado para fazer o monitoramento das atividades que a vítima faz na sua máquina e coletar dados confidenciais do usuário enviando para terceiros”.

Portanto, tem por objetivo se instalar no computador ou dispositivo do usuário para coletar dados e informações sigilosas da vítima e repassá-los a terceiros sem o conhecimento e consentimento do indivíduo.

4.6.4 *Adware*

Também chamado de programa de anúncios é considerado uma forma de invasão de privacidade, pois inicialmente se confunde com informações da página inicial de um site que um indivíduo está acessando.

Segundo o CERT.br (2020) O *adware* é um programa feito para disseminar grandes quantidades de anúncios sem a autorização do usuário, geralmente na web ou em programas sendo instalados na sua máquina.

Sendo assim, o *adware* tem como função jogar anúncios na tela do computador do indivíduo, na maioria das vezes no navegador web coletando informações do comportamento do usuário.

4.6.5 *Worms*

São programas maliciosos que geralmente distribuem cópias, ou seja, se replicam várias vezes, com o intuito de explorar vulnerabilidades, mas também de infectar os sistemas em diversos locais.

Segundo CERT.br (2020):

> *Worm* é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores. *Worms* são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

Portanto, o *worms* vem se multiplicando atualmente, pois se propagam rapidamente sem que a vítima tenha controle sobre este, deste modo assim que contaminam a máquina do usuário o programa malicioso cria cópias de mesmo várias vezes se espalhando por locais do sistema para roubar informações sigilosas.

4.6.6 *Trojan*

Também chamado de cavalo de troia, este *malware* vem disfarçado de *software* legítimo, induzindo o usuário a baixá-lo, também sendo iniciado junto com o sistema do usuário, visando controlar, espionar e roubar informações sigilosas da vítima atacada.

De acordo com CERT.br (2020):

> Cavalo de troia, *trojan* ou *trojan-horse*, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Exemplos de *trojans* são programas que você recebe ou obtém de *sites* na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para serem instalados no computador. *Trojans* também podem ser instalados por atacantes que, após invadirem um computador, alteram

> programas já existentes para que, além de continuarem a desempenhar as funções originais, também executam ações maliciosas.

Portanto, o *trojan* tem por finalidade enganar os usuários através de arquivos e programas camuflados que a seus olhos parecem inofensivos, mas que estão infectados com códigos maliciosos que controlam a máquina do indivíduo ou roubam informações sigilosas e repassam a um terceiro.

4.6.7 *Ransomware*

Este é um tipo de *malware* que bloqueia o acesso ao sistema infectado ou arquivo infectado e cobra um resgate geralmente em criptomoedas, dificultando o rastreamento do indivíduo malicioso responsável pelo ataque. Criptomoedas é um tipo de moeda virtual usada para forma de pagamento, transações comerciais, meios de troca e reserva de valor, mas que não é usada e nem regulamentada pelo governo.

De acordo com CERT.br (2020):

> O *ransomware* é um programa malicioso que torna inacessíveis os dados que estão armazenados em dispositivos usando criptografia para não permitir que o dono da informação tenha acesso a esta e exigindo pagamento de resgate para liberar o acesso à vítima.

Dessa maneira, o *ransomware* tem por finalidade infectar a máquina da vítima atacada através de códigos maliciosos, bloqueando o acesso a arquivos com informações sigilosas de grande importância para o usuário ou instituição atacada e depois exigindo um resgate para desbloqueá-lo.

4.6.8 DOS - Ataque de negação de serviço

O ataque de negação de serviço (*Denial of service*) é um tipo grande de investida contra servidores e recursos de rede, este usa várias requisições enviando múltiplas solicitações para recursos web deixando instável e inacessível diversos sistemas de instituições públicas e privadas quando invadidas.

De acordo com a Cloudflare(2022):

> O ataque de negação de serviço-DOS tem por objetivo deixar inoperante os serviços de um sistema hospedado em um servidor, redes e deixá-los sobrecarregados com um número de requisições(pacotes) enviados via internet para a vítima.

Para que um ataque de negação de serviço funcione é necessária uma máquina poderosa que possa disseminar ações contra vulnerabilidades ou falhas na máquina da vítima e enviar mensagens em massa até que se esgote todos os recursos do indivíduo que está sendo atacado.

4.6.9 DDoS - Ataque de negação de serviço distribuído

O ataque de negação distribuída (*Distributed Denial of Serv*ice) tem por objetivo deixar indisponível os recursos de uma máquina ou sistema da vítima atacada, porém para que este funcione é necessário um grupo de máquinas infectadas enviando mensagens em massa contra o seu alvo.

De acordo com a Cloudflare(2022):

> O ataque de negação de serviço distribuído utiliza de uma rede com várias máquinas *zumbis* enviando solicitações para servidores *web* que excedem o seu limite de processamento, deixando os recursos do sistema indisponíveis.

Diante disso, pode- se dizer que este ataque são mais comuns atualmente e muito prejudiciais para instituições que trabalhem com um grande fluxo de informação, pois quando o invasor ataca seu sistema utilizando uma ou várias máquinas infectadas, ocorre um grande fluxo de requisições enviadas para o servidor atacado deixando congestionado o sistemas e serviços inacessíveis para os usuários da web.

4.6.10 *Rootkit*

É um tipo de *software* malicioso usado por cibercriminosos para obter controle sobre a máquina ou rede atacada, sendo geralmente usada através de programas, arquivos ou de fontes desconhecidas que estejam infectadas.

De acordo com o CERT.br(2020):

> O *rootkit* é um grupo de programas e técnicas que autoriza um indivíduo malicioso a permanecer na máquina do usuário comprometida, dando acesso ao seu dispositivo e privilégio para ver seus dados no sistema operacional ou software da vítima.

Assim sendo, o *rootkit* tem por objetivo se infiltrar no sistema operacional da máquina do usuário ou a um software que este usa para obter acesso privilegiado para roubar informações que a vítima usa para compras como cartão de crédito ou disseminar ataques e mensagens falsas para outros indivíduos.

4.7 Tecnologias e Técnicas de Defesa

4.7.1 *Firewall*

O *firewall* é um sistema de segurança muito utilizado por organizações e instituições públicas ou privadas que visam proteger o tráfego de dados da sua rede na entrada e saída do tráfego de pacotes até a internet com base em um conjunto de regras de defesa para assegurar o bom funcionamento das máquinas que estão interligadas pela rede local até a web.

Este permite que usuários não autorizados sejam impedidos de acessar a rede, fazendo o exame de todo o pacote de informações desta, vendo se está ou não na lista aprovada.

O f*irewall* ajuda a ligar a rede interna da instituição com a internet de modo seguro. Também são responsáveis por fazer a filtração dos pacotes utilizando o endereçamento *IP, TCP ou UDP.*

De acordo com Tanenbaum (2020):

> São usadas quatro técnicas gerais pelos firewalls para controle de acesso e política de segurança de uma rede:Controle de serviço: Define os serviços que podem entrar e sair da rede interna para a Internet; Controle de direção: Define em qual direção as solicitações de serviço podem iniciar e passar pelo firewall; Controle de usuário: Define o controle de acesso a serviços conforme os usuários que o estão acessando; Controle de comportamento: Define como determinados serviços são utilizados dentro da rede.

O administrador que controla a rede da organização configura o *firewall* com base na política de segurança definida por esta, podendo estabelecer regras como o bloqueio de sites e serviços ou estabelecer uma quantidade de largura de banda que sua máquina irá consumir.

4.7.2 DMZ - Zona desmilitarizada

A *Demilitarized Zone ou* zona desmilitarizada faz parte do sistema de segurança da instituição que se encontra fora dos limites de segurança estabelecidos. É uma rede que provê a comunicação entre a rede interna com outra rede externa não confiável na internet.

De acordo com Tanenbaum(2020):

> A zona desmilitarizada tem como finalidade filtrar o tráfego de dados que sai da porta tcp da rede interna da instituição até a internet, usando regras que assegurem a proteção das máquinas internas até o servidor web usado para fazer as requisições com os serviços hospedados.

Portanto, a zona desmilitarizada permite que se faça um método de acesso das máquinas da rede interna para outra rede externa, garantindo que caso alguma máquina seja comprometida, a estrutura da rede vai permanecer intacta e segura contra alguma anormalidade ou ataque pela porta tcp usada.

4.7.3 Sistema de detecção de intrusos - IDS

Também chamado de sistema de detecção de intrusão, é muito usado para analisar e identificar arquivos de logs e tráfegos de pacotes pelo *firewall*, servidores ou dispositivos conectados à rede. São usados para examinar tentativas externas de invasão, em tempo real emitindo um alerta caso haja quebra na segurança da rede para o administrador do sistema e tomar medidas para cessar a ação de possíveis ameaças à segurança que possam infringir os fundamentos de proteção de dados.

Para Torres (2018) o IDS pode ser classificado em:

> NIDS (Network Intrusion Detection System, sistema de detecção de intrusos na rede): este sistema é instalado na rede e analisa todos os pacotes e tenta detectar ataques do tipo negação de serviço (DoS, Denial of Service; tipo de ataque onde uma enorme quantidade de pedidos é enviada a um determinado serviço, na esperança de sobrecarregá-lo e deixá-lo inoperante), varredura de portas (a primeira coisa que um hacker faz ao analisar um potencial alvo de ataque é fazer uma varredura para ver quais portas TCP/UDP estão abertas, isto é, aceitando conexões) e tentativas de ataque. É normalmente instalado na DMZ..

PIDS (*Protocol-Based Intrusion Detection System*, sistema de detecção de intrusos baseado em protocolo): sistema IDS que conhece fundamentalmente um determinado protocolo e analisa o tráfego deste protocolo. Por exemplo, pode ser instalado entre o servidor web e a rede (ou dentro do servidor web, caso seja montado por *software*), analisando o protocolo HTTP. Com isso qualquer anomalia será detectada rapidamente.

HIDS (*Host-Based Intrusion Detection System*, sistema de detecção de intrusos baseado na máquina): sistema IDS que analisa o comportamento interno de uma máquina, a fim de detectar qualquer anomalia.

4.7.4 Sistema de prevenção de intrusos - IPS

O IPS é um sistema de prevenção de intrusos que trabalha em conjunto com o IDS, pois quando é detectado alguma anomalia ou ataque pelo tráfego da rede é tomada ações que visam barrar pacotes perigosos.

De acordo com Kurose e Ross (2013) os sistemas de prevenção de intrusão (IPS) são semelhantes a um IDS, exceto pelo fato de bloquearem pacotes além de criar alertas.

Portanto, o IPS é um sistema de prevenção de intrusos muito eficaz, pois é capaz de fazer a identificação e fazer a análise do perigo que este representa para a instituição, além disso enviar um alerta para o administrador da rede e fazer o controle preventivo contra ciberataques detectados atuando em conjunto com outros sistemas de proteção como *firewall* e IDS.

Os *logs* do sistemas são registros de todos os eventos gerados é considerado uma medida básica do sistema de informação. Desde a inicialização do sistema

operacional da máquina os logs de evento começam a ser gravados, portanto, assim como o *windows, linux ou macOS*, ao acessar os registros é possível observar horário, data e o acompanhamento do kernel, assim como erros ou ação executada por terceiros.

Os *logs* de evento do sistema operacional são registros com uma cronologia de acontecimentos com data, hora e carregamento do *kernel* mostrando erros e ações executadas durante a sua inicialização até seu encerramento. (HOSTMÍDIA, 2022).

Sendo assim, os logs de eventos têm um papel essencial na segurança da informação, pois eles contêm os registros de todas as atividades do sistemas ou fluxo de informações, sendo extremamente útil para identificação de atacantes e exploração das falhas que permitiram invadir o sistema.

4.8 Criptografia

A segurança em redes de computadores é um assunto muito abrangente dentro de instituições públicas ou privadas que incluem diferentes problemas que podem ocorrer no presente ou futuro. De certo modo preocupa-se em impedir que indivíduos mal-intencionados tenham acesso às mensagens trocadas entre um emissor e o seu destinatário com o emprego de criptografia.

A criptografia protege as informações com algoritmos ou chaves para que só possam ser decifradas por pessoas autorizadas a ver a mensagem que foi enviada do emissor para o seu destinatário.

De acordo com Kurose Ross(2013, p. 498):

> Na segurança de redes são usadas técnicas para prover sigilo, autenticação e integridade de mensagens são baseadas em fundamentos da criptografia. Eles também definiram em quatro propriedades: confidencialidade, integridade da mensagem, autenticação do ponto final e segurança operacional.

As técnicas usadas com criptografia não permitem que indivíduos tenham acesso ao conteúdo da mensagem enviada da origem até seu destino final, pois concedem ao remetente disfarça as informações de forma que um invasor não seja capaz de decodificar os dados interceptados.

4.8.1 Assinatura digital

As assinaturas digitais é um método muito eficaz para fazer a autenticação de documentos eletrônicos nos meios virtuais. Esta utiliza chaves criptográficas com assinaturas digitais para identificar o indivíduo que assinou e proteger as informações juridicamente.

Segundo Tanenbaum (2020) a assinatura digital deve constar a autenticidade das informações de documentos em que o indivíduo que assinou e enviou para seu destinatário seja o verdadeiro dono.

As assinaturas digitais são um método que vem sendo bastante utilizado na segurança da informação por várias instituições públicas do Brasil, pois com base em chaves criptografadas pode se garantir a autenticidade da mensagem enviada do remetente até seu destinatário.

4.8.2 Email seguro

O correio eletrônico ou e-mail é um tipo de ferramenta da web muito eficaz para enviar mensagens, fazer compartilhamento de informações e arquivos através da internet, mas é sempre importante manter suas informações seguras principalmente quando vocẽ recebe mensagens e propagandas enganosas na sua caixa de mensagem.

Segundo Kurose Ross(2020):

> manter o e-mail seguro requer um sistema que seja eficaz para garantir a autenticidade das informações enviadas pelo indivíduo que enviou para o destinatário e a integridade da mensagem sem que esta tenha sofrido qualquer alteração ao longo do caminho percorrido.

Desta maneira, o *email* deve ser protegido devido ao grande fluxo de dados confidenciais que são enviados de um indivíduo para outro, pois este é usado como um meio de propagação de diferentes tipos de golpes e códigos maliciosos que permitem ao atacante acessar a máquina do usuário.

4.8.3 Antivírus

Os antivírus verificam a existência de ameaças em todas as pastas e arquivos do computador ou programas da máquina do usuário, podendo ser programado para tomar ações como limpeza quando algum malware é encontrado.

De acordo com kurose Ross(2013):

> O antivírus tem papel fundamental na máquina do indivíduo, pois faz a identificação e proteção com ações que são tomadas automaticamente contra ameaças virtuais sendo muito utilizado para resguardar a integridade das informações do indivíduo contra formas de roubo de dados por códigos maliciosos e malwares.

Portanto, o antivírus tem se tornado muito relevante para a proteção de dispositivos, pois além de fazer a proteção contra os mais diversos tipos de ameaças existentes no mundo virtual, ajuda o usuário a tomar medidas contra arquivos, mídias infectáveis e programa maliciosos que tenham como objetivo roubar informações sigilosas da pessoa.

4.8.4 Plano de contingência

Atualmente a informação é um ativo muito importante para as instituições no mundo, sabendo que documentos, um dado tem um alto grau de privacidade e necessário proteger com o máximo rigor estas informações sensíveis. Ter um plano de contingência dentro da instituição é muito importante, pois caso o seu sistema fique fora do ar será possível restabelecer o seu funcionamento com outros meios para que o seu funcionamento esteja disponível o tempo todo ou caso falte energia ter um gerador por exemplo seria algo de extrema importância para a continuidade das suas atividades e serviços.

> Quando uma violação de dados ocorre, um plano de contingência definido ajuda não apenas a manter os funcionários calmos, mas também a alertá-los quanto à importância dos procedimentos estabelecidos e orquestração das atividades para retomar o negócio da empresa e mitigar os efeitos do incidente (MOREIRA, 2016).

Para instituições grandes e que trabalhem com um grande fluxo de informações tornou-se alvo preferencial de hackers em várias partes do mundo que querem dados sigilosos para vender ou vazar na *web*, por isso acabou se tendo como obrigatoriedade ter um plano de contingência, sistemas de monitoramento e profissionais qualificados que terão a tarefa de proteger e garantir a integridade das informações da organização.

Sendo assim, ter um plano B é de suma importância para a organização, pois caso haja alguma anormalidade dentro dos seus serviços, a equipe ou sistema de monitoramento de tecnologia da informação irá fazer todo o possível para manter o sistema e a integridade das informações seguras.

4.8.5 *Backup*

O termo *backup* é um nome que faz referência a fazer cópias de segurança do sistema e seus dados, para que possam ser restaurados caso algum incidente com perdas das informações aconteça.

Nas instituições públicas é importante manter um sistema de backup de arquivos, documentos e dados de modo que haja um planejamento caso algum incidente aconteça no presente ou futuro como plano de contingência se porventura hackers invadirem seus sistemas e apagar arquivos importantes. Existem vários tipos de backups que vão implementar o salvamento de dados de instituições com diferentes formas que serão citados abaixo.

4.8.5.1 *Backup* completo

O backup completo é usado para a restauração de arquivos perdidos ou danificados, sendo empregado facilmente no sentido de localizar documentos da instituição. Embora seja usado para recuperar grande parte das informações, possui a desvantagem de fazer cópias dos arquivos em um grande espaço de tempo.

Segundo Macêdo (2012):

> O *backup* completo é simplesmente fazer a cópia de todos os arquivos para o diretório de destino (ou para os dispositivos de backup correspondentes), independente de versões anteriores ou de alterações nos arquivos desde o último backup. Este tipo de backup é o tradicional e a primeira ideia que vem à mente das pessoas quando pensam em *backup:* guardar TODAS as informações.

O *backup* completo serve para todos os tipos de arquivos, informações e como citado pelo autor acima este não muda independente das versões ou alterações do último *backup*.

4.8.5.2 *Backup* incremental

O *backup i*ncremental é o tipo mais eficiente para salvar dados, pois este tem por objetivo guardar somente aqueles arquivos que foram modificados desde o último backup. Embora salve somente os dados desde a última modificação, o backup incremental opera em cima do *backup* completo, pois será feito a cópia somente dos arquivos alterados.

De acordo com Macêdo (2012):

> Os *backups* incrementais primeiro verificam se o horário de alteração de um arquivo é mais recente que o horário de seu último *backup.* Se não for, o arquivo não foi modificado desde o último *backup* e pode ser ignorado desta vez. Por outro lado, se a data de modificação é mais recente que a data do último *backup,* o arquivo foi modificado e deve ter seu *backup* feito. Os backups incrementais são usados em conjunto com um backup completo frequente (ex.: um backup completo semanal, com incrementais diários).

Em vista disso, o *backup* incremental é uma forma muito importante de salvar as informações da organização, pois permite resguardar somente os dados alterados em relação à última rotina executada sendo mais rápido e usado pouco armazenamento.

4.8.5.3 *Backup* diferencial

O *backup* diferencial tem seu funcionamento parecido com o incremental. Ambos têm o modo de salvar as cópias dos arquivos somente daqueles que foram

alterados, mas a principal diferença é que o *backup* diferencial faz um mapeamento das modificações feitas no backup completo.

De acordo com Macêdo (2012):

> Como o *backup* diferencial é feito com base nas alterações desde o último *backup* completo, a cada alteração de arquivos, o tamanho do *backup* vai aumentando, progressivamente. Em determinado momento pode ser necessário fazer um novo *backup* completo, pois nesta situação o *backup* diferencial pode muitas vezes ultrapassar o tamanho do *backup* integral.

Assim sendo, o *backup* diferencial permite fazer a preservação dos dados, salvando apenas a diferença das informações que foram coletadas desde a última cópia de segurança do *backup* completo.

4.8.6 Protocolos de segurança da informação

4.8.6.1 SSL - *Secure sockets layer*

SSL foi o primeiro protocolo de criptografia a ser criado ele permite a comunicação criptografada entre servidor e navegador através da autenticação feita por ambas as partes.

Segundo Tanenbaum (2020, p.534) O SSL constrói uma conexão segura entre dois soquetes, incluindo: negociação de parâmetros entre cliente e servidor; autenticação mútua de cliente e servidor; comunicação secreta; proteção da integridade dos dados.

Portanto, o SSL permite criar uma camada de segurança em sites evitando que os dados do usuário não sejam capturados por terceiros durante a sua transferência até o servidor que está hospedando o site acessado.

4.8.6.2 TLS - *Transport layer security*

TLS é uma versão mais segura e atualizada do SSL fornecendo mais segurança na comunicação com a internet e aplicativos cliente servidor de forma mais confidencial através de técnicas criptográficas simétricas e assimétricas.

O protocolo TLS (T*ransport Layer Security*, segurança da camada de transporte) é um dos protocolos usados para criptografar dados não criptografados transferidos pelo protocolo HTTP que podem ser capturados por hackers (TORRES, 2018).

Deste modo, o TLS cria uma camada a mais de proteção quando se está navegando pela *web* protegendo a comunicação entre servidor e navegadores garantindo a privacidade e integridade dos dados entre os recursos computacionais ao se comunicarem.

4.8.6.3 VPN - *Virtual private network*

VPN faz uso de uma rede já existente, normalmente a internet, a fim de permitir a troca de informações entre redes geograficamente separadas como se estivessem na própria rede da empresa. Os dados são efetivamente protegidos – garantindo assim a sua integridade, autorização e autenticidade – enquanto são enviados.

De acordo com Kurose Ross(2020):

> A rede privada virtual(VPN) é muito utilizada dentro das organizações, pois estabelece uma conexão da rede interna ao acessar através de redes públicas criptografando o tráfego de dados e ocultando a identidade do usuário tornando mais difícil o rastreamento das suas atividades por indivíduos mal-intencionados.

Deste modo, a rede privada virtual é de extrema importância para a segurança da organização, pois além de estabelecer uma conexão segura fora desta, ajuda a proteger os dados e atividades dos indivíduos nos meios digitais da Internet.

4.9 Profissionais de segurança da informação

O profissional de segurança da informação vai monitorar toda a rede de computadores, disponibilizando recursos, identificando as vulnerabilidades existentes nos servidores dos órgãos, aplicações e medidas a serem tomadas para

inibir o roubo de informações garantindo a integridade e autenticidade dos dados disponibilizados pelo seu sistema de TI.

De acordo com Cabral e Caprino (2015, p.15):

> defendem que a qualificação é um fator chave para a determinação da qualidade dos profissionais, especialmente dos que irão se dedicar à Segurança em TI, afirmando que “essa é uma discussão que poderia ser bastante alongada, possivelmente levantando pontos nos quais mercados e academia poderiam interagir de forma eficiente para uma melhor definição das necessidades da formação de profissionais de segurança de TI”.

Com o advento da indústria 4.0 ou quarta revolução industrial, novas tecnologias estão surgindo e o profissional da área de segurança de TI precisa estar atento a novas formas de automação e proteção de dados, pois as empresas sempre buscam os melhores recursos tanto de *hardware* e *software* para seus sistemas de redes de computadores, então tendo em vista isso deve-se buscar forma de obter o conhecimento prévio sobre isto, dedicando seu conhecimento para implementação de novos sistemas no futuro.

4.10 Dados pessoais

Os dados pessoais são informações que identificam um indivíduo na sociedade como pessoa natural para saber que está vivo e tendo seus direitos, deveres assegurados pelas legislações brasileiras.

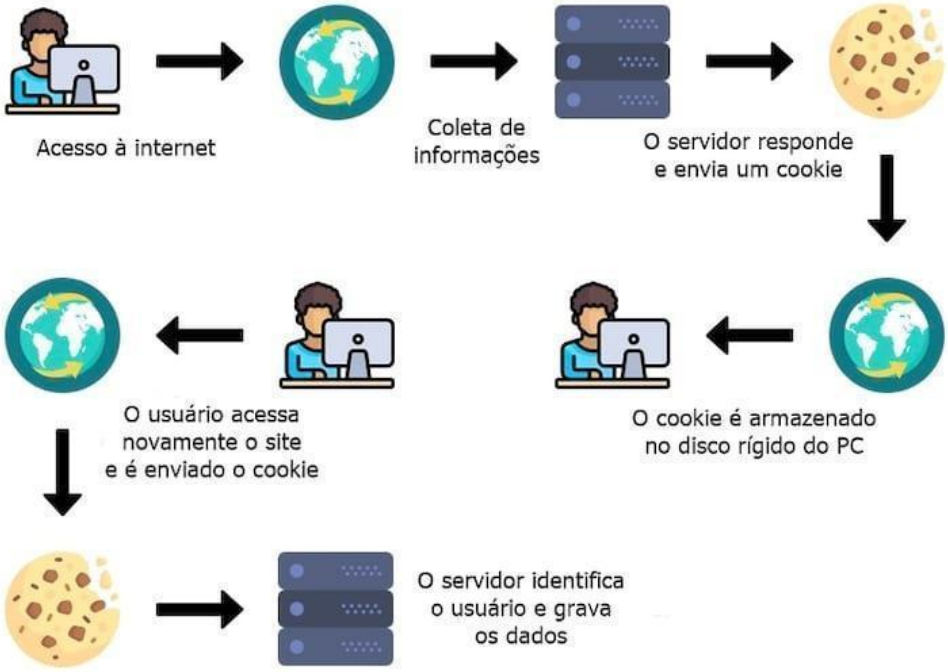
Os dados pessoais são considerados direta ou indiretamente ao indivíduo que esteja vivo sendo identificado com RG, CPF, endereço residencial, dados bancários, origem, raça, gênero e religião (LGPD, 2020).

Os dados são usados pelos indivíduos para fazer cadastro em diversos sites e plataformas para registrar e processar seu login de usuário, mas devido ao armazenamento e processamento dessas informações por terceiros é importante estar atento aos riscos existentes em certas plataformas ao se cadastrar.

4.10.1 *Cookies*

Os *cookies* são arquivos gerados por sites e plataformas visitadas e que são salvos na máquina do usuário quando este utiliza o navegador. Os arquivos salvos servem para a identificação da pessoa que visita o site para personalizar a página acessada de acordo com o perfil do usuário ou facilitar a movimentação de informações entre páginas de um mesmo website.

Figura 3 - O que são Cookies



Fonte: Oficina da Net(2019)

De acordo com a figura 3**,** o navegador por padrão salva os seus dados em um método de armazenamento a curto prazo, fazendo com que este se lembrou das suas informações inseridas ao navegar pela Internet, como as informações que o usuário usa para fazer login em plataformas e sites.

4.11 Instituto Federal do Amapá

Segundo o Ministério da educação - MEC (2008) Os Institutos Federais são instituições, pluricurriculares e multicampi (reitoria, campus, campus avançado, polos de inovação e polos de educação a distância), especializados na oferta de educação

profissional e tecnológica (EPT) em todos os seus níveis e formas de articulação com os demais níveis e modalidades da Educação Nacional, oferta os diferentes tipos de cursos de EPT, além de licenciaturas, bacharelados e pós-graduação stricto sensu.

Art. 6º Os Institutos Federais têm por finalidades e características:

> I - ofertar educação profissional e tecnológica, em todos os seus níveis e modalidades, formando e qualificando cidadãos com vistas na atuação profissional nos diversos setores da economia, com ênfase no desenvolvimento socioeconômico local, regional e nacional;
> II - desenvolver a educação profissional e tecnológica como processo educativo e investigativo de geração e adaptação de soluções técnicas e tecnológicas às demandas sociais e peculiaridades regionais;
> III - promover a integração e a verticalização da educação básica à educação profissional e educação superior, otimizando a infra-estrutura física, os quadros de pessoal e os recursos de gestão;
> IV - orientar sua oferta formativa em benefício da consolidação e fortalecimento dos arranjos produtivos, sociais e culturais locais, identificados com base no mapeamento das potencialidades de desenvolvimento socioeconômico e cultural no âmbito de atuação do Instituto Federal;
> V - constituir-se em centro de excelência na oferta do ensino de ciências, em geral, e de ciências aplicadas, em particular, estimulando o desenvolvimento de espírito crítico, voltado à investigação empírica;
> VI - qualificar-se como centro de referência no apoio à oferta do ensino de ciências nas instituições públicas de ensino, oferecendo capacitação técnica e atualização pedagógica aos docentes das redes públicas de ensino;
> VII - desenvolver programas de extensão e de divulgação científica e tecnológica;
> VIII - realizar e estimular a pesquisa aplicada, a produção cultural, o empreendedorismo, o cooperativismo e o desenvolvimento científico e tecnológico;
> IX - promover a produção, o desenvolvimento e a transferência de tecnologias sociais, notadamente as voltadas à preservação do meio ambiente.

O Instituto Federal do Amapá, com CNPJ 10.820.882/0001-95, fica localizado na rodovia BR-210, km 3, s/n-Brasil Novo, AP, 68909-398, é uma instituição de educação, ciência e tecnologia que oferta ensino superior, básico e profissional seguindo a política de atuação da rede federal de educação, ciência e tecnologia, ofertando cursos em diferentes modalidades de ensino desenvolvendo o conhecimento dos seus alunos.A história do Ifap se resume a criação da escola técnica federal do amapá(Ifap), autorizada pela Lei nº 11.534, foi organizada pela portaria do MEC nº 1066 que atribuía a competência ao centro federal de educação tecnológica do Pará (cefet/pa) o encargo de implementar a Etfap. Sendo esta dirigida através da portaria do MEC nº 1199, de 12 de dezembro de 2007, nomeando o professor Emanuel Alves de Moura para exercer o cargo de Diretor Geral

temporariamente.Na data de 29 de dezembro de 2008, a Lei 11.892, institui a rede federal de Educação, Ciência e Tecnologia do Amapá (IFAP)-sendo esta uma autarquia federal vinculada ao Ministério da Educação, tendo autonomia administrativa, patrimonial, financeira, disciplinar e didático-pedagógica conforme prever as outras instituições Federais do Brasil. No ano de 2015 o Ifap, realizou sua primeira consulta pública para a escolha do gestor que iria comandar a instituição de ensino, sendo eleita a professora Marialva do Socorro Ramalho Oliveira de Almeida, sendo reeleita em 2019 para um mandato até 2023. (Fonte: IFAP, 2019).

5 METODOLOGIA

O presente projeto utilizou-se do método de pesquisa bibliográfica que tem como intuito analisar os fatores do problema existente por meio de livros, artigos e periódicos sobre segurança da informação relacionada a ataques virtuais e vazamentos de dados nas Instituições Públicas e estudo de caso para analisar os principais fenômenos relativos a segurança dos alunos nos laboratórios de informática do Instituto Federal do Amapá.

Segundo Marconi e Lakatos (1992):

> A pesquisa bibliográfica é o levantamento de toda a bibliografia já publicada, em forma de livros, revistas, publicações avulsas e imprensa escrita. A sua finalidade é fazer com que o pesquisador entre em contato direto com todo o material escrito sobre um determinado assunto, auxiliando o cientista na análise de suas pesquisas ou na manipulação de suas informações. Ela pode ser considerada como o primeiro passo de toda a pesquisa científica.

Os dados foram coletados por meios de livros, artigos, dissertações estudados por autores da área de segurança da informação e análise dos fatores de riscos, inclusive toda a infraestrutura de proteção do SELABI para o gerenciamento dos laboratórios.

A cartilha foi elaborada com base em diversos autores e instituições que desenvolvem métodos e boas maneiras sobre segurança da informação para indivíduos sem o prévio conhecimento sobre a proteção dos dados na internet. Também foi desenvolvida com base em modelos do Centro de estudos, resposta e tratamento de incidentes de segurança do Brasil que monitora e divulga estatísticas sobre problemas nas redes conectadas à Internet do Brasil.

A cartilha de boas práticas em segurança da informação foi desenvolvida através do google docs sendo utilizado para colocar as informações, formatar e a utilização do google para buscar imagens, modelos de cartilhas e plataformas de design como o Canvas.

Na plataforma de design gráfico canvas foi utilizado diversos recursos para a estilização da cartilha com imagens, símbolos e fontes que deram uma aparência significativa no resultado final deste manual de boas práticas. O gerador de senhas foi elaborado e desenvolvido através da plataforma visual studio code com as

linguagens: HTML usado para fazer o esqueleto do projeto, CSS utilizado para a estilização e JAVASCRIPT que deu a interação com o objeto.

6 RESULTADOS E DISCUSSÃO

6.1 Laboratórios de informática - Campus macapá

O Instituto Federal do Amapá - *Campus* Macapá possui vários laboratórios de informática que são distribuídos entre o prédio principal e o ginásio para os alunos usarem para pesquisa, trabalhos acadêmicos, ensino e aprendizagem auxiliando na procura de informações na internet e o uso de ferramentas instaladas na máquina.

Laboratórios analisados:

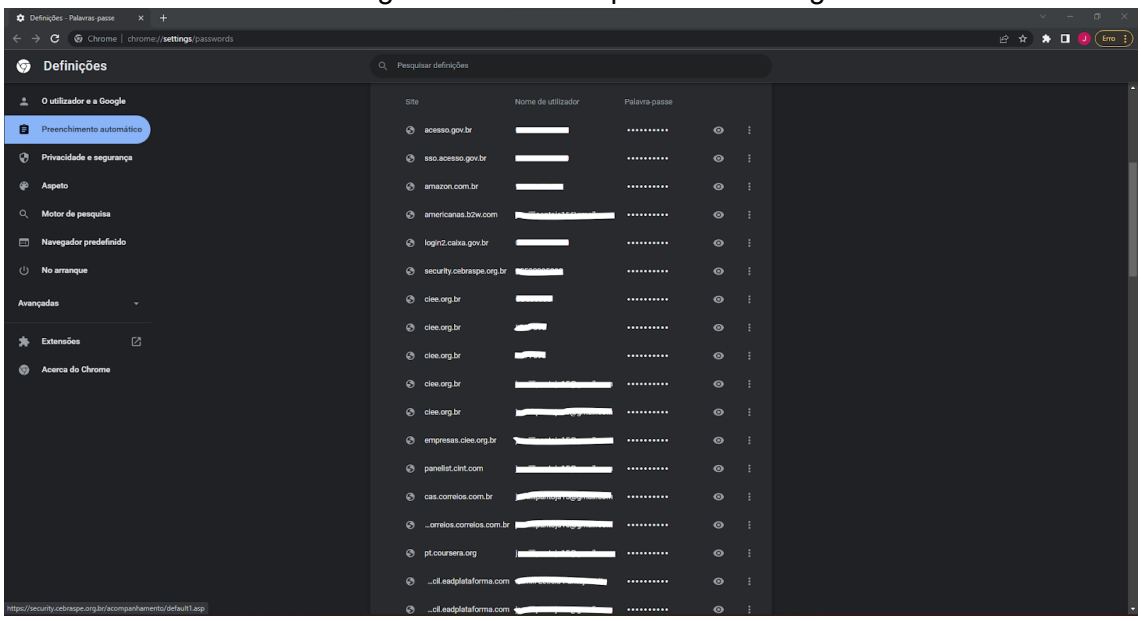
- Laboratório de Informática 1;
- Laboratório de Informática 3;
- Laboratório do Ginásio 1;
- Laboratório do Ginásio 2.

É importante ressaltar que o uso dos laboratórios pelos estudantes é utilizado pela coletividade, ou seja, por todos os discentes do ensino médio e superior que precisam usar para pesquisar ou fazer trabalhos usando as ferramentas que estão disponibilizadas nos computadores.

O acesso ao navegador da *internet* é algo de extrema preocupação, pois muitos estudantes não tendo a consciência de que seus dados podem ficar salvos neste, acabam não removendo seu histórico e *e-mail* do *browser*. É algo bastante alarmante já que por padrão muitos navegadores salvam os dados do usuário como forma de facilitar o acesso a sites e plataformas da *web* para caso eles voltem a logar de novo nos meios de comunicação da internet não precise digitar novamente sua senha e usuário.

Conforme a figura 4, por padrão vários navegadores utilizam dos dados armazenados para facilitar o acesso quando o usuário estiver navegando na *internet* não precisar digitar as suas informações de login novamente para acessar determinada plataforma ou site. Entretanto, os dados pessoais ficam expostos no navegador gerando um ambiente de insegurança interna nos laboratórios de informática do Instituto Federal do Amapá, pois qualquer indivíduo de má fé poderá ver estas informações e utilizar para benefício próprio ou vazar na internet gerando um grande problema para os alunos proprietários destes dados.

Figura 4 - Dados expostos no navegador



Fonte: Dados da pesquisa(2022)

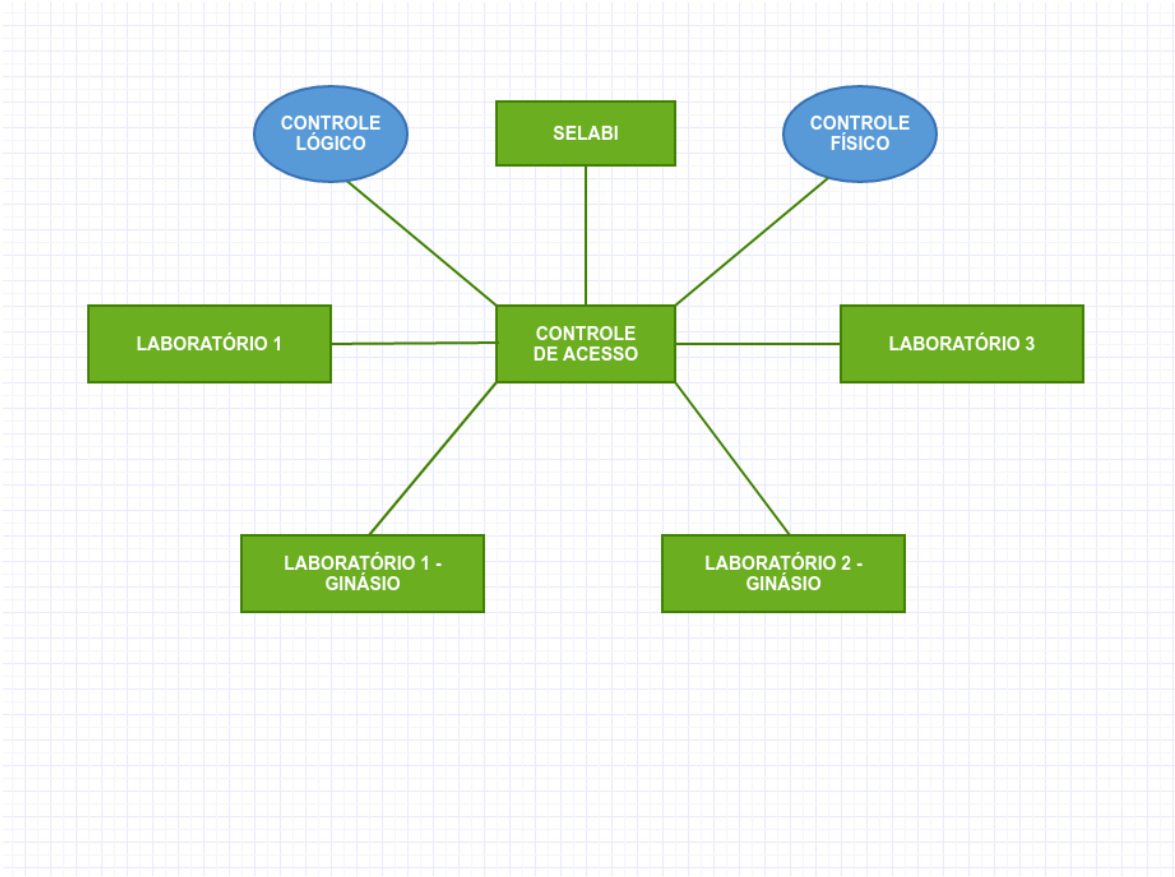
Os navegadores são um meio muito importante para acessar a Internet, fazer pesquisas e compartilhar arquivos, porém é importante evidenciar que sempre é importante ter cuidado ao compartilhar dados pela *web*, pois isto pode causar um dano muito grande caso algum indivíduo malicioso acesse a máquina do usuário e grave essas informações para benefício próprio ou divulgar sem o consentimento da vítima nos meios de comunicação.

Analisando os dados obtidos dos laboratórios de informática foram coletadas as seguintes informações:

Conforme a figura 5, o controle de acesso elaborado pelo respectivo setor que gerencia todos os laboratórios do IFAP - campus Macapá, se dá por meio de políticas que garantem a proteção dos alunos tanto no ambiente físico e lógico conforme a descrição abaixo.

6.2 Controle dos laboratórios

Figura 5 - Controle de acesso dos laboratórios



Fonte: Os autores(2022)

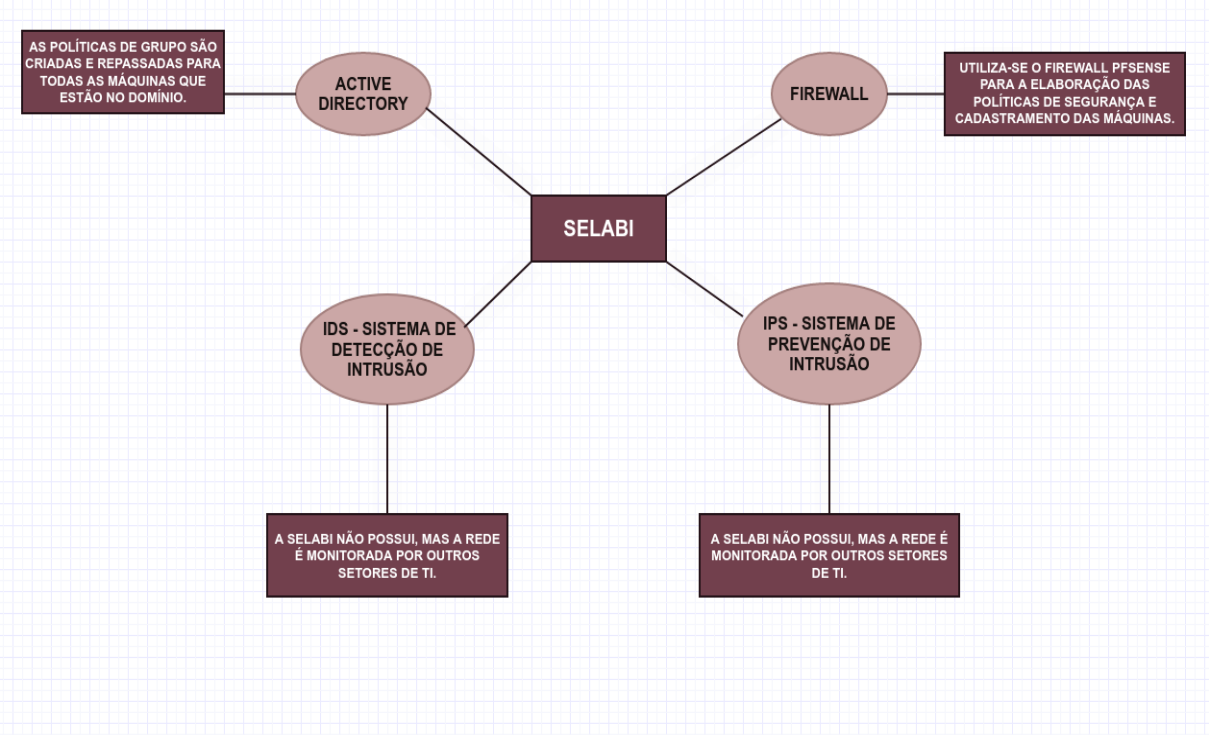
A figura 5, apresenta o meio Físico**,** onde os computadores dos laboratórios da instituição encontram-se separados pelos blocos de ensino do IFAP e no prédio principal e ginásio. O modo de acesso aos laboratórios é gerenciado pela Seção de Gerenciamento dos Laboratórios de Informática (SELABI) que só libera a entrada de alunos caso assinem uma lista de controle de acesso ou com a autorização do professor.

Ainda na figura 5, o meio Lógico é o acesso a máquina através de senha padrão para todos os alunos do IFAP - campus Macapá, que possam utilizar para os trabalhos acadêmicos, porém somente os administradores podem utilizar as máquinas para instalar aplicações ou serviços complexos que exigem alto nível de segurança.

6.3 Ferramentas de proteção e planos de contingência

Conforme a Figura 6, analisando o ambiente dos laboratórios da instituição foi observado que há uma política bem rigorosa de segurança estabelecida contra roubos de informações ou invasões pela rede. A SELABI faz o uso de ferramentas que controlam todo o acesso e monitoramento das máquinas dos laboratórios inspecionados, garantindo o total controle sobre estas e são listadas abaixo.

Figura 6 - Sistemas de proteção dos laboratórios



Fonte: Os autores(2022)

A figura 6, apresenta o *Firewall*, onde a instituição tem sua proteção variada pelos diversos setores de tecnologia do campus Macapá, porém os laboratórios são gerenciados pelo SELABI com o *firewall pfsense* que implementa as políticas de segurança do tráfego de dados da rede interna com a I*nternet,* além do controle de acesso com o cadastramento das máquinas neste servidor.

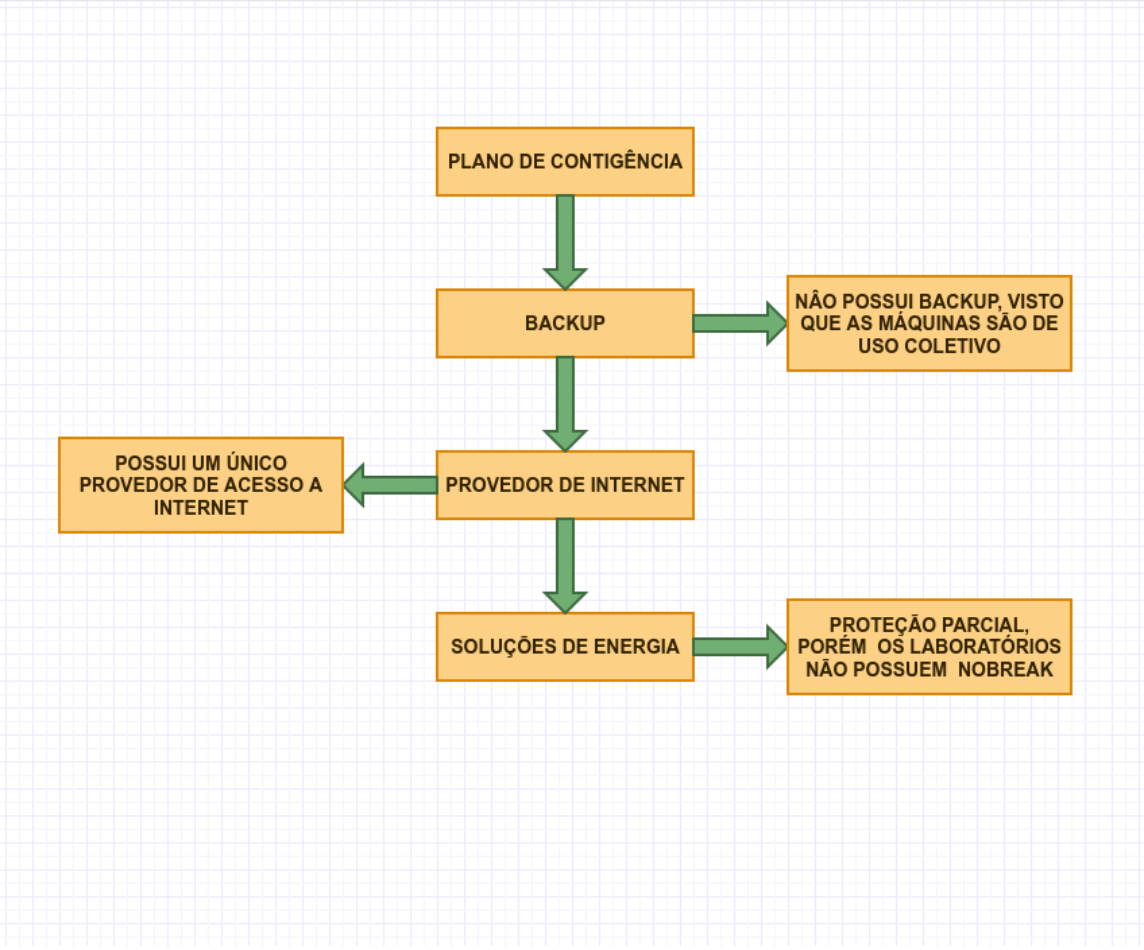
Conforme demonstrado na figura 6**,** o Sistema de Detecção de Intrusos(IDS), foi analisado e observado que nenhuma máquina ou os administrados possuem esta ferramenta, pois é usada por outro setor de TI da instituição.

O **Sistemas de Prevenção de Intrusos(IPS):** Conforme o disposto acima é uma ferramenta que está diretamente ligada ao IDS, então não se encontra em nenhuma máquina gerenciada pelo SELABI, porém deve estar sendo utilizada por outro setor de TI do campus - Macapá.

Active Directory(AD): As políticas de grupo são elaboradas pelo SELABI através do gerenciamento com o *Active Directory* no windows server 2012, assim sendo quando for implementada alguma política de segurança nova pelo administrador irá também para as contas de usuários cadastradas no domínio.

De acordo com a imagem 7, as máquinas e o setor responsável pelos laboratórios de informática informaram que não fazem *backup* dos dados presentes nesta, visto que é de uso coletivo dos alunos e professores, mas que somente é feito um clone de imagem com o sistema operacional feito pelo programa *Clonezilla.*

Figura 7 - Planos de contingência



Fonte: Os autores(2022)

Provedor de Internet: A instituição possui um provedor de internet único, mas que não garante 100% da disponibilidade de banda larga para o IFAP. O SELABI possui sua rede própria que é implementada via cabeamento e o *access point* para acesso via rede *wi-fi* para dispositivos móveis.

Soluções de Energia: Os computadores possuem uma proteção parcial contra problemas relacionados com a falta de energia nos laboratórios de informática. Entretanto, foi analisado e vistoriado que nenhum computador dos laboratórios possui *nobreak*, estabilizador ou filtro de linha para que poderiam evitar danos aos equipamentos caso houvesse queda de energia.

6.4 Análise dos fatores de riscos

Durante a análise dos laboratórios foram encontrados alguns fatores de segurança que podem se tornar um grande problema para os alunos da instituição como:

Navegadores: Foi analisado os navegadores padrões usados para acessar plataformas e sites da *web e* percebeu-se que muitos dos alunos ao utilizarem as máquinas acabam deixando os seus dados expostos no browser gerando assim um grande problema, pois como os computadores são de uso coletivo qualquer indivíduo que tenha acesso poderá ver essas informações.

Conscientização: Analisando todos os laboratórios em questão percebeu-se que nem todos os alunos têm o conhecimento devido sobre as ameaças e riscos ao utilizarem a Internet, muitos acabam baixando programas e arquivos de fontes desconhecidas na web que podem se tornar um grande problema para estes.

Senhas: Analisando os dados expostos nos navegadores observou-se que ambos não tinham uma senha de alta complexidade e que na maioria utilizavam as mesmas senhas para acessar sites e plataformas da *web*.

6.5 Soluções para o problema

Como a maioria das políticas de segurança é implementada pelo setor que gerencia todos os laboratórios de informática do IFAP - campus Macapá, propormos

duas soluções que irão focar na proteção dos alunos da instituição que serão abordados abaixo.

6.5.1 Cartilha sobre boas práticas em segurança

Esta cartilha é fruto de uma iniciativa dos acadêmicos do curso superior em redes de computadores, tendo em mente que nem todos têm o conhecimento relativo às boas práticas sobre segurança no uso de tecnologias como Internet e computadores do Instituto Federal do Amapá.

Portanto, neste manual propormos uma cartilha com assuntos relacionados a segurança da informação, ameaças e medidas que podem ser eficazes contra roubo de dados dos discentes do IFAP ao utilizar o laboratório de informática.

6.5.2 Resumo dos tópicos da cartilha

A cartilha contém os seguintes capítulos:

Capítulo 1 - Computadores

No primeiro capítulo mostra a importância de manter seu computador seguro, os problemas que podem ocorrer caso sua máquina esteja vulnerável, os riscos ao navegar na internet, golpes e medidas eficazes ao navegar no mundo virtual.

Capítulo 2 - Privacidade

No segundo capítulo buscou-se analisar a importância da proteção da privacidade do usuário nos meios digitais, os problemas ao ter sua privacidade exposta e como proteger suas informações

Capítulo 3 - Senhas

No capítulo 3 foi introduzido a importância dos dados do indivíduo nos meios de comunicação com senhas seguras, os riscos associados, problemas ao ter seus dados de usuário expostos e medidas eficazes para proteger suas informações nos meios digitais.

6.5.3 Gerador de senhas seguras

A importância de ter uma senha segura evita que seus dados sejam acessados ou decifrados por indivíduos mal-intencionados, mas que também ajuda na proteção ao navegar *web,* pois quanto mais difícil for a palavra-chave de usuário do indivíduo será quase impossível violar ou descobrir estas informações caso algum golpista ou hackers invade sua máquina.

O gerador de senhas funciona de maneira aleatória, caso você queira uma senha complexa poderá escolher o tamanho, caracteres com letras maiúsculas ou minúsculas, números e símbolos gerando palavras-chaves de alta complexidade para utilizar em sites e plataformas da *web*.

7 CONSIDERAÇÕES FINAIS

A segurança da informação de fato é uma das áreas mais importantes atualmente, pois globalmente estamos interconectados por longa distâncias podendo compartilhar informações via *Internet*, mas que é de grande relevância atentar-se para os meios digitais e seus perigos ao usar os dados de usuário para se cadastrar em sites ou plataformas, pois nem um sistema de defesa é 100% eficaz com roubos ou vazamentos de dados na web.

O trabalho foi elaborado no começo com o levantamento dos dados sobre segurança da informação por meio da metodologia bibliográfica que pode ajudar na análise dos principais assuntos abordados, tecnologias de defesa, ameaças e conceitos base para o andamento do trabalho de pesquisa a ser desenvolvido na instituição.

Analisando os laboratórios de informática pode-se perceber que a política de segurança desenvolvida pelo SELABI é bem rígida para mitigar os riscos lógicos e físicos, porém dando prosseguimento nesta análise foi feito o monitoramento das máquinas e descobriu-se que muitos dos alunos ao utilizarem os navegadores não davam a mínima importância de apagar seus dados salvos no browser correndo o risco de vazamento caso os computadores fossem hackeados ou algum indivíduo mal intencionado usa-se das informações pessoais dos discentes para benefício próprio.

Portanto, a segurança das informações dos alunos tornou-se algo muito importante nos laboratórios, pois nem todos têm a plena consciência dos riscos que estão sendo expostos por deixar seus dados salvos na máquina. Por isso, o desenvolvimento dos dois produtos: cartilha de segurança da informação e gerador de senhas seguras possibilita a conscientização sobre as boas práticas de proteção na Internet e a importância de ter senhas fortes para cadastrar nas plataformas, aplicativos e sites da *web*.

REFERÊNCIAS

ALVES, Gervânia**. Ciclo de Vida dos Dados e LGPD.** 2022. Disponível em:<https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgpd>. Acesso em: 23 de maio de 2022.

ASSIS e Mendes. **Histórico das Leis de Proteção de Dados e da Privacidade na Internet**. 2020. Disponível em:<https://assisemendes.com.br/historico-protecao-de-dados/>. Acesso em: 21 de setembro de 2021.

BRASIL. Ministério da Cidadania. **Lei Geral de Proteção de Dados (LGPD)**. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd>. Acesso em: 10 de outubro de 2022.

CLOUDFLARE. **Como fazer DDoS | Ferramentas de ataque de DoS e DDoS.** 2022. Disponível em:<https://www.cloudflare.com/pt-br/learning/ddos/ddos-attack-tools/how-to-ddos/>. Acesso em: 01 de Outubro de 2022.

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.br**. 2022. Disponível em:<https://www.cert.br/stats/incidentes/>. Acesso em 16 de Outubro de 2021.

CERT.br. **Cartilha de segurança para internet**. 2022. Disponível em: https://cartilha.cert.br/fasciculos/. 2022. Acesso em 21 de maio de 2022.

CABRAL, Carlos et. al.**Trilhas em Segurança da Informação:** Caminhos e ideias para a proteção de dados. Rio de Janeiro:Brasport, 2015.

DANTAS, Marcus. **Segurança da Informação:** Uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

ESR. **A importância da Segurança de Redes**. 2020. Disponível em:<https://esr.rnp.br/administracao-e-projeto-de-redes/open-9/>. Acesso em 03 de Abril de 2022.

ESR. **Segurança em Redes Sem Fio**. 2022. Disponível em:<https://esr.rnp.br/seguranca/seguranca-em-redes-sem-fio/. Acesso em: 08 de Abril de 2022.

FONTES, Edison. **Segurança da Informação:** O Usuário faz a diferença **.** São Paulo: Saraiva, 2006.

FONTES, Edison**. Políticas e Normas para a Segurança da Informação**. Brasport, 2012.

FILHO, Eduardo Tomasevicius. **Marco Civil da Internet:** Uma lei sem conteúdo normativo. Disponível

em:<https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?format=html&lang=pt#>. Acesso em: 06 de outubro de 2021.

GARRETT, Filipe. **O que significa Spam:** Veja como evitar no e-mail e nas redes sociais. 2020. Disponível em:<https://www.techtudo.com.br/listas/2020/07/o-que-significa-spam-veja-como-evitar-no-e-mail-e-nas-redes-sociais.ghtml>. Acesso em: 24 de Setembro de 2022.

G1. **Mega Vazamento de dados de 223 milhões de brasileiros:** o que se sabe e o que falta saber. 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 18 de Outubro de 2021.

GARRETT, Felipe. **O que é Deep Web ?**. 2019. Disponível em:< https://www.techtudo.com.br/noticias/2019/03/o-que-e-deep-web.ghtml>. Acesso em: 18 de outubro de 2021.

HOSTMÍDIA. **Logs do sistema operacional:** o que são e para que servem. 2022. Disponível em: <https://www.hostmidia.com.br/blog/logs-do-sistema-operacional/>. Acesso em: 24 de maio de 2022.

HINTZBERGEN, jule et al. **Fundamentos de segurança da informação**. São Paulo: Brasport, 2018

ISO. **Tecnologia da informação:** Técnicas de segurança – Sistemas de gerenciamento de segurança da informação - Visão geral e vocabulário. 2018. Disponível em:<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>. Acesso em: 14 de setembro de 2021.

ISO. **Segurança da informação:** segurança cibernética e proteção de privacidade – Controles de segurança da informação. 2022. Disponível em:<https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en>. Acesso em: 13 de Setembro de 2022.

INSTITUTO FEDERAL DO AMAPÁ. **Histórico**. Disponível em:< https://ifap.edu.br/index.php/quem-somos/historico#:~:text=A%20hist%C3%B3ria%20do%20Instituto%20Federal,encargo%20de%20implantar%20a%20 Letfap.> . Acesso em: 10 de outubro de 2021.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria**. Metodologia do trabalho científico**. São Paulo: Editora Atlas, 1992. 4. ed. p.43 e 44.

KUROSE, J. F. e ROSS, K. **Redes de computadores e a internet:** Uma abordagem top down**.** Pearson education do Brasil. 6° edição. São Paulo: Pearson, 2010.

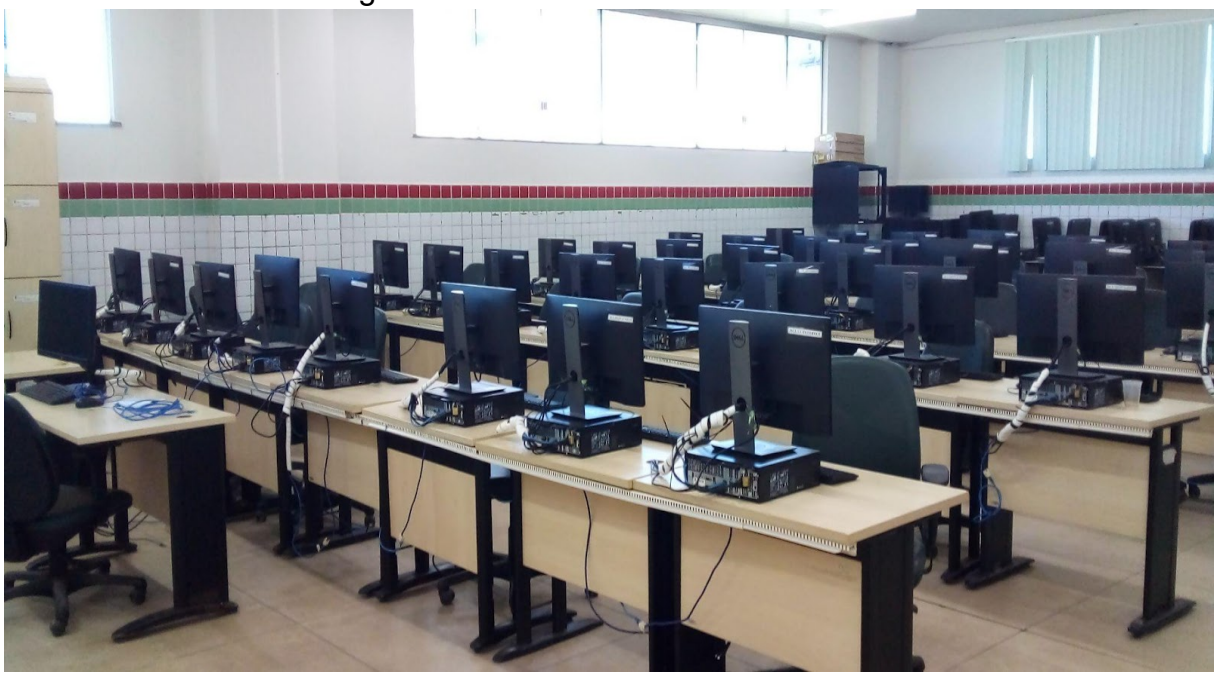
RNP. **RNP lança relatório anual de segurança**. 2021. Disponível em:<https://www.rnp.br/noticias/rnp-lanca-relatorio-anual-de-seguranca-2020>. Acesso em: 21 de setembro de 2021.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall. 2011.

TENÓRIO, Pedro; JUNQUEIRA, Wagner. **Segurança da Informação:** uma visão sistêmica para implementação em organizações. Livro Digital. Disponível em:<http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/downlo%20ad/209/75/905-1?inline=1>. Acesso em: 29 de agosto de 2021.

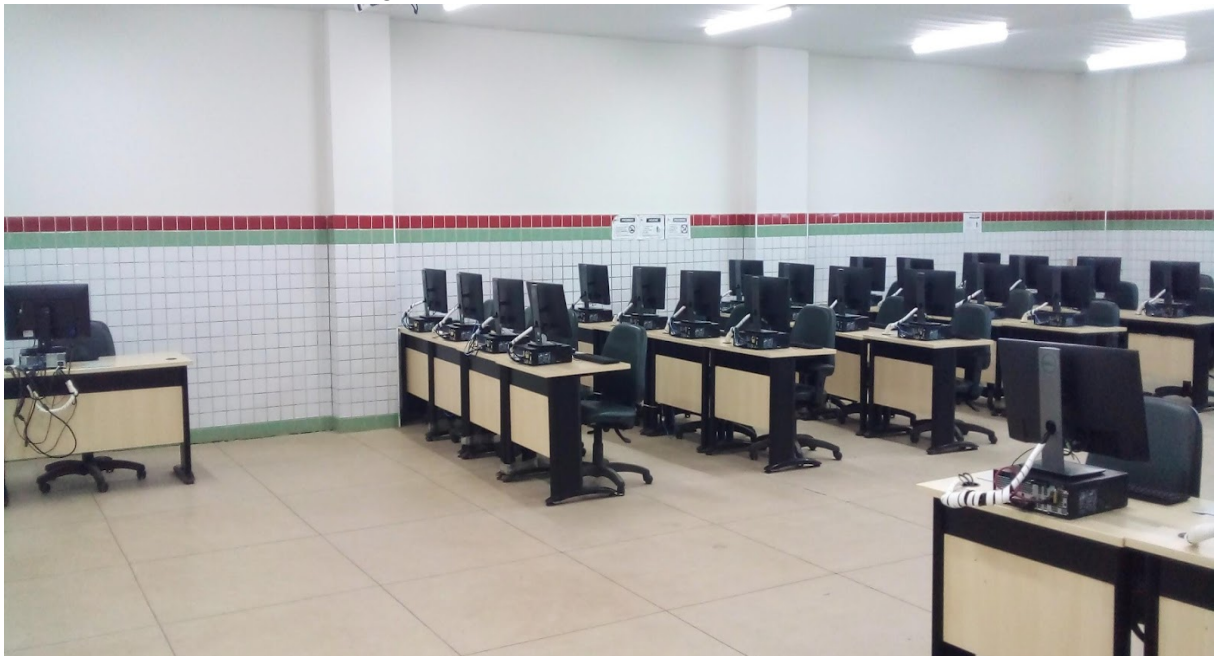
APÊNDICE A - Laboratórios de informática do IFAP

Figura 1 - Laboratório de Informática 1



Fonte: Os autores(2022)

Figura 2 - Laboratório de Informática 3



Fonte: Os autores(2022)

Figura 3 - Laboratório de informática 1 - Ginásio

Fonte: Os autores (2022)

Figura 4 - Laboratório de informática 2 - Ginásio

Fonte: Os autores(2022)

APÊNDICE B - Cartilha de boas práticas em segurança

CARTILHA SOBRE SEGURANÇA DA INFORMAÇÃO

Boas práticas para utilização dos laboratórios de informática do Instituto Federal do Amapá - campus macapá

Autores: Luis Abdon Almeida de Lima
Orlando Nazaré Tôrres Neto

Creditos: Prof. Me. Andrew Hemerson Galeno Rodrigues

Macapá
2022

Apresentação

Todos os alunos do Instituto Federal do Amapá utilizam os meios de comunicação para fazer suas pesquisas, atividades e trabalhos acadêmicos nos laboratórios de informática da instituição, mais é importante que os discentes tenham consigo as boas práticas de segurança ao navegar na Internet quando acessam serviços e plataformas que usam seus dados para fazer a autenticação de suas contas de usuários.

Esta cartilha é fruto de uma iniciativa dos acadêmicos do curso superior em redes de computadores, tendo em mente que nem todos tem o conhecimento relativo às boas práticas sobre segurança no uso de tecnologias como Internet e computadores do Instituto Federal do Amapá.

Neste manual propormos uma cartilha com assuntos relacionados a segurança da informação, ameaças e medidas que podem ser eficazes contra roubo de dados dos discentes do IFAP ao utilizar os laboratórios de informática.

Lista de Figuras

Figura 1 - Mantenha a segurança da sua máquina 6

Figura 2 - Ameaças e Riscos 7

Figura 3 - Riscos ao acessar a Internet 8

Figura 4 - Roubo de dados 9

Figura 5 - Proteção contra ameaças virtuais 10

Figura 6 - Proteja sua privacidade 11

Figura 7 - Riscos ao ter seus dados roubados 12

Figura 8 - Proteja seus dados 13

Figura 9 - Deixe sua senha segura 14

Figura 10 - Ataques virtuais 15

Figura 11 - Roubo de senhas do usuário 16

Figura 12 - Medida contra roubo de dados 17

Sumário

INTRODUÇÃO

1.COMPUTADORES.....6

1.1 PROBLEMAS.....7

1.2 INTERNET.....8

1.3 GOLPES.....9

1.4 MEDIDAS EFICAZES.....10

2. PRIVACIDADE.....11

2.1 PROBLEMAS.....12

2.2 PROTEJA SUAS INFORMAÇÕES.....11

3. SENHAS.....12

3.1 RISCOS.....13

3.2 PROBLEMAS.....14

3.3 MEDIDAS EFICAZES.....15

REFERÊNCIAS

INTRODUÇÃO

A tecnologia veio para facilitar a vida do ser humano nos meios de comunicação que antes eram empregados de forma física, mas com a evolução e o surgimento de novos meios computacionais foi possível se comunicar sem precisar sair de casa através de dispositivos interconectados pela rede mundial de computadores.

A Internet facilitou o modo como os indivíduos compartilham informações que podem chegar a grande distâncias no mundo todo, mas assim como novos recursos tecnológicos são criados, surgem novos problemas que ocasionam a insatisfação das pessoas frente aos meios de comunicação.

A necessidade de segurança do usuário é extremamente importante, pois sem a conscientização dos alunos do Instituto Federal do Amapá sobre as boas práticas de segurança da informação podem ocorrer vários problemas que tem potencial para ser porta de entrada ou roubar seus dados salvos nos navegadores padrão da Internet ao utilizar as máquinas dos laboratórios de informática do IFAP-campus macapá.

Através desta cartilha, esperamos que todos os alunos do Instituto Federal do Amapá - campus macapá tenham a consciência da importância de manter seus dados sempre seguros contra ameaças que muitas das vezes parecem ser invisíveis aos olhos do ser humano, mas que podem ser evitadas por algumas medidas de proteção básicas.

1. COMPUTADORES

Manter o computador seguro é de extrema importância ao acessar a Internet, visto que sempre deve se ter a prioridade e boas práticas de segurança com o uso de sistemas operacionais atualizados, antivírus e redes seguras para evitar possíveis problemas quando você usar o navegador para logar em sites ou baixar documentos e programas na web.

Figura 1 - Mantenha a Segurança da sua Máquina

Fonte: Pixabay(2022)

Os computadores são um equipamento muito importante por conta da sua velocidade e organização de trabalhos profissionais e acadêmicos dos usuários, pois nos dias atuais em que a tecnologia está evoluindo com a chegada de novos dispositivos eletrônicos tem possibilitado uma grande economia de tempo em atividades e sendo eficaz para realizar múltiplas tarefas ao mesmo tempo.

1.1 PROBLEMAS

Quando os usuários navegam na Internet estão sujeitos a diversas ameaças e riscos que podem comprometer sua privacidade com a divulgação de suas informações por indivíduos mal intencionados que tem com intuito roubar, manipular e aplicar golpes nos meios virtuais.

Figura 2 - Ameaças e Riscos

Fonte: Pixabay(2022)

Alguns problemas abaixo são bastantes recorrentes e muitas das vezes podem ser porta de entrada para atacantes virtuais:

- Contas de usuário com senhas iguais ou fracas;
- Vulnerabilidades em programas existentes na máquina;
- Mídias infectadas (Pen-Drive, Cartão de Memória etc...);
- Acessos à sites com conteúdos maliciosos;
- Acessos a códigos maliciosos (mensagem, Arquivos e programas de fontes desconhecidas).

1.2 INTERNET

Várias pessoas caem em golpes ou têm seus dados roubados na Internet por invasores infiltrados em sites, aplicativos e arquivos com conteúdos maliciosos que infectam a máquina do usuário com o intuito de roubar informações sigilosas da vítima.

Figura 3 - Riscos ao acessar a internet

Fonte: Moov app(2022)

Alguns riscos abaixo devem ser considerados ao navegar na Internet:

- Invasão de Privacidade;
- Perda de Dados;
- Perdas Financeiras;
- Comprometimento da Máquina.

1.3 GOLPES

Muitos invasores utilizam dados de usuários das suas vítimas para diversos fins ilícitos nos meios virtuais, mas também usam as informações para a ocultação de sua localização, impedindo as autoridades de descobrir de onde ocorreu o ataque planejado.

Figura 4 - Roubo de dados

Fonte: Na Prática(2020)

Alguns problemas abaixo podem ocorrer caso a máquina do usuário esteja comprometida ou infectada, podendo esta ser usado para:

- Atacar outros computadores;
- Aplicar vários golpes;
- Servir como armazenamento para dados roubados ou manipulados;
- Fazer a Propagação de códigos maliciosos;
- Divulgar mensagens em massa(SPAM);
- Ocultar a identificação e localização do Atacante.

1.4 MEDIDAS EFICAZES

Os indivíduos que forem navegar na internet devem tomar medidas que podem ser eficazes contra ameaças virtuais nos meios de comunicação usados para vários tipos fins.

Figura 5 - Proteção contra ameaças virtuais

Fonte: Pixabay(2022)

Algumas medidas abaixo devem ser consideradas por todos que forem utilizar a Internet em lugares públicos ou privados:

- Seja cauteloso ao permitir que programas de terceiros acessem suas informações ou sua máquina;
- Selecionar programas mais usados e com grande quantidade de usuários;
- Mantenha sempre os programas atualizados;
- Não baixar arquivos e programas de fontes desconhecidas;

- Instalar um antivírus que verifique seus arquivos e programas baixados;
- Fazer backups dos seus dados;
- manter sua senhas sempre seguras;
- Ao navegar na Web use a navegação anônima.

2. PRIVACIDADE

Proteger sua privacidade é um fator primordial não só na Internet, mas em outros meios de comunicação que fazem o armazenamento e o processamento das suas informações.

Figura 6 - Proteja sua privacidade

Fonte: Vokan(2021)

Atualmente utilizamos a Internet não só para o compartilhamento de arquivos ou programas, mas para acessar:

- serviços, sites ou aplicativos;
- Sites Educacionais;
- Cadastro em plataformas; e
- Visualizar mensagens.

Tais plataformas e sites necessitam de informações sensíveis como: E-mail, Telefone, CPF ou dados bancários. Os dados devem ser protegidos por todos os usuários que utilizam estes para não cair em golpe ou ter sua privacidade invadida por indivíduos maliciosos.

2.1 PROBLEMAS

Quando indivíduos têm sua privacidade exposta poderão ocorrer vários problemas que podem comprometer a vítima de várias formas nos meios de comunicação, dentre estes podemos citar a aplicação de golpes.

Figura 7 - Riscos ao ter seus dados roubados

Fonte: Pixabay(2022)

- Criar contas falsas(E-mail, Perfil em redes sociais e contas bancárias);
- Acessar informações sigilosas;
- Aplicar Golpes em seu nome;
- Pedir empréstimos ou dinheiro em seu nome;
- Vender ou acessar dados no seu navegador ou dispositivo.

2.2 PROTEJA SUAS INFORMAÇÕES

As informações pessoais necessitam de uma atenção maior do usuário quando estes usam para se cadastrar em diversas plataformas e meios sociais na Internet.

Figura 8 - Proteja seus dados

Fonte: Setcesp(2019)

Algumas medidas abaixo podem ser muito eficazes para proteger seus dados dentre elas podemos citar:

- Usar serviços ou aplicativos com criptografia para suas mensagens;
- Armazenar arquivos, E-mail pessoais com criptografia, isto permite que ambos não sejam acessados ou lidos por terceiros ou códigos maliciosos;
- Use uma conexão segura quando acessar e-mails no navegador;
- Tenha o cuidado ao acessar links ou sites recebidos por meio de mensagens eletrônicas no seu e-mail;
- Mantenha sempre seus dados salvos em backup com criptografia;
- Não utilize programas ou serviços de fontes não oficiais que pedem dados sensíveis como: CPF, Telefone, E-mail ou Dados Bancários.
- Utilize programas de proteção como: Antivírus, Antimalware e Firewall.

*** A criptografia** é um meio de proteção muito utilizaddo para a criptografar a informação, permitindo que a mensagem seja decodificada e lida somente pelo seu destinatário.

3. SENHAS

Todos os usuários da internet utilizam diversas senhas para logar nas plataformas que estes utilizam, mas é importante salientar que ter uma senha segura é algo essencial para a sua integridade.

Figura 9 - Deixe sua senha segura

Fonte: Pixabay(2022)

A Internet utiliza grande quantidade de contas e senhas para vários sites e programas ao navegar ou baixar estes, isto permite que ambos tenham sua segurança protegida ao ser acessado pelo usuário. Por meio destes, os sistemas estabelecidos conseguem autenticar a identidade do usuário e confirmar a veracidade das informações permitindo acessar os seus serviços.

Ao utilizar a Internet é importante que o indivíduo saiba usar os métodos de autenticação da sua conta e as boas práticas de navegação como o sistema anônimo do *browser* que permite que seus dados não fiquem salvos quando você sair deste.

*** Browser** é um programa criado para a navegação na internet.

3.1 RISCOS

Os atacantes virtuais utilizam de vários métodos para roubar informações dos usuários na Internet com o intuito de aplicar golpes, infectar máquinas e manipular dados.

Figura 10 - Ataques Virtuais

Fonte: Cepyme News(2019)

Seus dados de usuário e senhas podem ser descobertos por meio de:

- Computadores e aparelhos infectados;
- Computadores invadidos;
- Sites e Aplicativos falsos;
- Por ataque de força bruta;
- Ao navegar na rede;
- Por meio de técnicas de engenharia social;
- Por meio do Keylogger, programa utilizado para gravar o que a pessoa está digitando na máquina.

3.2 PROBLEMAS

Um indivíduo não autorizado que tenha acesso a sua senha ou seu usuário pode acessar suas informações que estejam salvas em diversas plataformas da internet em que você tenha login.

Figura 11 - Roubo de Senha do Usuário

Fonte: Pixabay (2022)

Um indivíduo não autorizado que tenha acesso a sua senha e Usuário pode:

- Acessar seu correio eletrônico (E-mail);
- Apagar ou ler seus e-mails;
- Ver seus contatos e aplicar golpes;
- Enviar mensagens com Spam ou códigos maliciosos;
- Acessar senhas de outras contas com o seu e-mail;
- Acessar seu computador indevidamente;
- Apagar seus arquivos ou roubar;
- Fazer a instalação de códigos maliciosos;
- Usar seu computador para atacar outros;
- Acessar suas redes sociais;
- Acessar sua conta bancária ou sites de comércio eletrônico em que você esteja cadastrado.

3.3 MEDIDAS EFICAZES

Proteger seus dados de usuário pode fazer muita diferença para você que utiliza os serviços de plataformas na Internet, fazendo que suas informações de login não sejam comprometidas e bloquear o acesso de indivíduos não autorizados na sua conta.

Figura 12 - Medidas contra roubo de dados

Fonte: Pixabay(2022)

Algumas medidas baixos podem ser muito eficazes contra roubo de dados e acessos indevidos na sua conta como:

- Seja cauteloso ao criar suas senhas;
- Evitar o envio de dados a pessoas desconhecidas;
- Criar senhas fortes;
- Utilizar medidas de verificação de identidade;
- Usar a verificação em duas etapas;
- Evitar expor suas senhas para outras pessoas;
- Evitar salvar seus dados de usuário e senhas no navegador;
- Armazenar suas senhas de forma segura;
- Fazer a alteração da senha;
- Não clicar em links de fontes desconhecidas;
- Mantenha seu computador seguro com antivírus e senhas.

REFERÊNCIAS

BENTIVEGNA, Adauto, 2019. **Lei Geral de Proteção de Dados**. Disponível em:<https://setcesp.org.br/noticias/lei-geral-de-protecao-de-dados-pessoais/>.Acesso em: 16 de Abril de 2022.

CEPYME News, 2019. **Principais ameaças à segurança cibernética para 2019.** Disponível em:<https://cepymenews.es/principales-amenazas-ciberseguridad-2019/>. Acesso em: 16 de Abril de 2022.

CERT.br, 2021. **Cartilha de Segurança para Internet.**Disponível em: <https://cartilha.cert.br/fasciculos/>. Acesso em 10 de Abril de 2022.

MOOV App, 2022. **23 Dicas de Como Navegar com mais Segurança na Internet**. Disponível em:<https://moovapp.com.br/dicas/seguranca-na-internet/#!>. Acesso em: 15 de Abril de 2022.

MENDES, Tatyane, 2020. **Segurança da Informação:entenda a alta demanda por profissionais de cibersegurança**. Disponível em: <https://www.napratica.org.br/seguranca-da-informacao-ciberseguranca/>.Acesso em: 16 de Abril de 2022.

Pixabay, 2022. **Segurança da Informação**. Disponível em: <https://pixabay.com/pt/images/search/seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o/>. Acesso em: 10 de Abril de 2022.

VOKAN, 2021. **Seguro Cibernético:porque proteger seus dados.** Disponível em:<https://vokan.com.br/seguro-cibernetico-porque-proteger-seus-dados/>.
Acesso em: 16 de Abril de 2022.

APÊNDICE C - Gerador de senhas seguras