**Política de Segurança da Informação de baixo custo para empresas de pequeno e médio porte**

**Igor da Silva Zagonel1**

1IFMT - Campus Cuiabá - Cel. Octayde Jorge da Silva, Departamento de Computação

igorzagonel@gmail.com

***Resumo.*** *A necessidade de utilizar sistemas de informação no meio empresarial para aumentar a produtividade e conseguir vantagem em relação a concorrência vem sendo amplamente difundido no mercado de trabalho o que levou a um aumento de crimes relacionados à segurança da informação que são prejudiciais ao funcionamento da empresa e no lucro obtido por ela. Por causa de tamanha importância os equipamentos necessários para realizar a segurança da parte computacional da empresa são extremamente custosos, o que influencia empresas de pequeno e médio porte a não adotarem esses sistemas, mesmo elas sendo tão vulneráveis quanto grandes empresas. Assim, o objetivo deste trabalho é desenvolver uma proposta de uma política de segurança de baixo custo para empresas de pequeno e médio porte. A partir do levantamento de conceitos utilizando as ferramentas de busca Google Acadêmico, BDTD e o Portal de Periódicos da CAPES foi possível escolher a composição de softwares e hardwares para a proposta. Nota-se que a proposta construída usa apenas softwares gratuitos e hardwares com preços extremamente acessíveis até mesmo para empresas pequenas.*

# 1. Introdução

Devido ao crescente avanço tecnológico nos sistemas de informação e do armazenamento de dados, resultou na redução do tempo gasto para realizar consultas e utilizar as informações, em virtude dessa vantagem muitas empresas atualizam suas tecnologias para aumentar sua produtividade (CAMPOS-FILHO, 1994).

Dessa maneira as empresas são expostas a novos riscos e vulnerabilidades, pois a segurança computacional trata-se de um processo vivo, enquanto alguns estão criando novas metodologias de segurança e obstáculos que dificultem o acesso aos dados sigilosos, outros estão estudando como burlar ou quebrar a metodologia ou modelo recém-criado (FERNANDES, 2000). Logo, é extremamente difícil construir um sistema de segurança da informação a prova de falhas, mas é possível minimizá-las a um nível aceitável.

A fim de minimizar essas falhas é necessário a existência de uma política de segurança da informação que consiste em um documento que é baseado nos requisitos de segurança necessários da empresa e é redigido a partir de uma análise profunda de todos os fundamentos da empresa para que seja possível obter a melhor eficiência e proteção possível (ASSAD, 2002). Dentre as falhas e brechas possíveis na segurança da informação de uma empresa Joel Witts (2021) descreve 5 das principais ameaças à segurança de uma empresa pequena, elas são respectivamente: ataques de phishing, ataques de malwares, ransomware, senhas fracas e ataques internos.

Partindo dessas falhas é possível encontrar algumas soluções para evitar a suas ocorrências. Em relação aos ataques de phishing e as senhas fracas um bom treinamento contra engenharia social é necessário, pois ambas as brechas fazem uso dessa técnica chamada engenharia social, esse método consiste de diversas maneiras de obter informações relevantes a partir de uma pessoa, nesse sentido os ataques de phishing baseiam-se em personificar identidades que tem a confiança da empresa ou do indivíduo com a finalidade de conseguir uma brecha na segurança através de um link ou um arquivo malicioso (WITTS, 2021; SILVA; ARAUJO; AZEVEDO, 2013).

Da mesma maneira que o ataque de phishing utiliza o próprio psicológico da pessoa para obter vantagens, a previsão das senhas usadas por esse indivíduo pode ocorrer utilizando essas técnicas de engenharia social dependendo de como essa senha é formada, um exemplo de uma senha com alta probabilidade de ser comprometida é utilizar a data de aniversário de um ente querido como uma senha, ao fazer uso desse tipo de senha, a probabilidade dela ser descoberta por terceiros é extremamente alta devido a facilidade de se conseguir esse tipo de informação em redes sociais ou até mesmo conversas informais (WITTS, 2021).

Além das vulnerabilidades geradas por atos maliciosos utilizando engenharia social existe também as falhas técnicas que podem levar a perdas enormes. No que se diz respeito as principais ameaças técnicas estão os ataques de malwares e os ransomware que exigem diversos cuidados a serem tomados pela empresa ou indivíduo para evitar danos desses métodos. Assim sendo os malwares podem ser definidos como softwares maliciosos que são usados para invadir e adquirir informações ou destruir dados de computadores de terceiros. O ransomware é essencialmente um malware, o que muda é a abordagem de como é realizado esse tipo de ataque, ele consiste em sequestrar os dados de uma organização encriptando-os com uma criptografia avançada de modo que seja praticamente impossível quebra-la e após o sucesso desse sequestro é pedido um resgate em dinheiro para liberar esses dados novamente, o que leva a empresa em um dilema, perder uma grande quantidade de dinheiro e recuperar os dados ou perder todos os dados presentes nos computadores (CERT.BR 2012).

Para evitar esses acontecimentos a organização deve implementar certas medidas para evitar essas ameaças, entre essas medidas as mais importantes são o antivírus e o firewall, assim sendo o firewall pode ser considerado como como uma combinação de software e hardware que separa a rede interna da organização da internet em geral, o que torna possível o administrador controlar certos aspectos da rede, já o antivírus pode ser considerado uma ferramenta antimalware que é desenvolvida com o intuito de eliminar possíveis ameaças e brechas de segurança de um computador. Consequentemente esses softwares tem extrema influência no confronto de ameaças como os malwares e os ransomware além de estarem intrinsicamente ligados ao nível de segurança da informação de uma empresa (CERT.BR 2012; KUROSE, 2013).

(Ver com a professora se eu coloco a parte de segurança física aqui ou já esta muito carregado a introdução)

Em consequência dessas ameaças aos sistemas computacionais, toda empresa que utiliza esses meios está sujeita ao mesmo risco de segurança independentemente do sistema utilizado por ela, porém as pequenas e médias empresas são severamente afetadas pelos problemas de adotar novas tecnologias porque não possuem um grande capital para investir em um sistema de qualidade, diferentemente das grandes empresas que podem adquirir um sistema de segurança da informação de alto nível pagando preços exorbitantes sem afetar o financeiro da empresa.

Sendo assim, este artigo tem como objetivo elaborar um modelo de política de segurança da informação utilizando softwares gratuitos e hardwares com preços acessíveis para diminuir os custos e cobrir boa parte das principais vulnerabilidades de empresas de pequeno e médio porte.

Para tanto, este artigo está estruturado, além desta primeira seção de introdução em mais quatro seções. Na seção 2, se encontra os materiais e métodos utilizados na pesquisa. Na seção 3, são apresentados os principais conceitos de segurança da informação. Na seção 4 é apresentado o modelo de segurança proposto por este artigo. Na seção 5, são realizadas as conclusões e discussões sobre a proposta sugerida.

# 2. Materiais e Métodos

Para a elaboração desta pesquisa aplicada foi utilizado o procedimento bibliográfico com o apoio das ferramentas de busca Google Acadêmico, BDTD (Biblioteca Digital Brasileira de Teses e Dissertações) e o Portal de Periódicos da CAPES, com base nas seguintes palavras-chaves: “Segurança da Informação”, “Empresas pequenas”, “Redes de computadores”. A pesquisa é formada por trabalhos mapeados entre 1994 e 2015.

O critério para escolha dos artigos desta pesquisa foram, trabalhos que abrangem métodos de segurança de rede, topologias de redes, protocolos de transferências de arquivos e políticas de segurança ISO recomendadas para uso comercial.

O desenvolvimento desta pesquisa consta as seguintes etapas: (1) revisão da literatura; (2) elaboração de uma proposta de aplicação; (3) análise dos resultados.

 Na etapa de revisão da literatura foram realizadas pesquisas nas áreas de segurança da informação e políticas regulamentadoras de segurança. Na etapa de elaboração da proposta foi feito o levantamento de softwares gratuitos de proteção e hardwares de baixo custo. Na etapa de discussão e conclusão é demonstrado a importância dos sistemas de segurança da informação e a relevância da proposta de baixo custo elaborada neste artigo.

# 3. Referencial Teórico

Esta seção consiste em revisar trabalhos existentes sobre segurança da informação, a fim de fundamentar todo o estudo baseando-se em artigos, monografias, teses e livros.

# 3.1 Segurança da Informação

De acordo com Castro (2011, *apud* DIAS; RODRIGUES; PIRES, 2012), a segurança da informação se resume em métodos que protegem a integridade das informações de uma empresa, tanto no quesito computacional como nos ambientes externos e internos da instituição. A proteção dessas informações é fundamentada no uso de uma série de softwares e hardwares que oferecem controle dos principais processos da empresa a fim de serem monitorados, analisados e melhorados caso haja a necessidade, com isso é possível obter-se um sistema com um nível aceitável de segurança, desde que o sistema apresente um controle pleno das informações da organização (ISO/IEC 17799, 2005).

A vulnerabilidade está intrinsecamente ligada ao erro do procedimento de segurança criado, o que resulta em uma informação não confiável (LYRA, 2015). Sendo assim, conforme as facilidades tecnológicas se expandem as empresas tendem a se tornarem dependentes dessas tecnologias, o que leva a vulnerabilidades que ocasionam crimes e fraudes de informações utilizando meios computacionais (CARUSO; STEFFEN, 1999 *apud* SILVA-NETTO; SILVEIRA, 2007).

Portanto, para garantir a confiabilidade e a integridade das informações da organização é necessário que seus gestores tenham conhecimento das possíveis ameaças, com o objetivo de apresentar uma solução específica para cada problema encontrado, pois a maioria dos dados de uma grande empresa estão contidos em seus sistemas computacionais e por isso é necessário que a integridade do dado esteja intacta a fim de evitar consequências graves para o funcionamento da empresa (SILVA-NETTO; SILVEIRA, 2007).

# 3.2 Políticas de Segurança

A política de segurança da informação utilizada em uma empresa pode ser definida como um documento que contém os valores, as responsabilidades e os requisitos necessários que a empresa e o sistema de segurança da informação devem cumprir a fim de manter a integridade das informações (DANTAS, 2011).

Para começar um sistema de segurança da informação que atenda a todos os requisitos necessários de proteção é preciso respeitar os controles essenciais da empresa definidos pela ISO/IEC 17799 (2005) como sendo: proteger dados e informações pessoais, proteger registros organizacionais e ter direito sobre a propriedade intelectual. Tendo em vista o controle exercido pela empresa sobre suas informações, é essencial que a empresa identifique os requisitos de segurança que são necessários para o seu funcionamento, existem três fontes de levantamento de requisitos de segurança da informação: 1º - A primeira é obtida através de uma análise dos possíveis riscos e brechas de segurança que a empresa pode sofrer, levando em conta todo o planejamento estratégico da organização para que não haja brechas e vulnerabilidades; 2º - A segunda pode ser obtida a partir da legislação que oferece regulamentos que demonstram as obrigações legais da empresa; 3º - A terceira é feita a partir dos requisitos de processamento de dados que a empresa necessita para seu funcionamento (ISO/IEC 17799, 2005).

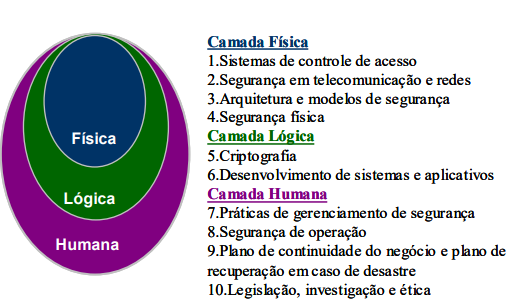
Como retratado anteriormente, uma política de segurança da informação é construída a partir de uma análise profunda de todos os requisitos de segurança da empresa, assim sendo, as políticas de segurança de empresas distintas podem ter inúmeros pontos em comum e serem baseadas nas mesmas normativas, mas é extremamente difícil elas serem iguais, pois podem diferenciar-se nos hardwares e softwares utilizados para a constituição do sistema de segurança da informação. Em vista disso, o estabelecimento de uma nova política de segurança em uma empresa normalmente é um processo longo e demorado, pois é necessário mudar rotinas consideradas corretas para novas práticas que levam em consideração a segurança e integridade da empresa (ASSAD, 2002).

# 3.3 Camadas da Segurança da Informação

Para a existência de um sistema de segurança da informação é necessário um conjunto elementar de componentes interligados que coleta, manipula e processa dados e informações essenciais para o funcionamento da organização, esse conjunto de componentes é composto por hardware, software, pessoas e processos que compõem a infraestrutura de segurança da empresa (DANTAS, 2011).

A partir desses componentes essenciais Sêmola (2003, *apud* SILVA-NETTO; SILVEIRA, 2007, p.379) define a gestão de segurança da informação em 3 aspectos principais: software, hardware, humano; e Adachi (2004) define a gestão de segurança da informação em três camadas distintas, sendo elas: física, lógica e humana. Logo, é necessário um equilíbrio entre esses aspectos para que não haja vulnerabilidades, pois é muito comum as empresas focarem apenas em softwares como firewalls, antivírus, e não dar importância para os demais componentes.

Desta maneira, a figura 1 demonstra de forma visual os domínios referentes a cada camada:



**Figura 1. Classificação dos domínios referentes a cada camada (ADACHI, 2004).**

1º - Camada Física: Ela é composta pelo ambiente onde os equipamentos e periféricos estão instalados, sendo eles computadores, servidores ou qualquer hardware interligado com o sistema, uma das formas para conduzir a segurança desta camada é o controle de acesso através de senhas ou leituras biométricas (ADACHI, 2004). A partir da forma de gerir a segurança da camada física é possível reconhecer o erro da maioria das empresas de pequeno e médio porte, pois estas empresas geralmente possuem dados em servidores locais que possuem conexão com a internet, o que aumenta o risco de invasão, e elas não se preocupam em restringir o acesso à apenas os funcionários responsáveis pela rede da organização (SILVA-NETTO; SILVEIRA, 2007).

2º - Camada Lógica: Esta camada é composta por todo software utilizado na empresa, ou seja, os softwares são os responsáveis por coordenar e gerenciar as informações da organização a fim de realizar uma ação em específico (ADACHI, 2004). Assim, para prevenir brechas de segurança é importante que se mantenha atualizado todos os softwares utilizados na empresa, a fim de minimizar os riscos (SILVA-NETTO; SILVEIRA, 2007).

3º - Camada Humana: Ela é formada por todo recurso e mão de obra humana que está presente no ambiente de trabalho, principalmente aqueles que têm acesso aos recursos computacionais da empresa, dentre os incidentes de segurança que ocorrem estão a falta de instrução dos usuários no uso da TI (tecnologia da informação), funcionários maliciosos ou ingênuos e a engenharia social (ADACHI, 2004). Segundo Schneier (2001) a camada humana é o elo mais frágil de toda a estrutura de gerenciamento de segurança da informação, sendo a responsável pela falha da corrente da segurança de muitos sistemas. Sendo assim, para uma gestão de segurança da informação eficiente é necessário atentar-se ao gerenciamento e supervisão de pessoas, pois muitas empresas se descuidam em relação a este fator (SILVA-NETTO; SILVEIRA, 2007).

# 4. Proposta de Aplicação

A fim de cumprir os requisitos necessários de segurança da empresa é preciso um grande investimento de tempo e dinheiro, pois como tratado anteriormente o processo de implantação de uma política de segurança é um processo longo e demorado e os softwares e hardwares de alta performance são extremamente custosos.

Logo, por consequência dessa complexidade, as empresas de médio e pequeno porte não conseguem arcar com as despesas para cumprir todos os requisitos e instruções contidas na ISO/IEC 27002, em vista disto, a proposta desenvolvida visa suprir o mínimo necessário de segurança para cada camada que compõe uma política de segurança.

1º - Camada Física:

Como demonstrado anteriormente, as medidas de segurança presentes nesta camada são os controles de acesso, os periféricos e toda a segurança física que reside na empresa. Assim sendo, o melhor meio de conduzir a segurança física da empresa a fim de ter pleno domínio das ações dos funcionários é utilizando o controle de acesso fundamentado em leitura biométrica, que por sua vez são sistemas caros e de difícil manutenção, porém existem alternativas de custo mais reduzido que possuem níveis aceitáveis de segurança, pois eles têm total controle das informações, dentre essas alternativas está a identificação por radiofrequência (RFID).

A RFID é uma tecnologia de identificação que tem como funcionalidades gerir, analisar e responder dados coletados por sensores eletrônicos e para a captura desses dados é utilizado uma etiqueta com dados pré-estabelecidos (GREEF, 2009).



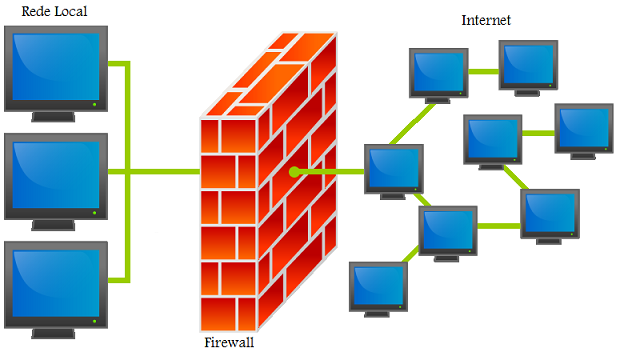
**Figura 2. Sensor RFID e *tags* (THOMSEN, 2017).**

 Logo, essa tecnologia é perfeita para fazer o controle de acesso, pois ela se tornou muito conhecida ao longo do tempo o que influenciou na diminuição do preço dos sensores, e como é possível utilizar um microcontrolador como o Arduino para obter os dados, esta tecnologia se torna fácil de ser utilizadas até para leigos no meio de microeletrônica (MCROBERTS, 2015).

2º - Camada Lógica:

Conforme demonstrado previamente no referencial teórico, nesta camada contém todo software utilizado pela empresa, por isso, a fim de diminuir as brechas de segurança é necessário manter atualizado os programas nas mais recentes versões. A partir disso, um dos softwares com maior importância para a segurança da empresa é o *Firewall,* por esse motivo, normalmente são softwares com licenças extremamente custosas e que necessitam de um hardware com alto desempenho para ser executado ou necessita de pessoas especializadas em tecnologia da informação para operá-los, o que dificulta sua aplicação em empresas de pequeno e médio porte (BORGIANI et al., 2016).

De uma maneira simples, o firewall é o responsável por filtrar qualquer ação que ocorre dentro de uma rede local a partir de regras que decidem ações válidas e inválidas para aquela rede, como representado na figura 3.



**Figura 3. Funcionamento Firewall (BRITO, 2016).**

Definindo firewall de uma maneira técnica, ele é uma solução de segurança baseada em hardware ou software que baseado em um conjunto de regras analisa toda as informações que trafegam na rede, diferenciando operações válidas e inválidas de acordo com as regras pré-estabelecidas baseadas nas necessidades de segurança da empresa (NEVES; MACHADO; CENTENARO, 2014).

Uma vez que grande parte dos softwares de *firewall* possuem requisitos custosos para seu funcionamento, existem aqueles que são livres e gratuitos para serem utilizados e que cumprem bem o seu papel de mediador da comunicação da rede. O pfSense é um software livre que é adaptado para ser usado como firewall e roteador através de uma simples interface web, o que o torna perfeito para ser implantado em empresas de pequeno e médio porte porque não há necessidade de um computador com hardware de alta performance para utilizar esse software, além de que há uma enorme simplicidade na instalação e na utilização (PFSENSE, 2014).

3º - Camada Humana:

Como tratado anteriormente essa camada é o elo mais fraco de todo sistema de segurança da informação, pois ela engloba todo recurso humano, processo operacional e a política de segurança da informação da empresa. Para que não haja brechas causadas por erros humanos é necessário um treinamento adequado dos recursos humanos da empresa que enfatize a importância de seguir os protocolos de segurança.

         Dentre essas ações de segurança, existem aquelas que podem ser aplicadas facilmente até mesmo por em empresas de pequeno e médio porte, dentre elas são: limitar o acesso de pessoas ao servidor da empresa, permitir o acesso às informações da empresa apenas para os funcionários que necessitam delas para executar seu trabalho, não divulgar informações da empresa em mídias sociais, pois com isso é possível *hackers* aplicarem engenharia social para obterem dados importantes da companhia.

# 5. Discussão e Conclusão

Por causa de acontecimentos criminosos relacionados a sistemas de informação houve a necessidade de desenvolver métodos para prevenir essas casualidades utilizando softwares e hardwares. E para direcionar todos esses métodos de segurança de informação, foram criadas as políticas de segurança da informação, que são documentos que contém os requisitos necessários de segurança da organização.

E é nesse cenário que a proposta de uma política de segurança de baixo custo se torna essencial para empresas de pequeno e médio porte, porque mesmo sendo de um porte minoritário elas estão sujeitas às mesmas ameaças das grandes corporações, porém não possuem o recurso monetário necessário para implantar um sistema de alta performance.

O estudo permitiu verificar que é possível organizar uma política de segurança da informação de baixo custo utilizando. Isto fica claro ao analisar as recomendações presente na proposta desenvolvida, pois para a sua elaboração foram utilizados softwares gratuitos como o pfSense, e hardwares de controle de entrada utilizando o RFID que possui preços acessíveis até mesmo para empresas pequenas, o que torna a proposta válida levando em consideração seu propósito de criação.

Como perspectivas de trabalhos futuros propõe-se a implementação dessa proposta em empresas de pequeno e médio porte a fim de comprovar a veracidade e integridade dessa proposta desenvolvida.

Face ao exposto anteriormente, pode-se concluir que há um grande potencial para a aplicação de propostas de baixo custo no mercado de trabalho, porque a partir delas é possível aumentar a abrangência de segurança para a maioria das empresas presentes no mercado de trabalho.

Assim espera-se que este trabalho sirva de alicerce para novos estudos e no desenvolvimento de novas propostas de políticas de segurança da informação.

# Referências

ASSAD, R. E. **Gerenciamento de políticas de segurança para redes de computadores, baseado em ferramentas de auditoria de sistemas**. 2005. 119 f. Dissertação (Mestrado em Ciência da Computação) – Centro de informática da Universidade Federal do Pernambuco, Universidade Federal do Pernambuco, Recife, 2002.

FERNANDES, D. W. **Segurança na internet*?*** 2000. 203 f. Dissertação (Mestrado em Engenharia de produção) – Colegiado do Curso de Mestrado em Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, 2000.

SILVA-NETTO, A.; SILVEIRA, M. A. P. Gestão da segurança da informação: Fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação**, São Paulo, v. 4, n. 3, p. 375-397, 2007.

DIAS, J. M. F.; RODRIGUES, R. C. M. C.; PIRES, D. F. A segurança de dados na computação em nuvens nas pequenas e médias empresas. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica**, São Paulo, v. 2, n. 1, 2012.

ABNT - Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 17799:2005**: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 116 p.

CAMPOS-FILHO, M. P. Os sistemas de informação e as modernas tendências da tecnologia e dos negócios. **Revista de administração de empresas**, São Paulo, v. 34, n. 6, p. 33-45, 1994.

LYRA, M. R. (org.). **Governança da segurança da informação**. 1. ed. Brasília: 2015, 145 p.

DANTAS, M. L. **Segurança da informação: Uma abordagem focada em gestão de riscos**. 1. ed. Olinda: 2011, 152 p.

SCHNEIER, B. **Segurança.com – segredos e mentiras sobre a proteção na vida digital**. 1. ed. Rio de Janeiro: Editora Campus, 2001.

ADACHI, T. **Gestão de Segurança em Internet Banking**. 121 p. Dissertação (Mestrado em administração de empresas) - Fundação Getúlio Vargas, São Paulo, 2004.

MCROBERTS, M. **Arduino Básico**. 1. ed. São Paulo: Novatec Editora, 2011. 443 p.

FILIPEFLOP. Controle de acesso usando leitor RFID com Arduino. 2014. Disponível em: https://www.filipeflop.com/blog/controle-acesso-leitor-rfid-arduino/. Acesso em: 23 out. 2019.

PFSENSE. pfSense. Disponível em: https://www.pfsense.org/. Acesso em: 17 out. 2019

NEVES F. C.; MACHADO L. A.; CENTENARO R. F. **Implantação de firewall pfSense**. 2014. 66 f. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Sistemas de Telecomunicações) - Universidade Tecnológica Federal do Paraná, Paraná.

WITTS, J. The top 5 Biggest Cyber Security Threats That Small Businesses Face And How To Stop Them. 2021. Disponível em: https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/. Acesso em: 1 nov. 2021.

file:///C:/Users/igor\_/OneDrive/Área%20de%20Trabalho/Faculdade/Projeto%20integrador%202/Artigos%20Mapeados/Engenharia%20social%20nas%20redes%20sociais%20online.pdf

https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

file:///C:/Users/igor\_/OneDrive/Área%20de%20Trabalho/Faculdade/Redes%201/Redes%20De%20Computadores%20E%20A%20Internet%20-%20Kurose%20-%206ª%20Ed%20-%20Pdf-1.pdf