UNIVERSIDADE FEDERAL DE OURO PRETO
ESCOLA DE MINAS
COLEGIADO DO CURSO DE ENGENHARIA DE CONTROLE E AUTOMAÇÃO - CECAU

CLEYSON FERNANDO ARAÚJO TEIXEIRA

SEGURANÇA CIBERNÉTICA EM REDES MODERNAS: COMO PROTEGER E MITIGAR ATAQUES CIBERNÉTICOS

MONOGRAFIA DE GRADUAÇÃO EM ENGENHARIA DE CONTROLE E AUTOMAÇÃO

Ouro Preto, 2021

CLEYSON FERNANDO ARAÚJO TEIXEIRA

SEGURANÇA CIBERNÉTICA EM REDES MODERNAS: COMO PROTEGER E MITIGAR ATAQUES CIBERNÉTICOS

Monografia apresentada ao Curso de Engenharia de Controle e Automação da Universidade Federal de Ouro Preto como parte dos requisitos para a obtenção do Grau de Engenheiro de Controle e Automação.

Orientador: Prof. José Alberto Naves Cocota Júnior, DSc

Coorientador 1: Prof. Agnaldo José da Rocha Reis, DSc

Coorientador 2: Cristiano Coelho Ferreira

Ouro Preto
Escola de Minas – UFOP
2021

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

T266s Teixeira, Cleyson Fernando Araújo.
Segurança cibernética em redes modernas [manuscrito]: como proteger e mitigar ataques cibernéticos. / Cleyson Fernando Araújo Teixeira. - 2021.
93 f.: il.: color., gráf., tab.. + Anexo.

Orientador: Prof. Dr. José Alberto Naves Cocota Júnior.
Coorientadores: Prof. Dr. Agnaldo José da Rocha Reis, Cristiano Coelho Ferreira.
Monografia (Bacharelado). Universidade Federal de Ouro Preto. Escola de Minas. Graduação em Engenharia de Controle e Automação .

1. Redes de computadores - Medidas de segurança. 2. Segurança cibernética. 3. Teletrabalho. 4. Framework (Arquivo de computador). I. Cocota Júnior, José Alberto Naves. II. Ferreira, Cristiano Coelho. III. Reis, Agnaldo José da Rocha. IV. Universidade Federal de Ouro Preto. V. Título.

CDU 004.72.056.52

Bibliotecário(a) Responsável: Sione Galvão Rodrigues - CRB6 / 2526

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE MINAS
DEPARTAMENTO DE ENGENHARIA CONTROLE E AUTOMACAO

FOLHA DE APROVAÇÃO

Cleyson Fernando Araújo Teixeira

Segurança Cibernética em Redes Modernas: Como Proteger e Mitigar Ataques Cibernéticos

Monografia apresentada ao Curso de Engenharia de Controle e Automação da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de de Engenheiro de Controle e Automação

Aprovada em 18 de outubro de 2021.

Membros da banca

DSc. José Alberto Naves Cocota Júnior – Orientador
DSc. Agnaldo José da Rocha Reis – Coorientador
Cristiano Coelho Ferreira – Coorientador
DSc. Paulo Marcos de Barros Monteiro – Professor Convidado
DSc. Luciana Gomes Castanheira – Professora Convidada

José Alberto Naves Cocota Júnior, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 26/10/2021

Documento assinado eletronicamente por **Jose Alberto Naves Cocota Junior**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 27/10/2021, às 23:24, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0238465** e o código CRC **19F91061**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 23109.011137/2021-10 SEI nº 0238465

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: 3135591533 - www.ufop.br

Este trabalho é dedicado aos meus pais, que não mediram esforços para meu desenvolvimento acadêmico-profissional, tornando esse sonho em uma realidade.

AGRADECIMENTOS

A Deus, por tudo que Ele tem feito em minha vida, por ter me dado saúde e força para ultrapassar todos os meus desafios ao longo do curso, a aprender com meus erros e, por fim, me transformar em um vencedor.

Ao meu pai, por trabalhar duro a fim de me proporcionar uma educação que, infelizmente, não teve oportunidade de ter. À minha mãe, por dedicar seu tempo para comigo, por cuidar de mim e fazer com que tudo desse certo. E aos meus dois irmãos, por servirem de espelho para mim e por me incentivarem a seguir meus estudos.

À Universidade Federal de Ouro Preto (UFOP) e todo o seu corpo docente e servidores, especificamente ao Departamento de Controle e Automação (DECAT), cujos professores capacitam os alunos de Engenharia de Controle e Automação e compartilham suas experiências.

À Fundação Gorceix, por todo apoio financeiro e educacional durante todo a minha trajetória educacional.

Aos meus amigos e colegas da Universidade, com quem pude compartilhar alguns dos meus melhores momentos da minha vida, que estiveram comigo em momentos de alegria, de tristeza e dificuldades. Mas juntos, superamos tudo isso.

À Equipe 12 Bis, ao SAAE Mariana e à Samarco, por me darem a oportunidade de estagiar/treinar, aprender, melhorar e potencializar minhas *Soft* e *Hard Skills*.

"O espírito humano precisa prevalecer sobre a tecnologia" (Albert Einstein)

RESUMO

O avanço tecnológico da Internet, computação e eletrônica, bem como a implementação da modalidade *Home Office* no atual cenário pandêmico da COVID19, potencializa o surgimento de novas formas de comunicação, o aumento da competitividade, a modernização dos serviços oferecidos à população e a transformação das modalidades e das posições de trabalho. Tratando-se de uma evolução tecnológica, muitos serviços, sistemas e dados conectados em rede podem ter inúmeros benefícios e comodidades. Entretanto, podem estar vulneráveis e a mercê de ataques cibernéticos.

Com uma abordagem exploratória e qualitativa, este trabalho visa apresentar o conceito de segurança cibernética, assim como a aplicação de uma ferramenta de maturidade cibernética em uma indústria. Para isso, conceitos introdutórios às redes, proteção às redes, tecnologias de teletrabalho, ameaças à segurança, ataques cibernéticos e mitigação desses ataques serão abordados.

Palavras-chaves: Introdução às Redes; Segurança de Redes; Ataques Cibernéticos; Segurança Cibernética; *Frameworks* de Segurança Cibernética; *NIST CSF Maturiy Tool*.

ABSTRACT

The technological advancement of Internet, computing and electronics, as well as Home Office modality for work in the current COVID19 pandemic scenario, enhance the emergence of new forms of communication, foster the increased competitiveness and the modernization of services offered to the population, and change modalities and working positions.Thus, many services, systems and data connected in a network may have a several benefits and amenities. However, they can be vulnerable and at the mercy of cyber attacks.

With an exploratory and qualitative research, this work aims to introduce the cybersecurity concept, in addition to the application of a cybersecurity maturity tool in an industry. Therefore, it will be present the introduction of concepts of networks, networks protection, teleworking technologies, security threats, cybernetics attacks and how to mitigate them.

Key-words: Introduction to Networks; Networks Security; Cyberattacks; Cybersecurity; Cybersecurity Frameworks; NIST CSF Maturity Tool.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

WWW	*World Wide Web* - Rede de Alcance Mundial
HTTP	*Hypertext Transfer Protocol* - Protocolo de Transferência de Dados
HTTPS	*Hypertext Transfer Protocol Secure* - Protocolo de Transferência Segura de Dados
SMTP	*Simple Mail Transfer Protocol* - Protocolo Transferência de Mensagem Simples
SSH	*Secure Shell* - Protocolo de Segurança de Troca de Arquivos Entre Cliente e Servidor
SSL	*Secure Socket Layer* - Camada de Soquete Seguro
TLS	*(Transport Layer Security* - Segurança Camada de Transporte
RADIUS	*Remote Authentication Dial-In User Service* - Serviço de Usuário Discado com Autenticação Remota
WEP	*Wired Equivalent Privacy* - Privacidade Equivalente com Fio
WPA	*Wi-Fi Protected Access* - Acesso Wi-Fi Protegido
Telnet	Protocolo de Internet Para Acesso Virtual via Terminal Virtual
FTP	*File Transfer Protocol* - Protocolo de Transferência de Arquivo
SFTP	*Secure File Transfer Protocol* - Protocolo de Transferência Segura de Arquivo
NNTP	*Network News Transfer Protocol* - Protocolo da Internet para Grupos de Discussão da *Usenet*
RDP	*Remote Desktop Protocol* - Protocolo de Acesso Remoto
IRC	*Internet Relay Chat* - Protocolo de Comunicação na Internet
SNMP	*Simple Network Management Protocol* - Protocolo de Gerenciamento Simples de Rede
POP3	*Post Office Protocol* - Protocolo de Acesso Remoto a um Servidor de Correio Eletrônico

IMAP	*Internet Message Access Protocol* - Protocolo de Acesso a Mensagem e Gerenciamento de Correio Eletrônico
SIP	*Session Initiation Protocol* - Protocolo de Iniciação e Sessão
DNS	*Domain Name System* - Sistema de Nome de Domínio
TCP	*Transmission Control Protocol* - Protocolo de Controle de Transmissão
UDP	*User Datagram Protocol* - Protocolo de Datagrama de Usuário
RTP	*Real-time Transport Protocol* - Protocolo de Transporte em Tempo Real
DCCP	*Datagram Congestion Control Protocol* - Protocolo de Controle de Congestionamento de Datagramas
SCTP	*Stream Control Transmission Protocol* - Protocolo de Transmissão de Controle de Fluxo
IP	*Internet Protocol* - Protocolo de Internet
IPv4	*Internet Protocol Version 4* - Protocolo de Internet Versão 4
IPv6	*Internet Protocol Version 6* - Protocolo de Internet Versão 6
IPsec	*Internet Protocol Security* - Protocolo de Segurança de Internet
ISP	*Internet Service Provider* - Provedor de Acesso à Internet
ICMP	*Internet Control Message Protocol* - Protocolo de Controle de Mensagem
IGMP	*Internet Group Management Protocol* - Protocolo de Gerenciamento de Internet por Grupos
ARP	*Address Resolution Protocol* - Protocolo de Resolução de Endereços
TCP/IP	*Transmission Control Protocol/Internet Protocol* - Protocolo de Transmissão e Controle/Protocolo de Internet
OSI	*Open Systems Intercommunication* - Sistema Aberto de Intercomunicação
MAC	*Media Access Control* - Controle de Acesso à Mídia
LLC	*Logical Link Control* - Controle de Ligação Lógica
ATM	*Asynchronous Transfer Mode* - Modo Assíncrono de Transferência
Ethernet	Arquitetura de interconexão para redes locais
FDDi	*Fiber Distributed Data Interface* - Interface de Dados Distribuídos por Fibra

PPP	*Point-to-Point Protocol* - Protocolo Ponto-a-Ponto
P2P	*Peer-to-Peer* - Ponto a Ponto
LAN	*Local Area Network* - Rede de Área Local
WAN	*Wide Area Network* - Rede de Longa Distância
WLAN	*Wireless Local Area Network* - Rede de Área Local Sem Fio
CAN	*Campus Area Network* - Rede de Área de Campus
MAN	*Metropolitan Area Network* - Rede de Área Metropolitana
VPN	*Virtual Private Network* - Redes Privadas Virtuais
PGP	*Pretty Good Privacy* - Privacidade Muito Boa
ISO	*International Organization for Standardization* - Organização Internacional de Normalização
ITU-T	*International Telecommunication Union — Telecommunication Standards Sector* - Setor de Normatização das Telecomunicações
ANSI	*American National Standards Institute* - Instituto Nacional Americano de Padrões
IEEE	*Institute of Electrical and Electronics Engineers* - Instituto de Engenheiros Eletricistas e Eletrônicos
EIA	*Electronic Industries Alliance* - Aliança das Indústrias Eletrônicas
Anatel	Agência Nacional de Telecomunicações
FCC	*Federal Communications Commission* - Comissão Federal de Comunição
NIST	*National Institute of Standards and Technology* - Instituto Nacional de Padrões e Tecnologias dos EUA
ISO	*International Organization for Standardization* - Organização Internacional de Padronização
IASME	*Information Assurance for Small to Medium-sized Enterprises* - Garantia de Informação para Pequenas-Médias Empresas
AICPA	*American Institute of Certified Public Accountants* - Instituto Americano de Conatdores Públicos Certificados
SOC	*Service Organization Control* - Controle de Organização de Serviços

NERC CIP	*North American Electric Reliability Corporation - Critical Infrastructure Protection* - Corporação de Confiabilidade Elétrica Norte Americana - Proteção de Infraestruturas Críticas
HIPAA	*Health Insurance Portability and Accountability Act* - Lei de Portabilidade e Responsabilidade de Seguro Saúde
FISMA	*Federal Information Security Management Act* - Lei Federal de Gestão de Segurança da Informação
CIS	*Center for Internet Security* - Centro de Segurança da Internet
COBIT	*Control Objectives for Information and elated Technology* - Objetivos de Controle para Informações e Tecnologias Relacionadas
COSO	*Committee of Sponsoring Organizations of the Treadway Commission* - Comitê de Organizações Patrocinadoras
TC CYBER	Technical Committee of Cybersecurity - Comitê Técnico de Segurança Cibernética
CISQ	*Consortium for IT Software Quality* - Consórcio para Qualidade de Software de TI
FedRAMP	*Federal Risk and Authorization Management Program* - Programa Federal de Gerenciamento de Riscos e Autorizações
ANSI	*American National Standards Institute* - Instituto Norte Americano de Padrões
SCADA	*Supervisory Control And Data Acquisition* - Sistema de Supervisão e Aquisição de Dados

SUMÁRIO

1 INTRODUÇÃO

1.1 Estado da Arte

Com o avanço tecnológico da internet, computação e eletrônica, a sociedade, em geral, segue cada vez mais "conectada". Ao mesmo tempo que desfruta de seus benefícios e comodidades no trabalho, na educação, na saúde, nos serviços em geral e no lazer, podem estar visivelmente vulneráveis nesse meio.

"Se você colocar uma chave debaixo do tapete, permitirá que um ladrão a encontre", afirma o *CEO* da *Apple*, Tim Cook. Cook, em seu discurso sobre criptografia e privacidade durante a conferência *Champions of Freedom*, em *Washington DC*, faz uma analogia desse ladrão aos cibercriminosos, que atuam como ladrões de senhas e dados, usam todas as ferramentas disponíveis da tecnologia para invadir contas pessoais e, se descobrem que há uma chave escondida em algum lugar, não cessam até encontrá-la (DIAS, 2015). Por fim, o executivo acredita que seus clientes devem estar no controle de suas informações pessoais, com privacidade e segurança (PANZARINO, 2015).

Constantemente, a Internet vem transformando carreiras, processos e serviços em nossa sociedade contemporânea. Com a rede das redes, surgem-se novas formas de comunicação capazes de modificar os tradicionais processos de interação política, econômica e social. Ao vencer os obstáculos territoriais dos Estados com todas as infraestruturas de informação pela rede, constrói-se um espaço em escala global, denominado ciberespaço (NUNES, 2012).

O ciberespaço favorece o crescimento do país, no qual promove o desenvolvimento de infraestruturas de telecomunicações, moderniza os serviços oferecidos à população, potencializa o crescimento industrial e econômico, e aumenta a competividade que, por sua vez, contribui com produtos e serviços de melhor qualidade a um custo cada vez menor. Entretanto, ter total ou parcial dependência ao ciberespaço nos serviços e operações podem evidenciar vulnerabilidades e, assim, ocorrer possíveis ataques. Dessa maneira, o mecanismo usual para mitigar vulnerabilidades em ambientes acessíveis provenientes da conectividade é a segurança cibernética.

O país báltico Estônia, localizado no continente europeu, pode ser considerado um dos países com maior infraestrutura de segurança cibernética do mundo e isso o torna referência mundial. A Estônia introduziu a digitalização de seus serviços muito mais cedo que os demais países, como seu sistema de ensino *online* e serviços governamentais *online*, incluindo o sistema eleitoral. Por estar em um grau de digitalização acima da média, no ano de 2007 foi alvo do maior ataque cibernético a um país até hoje registrado (KOTTASOVÁ, 2021).

Czosseck, Ottis e Talihärm (2011) afirmam que, embora nenhum dado tenha sido roubado ou perdido durante o ataque, vários serviços e sistemas ficaram indisponíveis por 22 dias após ser

alvo de *Distributed Denial of Service* (*DDoS*), conhecidos também como ataques distribuídos de negação de serviço. Como forma de mitigar os ataques, o país se associou a empresas privadas para construir sistemas seguros e montou um *datacenter* seguro com *backups*, uma espécie de "embaixada de dados" em Luxemburgo, a fim de manter os dados seguros do território caso sofra ataques. A infraestrutura do governo possui várias camadas de segurança, armazena dados de forma bastante segmentada, não possui dados duplicados em seus bancos de dados e utilizam a tecnologia *blockhain* que garante a integridade dos dados, sendo um dos primeiros países a adotar essa tecnologia. Além disso, o governo estoniano tem investido fortemente em programas de educação e treinamentos em cibersegurança. Após o incidente sofrido, o governo estoniano atribuiu a responsabilidade do ataque ao governo russo que, por sua vez, negou ser de sua autoria (KOTTASOVÁ, 2021).

Atribuir crime de ataque a um agente é fundamental e de suma importância, como informa Rid e Buchanan (2015). Este estudo apresentou um modelo sistemático para atribuição de ataques cibernéticos e articulou três argumentos centrais sobre a atribuição de um ataque: é uma arte, na qual a atribuição de alta qualidade depende de habilidades, ferramentas e cultura organizacional; é um processo gradativo e em várias camadas, visto que requer gerenciamento cuidadoso, capacitação, treinamento e liderança; é dependente das apostas políticas, uma vez que quanto mais graves forem as consequências de um incidente específico e quanto maior for o seu dano, mais recursos e capital político o governo investirá na identificação dos agentes causadores dos danos.

Os autores ainda afirmam que os infratores, de criminosos a espiões e sabotadores, podem encobrir seus rastros, permanecer anônimos e se esconder atrás do problema de atribuição de autoria do ataque. Ilustram também que apenas os estados têm os recursos suficientes para atribuir às operações mais sofisticadas um alto nível de certeza, mas que atualmente a internet está tirando o poder dos estados e distribui-os à atores não-estatais, entidades privadas e criminosos fracos. Por fim, uma terceira suposição comum que eles evidenciam é que os países mais "conectados" e mais industrializados são também os mais vulneráveis, enquanto os países menos desenvolvidos acabam sendo menos vulneráveis, embora pela lógica, quanto maior a capacidade técnica de um governo e quanto maior o conjunto de talentos e habilidades à sua disposição, maior será a capacidade do estado de proteger suas próprias operações secretas, descobrir outras e responder à altura (RID; BUCHANAN, 2015).

Um relatório recentemente publicado pela *Fortinet*, uma das maiores empresas especializadas em segurança cibernética, por meio de seu laboratório de inteligência de ameaças *FortiGuard Labs*, informou que houveram mais de 41 bilhões de tentativas de ataque cibernético em 2020 em toda a América Latina e Caribe. Desse montante, 8,4 bilhões de tentativas foram direcionadas apenas ao Brasil e cerca de 5 bilhões de tentativas foram registradas nos 3 últimos meses do ano de 2020. Foram registradas ameaças bem conhecidas, como o *malware* baseado em *web* (*e-mails* de *phishing*, por exemplo), muita das vezes tornando-se a porta de entrada para

ransomware. Além disso, foi observado o grau de sofisticação e eficiência que os cibercriminosos estão alcançando ao usarem tecnologias avançadas e Inteligência Artificial (IA) para o ataque ser cada vez mais direcionado, eficiente e realizado em menos tentativas (FORTINET, 2021).

Para o ano de 2021, a empresa emite um alerta acerca da expansão do 5G e recomenda atenção ao setor corporativo no que tange ao poder da inteligência artificial e do aprendizado de máquina a ambientes automatizados, a ambientes *multi-cloud*, em filiais e na modalidade *Home Office* (FORTINET, 2021). Contextualizando todas essas informações, é notória a preocupação que devemos ter em proteger todos os nosso sistemas que se comunicam por redes, visto que Convergência Digital (2021) afirma que os *Hackers* elegeram o Brasil como alvo preferido para tentativa de ataques cibernéticos na América Latina e Monitor Mercantil (2021) afirma que apenas no primeiro trimestre de 2021 foram registrados mais de 3,2 bilhões de tentativas de ataques cibernéticos no Brasil, potencializados pelo trabalho remoto, com várias tentativas de execução de código remoto a roteadores domésticos, o que evidencia que os criminosos estão procurando maneiras de comprometer usuários em *Home Office*, a fim de os redirecionar a endereços fraudulentos, como sites maliciosos.

Com o surgimento da pandemia mundial da COVID-19, causada pelo vírus Sars-Cov-2, à partir do ano de 2019 até o momento, Lallie et al. (2021) destacam o aumento nas ocorrências de tentativas de ataques influenciadas à ampliação de práticas de trabalho e socialização de modo virtual, como o *Home Office*, ferramentas de comunicação e pessoas que acabaram perdendo o emprego, o que significa que há mais pessoas em casa conectadas à rede. Muitos ataques cibernéticos começam com uma campanha *phishing* que direciona as vítimas a baixar um arquivo ou acessar um *URL*, que por sua vez, atua como a transportadora de malware a fim de atuar como um veículo em busca de causar fraude financeira.

Diante disso, um estudo realizado em 2020, conduzido pelo *IBM Institute for Business Value (IBV)*, intitulado por "COVID-19 e o futuro dos negócios", que inclui contribuições de mais de 3.800 executivos em 20 países e 22 setores, apresentou resultados interessantes. De acordo com os pesquisadores, 51% dos executivos participantes informaram que planejam priorizar a cibersegurança, 51% do executivos brasileiros informaram que a transformação digital será prioridade para os próximos dois anos, mas apenas 2% dos executivos brasileiros informaram que já implementavam tecnologias a fim de garantir a seguridade há pelo menos 2 anos (IBM, 2020).

De forma análoga, um estudo realizado no ano de 2021 com 122 empresas brasileiras dos setores de TI e telecomunicações (27%), serviços (22%), infraestrutura e construção (16%), bens de consumo (14%), serviços financeiros (8%), agronegócio, alimentos e bebidas (7%) e comércio (6%), realizado pela Deloitte, maior organização de serviços profissionais do mundo, mostrou que investir em segurança cibernética pode alavancar a transformação digital no Brasil. Da totalidade de empresas estudadas, 41% delas informaram que já sofreram ataques, 56% delas acreditam que o investimento na área podem alavancar seus negócios e, por fim, 90% delas

indicaram que investiriam em pelo menos uma iniciativa para impulsionar seus negócios, caso tivessem garantia de segurança cibernética (DELOITTE, 2021).

Além de garantir que processos e sistemas corporativos estejam totalmente seguros nesse meio é importante enaltecer a necessidade de possuir boas relações internacionais entre os países e que os setores nacionais de segurança estejam preparados para agir em caso de ataque. Galoyan (2019) realiza um estudo acerca das relações internacionais entre 4 Estados no âmbito segurança cibernética: Estados Unidos da América, Rússia, Brasil e Israel. O autor defende que o Brasil, apesar de ser um dos mais novos no quesito segurança cibernética, lançou programas de defesas digitais e de prevenção e resposta ao cibercrime, como o *CDCiber* e a Unidade de Combate ao Cibercrime (URCC), respectivamente. Já Cruz (2020) aborda sobre a segurança cibernética no Brasil, incluindo políticas e organizações voltadas a ciber segurança no Brasil, com ênfase nas Forças Armadas, especificamente sobre o Exército Brasileiro, que é o órgão responsável pela defesa do espaço cibernético no contexto da guerra cibernética, o qual segue diretrizes da legislação internacional que tangem o assunto.

Georgiadou, Mouzakitis e Askounis (2021) afirmam que para estabelecer segurança cibernética é necessário um foco maior nas características de segurança individuais, como comportamento, atitude, consciência e conformidade nos colaboradores da organização e realizar uma pesquisa torna-se obrigatória para quantificar esses indicadores de qualidade principalmente para ter uma abordagem cultural confiável para a segurança cibernética. O autor finaliza enfatizando que o fator humano é a chave para o progresso da segurança da informação. De forma semelhante, para Anwar et al. (2017) as violações de segurança prevalecem nas organizações e muitas delas são atribuídas a erros humanos. Em seu estudo, os autores evidenciam que as organizações precisam aumentar a conscientização dos seus funcionários sobre segurança e realizam um estudo para verificar se, entre os gêneros masculino e feminino, por meio de modelagem de equações estruturais, há algum efeito na eficácia da segurança. Como resultados, os autores constatam que há uma vulnerabilidade significativa no gênero feminino em autoeficácia, que pode ser alvo de ataques, sugerindo treinamento em segurança cibernética direcionado a este grupo.

Por fim, pode-se concluir então que a maior preocupação para o Brasil, nesse atual cenário, se resume ao domínio de conhecimentos específicos sobre o tema ser concentrado em um pequeno grupo de pessoas capacitadas e, ao mesmo tempo, que recursos financeiros devem ser suficientes para garantir proteção (CANONGIA; JUNIOR, 2010 apud WOLOZIN, 2009).

1.2 Objetivos gerais e específicos

Este presente trabalho tem por objetivo descrever e discutir acerca da segurança em redes modernas, dando ênfase à segurança cibernética, com uma abordagem contemporânea, observada pelo atual cenário da pandemia da COVID-19 no Brasil e no mundo. Além disso, uma ferramenta prática de análise de maturidade será implementada. Portanto, serão abordados os

seguintes itens:

- Introdução às redes;
- Proteção às redes;
- Tecnologias de teletrabalho;
- Ameaças à segurança;
- Ataques Cibernéticos;
- Mitigação de ataques cibernéticos;

1.3 Justificativa do trabalho

Há décadas, muitas corporações têm sofrido com ataques cibernéticos. Com o surgimento da pandemia da COVID-19, a modalidade de teletrabalho, também conhecida como *Home Office*, tornou-se necessária. Aliada às fraquezas em segurança que já temos em nossas redes domésticas e nas empresas de diversos setores, essa nova modalidade colocou em evidência as vulnerabilidades a qual estamos expostos. Portanto, se faz necessário um estudo acerca da segurança de redes e segurança cibernética, a fim de apresentar os ataques e tentativas de ataques em diversos setores, quais os efeitos ocasionados e quais as tecnologias e métodos que os agentes de ataques estão utilizando. Esse estudo, além de apresentar conceitualmente o problema, poderá ser considerado como base de orientação e treinamento àqueles que não conhecem o tema, ou possuem pouca experiência e, em sua postura navegando ou trabalhando pela internet, podem ser alvo de cibercriminosos.

1.4 Estrutura do trabalho

O texto dessa monografia está estruturado em 5 capítulos e 1 anexo. No capítulo 1 é abordado o estado da arte acerca da segurança cibernética de redes modernas, os objetivos gerais e específicos, bem como a justificativa do trabalho. O capítulo 2 engloba a revisão de literatura pertinente ao embasamento teórico do trabalho, incluindo-se a introdução às redes, Internet, protocolos de rede, modelos de rede, dispositivos de rede, proteção das redes, tecnologias de segurança para o regime de teletrabalho, segurança cibernética e *frameworks* de segurança cibernética. No capítulo 3 é apresentado o desenvolvimento do trabalho abordando a pequisa exploratória de ataques cibernéticos e uma pesquisa qualitativa com a aplicação de uma ferramenta de maturidade em segurança cibernética. No capítulo 4 são expostos os resultados experimentais por meio de tabelas e gráficos. No capítulo 5 são apresentadas as conclusões, as relevâncias dos resultados e propostas para trabalhos futuros. E, por fim, no Anexo A encontra-se o guia *NIST CSF* completo da ferramenta de maturidade utilizada.

2 REVISÃO DA LITERATURA

2.1 Introdução às Redes

De acordo com Forouzan (2009), as redes de computadores e sistemas de comunicação, atualmente, são uma das tecnologias que mais crescem e tem atraído diversos estudos para essa área, bem como surgem-se muitas profissões que utilizam dessas ferramentas para seu êxito operacional. A utilização de computadores em rede, assim como os sistemas de comunicação, vem sendo amplamente utilizados e necessários nas empresas, nos diversos setores da economia, nas instituições de ensino e em órgãos governamentais a níveis municipal, estadual e federal. Essa ampla necessidade faz com que a maioria das corporações e organizações possuam múltiplas redes, a fim de garantir a efetividade de seus serviços e operações (COMER, 2016).

Comer (2016) afirma ainda que as redes são dinâmicas e mudam repentinamente. Podem até parecer complexas e até ser consideradas como tal, visto que além de possuir um conjunto de tecnologias diverso e que se atualiza rapidamente, muitas empresas criam padrões de redes de comunicação próprios que podem ser incompatíveis em dispositivos de fabricantes distintos.

SOUSA (apud TANENBAUM, 2003) define redes de computadores como computadores autônomos interconectados por uma única tecnologia, como pode ser visualizado na figura 1. De forma geral, a rede pode ser entendida como um conjunto de dispositivos, normalmente conhecidos como nós, conectados por *links* de comunicação. A comunicação de dados ou informações ocorre no momento em que há trocas de dados entre dispositivos e essa comunicação pode ser estabelecida por meio de uma rede, envolvendo a conexão de computadores, mídias e equipamentos de rede (FOROUZAN, 2009).

Figura 1 – Rede de computadores (CITTÀ TELECOM, 2016)

2.1.1 Topologia das Redes

De acordo com Forouzan (2009), o fluxo das informações transmitidas entre dispositivos em rede ocorre de três formas: *Simplex* - comunicação unidirecional; *Half-Duplex* - cada dispositivo pode transmitir e receber dados, mas não ao mesmo tempo; *Full-Duplex* - cada dispositivo pode transmitir e receber dados simultaneamente. Um resumo dessas informações pode ser visualizado na figura 2.

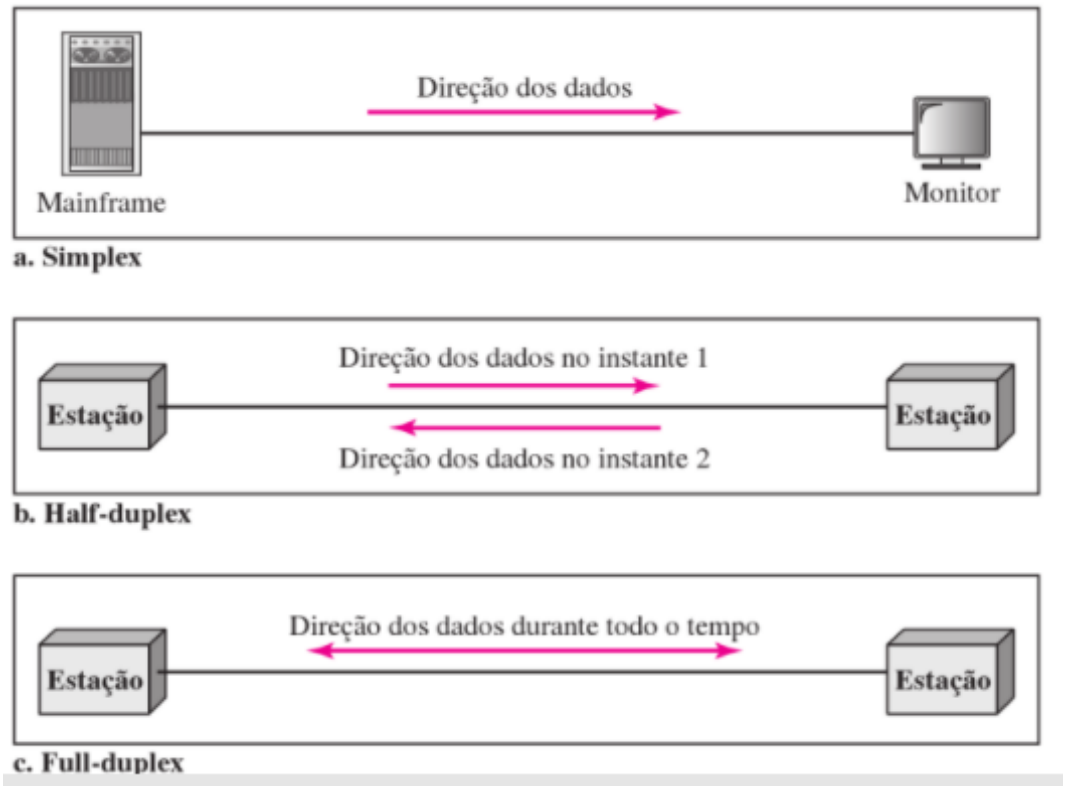


Figura 2 – Fluxo de Informações (FOROUZAN, 2009).

Na figura 3 temos ilustrado os tipos de conexões entre dispositivos em uma rede de computadores e de sistemas de comunicação. Ademais, Forouzan (2009) informa que há duas possibilidades de conexão:

- Ponto a Ponto: conhecido também por conexão P2P, fornece um *link* dedicado entre dois dispositivos, sendo que toda sua capacidade é reservada para a transmissão de dados entre os dois dispositivos. A maioria das conexoes ponto a ponto usa um pedaco real de fio ou de cabo para conectar as duas extremidades. Entretanto, há também a possibilidade de *links* via satélite e microondas, por exemplo;
- Multiponto: tambem chamada multidrop, ou conhecida também por difusão, e uma conexao na qual mais de dois dispositivos compartilham um unico *link*. Em um ambiente multiponto, a capacidade do canal e compartilhada quando os dispositivos o usam simultaneamente ou o revezam, de forma espacial e temporal, respectivamente.

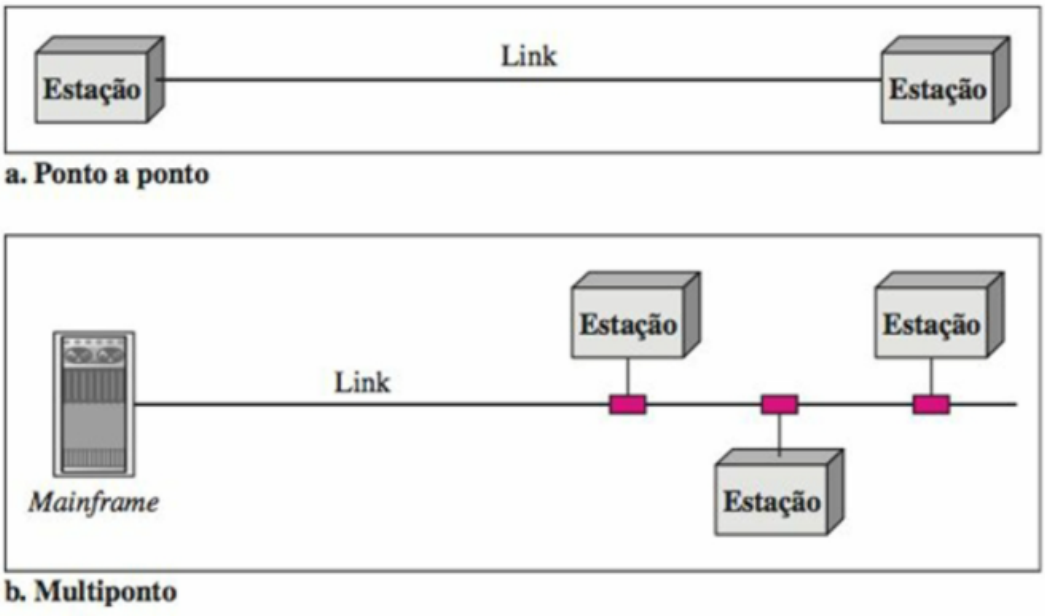
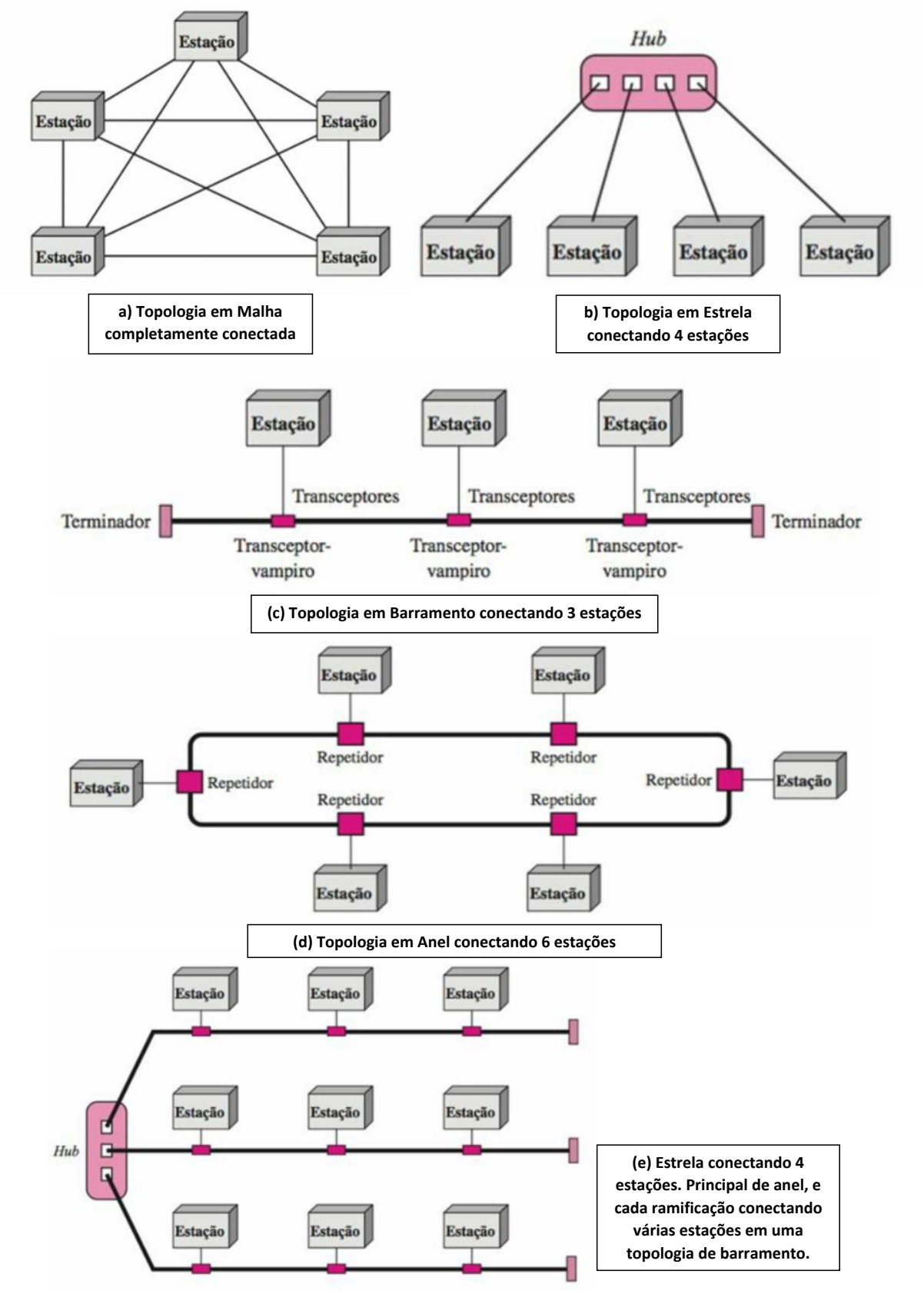


Figura 3 – Tipos de conexão: ponto a ponto e multiponto (FOROUZAN, 2009).

Após o estudo do fluxo de dados e das possibilidades de conexão dos dispositivos nas redes, é importante salientar a respeito da topologia física, na qual esses dispositivos estão interconectados. O termo topologia física se refere à maneira pela qual uma rede é organizada fisicamente, no qual dois ou mais dispositivos se conectam a um *link* e dois ou mais *links* formam uma topologia. A topologia de uma rede é a representação geométrica da relação de todos os *links* e os dispositivos de uma conexão, geralmente denominados nós, entre si (FOROUZAN, 2009).

Os distintos tipos de topologias físicas podem ser visualizados abaixo, na figura 4 e são subdivididos em: (a) topologia em malha; (b) topologia em estrela; (c) topologia em barramento; (d) topologia em anel; e (e) topologia híbrida.

Em uma topologia de malha, cada dispositivo possui um *link* ponto a ponto dedicado com cada um dos demais dispositivos. Em uma topologia estrela, cada dispositivo tem um *link* ponto a ponto dedicado, ligado apenas com o controlador central, em geral, denominado *hub*. Em uma topologia de barramento, a única representante da conexão multiponto, um longo cabo atua como um *backbone* que interliga todos os dispositivos da rede. Em uma topologia de anel, cada dispositivo possui uma conexão ponto a ponto dedicada com os outros dois dispositivos conectados de cada lado. Por fim, em uma conexão híbrida, é possível encontrar a combinação de dois ou mais modelos já citados anteriormente (FOROUZAN, 2009).



a) Topologia em Malha completamente conectada

b) Topologia em Estrela conectando 4 estações

(c) Topologia em Barramento conectando 3 estações

(d) Topologia em Anel conectando 6 estações

(e) Estrela conectando 4 estações. Principal de anel, e cada ramificação conectando várias estações em uma topologia de barramento.

Figura 4 – Topologias físicas das redes. Adaptado de (FOROUZAN, 2009).

Por fim, as redes podem ser divididas em 2 categorias principais: *Local Area Network* (LAN) e *Wide Area Network* (WAN) (FOROUZAN, 2009). Entretanto, Kurose e Ross (2006) destaca a importância de outras categorias, como a *Wireless Local Area Network* (WLAN), *Campus Area Network* (CAN) e *Metropolitan Area Network* (MAN), como é apresentado na tabela 1:

Tabela 1 – Categorias Principais das Redes (FOROUZAN, 2009) e (KUROSE; ROSS, 2006)

Categoria	**Descrição**
LAN	É a interconexão de computadores localizados em uma mesma sala ou em um mesmo prédio. Extensão típica de até aproximadamente 200 metros.
WLAN	Idêntica a rede LAN, entretanto sem fio. É uma rede local que usa ondas de rádio para fazer a conexão em rede dos dispositivos. Extensão típica de 15 a 100 metros.
WAN	É a interconexão de computadores localizados em diferentes prédios em cidades distantes em qualquer ponto do mundo. Usa rede telefônica, antenas parabólicas, satélites, etc. Extensão típica acima de 50 quilômetros.
CAN	É a interconexão de computadores situados em prédios diferentes em um mesmo campus ou unidade fabril. Extensão típica de até 5 quilômetros.
MAN	É a interconexão de computadores em locais diferentes da mesma cidade. Pode usar rede telefônica pública ou linha dedicada. Extensão típica de até 50 quilômetros.

2.2 Internet

A história da criação e do desenvolvimento da Internet é uma história de uma aventura extraordinária. Ela evidencia a quebra de barreiras burocráticas e metas institucionais, bem como reforça a ideia de que a cooperação e a liberdade de informação podem ser mais propícias à inovação, do que a competição e os direitos de propriedade (CASTELLS, 2003).

Uma internet (com "i"minúsculo) são duas ou mais redes que podem se comunicar entre si e a mais notável das internets é a Internet (com "I"maiúsculo), que nada mais é que uma colaboração de centenas de milhares de redes interconectadas. A Internet percorreu um longo caminho desde os anos 1960. Atualmente, a Internet não é uma estrutura hierárquica única, sendo composta por várias redes locais e remotas, reunidas por meio de dispositivos de conexão e estações comutadoras (FOROUZAN, 2009).

> “A Internet é uma rede de computadores que interconecta centenas de milhões de dispositivos de computação ao redor do mundo. Há pouco tempo, esses dispositivos eram basicamente PCs de mesa, estações de trabalho Linux, e servidores que armazenam e transmitem informações,

> como páginas da *Web* e mensagens de *e-mail*. No entanto, cada vez mais sistemas finais modernos da Internet, como TVs, laptops, consoles para jogos, telefones celulares, webcams, automóveis, quadros de imagens, e sistemas internos elétricos e de segurança, estão sendo conectados à rede" (KUROSE; ROSS, 2014).

Portanto, podemos entender que a internet nada mais é que uma rede de redes e estabelece a conexão entre múltiplos dispositivos, como pode ser visto pela figura 5:

Figura 5 – Internet: a rede de redes (BERNARDO, 2019).

Para o usuário obter acesso aos serviços disponíveis na Internet é necessário que utilize serviços de *Internet Service Provider* (ISP), ou seja, provedor de acesso à Internet. Como pode ser observado na tabela 2, os provedores podem ser classificados em 4 categorias:

Tabela 2 – Provedores de Serviços de Internet (FOROUZAN, 2009)

Provedores	**Descrição**
Internacionais	Encontram-se no topo da hierarquia dos provedores de serviços de Internet.
Nacionais	São redes *backbone* criadas e mantidas por empresas especializadas. Existem diversos ISPs nacionais operando na América do Norte. Alguns dos mais conhecidos são: *SprintLink*; *PSINet*; *UUNet Technology*; *AGIS*; e *internet MCI*. Geralmente, operam a uma alta taxa de transmissão de dados;
Regionais	São ISPs menores, que são conectados a um ou mais ISPs nacionais. Eles se encontram no terceiro nível da hierarquia com menores taxas de transmissão de dados.
Locais	Fornecem serviços diretamente a seus usuários finais. Os ISPs locais podem estar conectados a ISPs regionais ou diretamente a ISPs nacionais. A maioria dos usuários finais está conectada a ISPs locais.

Os padrões nos serviços da Internet são essenciais na criação e na manutenção de um mercado competitivo para fabricantes de equipamentos, fornecendo diretrizes aos fabricantes, fornecedores, órgãos do governo e outros provedores de serviços para garantir padronização necessária no mercado atual e nas comunicações internacionais (FOROUZAN, 2009). Os padrões são desenvolvidos por meio da cooperação de comitês de criação de padrões, fóruns e órgãos governamentais reguladores. Veja a seguir na tabela 3:

Tabela 3 – Comitês, Fóruns e Órgãos Governamentais reguladores (FOROUZAN, 2009)

Órgãos	**Descrição**
ISO	Um comitê multinacional cujos associados são provenientes de comitês de criação de padrões dos vários governos ao redor do mundo.
ITU-T	Dedica-se à pesquisa e ao estabelecimento de padrões para telecomunicações em geral e para sistemas de dados e telefonia em particular.
Ansi	Uma organização sem fins lucrativos, totalmente privada, e não afiliada ao governo federal norte-americano, mas com a assistência dos Estados Unidos e de seus cidadãos.
IEEE	A maior sociedade de profissionais de engenharia do mundo. Seu intuito é obter avanços na teoria, criatividade e qualidade de produtos, supervisionando o desenvolvimento e a adoção de padrões internacionais para computação e comunicação nos campos da engenharia elétrica, eletrônica e radiofonia.
EIA	Uma organização sem fins lucrativos dedicada à promoção de questões de fabricação na eletrônica.
Fóruns	Trabalham em cooperação com universidades e usuários para testar, avaliar e padronizar novas tecnologias. Eles são capazes de acelerar a aceitação e o emprego dessas tecnologias na comunidade das telecomunicações e apresentam suas conclusões para os órgãos padronizadores.
Órgãos Reguladores	Protegem o interesse público, regulamentando as comunicações via rádio, televisão e fios/cabos, tendo autoridade sobre o comércio interestadual e internacional naquilo que se refere às comunicações. No Brasil tem-se a Anatel e nos Estados Unidos da América a FCC.

2.3 Protocolos de Rede

Para que haja a comunicação efetiva entre dispositivos é necessário respeitar um conjunto de regras, normas e padronizações no estabelecimento da comunicação entre si. Essa normatização é conhecida como protocolos de rede.

Gomes (2019) informa que os protocolos são um conjunto de normas que permitem a comunicação de duas ou mais máquinas entre si, funciona como uma linguagem universal (máquinas de qualquer fabricante interpretam) e são responsáveis por pegar os dados transmitidos

pela rede e dividi-los em pequenos pedaços, que são chamados de pacotes, sendo que cada pacote carrega em si informações de endereçamento de origem e destino. Existem 3 elementos chaves que definem o protocolo de rede:

- Sintaxe: representa o formato dos dados e a ordem pela qual eles são apresentados;
- Semântica: refere-se ao significado de cada conjunto sintático que dá sentido à mensagem enviada;
- *Timing*: define uma velocidade aceitável de transmissão dos pacotes

Como a rede é dividida por camadas (veja subseção 2.3 e na figura 6), os protocolos variam de acordo com o tipo de serviço utilizado e a camada correspondente (GOMES, 2019). Os principais protocolos para cada camada correspondente podem ser visualizados na tabela 4:

Tabela 4 – Camadas e Protocolos (GOMES, 2019) e (IPERIUS BACKUP BRASIL, 2019)

Camadas	**Principais Protocolos**
Aplicação	WWW, HTTP e HTTPS, SMTP, Telnet, SSH, FTP, SFTP, NNTP, RDP, IRC, SNMP, POP3, IMAP, SIP e DNS.
Transporte	TCP, UDP, RTP, DCCP e SCTP.
Rede	IP, IPv4, IPv6, IPsec, ICMP, IGMP e ARP.
Física	Ethernet, FDDi e PPP.

2.4 Modelos de Rede

Comunicações de dados entre diferentes redes não podem ser estabelecidas se não houver regras comuns para transmissão e recepção dos pacotes de dados. Pensando nisso, foram criados os modelos TCP/IP e OSI, sendo que ambos são similares ao descrever as comunicações de dados em rede. Ao mesmo tempo que são semelhantes pela atribuição acima citada, são distintos na segregação de suas camadas. Veja a seguir na figura 6:

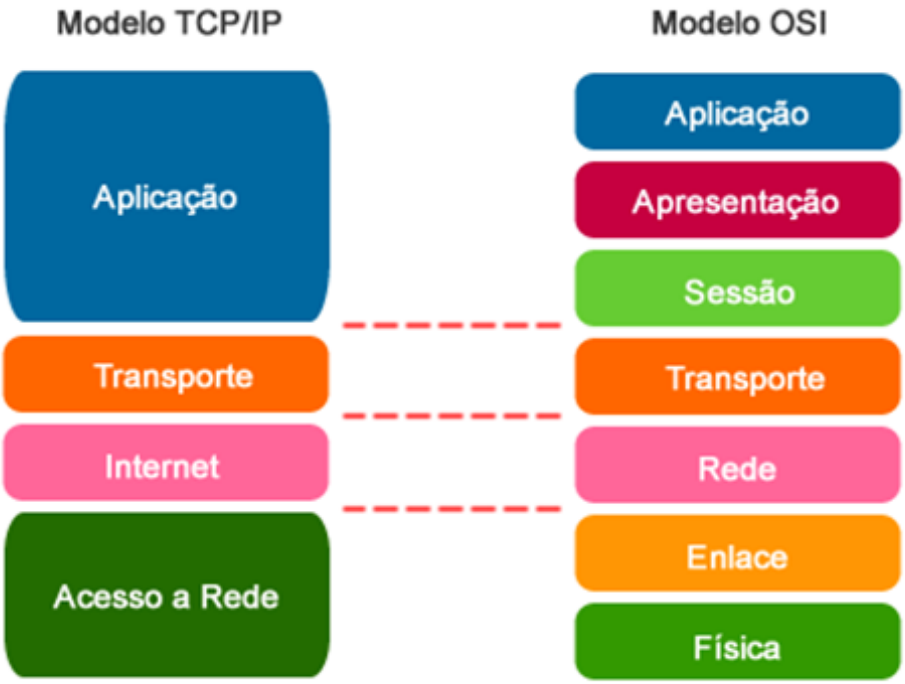


Figura 6 – Modelos TCP/IP x OSI (NASCIMENTO, 2019).

2.4.1 OSI

Introduzido inicialmente no final da década de 1970 pela ISO, o modelo OSI, um modelo de sistema aberto cujo propósito é facilitar a comunicação entre sistemas diferentes sem a necessidade de realizar mudanças na lógica do hardware e software de cada um deles. O modelo OSI não é um protocolo, trata-se de um modelo para compreender e projetar uma arquitetura de redes flexível, robusta e interoperável. Importante salientar que ISO é um organização e OSI um modelo (FOROUZAN, 2009).

Como visualizado na figura 6, o modelo OSI é categorizado em 7 camadas: Aplicação; Apresentação; Sessão; Transporte; Rede; Enlace; e Física. As 7 camadas desse modelo da podem ser visualizadas na tabela 5:

Tabela 5 – Camadas e Protocolos no Modelo OSI (IPERIUS BACKUP BRASIL, 2019)

Camadas	**Descrição**
7 - Aplicação	Interage diretamente com aplicações de software, fornecendo funções de comunicação conforme necessário, sendo o mais próximo dos usuários finais. Define protocolos para aplicações finais, tais como DNS, FTP, HTTP, IMAP, POP, SMTP, SNMP e Telnet.
6 - Apresentação	Verifica os dados garantido ser compatível com os recursos de comunicação, convertendo-os para a forma que o nível de aplicação e os níveis mais baixos aceitem. É utilizada em chamadas de vídeo onde serão compactadas durante a transmissão e em criptografia de mensagem de texto, por exemplo.
5 - Sessão	Controla os diálogos (conexões) entre os dispositivos, estabelecendo, gerenciando, mantendo e finalizando as conexões entre a aplicação local e a remota. Também lida com funções de autenticação e autorização, verificando também a entrega dos dados e é comumente implementada em ambientes de aplicativos que utilizam chamadas para gerenciamento remoto.
4 - Transporte	Fornece as funções e meios de transferência de sequências de dados de uma fonte para um hospedeiro de destino através de uma ou mais redes, assegurando a qualidade de funções de serviços e a entrega completa dos dados. TCP e UDP são protocolos essenciais nesta camada.
3 - Rede	Trata o encaminhamento de pacotes através de funções de comutação e de endereçamento lógico. Se a mensagem for muito longa, a rede pode dividi-la em vários segmentos de um nó, enviando-os separadamente, remontando os fragmentos em outro nó.
2 - Enlace	Fornece transferência entre nós – uma ligação entre dois nós diretamente conectados. Lida com empacotamento e desempacotamento dos dados em quadros. A camada de ligação de dados está geralmente dividida em duas subcamadas – MAC, o controle de acesso à mídia, e LLC, o controle de ligação lógica. A camada MAC é responsável por controlar como os dispositivos recebem acesso à rede e permissão numa mídia para transmitir dados. A camada LLC fica responsável por identificar e encapsular os protocolos da camada de rede e controlar a validação de erros e sincronização dos quadros.
1 - Física	Define as especificações elétricas e físicas da ligação de dados, como a disposição de pinos do conector, a operação de tensões num cabo eléctrico, especificações de cabos de fibra óptica e a frequência para os dispositivos sem fios. Também responsável pela transmissão e recepção de dados brutos, não estruturados em um meio físico. o controle da taxa de bits é executado na camada física.

2.4.2 TCP/IP

O conjunto de protocolos TCP/IP foi desenvolvido antes do modelo OSI. O TCP/IP é um conjunto de protocolos hierárquicos compostos por módulos interativos, sendo que cada um deles provê funcionalidades específicas. Entretanto, os módulos não são necessariamente interdependentes. Enquanto o modelo OSI especifica quais funções pertencem a cada uma de suas camadas, as camadas do conjunto de protocolos TCP/IP contêm protocolos relativamente independentes que podem ser mesclados e combinados dependendo das necessidades do sistema (FOROUZAN, 2009).

Como visualizado na figura 6, o modelo TCP/IP é categorizado em 4 camadas: Aplicação; Transporte; Internet; e Acesso a Rede. Veja a seguir, na tabela 6 suas camadas:

Tabela 6 – Camadas e Protocolos no Modelo TCP/IP (IPERIUS BACKUP BRASIL, 2019)

Camadas	**Descrição**
Aplicação	Fornece às aplicações a capacidade de acesso a serviços de outras camadas, definindo os protocolos onde os aplicativos usarão para trocar dados. Os protocolos da camada de aplicação mais amplamente conhecidos incluem HTTP, FTP, SMTP, Telnet, DNS, SNMP e RIP.
Transporte	Responsável pelo fornecimento da camada de aplicação com serviços de sessão de comunicação e datagrama. Os protocolos de núcleo desta camada são o TCP e UDP. O protocolo TCP fornece um serviço de comunicação orientada a conexão confiável um-para-um. O protocolo UDP fornece um serviço de comunicação orientada a conexão não confiável um-para-um ou um-para-muitos.
Internet	Responsável pelo endereçamento de Internet do hospedeiro, empacotamento e funções de encaminhamento. Os principais protocolos dessa camada de protocolo Internet são IP, ARP, ICMP e IGMP. Nesta camada o IP adiciona um cabeçalho aos pacotes tornando-se conhecida como endereço de IP.
Acesso a Rede	Conhecida também por camada de enlace, é responsável por inserir os pacotes TCP/IP no caminho de rede e receber pacotes TCP/IP fora dele. O TCP/IP foi projetado para ser independente do método de acesso à rede, formato de quadro e tipo de mídia. Em outras palavras, é independente de qualquer tecnologia de rede específica. Desta maneira o TCP/IP pode ser utilizado para conectar diferentes tipos de rede como *Ethernet*, *Token Ring*, *X.25*, *Frame Relay* e ATM.

2.4.3 TCP/IP x OSI

Com o conhecimento da divisão de camadas em ambos os modelos, é possível diagnosticar onde o problema está quando falha uma conexão. O princípio está em verificar a partir do nível mais baixo ao invés de partir do nível mais alto (IPERIUS BACKUP BRASIL, 2019).

Pela figura 6 é possível identificar as principais diferenças na categorização de cada modelo. A camada de aplicação do modelo TCP/IP é semelhante às camadas 5, 6, 7 do modelo OSI combinadas, embora o modelo TCP/IP não tenha uma camada de apresentação separada, ou camada de sessão. A camada de transporte do TCP/IP engloba tanto as responsabilidades da camada de transporte OSI quanto algumas das responsabilidades da camada de sessão OSI. A camada Internet do modelo TCP/IP é semelhante à Rede no modelo OSI. Por fim, a camada de acesso de rede do modelo TCP/IP contempla as camadas de enlace e física do modelo OSI (IPERIUS BACKUP BRASIL, 2019).

As corporações de padronização optaram por seguir com o modelo OSI. Todavia, o modelo mais utilizado atualmente é o modelo TCP/IP. Comer (2016) enfatiza que, além das camadas 6 e 5 (Apreentação e Sessão, respectivamente) do modelo OSI serem desnecessárias, com o tempo ficou bastante clara a superioridade da tecnologia TCP/IP perante à OSI em redes internas e também externas.

2.5 Dispositivos de Rede

Há vários equipamentos compreendidos em uma determinada rede, veja na figura 7. Mesmo que o argumento seja trivial, é importante destacar que quanto maior for a rede, maior será a quantidade de equipamentos que a mesma possuirá. Os equipamentos e dispositivos das redes estão compreendidos desde a infraestrutura da mesma à seu cliente final. Kurose e Ross (2014) afirmam que, no jargão da rede, todos esses equipamentos são denominados hospedeiros ou sistemas finais e que em julho de 2011, desconsiderando os *smartphones*, *laptops* e outros dispositivos que são conectados à rede de maneira intermitente, haviam cerca de 850 milhões de sistemas finais ligados à Internet.

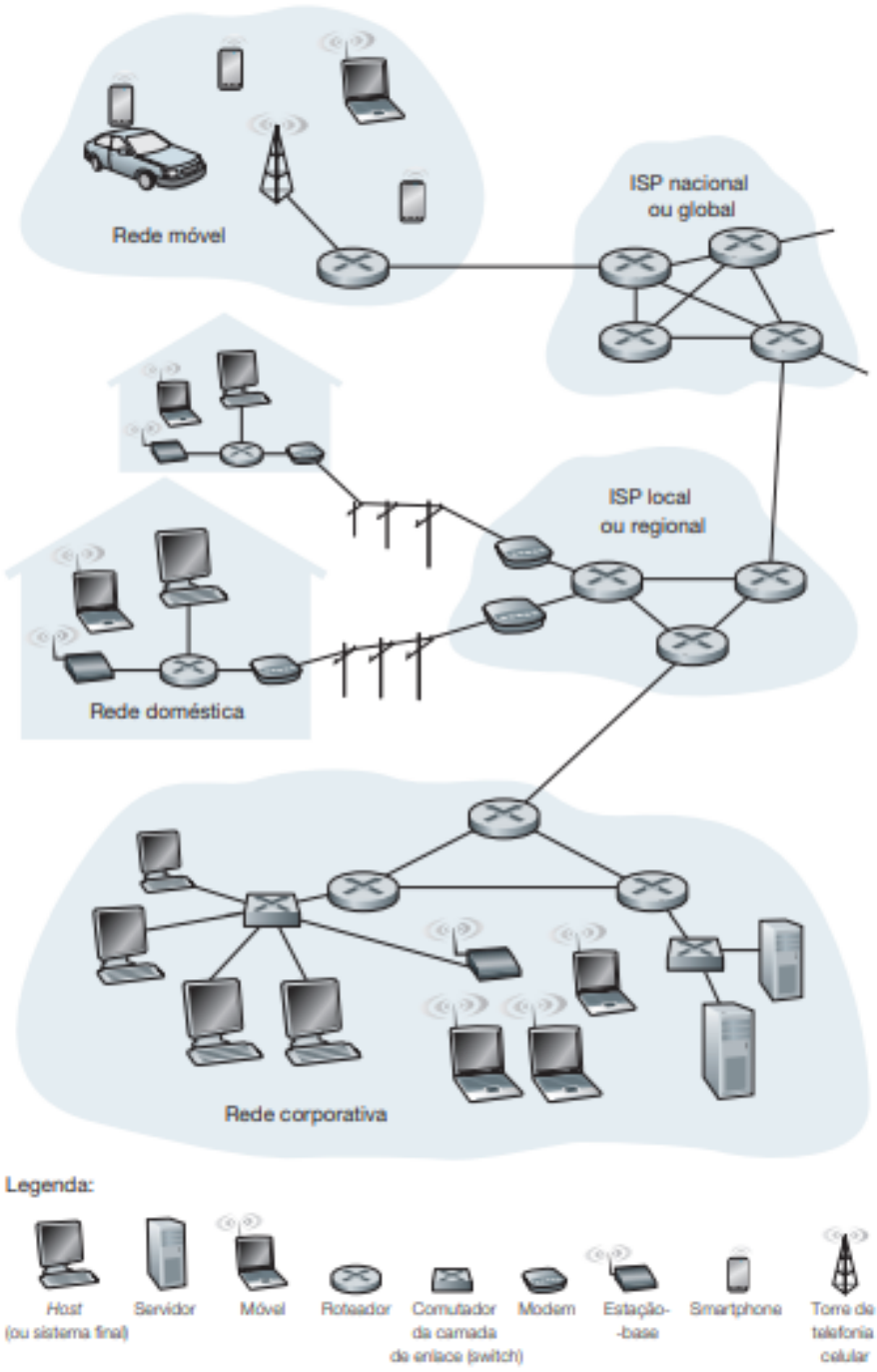


Figura 7 – Alguns Componentes da Internet (KUROSE; ROSS, 2014).

Em outras palavras, Santos (2016) informa que há dois principais grupos de dispositivos que são normalmente citados: dispositivo ativo e passivo.

2.5.1 Dispositivos Passivos de Rede

O grupo de componente passivo é representado pelos elementos responsáveis pelo transporte dos dados através de um meio físico. São todos dispositivos que funcionam com pulsos/sinais elétricos e não procedem com uma análise dos dados, como os Painéis de Conexão (Blocos, *Patch Panel*), *Rack* de Rede (Parede ou Piso), *Voice Panel*, Cabos Metálicos, Cabos

Ópticos, Conectores e Extensores e Cordões de Manobra (*Patch Cable*, *Adapter Cable*, *Cable Link*, entre outros).

2.5.2 Dispositivos Ativos de Rede

Já o grupo de dispositivos ativos são os que analisam e decidem sobre o modo como a informação atravessa o equipamento, afetando o funcionamento dos sistemas. São eles os responsáveis pela comunicação adequada entre as estações de trabalho e os servidores, e garantem uma comunicação confiável com a performance requerida pela aplicação. Os dispositivos ativos de rede podem ser os *Switches*, *Hubs*, *Bridges* (Pontes), *Modems*, Roteadores, Placas de Rede, *Firewall*, *Gateway*, Repetidores, Chaveador KVM, Conversores de Mídia, *Access Points* (Pontos de Acesso) e Servidores.

2.6 Proteção das Redes

É de suma importância assegurar o sigilo de dados pessoais e empresariais, de movimentações bancárias e de senhas. Entre as principais questões de segurança em redes, Forouzan (2009) destaca a proteção ao acesso não autorizado de dados confidenciais, a proteção aos danos acidentais ou intencionados e a implementação de políticas e procedimentos para a recuperação de violações e perdas de dados.

Kurose e Ross (2014) identifica 4 propriedades desejáveis para uma comunicação segura: confidencialidade, no qual apenas o remetente e o destinatário pretendido devem entender o conteúdo da mensagem transmitida; integridade de Mensagem, para assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão; autenticação do ponto final, onde o remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação se é de verdade quem alega ser; e segurança operacional que é a segurança de rede nas organizações (empresas, universidades etc.) que estão conectadas à Internet pública.

A segurança em redes está embasada em um outro conceito: a criptografia. Técnicas criptográficas permitem que o remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação dos dados interceptados. Além disso, é necessário que o destinatário esteja habilitado a recuperar os dados originais a partir dos dados disfarçados (KUROSE; ROSS, 2014). Veja a seguir uma breve descrição do termo:

> "Criptografia, palavra de origem grega, cujo significado é "escrita secreta". Ciência e arte de transformar mensagens para torná-las seguras e imunes a ataques, a criptografia pode fornecer diversos aspectos de segurança relacionados a troca de mensagens através de redes. Tais aspectos estão relacionados a confidencialidade, integridade, autenticação e o não-repúdio. A criptografia também fornece autenticação de emissor

> e receptor no envio e recebimento de mensagens entre si." (FOROUZAN, 2009).

Ainda, de acordo com Forouzan (2009), os algoritmos de criptografia podem ser divididos em 2 grupos: chaves simétricas e chaves assimétricas. Na criptografia de chaves simétricas, também conhecidas por chaves secretas, a chave é compartilhada, ou seja, a mesma chave usada pelo emissor no ato de criptografia é usada pelo receptor ao ser descriptografada. Na criptografia de chaves assimétricas, também conhecidas por chaves públicas, é combinação de chaves públicas e privadas, no qual a chave privada é mantida pelo receptor e chave pública fica disponível ao público, em geral.

No que se refere às principais técnicas utilizadas para implementar políticas de segurança em redes, Forouzan (2009), Kurose e Ross (2014) e Comer (2016) destacam-as pelos seguintes itens: *hash* (ou *hashing*); criptografia; assinatura digital; certificados digitais; sistemas de detecção de intrusão; e varredura de conteúdo e inspeção detalhada de pacotes. Além desses já citados, os autores ainda ressaltam a utilização de *Firewalls*, de VPN e de tecnologias de segurança, como: PGP; SSH; SSL; TLS; HTTPS; IPsec; RADIUS; e WEP e WPA.

2.7 Tecnologias de Segurança Para o Regime de Teletrabalho

Todas as tecnologias e ferramentas no tópico acima são de extrema importância para estabelecer a proteção de informações confidenciais e a segurança nas operações que estão disponibilizadas em rede. Devido ao atual cenário pandêmico da COVID-19 que estamos vivenciando desde o final do ano de 2019, houve um aumento vertiginoso na modalidade de teletrabalho, conhecida também por *Home Office*. Esse aumento deve-se à influência do isolamento social e pela limitação do contato social em ambientes corporativos e industriais, no qual teve-se que substituir atividades presenciais pelas remotas, assim como pelo recente interesse de algumas empresas em criar vagas exclusivas nesta modalidade. Mesmo que ela já estivessem sendo esperada há muitos anos por aqueles interessados em trabalhar de casa, alguns entraves que rodeavam o trabalho remoto, não a permitiam evoluir.

No ano de 2020 foram criadas 2428 vagas a mais na modalidade de tele-trabalho, o que equivale a um aumento de 309%, o que correspondeu a 41% das oportunidades abertas em site de recrutamento e seleção (VICENTIN; LUCENA, 2021). Ainda no ano de 2020, ápice da doença e da transformação nas modalidades trabalhistas, um estudo elaborado pela Fundação Instituto de Administração (FIA) coletou, em abril, dados de 139 pequenas, médias e grandes empresas que atuam em todo o Brasil e foi observado que 46% delas adotaram o regime *Home Office*. 67% das companhias relataram dificuldades na implementação da modalidade, mas apesar das dificuldades, 50% das empresas disseram que a experiência com o teletrabalho superou as expectativas, 44% afirmaram que o resultado ficou dentro do esperado e 34% pretendem manter essa modalidade após o término da pandemia (MELLO, 2020).

Analisando o crescente aumento desse regime de trabalho, é interessante ficar atento as vulnerabilidades que possamos estar expostos. Portanto, uma das primeiras recomendações é que se use uma máquina para trabalhar de uso exclusivo para este fim, impedindo o vazamento de dados ou acesso a páginas que podem prejudicar o seu computador. Ao realizar ligações e/ou chamadas de vídeo é importante utilizar ferramentas confiáveis e que o departamento de Tecnologia da Informação (TI) da empresa tenha aprovado o uso. Quanto a utilização de senhas, é recomendado que sejam alteradas com frequência as senhas de acesso restrito a informações pessoais e corporativas, a estações de trabalho, bem como senhas de roteadores e que elas devem ser armazenadas em servidores e sistemas de gerenciamento de senhas, e nunca serem anotadas em papel ou locais visivelmente desprotegidos. Tratando-se de proteção, é necessária a utilização frequente de antivírus e atualizações em *drivers*, *software* e *firmware*, a fim de inibir tentativas de roubo de informações e proteger o sistema contra ameaças danosas (SCHULTZ, 2020b).

Schultz (2020b) ressalta que a criptografia segue sendo a maior aliada a proteção de informações, impedindo que pessoas não autorizadas acessem mensagens privadas, através da construção e análise de protocolos de segurança. Outra ferramenta extremamente importante, que garante a segurança cibernética no acesso remoto das empresas é a VPN, uma tecnologia que liga dois ou mais computadores através de uma conexão particular, segura e criptografada. Na VPN, utilizando de um nome de usuário, senha e, de preferência, um segundo fator de autenticação, é possível conectar o computador do funcionário, em regime remoto, ao servidor da empresa, o permitindo utilizar as ferramentas e dos dados necessários para trabalhar com segurança e tranquilidade. Ademais, ferramentas de abertura e gerenciamento de chamados tendem a quantificar os problemas enfrentados, e ferramentas de monitoramento de rede, responsáveis por medir, em tempo real, os recursos das redes de computadores visam a detecção de anomalias na performance e na disponibilidade. Por fim, a mais importante de todas, é de suma importância que cada empresa implemente sua política de proteção dos dados e engaje seus funcionários a seguirem a normatização.

Além das VPNs, existem outras ferramentas de acesso remoto focadas em suporte de computadores e softwares, e em acesso a informações e recursos, como o *Terminal Service* e a Computação em Nuvem. O *Terminal Service*, de acordo com Bug Buster (2020) pode ser obtido por ferramentas já conhecidas no mercado: Microsoft Remote Desktop – (Conexão de Área de Serviço Remota), Chrome Remote Desktop, TeamViewer, AnyDesk e Getscreen.me.

A *cloud computing*, a computação em nuvem, pode ser entendida como o fornecimento de serviços de computação pela Internet (“a nuvem”), incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência, para oferecer inovações mais rápidas, recursos flexíveis e economias de escala, consumindo apenas os serviços de nuvem que necessita, ajudando a reduzir os custos operacionais, a executar sua infraestrutura com mais eficiência e a escalonar conforme as necessidades da sua empresa mudam (MICROSOFT AZURE, 2015).

Quanto à nuvem, há quatro categorias diferentes na implementação de seus serviços.

Veja a seguir na tabela 7.

Tabela 7 – Serviços em nuvem (MICROSOFT AZURE, 2015)

Nuvem	**Descrição**
Nuvem Pública	Compartilha recursos e oferece serviços ao público em geral da Internet, no qual todo o hardware, software e outras infraestruturas de suporte são de propriedade e gerenciadas pelo provedor de nuvem seus serviços são gerenciados por uma conta usando um navegador da Web.
Nuvem Privada	Não é compartilhada e oferece serviços em uma rede interna privada (geralmente hospedada localmente), pode estar localizada fisicamente no *datacenter* local da empresa ou pelo disponibilidade de algumas empresas que pagarem provedores de serviços terceirizados para hospedar sua nuvem privada.
Nuvem Híbrida	Compartilha serviços entre nuvens públicas e privadas ligadas por uma tecnologia que permite que dados e aplicativos sejam compartilhados entre elas.
Nuvem de Comunidade	Compartilha recursos apenas entre organizações, como instituições governamentais.

Portanto, de forma sintetizada, a utilização dos recursos de computação em nuvem geram economia de dinheiro e tempo, trazem mais segurança e maximiza recursos, visto que os dados ficam protegidos em um *datacenter* do provedor de computação em nuvem.

De forma análoga aos recursos de acesso remoto, temos bastante ferramentas de computação em nuvem reconhecidas e renomadas no mercado. Há ferramentas em nuvem para o uso de armazenamento de dados e *backups*, de *e-mails*, de agenda e tarefas, chamadas e videoconferência, espaços de trabalho virtualizados, bem como provedores de nuvem pública que dispõem de servidores dedicados para os serviços contratados, entre outros. Dentre esses e tantos outros serviços disponibilizados pela nuvem, destacam-se as grandes empresas de tecnologias: a *Microsoft*, com o provedor *Microsoft Azure* e os serviços do *Microsoft Office 365* e *Onedrive*; *Google*, com o provedor *Google Cloud* e os serviços do *Google G-Suite* e *Google Drive*; *Amazon* com o provedor *Amazon Web Services* (AWS) e os serviços do *Amazon Cloud Drive*; *Alibaba Cloud*; e *IBM Cloud*.

Vale destacar que há muitos outros provedores e serviços de nuvens espalhados no mundo da Internet e cabe ao cliente optar por aquele que lhe for mais acessível, que supra suas necessidades e seja vantajoso em suas necessidades.

2.8 Segurança Cibernética

Atualmente, o avanço tecnológico e a quantidade de sistemas e redes conectadas à Internet estão crescendo vertiginosamente, além de sofrerem repentinas mudanças, entendidas por atualizações e/ou evoluções à tecnologia já existente. Com isso, aumenta-se a preocupação

quanto a segurança desses sistemas "conectados"e requer-se mecanismos que possam normatizar proteções e mitigar vulnerabilidades.

Canongia e Junior (2010) afirma que a segurança cibernética pode ser entendida pela prevenção aos danos causados pelo uso não autorizado da informação eletrônica e de sistemas de comunicações e respectiva informação neles contida, visando assegurar a confidencialidade, integridade, e disponibilidade, incluindo, também, ações para restaurar a informação eletrônica e os sistemas de comunicações no caso de um ataque terrorista ou de um desastre natural. É como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas. Os autores ainda definem o que vem a ser o Espaço Cibernético:

> "O ciberespaço, ou espaço cibernético, é considerado como a metáfora que descreve o espaço não físico criado por redes de computador, notadamente a Internet, onde as pessoas podem se comunicar de diferentes maneiras, como mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros" (CANONGIA; JUNIOR, 2010).

A segurança cibernética, ou cibersegurança, ou ainda *cybersecurity*, pode ser considerado um tema transversal, multidisciplinar e multissetorial. A Agência Nacional de Telecomunicações, a Anatel, a define por:

> "A segurança cibernética são ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético que visam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis" (ANATEL, 2021).

Para Schultz (2020a), a segurança cibernética é um ramo da segurança da informação e tem como objetivo prevenir os ataques realizados por sistemas maliciosos que se aproveitam de falhas sistêmicas para invadir dispositivos, roubando, manipulando e tornando indisponível uma série de dados ou arquivos. Dessa forma, segurança cibernética envolve a prevenção e proteção no que tange o ciberespaço e a segurança da informação envolve a prevenção e proteção contra todo tipo de risco, seja físico ou digital, controlando acessos de pessoas a locais, permissões para acessos de arquivos, entre outros.

Os agentes causadores de ataques são popularmente conhecidos por *Hackers* ou cibercriminosos. A definição de *hackers*, de acordo com o Mcafee (2019), uma das mais expressivas empresas de software de segurança, baseia-se na subdivisão do termo em 9 categorias, como pode ser visualizado na tabela 8 a seguir.

Tabela 8 – A Definição de *Hackers* - (MCAFEE, 2019)

Hackers	**Descrição**
Hackers White Hat	Considerados os *hackers* bonzinhos, são especialistas em segurança computacional que se concentram em fazer testes de penetração e outras metodologias de modo a garantir que os sistemas de informação de empresas estejam realmente seguros.
Hackers Black Hat	Considerados os *hackers* malvados, geralmente chamados apenas por *hackers*. O termo costuma ser usado especificamente para criminosos que invadem redes ou computadores, ou ainda que criam vírus de computador. *Hackers* desse tipo agem mais rapidamente do que *Hackers White Hat*, visto que costumam encontrar o caminho que oferece menor resistência, por erro humano ou negligência – ou criam um novo tipo de ataque.
Hackers Gray Hat	Esses são *hackers* não usam suas habilidades para benefício próprio, mas também não operam de forma totalmente legal. Um *hacker* que invade o sistema de uma empresa para revelar uma vulnerabilidade e posta a descoberta na internet, mesmo que faça algo de positivo para a empresa, comete um crime ao invadir um sistema sem permissão.
Script Kiddies	Termo pejorativo ao *Hackers Black Hat* que usam programas baixados da internet para atacar redes, alterar sites para se tornarem conhecidos. Alguns deste se enquadram na categoria *Hackers Green Hat*: são amadores curiosos que desejam aprender e um dia se tornar um *Black Hat* de verdade.
Hacktivists	*Hackers* que almejam fazer parte de mudanças sociais.
Hackers Patrocinados por Governos	Governos ao redor do mundo estão conscientes de que é útil a seus objetivos militares estarem bem posicionados no mundo *online*, no qual o controle do ciberespaço é decisivo. Esses *Hackers* não têm limite de tempo e contam com orçamento para focar civis, empresas e outros governos.
Hackers espiões	Empresas contratam *hackers* para que se infiltrem em concorrentes e roubem segredos comerciais. Esses *hackers* podem tentar ataques externos ou podem conseguir empregos para agir como infiltrados.
Whistleblowers	Chamados de “Infiltrados mal-intencionados”, trata-se de uma pessoa inserida em uma organização que usa seu acesso a sistemas para vazar informações que podem ser preocupantes. Esses *hackers* podem acessar informações para vender segredos comerciais ou conseguir emprego em outras empresas.
Ciberterroristas	Geralmente, motivados por crenças religiosas ou políticas, esses *hackers* tentam criar e espalhar medo, caos e violência ao interromper o funcionamento de serviços cruciais de infraestrutura. Os ciberterroristas são, de longe, os mais perigosos e contam com uma ampla variedade de habilidades e objetivos.

Entretanto, de acordo com Chema Alonso, espanhol especialista em segurança na Internet, há uma grande diferença entre os dois termos. Para ele, os *hackers* buscam aumentar a segurança de todos os usuários da internet, identificando vulnerabilidades e fraquezas nos sistemas para então corrigi-los, ao passo que os cibercriminosos, os verdadeiros criminosos nesse ambiente conectado, infectam sistemas para invadi-los, roubar senhas e furtar dados (MORELLI, 2015).

A segurança cibernética, obviamente, previne ameaças e ataques cibernéticos. Mas quais são os principais ataques e ameaças cibernéticas? A tabela 9 a seguir apresenta os principais problemas enfrentados pelo usuário ao utilizar a Internet.

Tabela 9 – Principais Problemas de Segurança na Internet (COMER, 2016)

Ameaça	**Descrição**
Phishing	Técnica da Engenharia Social, usada para disfarçar-se como um site bem conhecido, como o de um banco, para obter informações pessoais de um usuário, como número de conta e código de acesso.
Misrepresentation	A falsificação ocorre ao fazer afirmações falsas ou exageradas sobre produtos ou serviços, ou entregar produtos falsos ou de qualidade inferior.
Scams	Os golpes são várias formas de trapaça destinadas a enganar usuários ingênuos para fazê-los investir dinheiro ou cometer algum crime.
Denial of Service (DoS)	Negação de Serviço, usada para bloquear intencionalmente um determinado *site* da Internet para impedir ou dificultar atividades de negócios e comércio.
Perda do Controle	Um intruso ganha o controle do computador de um usuário e usa o computador para cometer um crime.
Perda de Dados	Perda de propriedade intelectual ou outra informação valiosa da empresa

Na tabela 9 foram apresentados os principais problemas de segurança na internet. Como ameaças à segurança, podem-se apresentar os *malwares*, vírus, *worms*, *adwares* e *ransomwares*, *trojans*, *bot/botnet*, *spyware*, *backdoor* e *rootkit* - suas definições podem ser visualizadas na tabela 10.

Tabela 10 – *Software* mal intensionados (SCHULTZ, 2020a) e (CERT.BR, 2017)

Técnica	**Descrição**
Malware	Abreviação de "*software* mal-intencionado", compreendidos pelos vírus, *worms*, *trojans*, entre outros, pode ser visto como um termo abrangente que se refere a qualquer *software* projetado para causar danos a um computador, servidor ou rede. Ele é apresentado de várias formas e pode causar sérios danos a um computador ou a uma rede corporativa.
Vírus	É um programa que, quando executado, é capaz de infectar todos os computadores conectados em uma mesma rede, roubando dados, corrompendo arquivos e enviando *spams* para contatos de *e-mail* (ampliando o ataque), ou até controlar o computador por completo.
Worms	Ao contrário dos vírus, os *worms* não necessitam de nenhuma ação do usuário, chegam como anexos de um *e-mail* ou mídia infectada e se replicam sobre a rede, causando congestionamento na mesma.
Ransomware	É um sequestrador de dados, que invade o sistema, rouba dados e pede um valor, geralmente em criptomoedas, como resgate.
Adwares	Proveniente de anúncios em sites da Internet, o *malware* se disfarça de propaganda para buscar o seu clique.
Trojans	Os *trojan-horse*, ou cavalos de troia, 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. Além disso, são um dos códigos maliciosos mais perigosos, pois permeiam em todos os ataques existentes, ou sejam, são capazes de instalar códigos maliciosos, possibilitar o acesso remoto do atacante ao computador, instalar ferramentas de negação de serviço, alterar e apagar arquivos e diretórios, formatar o disco rígido, monitorar e coletar informações confidenciais, e instalar servidor de *proxy* para direcionar um determinado computador a disparar *spam* à rede.
bot/botnet	Um computador infectado por um *bot* costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Já o *Botnet* é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*.
Spyware	É um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado tanto de forma legítima quanto maliciosa.
Backdoor	É um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
Rootkit	É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

As principais técnicas utilizadas pelos cibercriminosos podem até ser de conhecimento de muitos. Todavia, acompanhando o crescimento da tecnologia e dos métodos de segurança, esses agentes buscam inovar em sua ações e técnicas para conseguir invadir sistemas. Veja a seguir, na tabela 11, algumas das principais técnicas utilizadas em ataques.

Tabela 11 – Principais Técnicas Utilizadas em Ataques (COMER, 2016)

Técnica	**Descrição**
Escutas Telefônicas	Fazer uma cópia dos pacotes à medida que eles passam pela rede para obter informações.
Repetição	Enviar pacotes capturados de uma sessão anterior, por exemplo: um pacote de senha obtido em um *login* anterior.
Buffer Overflow	Enviar mais dados do que um receptor espera para forçá-lo a armazenar os valores em variáveis fora do *buffer*.
Spoofing de Endereços	Falsificar o endereço IP de origem em um pacote fingindo ser o transmissor para enganar um receptor no processamento do pacote.
Spoofing de Nomes	Usar uma *URL* muito similar a de algum site bem conhecido, porém com um pequeno erro de ortografia, para receber o direcionamento de *DNS* quando o usuário digitar o nome errado sem querer. Outra forma é atacar o servidor *DNS* para ele efetuar uma tradução incorreta de nome para IP.
DoS e *DDoS*	Inundar um site com pacotes para impedir que ele opere normalmente.
SYN Flood	Enviar um fluxo de segmentos TCP do tipo *SYN* buscando exaurir o total de conexões TCP possíveis em um receptor.
Quebra de senha	Criar sistemas automatizados que quebrem a senha ou a chave de criptografia visando obter acesso não autorizado.
Port Scanning	A varredura de portas tenta conexão com cada porta, possivelmente buscando encontrar uma vulnerabilidade.
Interceptação de Pacotes	Remover um pacote da Internet a fim de substituí-lo num ataque do tipo *man-in-the-middle*.

Além dos métodos já tradicionais, como podem ser visualizados na tabela 11 abaixo, os criminosos intensificaram no primeiro semestre do ano de 2020, impulsionados pela pandemia da COVID-19, os golpes de Engenharia Social - manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais: os golpes de doação; 12 aplicativos móveis nas lojas oficiais da *Apple* e *Google* e mais de 60 sites e aplicações falsas para furtar o benefício do Auxílio Emergencial do Governo Federal; currículos maliciosos; sites maliciosos sobre a COVID-19; *Spear-Phishing* - *phishing* direcionado; *Vishing* - *phishing* por voz; e a ciberespionagem - suspeitas de países que ordenaram invasões a hospitais e entidades de saúde presentes em outras nações (MUNDO+TECH, 2020).

2.9 *Cybersecurity Frameworks*

Um *framework* é um termo da língua inglesa que, em sua tradução direta, significa estrutura. De maneira geral, essa estrutura é feita para resolver um problema específico, que nesse caso fornece uma solução para cibersegurança.

Uma estrutura de segurança cibernética fornece uma linguagem comum e um conjunto de padrões para que os líderes de segurança dos países e dos distintos setores da economia entendam suas posturas de segurança e as de seus fornecedores. Com uma estrutura em vigor, torna-se muito mais fácil definir os processos e procedimentos que sua organização deve seguir para avaliar, monitorar e mitigar os riscos de segurança cibernética (CISTERNELLI, 2020).

Além disso, para Mutune (2019), as estruturas de segurança cibernética referem-se a estruturas definidas contendo processos, práticas e tecnologias que as empresas podem usar para proteger a rede e os sistemas de computador contra ameaças à segurança e as empresas devem compreendê-las para aprimorar sua segurança organizacional.

Com base nos estudos de Cisternelli (2020) e Mutune (2019), serão apresentadas as principais estruturas de cibersegurança e suas particularidades:

2.9.1 *Frameworks NIST* para Segurança Cibernética

2.9.1.1 *NIST Cybersecurity Framework - NIST CSF*

O *NIST*, por meio do decreto nº 13636 “Aperfeiçoando a Segurança Cibernética da Infraestrutura Crítica”, em fevereiro de 2013, desenvolveu a Versão 1.0 do Guia. Posteriormente, no ano de 2018, o mesmo órgão atualizou para a Versão 1.1 do Guia. O objetivo do decreto executivo é aumentar a segurança da infraestrutura crítica do país, protegendo-os de ataques internos e externos (NIST, 2018).

Portanto, foi criado um guia gratuito de aperfeiçoamento da segurança cibernética para infraestrutura crítica, conhecido pela sigla *NIST CSF*. Embora tenha sido criado para estruturas críticas, o mesmo guia pode ser utilizado por órgãos públicos, organizações privadas e pela sociedade, para fortalecer suas defesas cibernéticas, independente do setor na economia em que atua e seu tamanho (NIST, 2018).

Com base nesses padrões, diretrizes e práticas, o Guia oferece uma taxonomia e mecanismos comuns para que as organizações (NIST, 2018):

- Descrevam sua situação atual no que tange à segurança cibernética;
- Descrevam seus objetivos no que tange à segurança cibernética;
- Identifiquem e priorizem oportunidades de aperfeiçoamento dentro do contexto de um processo contínuo e reproduzível;

- Avaliem seus progressos frente aos objetivos:
- Comuniquem-se com *stakeholders* internos e externos sobre os riscos apresentados na atual segurança cibernética.

Em particular, o NIST CSF descreve cinco funções que gerenciam os riscos à segurança de dados e informações, como pode ser observado na figura 8. Veja a seguir, na tabela 12, as funções identificar, proteger, detectar, responder e recuperar (NIST, 2018).

Figura 8 – Funções do *Framework NIST CSF* (NIST, 2018).

Tabela 12 – Funções do *Framework NIST CSF* (NIST, 2018)

Funções	**Descrição**
Identify (Identificar)	Desenvolver uma compreensão organizacional para gerenciar o risco de segurança cibernética no que tange a sistemas, pessoas, ativos, dados e recursos.
Protect (Proteger)	Desenvolver e implementar proteções necessárias para garantir a prestação de serviços críticos.
Detect (Detectar)	Desenvolver e implementar atividades necessárias para identificar a ocorrência de um evento de segurança cibernética.
Respond (Responder)	Desenvolver e implementar atividades apropriadas para agir contra um incidente de segurança cibernética detectado.
Recover (Recuperar)	Desenvolver e implementar atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um incidente de segurança cibernética.

2.9.1.2 *NIST CSF Maturity Tool*

A Ferramenta de Maturidade, criada por John J. Masserini, baseian-se no *NIST Cybersecurity Framework (CSF)* 2018, versão 1.1. A ferramenta busca oferecer ao setor industrial uma

avaliação de seu programa de segurança, por intermédio de uma planilha em *Excel*.

Em um esforço para separar o que deve ser feito do que está sendo feito, a ferramenta mede o programa de segurança em duas frentes: políticas e práticas. A avaliação da Maturidade Política mede o quão bem sua política escrita atende aos requisitos do CSF, fornecendo um delineamento claro em torno dos níveis de maturidade da política que geralmente se alinham com as melhores práticas do setor. Em contrapartida, a avaliação da maturidade prática tentará avaliar o grau de maturidade de suas práticas operacionais reais em relação ao CSF, sendo fundamental a honestidade ao responder às perguntas da avaliação (MASSERINI, 2019).

Masserini (2019) informa que, como resposta a essas perguntas, os avaliadores podem atribuir pontuações que variam de 0 a 5 para a política e prática (*policy score* e *practice score*, respectivamente): 0 - não existente; 1 - estado inicial; 2 - estado de reconhecimento; 3 - definido; 4 - gerenciado; e 5 - ótimo. É possível também estabelecer uma pontuação a ser alcançada (*target score)*. À partir dessas pontuações, é obtido um gráfico, como pode ser visto na figura 9, apresentando os resultados alcançados. Esse gráfico serve para identificar quais itens e áreas estão acima e abaixo do esperado, bem como nortear os avaliadores sobre ações que podem ser realizadas a fim de mitigar vulnerabilidades.

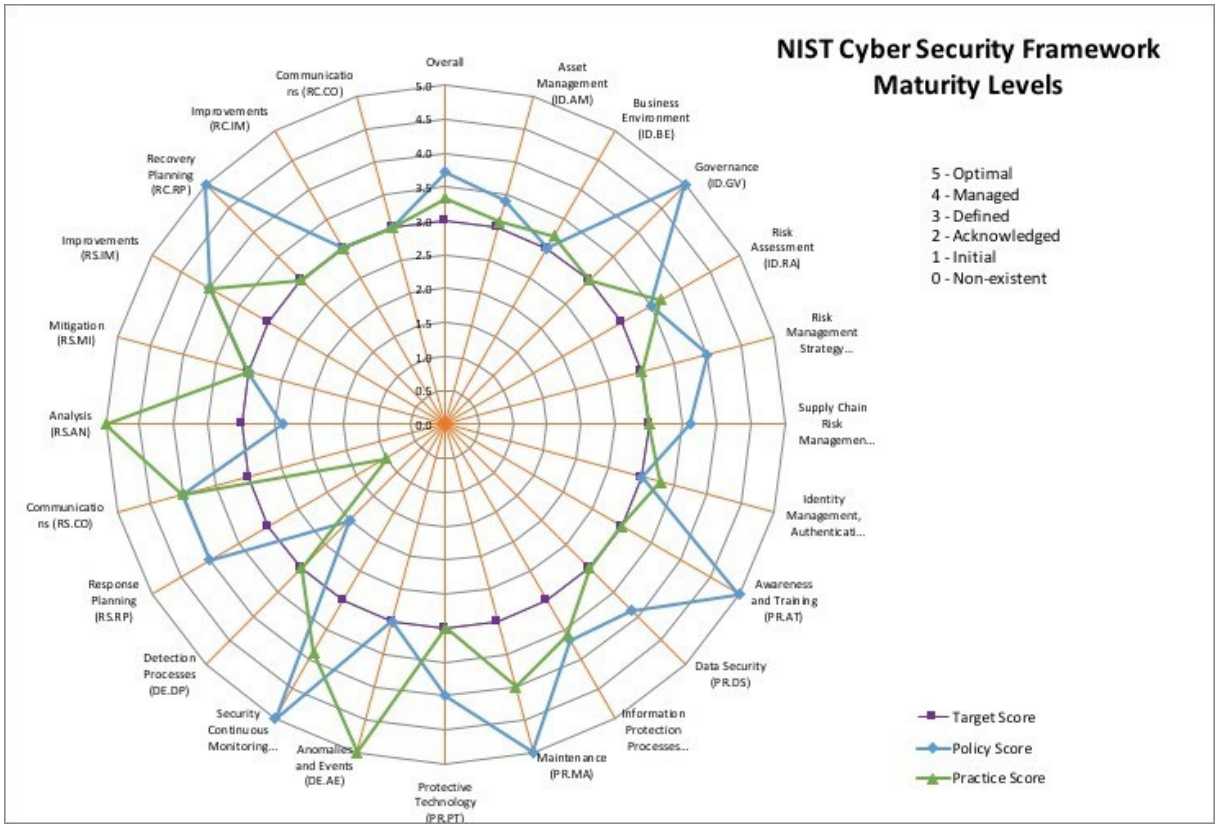


Figura 9 – *Maturity Tool* - Ferramenta de Maturidade baseada no *framework NIST CSF* (MASSERINI, 2019).

2.9.1.3 *NIST SP 800-12*

O *NIST SP 800-12* fornece uma visão geral do controle e da segurança do computador em uma organização e traz o enfoque aos diferentes controles de segurança que uma organização pode implementar para fortalecer a defesa da segurança cibernética. Embora a maioria dos requisitos de controle e segurança tenham sido projetados para agências federais e governamentais, eles são altamente aplicáveis a organizações privadas que buscam aprimorar seus programas de segurança cibernética. Portanto, o NIST SP 800-12 permite que as agências governamentais e empresas mantenham políticas e programas para proteger dados e infraestrutura de TI confidenciais (MUTUNE, 2019).

2.9.1.4 *NIST SP 800-14*

O *NIST SP 800-14* trata-se de uma publicação exclusiva que fornece descrições detalhadas dos princípios de segurança comumente usados, permitindo que as organizações entendam tudo o que precisa ser incluído nas políticas de segurança cibernética. Como resultado, as empresas garantem o desenvolvimento de programas e políticas de segurança cibernética em dados e sistemas essenciais. Além disso, as publicações apresentam medidas específicas que as empresas devem adotar para fortalecer as políticas de segurança já implementadas. No total, a estrutura do NIST SP 800-14 descreve oito princípios de segurança com um total de 14 práticas de segurança cibernética (MUTUNE, 2019).

2.9.1.5 *NIST SP 800-26*

Enquanto a estrutura do *NIST SP 800-14* discute os vários princípios de segurança usados para proteger informações e ativos de TI, o *NIST SP 800-26* fornece diretrizes para o gerenciamento da segurança de TI. É uma estrutura instrumental, que garante que as organizações mantenham políticas eficazes de segurança cibernética. Uma combinação de diferentes publicações do NIST pode garantir que as empresas mantenham programas de segurança cibernética adequados (MUTUNE, 2019).

2.9.2 *ISO IEC 27001 e 27002*

Criadas pela *ISO*, as certificações *ISO 27001 e 27002* (Figura 10) são consideradas um padrão internacional para validar um programa de segurança cibernética. Com uma certificação *ISO*, as empresas podem demonstrar ao conselho, clientes, parceiros e acionistas que estão fazendo as coisas certas para gerenciar o risco cibernético. Da mesma forma, se um fornecedor é certificado pela *ISO 27001/2*, é um bom indicador (embora não o único) de que ele possui práticas e controles de segurança cibernética maduros em vigor (CISTERNELLI, 2020).

A estrutura de segurança cibernética *ISO 27001* consiste em padrões internacionais que recomendam os requisitos para o gerenciamento de Sistemas de Gerenciamento de Segurança

da Informação (SGSI). A *ISO 27001* observa um processo baseado em risco que exige que as empresas implementem medidas para detectar ameaças à segurança que afetam seus sistemas de informação. Para lidar com as ameaças identificadas, os padrões *ISO 27001* recomendam vários controles. Uma organização deve selecionar controles adequados que podem mitigar os riscos de segurança para garantir que permaneça protegida contra ataques. No total, a *ISO 27001* defende 114 controles, que são categorizados em 14 categorias diferentes (MUTUNE, 2019).

Por outro lado, a estrutura *ISO 27002* compreende padrões internacionais que detalham os controles que uma organização deve usar para gerenciar a segurança dos sistemas de informação. A *ISO 27002* foi projetada para uso em conjunto com a *ISO 27001*, e a maioria das organizações usa ambas para demonstrar seu compromisso em cumprir com vários requisitos exigidos por diferentes regulamentações. Alguns dos controles de segurança da informação recomendados no padrão *ISO 27002* incluem políticas para aumentar a segurança da informação, controles como inventário de ativos para gerenciamento de ativos de TI, controles de acesso para vários requisitos de negócios, gerenciamento de acesso de usuários e controles de segurança de operações (MUTUNE, 2019).

Figura 10 – *ISO 27001 e 27002* (PATHCOM, 2018).

2.9.3 *IASME Governance*

A governança do *IASME* (Figura 11) refere-se aos padrões de segurança cibernética projetados para permitir que pequenas e médias empresas realizem a garantia de informações adequadas. A governança do *IASME* descreve um critério pelo qual uma empresa pode ser certificada como tendo implementado as medidas de segurança cibernética relevantes. Em suma, é usado para credenciar a postura de segurança cibernética de uma empresa, permitindo que elas demonstrem a clientes novos ou existentes sua prontidão para proteger dados comerciais ou pessoais (MUTUNE, 2019).

Há uma certa vantagem no credenciamento de governança do *IASME* perante à certificação *ISO 27001*. Mesmo que ambos sejam semelhantes, implementar e manter o padrão com

o *framework IASME* vem com custos reduzidos, sobrecargas administrativas e complexidades. Além disso, a certificação de padrões *IASME* inclui seguro em cibersegurança gratuito para empresas que operam no Reino Unido (MUTUNE, 2019).

Figura 11 – *Framework IASME* (IASME, 2020).

2.9.4 *SOC 2*

Desenvolvido pelo *AICPA*, o *SOC*2 é um padrão de cibersegurança baseado na confiança e padrão de auditoria, a fim de verificar se os fornecedores e parceiros estão gerenciando com segurança os dados do cliente. Para tanto, o *SOC2* especifica mais de 60 requisitos de conformidade e extensos processos de auditoria para sistemas e controles de terceiros. As auditorias podem levar um ano para serem concluídas. Nesse ponto, é emitido um relatório que atesta a postura de segurança cibernética de um fornecedor (CISTERNELLI, 2020).

Cisternelli (2020) e Mutune (2019) afirmam que, devido à sua abrangência (seus requisitos de conformidade), o *SOC2* (Figura 12) é uma das estruturas mais difíceis e desafiadoras de se implementar. Os requisitos incluem diretrizes para destruição de informações confidenciais, sistemas de monitoramento de anomalias de segurança, procedimentos para resposta a eventos de segurança, diretrizes de comunicação interna, entre outros. Especialmente para organizações no setor financeiro ou bancário, esse *framework* é desafiador, visto que elas enfrentam um padrão mais alto de conformidade do que outros setores.

Figura 12 – *Framework SOC2* (ACCELLION, 2018).

2.9.5 *NERC CIP*

O *NERC CIP* (Figura 13) foi criado para mitigar o aumento de ataques à infraestrutura crítica dos EUA e o crescente risco de terceiros. Trata-se de um conjunto de padrões de segurança cibernética projetados para ajudar os setores de serviços públicos e de energia a garantir a confiabilidade dos sistemas elétricos em massa, além de identificar e mitigar os riscos cibernéticos em sua cadeia de suprimentos (CISTERNELLI, 2020).

O *framework* possui uma variedade de controles, incluindo sistemas de categorização e ativos críticos, treinamento de pessoal, resposta a incidentes e planejamento, planos de recuperação para ativos cibernéticos críticos, avaliações de vulnerabilidade e muito mais. No total, a estrutura tem nove padrões que abrangem 45 requisitos. Por exemplo, o padrão de relatório de sabotagem exige que uma organização elétrica relate ocorrências incomuns e distúrbios de segurança aos órgãos relevantes (MUTUNE, 2019).

Figura 13 – *Framework NERC* (NERC, 2021).

2.9.6 *HIPAA*

A *HIPAA* (Figura 14) é uma estrutura de segurança cibernética que exige que as organizações de saúde implementem controles para proteger e proteger a privacidade das informações eletrônicas de saúde. De acordo com a *HIPAA*, além de demonstrar conformidade com as melhores práticas cibernéticas - como treinamento de funcionários - as empresas do setor também devem realizar avaliações de risco para gerenciar e identificar riscos emergentes. Além disso, o *framework* contém várias diretrizes para permitir que as organizações implementem controles suficientes para proteger informações de saúde de funcionários ou clientes (CISTERNELLI, 2020).

Figura 14 – *Framework HIPAA* (PAUBOX, 2017).

2.9.7 *FISMA*

A *FISMA* (Figura 15) é uma estrutura abrangente de segurança cibernética que protege as informações e os sistemas do governo federal norte americano contra ameaças cibernéticas, a fim de verificar se as agências federais implementam medidas adequadas para proteger os sistemas de informação críticos de diferentes tipos de ataques. A FISMA também se estende a terceiros e fornecedores que trabalham em nome de agências federais. A estrutura da FISMA está alinhada com os padrões do *NIST* e exige que agências e terceiros mantenham um inventário de seus ativos digitais e identifiquem quaisquer integrações entre redes e sistemas. As organizações afetadas também devem realizar avaliações de risco de segurança cibernética, análises anuais de segurança e monitorar continuamente sua infraestrutura de TI (CISTERNELLI, 2020).

Mutune (2019) informa que o principal objetivo do padrão de segurança é permitir que as agências federais desenvolvam e mantenham programas de segurança cibernética altamente eficazes e para conseguir isso, o *framework* consiste em uma estrutura de segurança cibernética abrangente com nove etapas para proteger as operações do governo e ativos de TI:

Figura 15 – *Framework FISMA* (COACT, 2020).

2.9.8 *CIS v7*

CIS (Figura 16) é o órgão responsável pelo desenvolvimento e manutenção do *framework CIS v7* e lista 20 requisitos acionáveis de segurança cibernética destinados a aprimorar os padrões de segurança de todas as organizações. A estrutura categoriza os controles de segurança da informação em três grupos de implementação. O grupo de implementação 1 é para empresas que possuem conhecimentos e recursos limitados de segurança cibernética. O grupo de implementação 2 é para todas as organizações com experiência e recursos técnicos moderados na implementação dos sub controles, enquanto o grupo de implementação 3 tem como alvo empresas com vasta experiência e recursos em segurança cibernética. O *CIS v7* se destaca do resto, pois permite que as organizações criem programas de segurança cibernética que respeitem o orçamento (MUTUNE, 2019).

Figura 16 – *Framework CIS v7* (CIS, 2021).

2.9.9 *COBIT*

COBIT (Figura 17) é uma estrutura de segurança cibernética que integra os melhores aspectos de uma empresa à segurança, governança e gerenciamento de TI. Os fatores que levaram à criação da estrutura são a necessidade de atender a todas as expectativas de segurança cibernética das partes interessadas, controles de procedimento ponta a ponta para empresas e a necessidade de desenvolver uma estrutura de segurança única, porém integrada. A estrutura de segurança cibernética *COBIT* é útil para empresas que buscam melhorar a qualidade da produção e, ao mesmo tempo, aderir a práticas de segurança aprimoradas (MUTUNE, 2019).

Figura 17 – *Framework COBIT* (ISACA, 2021).

2.9.10 *COSO*

COSO (Figura 18) é uma estrutura que permite que as organizações identifiquem e gerenciem os riscos de segurança cibernética. Seus pontos principais incluem monitoramento, auditoria, relatórios e controle. O uso da estrutura identifica e avalia rotineiramente os riscos de segurança em todos os níveis organizacionais, melhorando assim suas estratégias de segurança cibernética. Para isso, o *framework* consiste em 17 requisitos, que são categorizados em cinco categorias diferentes: ambiente de controle; avaliações de risco; atividades de controle; informação e comunicação; e monitoramento e controle (MUTUNE, 2019).

Figura 18 – *Framework COSO* (COSO, 2021).

2.9.11 *TC CYBER*

A estrutura do *TC CYBER* foi desenvolvida para melhorar os padrões de telecomunicações em países localizados nas zonas europeias - embora outros países em todo o mundo também a utilizam. A estrutura recomenda um conjunto de requisitos para melhorar a conscientização sobre privacidade para indivíduos ou organizações. Se concentra em garantir que organizações e indivíduos possam desfrutar de altos níveis de privacidade ao usar vários canais de telecomunicações. Além disso, a estrutura recomenda medidas para aumentar a segurança da comunicação (MUTUNE, 2019).

2.9.12 *CISQ*

CISQ (Figura 19) fornece padrões de segurança que os desenvolvedores de *software* devem manter ao desenvolver suas aplicações. Além disso, os desenvolvedores usam os padrões *CISQ* para medir o tamanho e a qualidade de um programa de *software*. Os padrões *CISQ* permitem que eles avaliem os riscos e vulnerabilidades presentes em um aplicativo concluído ou em desenvolvimento. Como resultado, eles podem abordar com eficiência todas as ameaças para garantir que os usuários acessem e usem aplicativos seguros (MUTUNE, 2019).

Figura 19 – *Framework CISQ* (CISQ, 2021).

2.9.13 *FedRAMP*

FedRAMP (Figura 20) é uma estrutura projetada para agências governamentais. A estrutura fornece diretrizes padronizadas que podem permitir que agências federais avaliem ameaças e riscos cibernéticos para as diferentes plataformas de infraestrutura e serviços baseados em nuvem e soluções de *software*.A estrutura permite a reutilização de pacotes e avaliações de segurança existentes em várias agências governamentais (MUTUNE, 2019).

Mutune (2019) continua dizendo que o *framework* também é baseado no monitoramento contínuo da infraestrutura de TI e produtos em nuvem para facilitar um programa de segurança cibernética em tempo real para uma infraestrutura de TI mais segura e rápida. Os objetivos são garantir que as agências federais tenham acesso a tecnologias modernas e confiáveis sem comprometer sua segurança, acelerar as migrações para a nuvem reutilizando autorizações e avaliações, aumentar a confiança na segurança da nuvem, garantir que as agências federais apliquem de forma consistente as práticas de segurança recomendadas e aumentar a automação para monitoramento contínuo.

Figura 20 – *Framework FedRAMP* (FEDRAMP, 2021).

2.9.14 *SCAP*

Security Content Automation Protocol (SCAP) é um padrão regulamentar que contém especificações de segurança para padronizar a comunicação de produtos e ferramentas de segurança. A especificação visa padronizar os processos por meio dos quais os programas de software de segurança comunicam problemas de segurança, informações de configuração e vulnerabilidades. Por meio das especificações padronizadas, o *SCAP* pretende permitir que uma empresa meça, expresse e organize dados de segurança usando critérios e formatos universais. O software de segurança pode permitir que uma empresa mantenha a segurança corporativa, utilizando processos como verificação e instalação automática de *patches* de segurança (MUTUNE, 2019).

2.9.15 *ANSI*

ANSI (Figura 21) contém padrões, informações e relatórios técnicos que descrevem os procedimentos para a implementação e manutenção de sistemas de automação e controle industrial (IACS). A estrutura se aplica a todas as organizações que implementam ou gerenciam sistemas IACS. A estrutura consiste em quatro categorias: a primeira categoria contém informações básicas como modelos de segurança, terminologias e conceitos; a segunda categoria aborda os aspectos envolvidos na criação e manutenção de programas de segurança cibernética SIGC; as terceira e quarta categorias descrevem os requisitos para a integração segura do sistema e os requisitos de segurança para o desenvolvimento do produto (MUTUNE, 2019).

Figura 21 – *Framework ANSI* (ANSI, 2018).

3 DESENVOLVIMENTO

Os ataques cibernéticos são atividades criminosas que têm como alvo ou fazem uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. A maioria desses crimes são cometidos por cibercriminosos ou *hackers* que querem ganhar dinheiro. Raramente o crime cibernético visa danificar os computadores, a não ser que esse seja o principal objetivo. Nesses casos, os motivos podem ser pessoais ou políticos.

É importante salientar que o cibercrime é configurado como um crime passível a punição. No Brasil, as principais normas criadas pelo Congresso Nacional para à asseguridade dos usuários são: a Lei dos Crimes Informáticos (Lei 12.737/12) e o Marco Civil da Internet (Lei 12.965/14). A Lei 12.737/12 estabelece que certas condutas surgidas com a tecnologia serão consideradas crimes, como invadir o dispositivo de informática (computador, celular, equipamentos de rede, entre outros) alheio, conectado ou não à rede de computadores, e interromper fraudulentamente o serviço telefônico, telegráfico ou de internet. Já a Lei 12.965/14 regula os direitos e deveres dos internautas, protege os dados pessoais e a privacidade dos usuários, e somente mediante ordem judicial pode haver quebra de informações particulares existentes em sites ou rede sociais (COSTA, 2019).

Uma estratégia interessante, a fim de prevenir e mitigar ataques cibernéticos é utilizar estruturas de cibersegurança (*cybersecurity frameworks*). Essas estruturas são desenvolvidas por órgãos íntegros, nacionais e internacionais, focados em padronização e segurança. Como informado na subseção 2.9, uma estrutura de segurança cibernética fornece uma linguagem comum e um conjunto de padrões para que os líderes de segurança dos países e dos distintos setores da economia entendam suas posturas de segurança e as de seus fornecedores. Com uma estrutura em vigor, torna-se muito mais fácil definir os processos e procedimentos que sua organização deve seguir para avaliar, monitorar e mitigar os riscos de segurança cibernética.

3.1 Metodologia

A metodologia utilizada nesse trabalho baseia-se em uma pesquisa exploratória e qualitativa. Em outras palavras, serão apresentados registros acerca dos maiores ataques cibernéticos registrados no Brasil e no mundo, tal como a utilização da ferramenta de cibersegurança, proposta por Masserini (2019), baseada no *framework NIST CSF*, em uma indústria. Dessa forma, o conteúdo está segmentado em duas subseções: 3.2 (Ataques Cibernéticos) e 3.3 (*NIST CSF Maturity Tool*).

3.2 Ataques Cibernéticos

Um crime cibernético é realizado por pessoas ou organizações, como pode ser visualizado na tabela 8. Alguns cibercriminosos são organizados, usam técnicas avançadas e são altamente capacitados em termos técnicos, já outros são *hackers* novatos.

Grande parte dos ciberataques são bastante comuns, como telefonemas, *sms* e *e-mail*, solicitando informações confidenciais (senhas, cartões, documentos de identificação pessoal, etc). Nos piores casos, o usuário se vê perante a um pedido de resgate para que os sistemas e dados afetados pelo ataque possam ser desbloqueados e restaurados, mediante ao pagamento em dinheiro. Muitas vezes nada visível acontece, visto que muitos tipos de *malwares* agem o mais discretamente possível para maximizar o roubo de dados antes de serem detectados. Entretanto, com o tempo, alguns ciberataques e alguns *hackers* têm apresentado sofisticação tecnológica em suas atividades.

Snow (2018), no portal *Kaspersky Daily* - empresa tecnológica russa especializada na produção de softwares de segurança para a Internet, apresenta os 5 ciberataques mais famosos dos últimos tempos: *WannaCry*; *NotPetya/ExPetr*; *Stuxnet*; *DarkHotel*; e *Mirai*. Além desses ataques mundialmente conhecidos, serão incluídos os ataques cibernéticos mais evidenciados do Brasil: o do Supremo Tribunal de Justiça; e do conglomerado brasileiro JBS.

3.2.1 *WannaCry*

O ataque do *Ransomware WannaCry* foi uma epidemia global que aconteceu em maio de 2017, com duração de quatro dias, se espalhou por computadores com o *Microsoft Windows* e derrubou cerca de 230 mil computadores em 150 países, incluindo infraestruturas críticas. Os arquivos dos usuários eram mantidos como reféns e, para que fossem devolvidos, era exigido um resgate em *bitcoins*. Em alguns hospitais, o ataque encriptou todos os dispositivos, até mesmo equipamentos médicos e algumas indústrias foram obrigadas a parar de produzir. Dentre os ataques recentes, o WannaCry foi o que obteve maior alcance. Os invasores exigiram US$ 300 em *bitcoins* e, mais tarde, aumentaram o valor do resgate para US$ 600 em *bitcoins*. Se as vítimas não pagassem o resgate dentro de três dias, os responsáveis pelo ataque do *WannaCry* ameaçavam excluir os arquivos permanentemente (KASPERSKY, 2019).

De acordo com Kaspersky (2019), os cibercriminosos responsáveis pelo ataque se aproveitaram de uma deficiência no sistema operacional *Microsoft Windows* usando um *hack*, uma modificação, conhecido como *EternalBlue* - supostamente criado pela Agência de Segurança Nacional dos EUA. Esse *hack* se tornou público por um grupo de *hackers* chamado *Shadow Brokers* antes do ataque. Dois meses antes, a *Microsoft* lançou a correção de segurança MS17-010, em 14 de março de 2017, que protegia os sistemas de usuários contra esse *exploit* (código malicioso). Devido a falha por parte dos usuários em não atualizar regularmente seus sistemas operacionais, aqueles que não executaram o *Microsoft Windows Update* antes do ataque não se

beneficiaram da correção. Assim, essa vulnerabilidade explorada pelo *EternalBlue* deixaram os usuários de sistemas desatualizados expostos ao ataque. Para executar o código malicioso, foi utilizado uma ferramenta *backdoor* chamada *DoublePulsar* para se autoinstalar e executar.

Ao infectar um computador, o *WannaCry* pOde infectar toda uma rede local e por isso, as grandes empresas sofreram mais – quanto mais computadores na rede, maior foi o dano. Ele codificou arquivos de vários tipos, incluindo documentos do *Office*, fotos, vídeos, arquivos e outros formatos que potencialmente contêm dados críticos do usuário. As extensões dos arquivos criptografados foram renomeadas para "*.WCRY*"e os arquivos ficaram completamente inacessíveis. Depois disso, o Trojan alterou o papel de parede da área de trabalho para uma imagem que contém informações sobre a infecção e ações que o usuário deve executar para recuperar os arquivos, como pode ser visualizado na figura 22. Ele também espalhou notificações, como arquivos de texto com as mesmas informações, em pastas no computador para garantir que o usuário receba a mensagem (PEREKALIN, 2017).

Figura 22 – Ação do *Ransomware WannaCry*: resgate de dados sendo solicitado (PEREKALIN, 2017).

Uma das primeiras organizações afetadas foi a empresa espanhola de telefonia móvel, a *Telefónica*. E, em 12 de maio, milhares de consultórios e hospitais do *National Health Service* (NHS), sistema de saúde do Reino Unido, foram afetados em todo o território, no qual um terço de suas fundações hospitalares foram afetadas pelo ataque e ainda houve a mudança de rotas em ambulâncias, deixando de atender pessoas que precisavam de cuidados urgentes. O

custo estimado para o NHS foi de 92 milhões após 19 mil consultas terem sido canceladas como resultado do ataque (KASPERSKY, 2019). No Brasil, por exemplo, o ataque causou a interrupção dos atendimentos do INSS, afetou os sistemas do Santander e da Vivo e como forma de proteção, o Ministério Público de SP e o Tribunal de Justiça de SP decidiram desligar seus sistemas para impedir prejuízos maiores (NOGUEIRA, 2020).

Ainda, de acordo com Kaspersky (2019), o ataque do *ransomware WannaCry* teve um impacto financeiro considerável em todo o mundo. Estima-se que as perdas causadas por esse crime cibernético tenham somado US$ 4 bilhões em todo o mundo.

3.2.2 *NotPetya/ExPetr*

O título de epidemia mais cara, até então registrado, é do *ransomware ExPetr*, também conhecido como *NotPetya*. Seu princípio operacional era o mesmo do *WannaCry*: usar *exploits* do *EternalBlue* com o *EternalRomance* - obtidos a partir de falhas de segurança do *Microsoft Windows* nos protocolos *Server Message Block (SMB)*. Dessa forma, o *worm* se espalhou pela internet e criptografou, irreversivelmente, os dados encontrados em sistemas vulnerabilizados (SNOW, 2018).

Seguindo o mesmo exemplo do *WannaCry*, os cibercriminosos do *NotPetya/ExPetr* exigiram US$ 300 em *bitcoins* para descriptografar os dados e informações que eles modificaram, conforme é apresentado na figura 23. Cossetti (2017a) informa que, mesmo que os usuários pagassem o resgate, não receberiam seus dados de volta, reforçando o alerta aos usuário em não efetuar qualquer pagamento para o resgate dos dados e, além disso, pôde-se constatar que a motivação do ataque não era financeira, entretanto, ser destrutivo e sem solução. O ataque apresenta pistas de que se trata de algo maior, com foco político, por exemplo, visto que não é lucrativo financeiramente falando, no qual são poucos os que pagam as quantias solicitadas em *bitcoin*.

Embora o número de máquinas infectadas tenha sido menor, o *NotPetya* focou principalmente em empresas, por meio do *software* financeiro *MeDoc*. Após conseguir obter o controle do servidor de atualização do programa, os cibercriminosos enviaram um *malware* disfarçado de uma atualização que se espalhava pela rede. O prejuízo desse ciberataque foi estimado em U$10 bilhões, sendo considerado o ciberataque global mais caro da história (SNOW, 2018).

3.2.3 *Stuxnet*

A história do vírus *Stuxnet* foi manchete em centenas de jornais e preocupou os responsáveis pela segurança da indústria e informática. O vírus foi empregado pela primeira vez em 2007 no Irã. Quem o criou e o motivo ainda é um mistério, no entanto, há rumores de que a inteligência americana e israelense queriam usá-lo para sabotar o programa nuclear iraniano. (PEREKALIN, 2014).

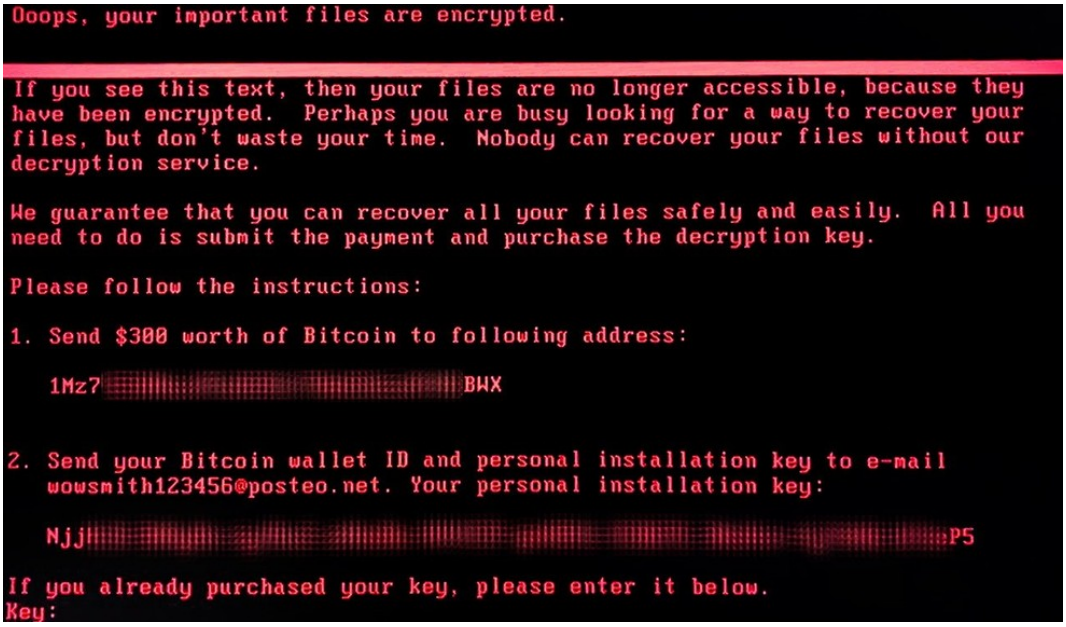


Figura 23 – Ação do *NotPetya/ExPetr*: resgate de dados sendo solicitado (COSSETTI, 2017b).

Provavelmente, o *Stuxnet*, vide figura 24, é o ciberataque mais conhecido. Esse *malware* complexo e multifacetado desligou centrífugas de enriquecimento de urânio no Irã, atrasando o programa nuclear do país por vários anos. A partir do *Stuxnet*, iniciou-se o levantamento sobre o uso de armas cibernéticas contra sistemas industriais. Na época, não havia nada mais complexo ou astuto do que o *Stuxnet* – o *worm* foi capaz de se espalhar imperceptivelmente por meio de *pendrives USB* e penetrar até mesmo em computadores que não estavam conectados à Internet ou às redes locais (SNOW, 2018).

Figura 24 – *Malware Stuxnet*: ciberataque em usina nuclear do Irã (ZETTER; MODDERKOLK, 2019).

O *vírus* ficou fora de controle e rapidamente se proliferou pelo mundo, infectando centenas de milhares de computadores. O *malware* se manifestou apenas em dispositivos operados por *softwares* e controladores programáveis, do sistema de controle *Supervisory Control And Data Acquisition* (SCADA), Sistema de Supervisão e Aquisição de Dados, da empresa *Siemens*. Após alcançar esses dispositivos, o código malicioso reprogramou esses controladores e então, ao aumentar muito a velocidade rotacional das centrífugas de enriquecimento de urânio, acabou por destruí-las fisicamente (SNOW, 2018).

A funcionalidade deste *malware* foi realizar uma ponte entre o computador invadido e um servidor remoto - para onde foram todas as informações roubadas. Neste processo foram capturados projetos de pesquisa e relatórios, além de permitir o acesso remoto às configurações do sistema SCADA (HAMANN, 2010).

Os criadores do *Stuxnet* conseguiram atacar sistemas industriais e conseguiram infectar computadores pessoais e de empresas em grande escala. Em seguida, o vírus perdeu o controle e começou a distribuir-se ativamente, sem danos visíveis para PCs domésticos e corporativos (DROZHZHIN, 2014). De acordo com (KELVIN, 2020), o ataque direcionado ao programa nuclear iraniano, arruinou 20% das centrífugas existentes no Irã e mais de 1.000 dispositivos com o sistema operacional *Microsoft* e dispositivos *Siemens*.

Hamann (2010) informa que, além da indústria nuclear iraniana, o *Stuxnet* também já foi detectado em milhões de computadores na China, Índia, Indonésia, Estados Unidos, Austrália, Inglaterra e Paquistão. Além de números não oficiais que também apontam para infecções na Alemanha e outros países na Europa.

3.2.4 *DarkHotel*

Em 2014, a *Kaspersky Lab* descobriu uma rede de espionagem, batizada de *Darkhotel*, ativa há mais de 07 anos em distintos hotéis asiáticos - os criminosos estavam operando principalmente no China, Japão e Taiwan. Os espiões inteligentes e profissionais envolvidos nesta operação de longa duração criaram um conjunto de ferramentas que consiste em variadas formas e métodos para invadir os computadores das vítimas (DROZHZHIN, 2014).

O primeiro registro do ataque foi anunciado pelo FBI em 2012. No entanto, o *malware* usado na campanha de espionagem (conhecido como *Tapaoux*) surgiu em 2007. O método que os cibercriminosos utilizaram com maior frequência para se infiltrar nos computadores das vítimas foram as redes *Wi-Fi* de vários hotéis de luxo do continente asiático (DROZHZHIN, 2014).

O equívoco de achar que as redes públicas de *WiFi* em hotéis são seguras custou caro para muitos gerentes e funcionários de alto escalão de hotéis asiáticos. Os usuários, ao conectarem-se pelo *WiFi* dos hotéis, foram surpreendidos ao ser solicitada a instalação de uma atualização, aparentemente legítima, de um software popular (SNOW, 2018).

Entretanto, os dispositivos foram imediatamente infectados com o *spyware DarkHotel*,

que os criminosos introduziram especificamente na rede alguns dias antes da chegada desse grupo e removeram depois. O *spyware* permitiu que os cibercriminosos lançassem ataques de *phishing* direcionados (SNOW, 2018). Tudo indica que os criminosos exploraram vulnerabilidade de *zerp-day*, presentes no *Adobe Flash* e outros programas populares de importantes empresas. Outras táticas utilizadas por eles incluíram *trojans* ocultos em arquivos de entretenimento para adultos, bem como o disparo de *phishing* enviados para e-mails de empregados do Estado e organizações não governamentais (DROZHZHIN, 2014). Veja na figura 25 uma ilustração do ocorrido.

Figura 25 – *DarkHotel*: ciberataque em hotéis no continente asiático (DROZHZHIN, 2014).

Drozhzhin (2014), levando em consideração que essas vulnerabilidades não são fáceis de se encontrar, supõe-se duas hipóteses: a campanha foi financiada economicamente por pessoas com muito dinheiro, visto que as armas cibernéticas de alta complexidade são muito caras; e os agente envolvidos nesta campanha de espionagem possuem alto nível tecnológico e profissional. O mais provável é que ambos os fatores sejam verdadeiros.

Eles chegaram tão longe que inclusive conseguiram criar certificados de segurança digital, com o objetivo de espionar os canais de comunicação utilizados pelas vítimas. Estes ladrões digitais utilizaram um *keylogger* sofisticado que consistiu em um módulo integrados para roubar senhas salvas nos navegadores populares. Além disso, eles eram extremamente

cautelosos e projetaram uma série de medidas para impedir a detecção do *malware*: garantiram que o vírus tivesse um “período de incubação” muito longo, ou seja, a primeira vez que o *Trojan* se conectou aos servidores *C&C* foi registrada após 180 dias da infiltração nos sistemas e o programa *spyware* tinha um protocolo de auto-destruição, caso o idioma do sistema mudasse para coreano (DROZHZHIN, 2014).

3.2.5 *Mirai*

Uma frota de zumbis, conhecido também por *botnets*, criada com um *malware* batizado por nome de *Mirai* - "futuro” em japonês. O *malware* cresceu e ficou à espera de receber instruções para agir (SNOW, 2018). Com o surgimento da *Internet of Things* (*IoT*), a Internet das Coisas, dispositivos cuja segurança nunca foi considerada e para os quais não existia antivírus começaram a ser infectados subitamente em larga escala. Dessa forma, após a infecção, esses dispositivos rastrearam uns aos outros e os infectaram imediatamente (SNOW, 2018).

Precisamente, no dia 21 de outubro de 2016, os donos dessa *botnet* gigante decidiram testar suas capacidades e fizeram com que milhões de gravadores de vídeo, roteadores, câmeras IP, impressoras e outros equipamentos inteligentes da *IoT* inundassem a provedora de serviços de *DNS*, a *Dyn*, com solicitações. Obviamente, o serviço simplesmente não foi capaz de suportar um ataque *Distributed Denial of Service* (DDoS), Ataque de Negação de Serviço em grande escala. Dessa forma, o servidor, assim como os seus serviços dependentes, ficaram indisponíveis, como *PayPal*, *Twitter*, *Netflix*, *Spotify* e serviços online da *PlayStation*. A empresa eventualmente se recuperou, mas a amplitude do ataque fez o mundo parar e refletir sobre a segurança nos dispositivos inteligentes e conectados, no qual desfrutamos em nosso cotidiano (SNOW, 2018).

O ataque, na verdade, foi uma série três ataques contra a infraestrutura da Internet norte americana - um dos sites reivindicou 1,2 *terabits* por segundo. A primeira onda afetou a costa leste norte americana e na segunda, usuários da Califórnia e no Centro-Oeste, bem como a Europa. A terceira onda foi atenuada pelos esforços da *Dyn*, que foi o principal alvo dos três ataques e provocou a interrupção dos serviços mundialmente. A figura 26 mostra alguns dos locais afetados pelo código malicioso (KOCHETKOVA, 2016).

Kochetkova (2016) informa que, talvez o ponto mais marcante sobre o grande ataque *DDoS* que tirou do ar 85 sites populares e serviços online, é que os criminosos por trás dele não usaram meios particularmente sofisticados ou tecnologia de ponta. Eles agiram por meio de um verdadeiro exército de dispositivos conectados *IoT*. O dano estimado é de cerca de 110 milhões de dólares, no entanto, os criminosos responsáveis não pediram resgate ou fizeram quaisquer exigências.

3.2.6 Superior Tribunal de Justiça - STJ

O ataque cibernético ao Superior Tribunal de Justiça (STJ), vide figura 27, pode ser considerado o mais grave e de maior impacto já dirigido contra uma instituição de Estado do

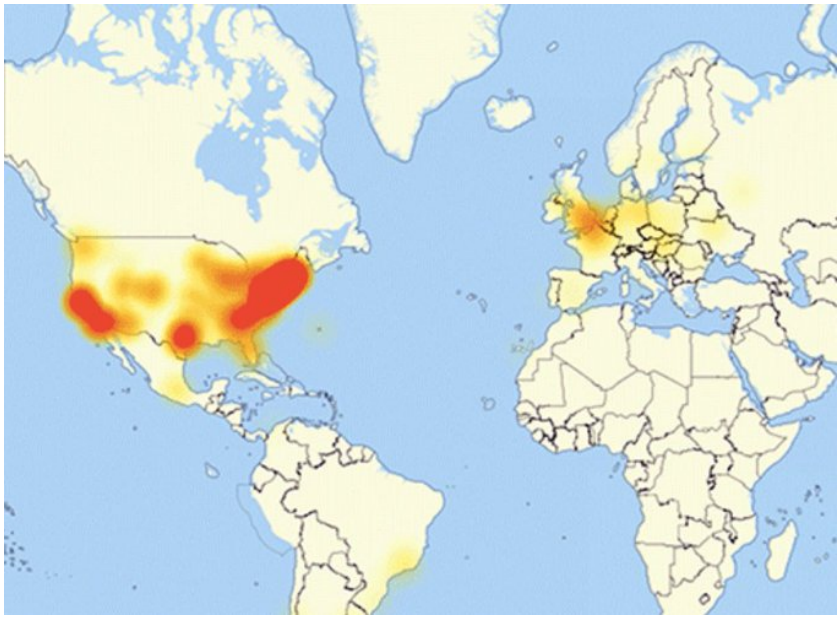


Figura 26 – *Mirai*: Países e continentes afetados pelo ataque *DDoS* ao servidor *Dyn* (KOCHETKOVA, 2016).

Brasil. O site do STJ ficou fora do ar no dia 03 de novembro de 2020, quando foi identificado o ataque e no dia 05 de novembro de 2021 foi identificado que o *hacker* responsável por invadir o sistema do STJ criptografou todo o acervo de processos do tribunal, além de ter bloqueado o acesso às caixas de *e-mail* de ministros, além dos *backups* de dados da corte que também foram criptografados (BOSCO, 2020).

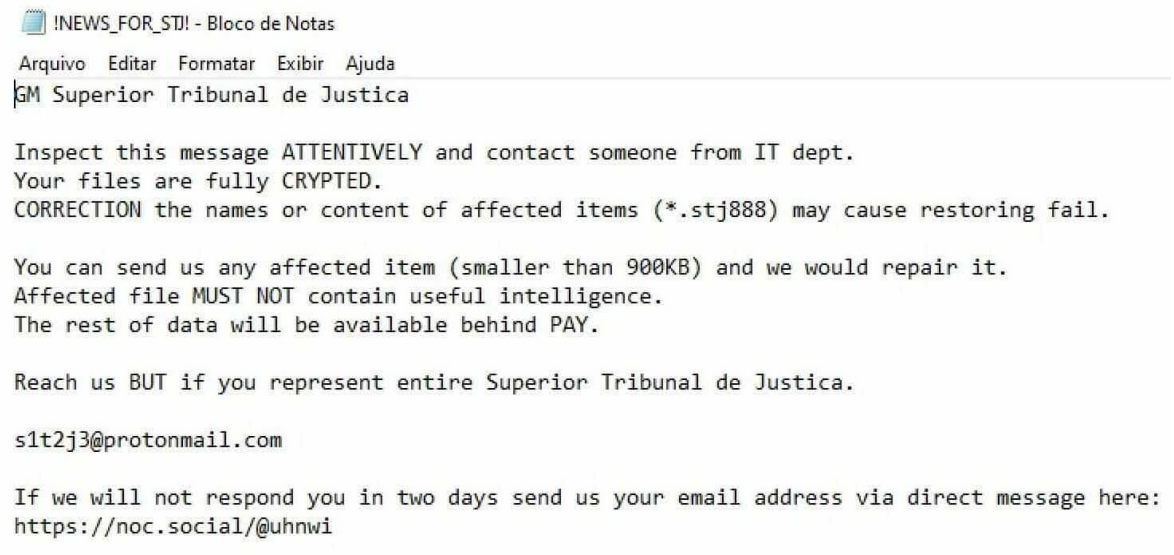


Figura 27 – *STF*: Aviso ao órgão sobre da invasão (NOGUEIRA, 2020).

A Polícia Federal foi chamada para investigar o caso. O site da instituição contava apenas com duas notas de esclarecimento: a primeira avisava aos visitantes do site de que a plataforma se encontrava em regime de plantão até o restabelecimento da rede, sendo que o STJ analisaria

apenas pedidos urgentes; e a segunda dizia que em razão de ataque cibernético, STJ funcionaria em regime de plantão até o dia 9 de novembro de 2020. Além da informação que todos os prazos processuais administrativos, cíveis e criminais ficariam suspensos com data provável de volta ao funcionamento normal no dia 10 de novembro (BOSCO, 2020).

Inicialmente, imaginava-se que somente o Superior Tribunal de Justiça (STJ) tivesse sido atacado e tido as informações roubadas. Entretanto, foram identificadas que outras bases de dados foram atacadas e os sistemas do *Datasus*, do Ministério da Saúde, e do Governo do Distrito Federal, ficaram fora do ar. Há ainda registros que alguns sistemas da Receita Federal também foram alvo da ação (MACHADO DA COSTA, 2020).

3.2.7 JBS

A empresa *JBS* foi alvo de um ciberataque, no dia 30 de maio de 2021, em suas unidades dos Estados Unidos, Canadá e Austrália, afetando alguns servidores da empresa (G1, 2021b). As redes de computadores da empresa foram invadidas, fazendo com que algumas de suas operações nesses países fossem temporariamente fechadas, afetando milhares de trabalhadores. De acordo com a assessoria brasileira da empresa, o ataque não teve impacto no Brasil (BBC NEWS BRASIL, 2021). De acordo com Lima e Rigues (2021), a empresa teve ciência do ataque após membros da área de tecnologia perceberem anormalidades no funcionamento de alguns servidores e, em seguida, eles encontraram uma mensagem que exigia o pagamento de um resgate para liberação do sistema da empresa. Imediatamente, a *JBS* denunciou o ataque ao *FBI*, e a equipe de tecnologia da empresa fez o desligamento do sistema fornecedor de carne para tentar retardar o avanço do ataque.

A *JBS*, fundada no Brasil em 1953, a maior fornecedora mundial de carnes e a maior empresa de processamento de carne do mundo, com mais de 150 fábricas em 15 países (BBC NEWS BRASIL, 2021) sofreu um ataque do tipo *ransomware* pelo grupo cibercriminoso russo, o *REvil* ou *Sodinokibi*. O *REvil* é uma rede criminosa de *hackers* de *ransomware* e é conhecida como uma empresa do tipo *Ransomware-As-A-Service* (*RAAS*), pela forma como opera, visto que envolve desenvolvedores de *ransomware* e recrutam parceiros para espalhar seu *malware*. O grupo ganhou destaque em 2019, é considerado um dos grupos cibercriminosos mais lucrativos do mundo e acredita-se que a maioria de seus membros residam na Rússia ou em países que antes faziam parte da União Soviética (BBC NEWS BRASIL, 2021).

Os servidores de *backup* da empresa não foram afetados e a organização declarou que tomou medidas imediatas, suspendendo todos os sistemas afetados, notificando as autoridades e ativando a rede global da empresa de profissionais de TI e especialistas terceirizados para resolver a situação (G1, 2021b).

G1 (2021a) informam que o ataque à companhia afetou alguns dos seus servidores no dia 30 de maio de 2021. Já no dia 03 de junho de 2021, a empresa anunciou o retorno de 100% das suas operações. No dia 09 de junho de 2021, a subsidiária norte americana informou que pagou o

equivalente a US$ 11 milhões em resgate após o ataque. Essa decisão foi tomada após consultar especialistas em segurança digital sendo que seu objetivo foi reduzir problemas relacionados à invasão e evitar o vazamento de dados. Lima e Rigues (2021) informam que o resgate foi pago em *bitcoin* após o retorno da produção na maior parte das fábricas, graças a *backups* secundários dos dados da empresa que são criptografados e uma espécie de seguro para a proteção dos seus clientes.

3.3 *NIST CSF Maturity Tool*

Após o estudo dos tipos de ataques cibernéticos mais comuns e aqueles mais famosos, devido ao impacto causado em empresas e pessoas envolvidas, é de suma importância propor uma ferramenta prática e eficaz para mitigar ataques cibernéticos. Como visto nos exemplos anteriormente, os impactos causados por um ataque cibernético são enormes e, se uma determinada organização estiver despreparada e vulnerável, eles podem ser irreversíveis. Desse modo, o seguinte estudo foi realizado com a utilização da ferramenta *NIST CSF Maturity Tool*, proposta por Masserini (2019) - uma análise e contribuição acerca da segurança cibernética para a indústria.

Após o estudo técnico do assunto segurança cibernética, discutido nas seções e subseções anteriores, torna-se interessante continuá-lo, entretanto, sob uma metodologia prática, voltada à aplicação de normas e métodos para a compreensão, gerenciamento e apresentação do risco de segurança cibernética em organizações. Portanto, a ferramenta além de estar baseada nas normas e metodologias do *framework NIST*, é gratuita e fornece uma gama de resultados aplicáveis aos *stakeholders* externos e internos à organização. Dessa forma, essa ferramenta será a escolhida e, a seguir, serão detalhados todos os passos realizados para a utilização da mesma.

O estudo foi realizado internamente na Empresa X, cujas atividades econômicas e produtivas são dos setores primário e secundário da economia - extração e indústria. A ferramenta utilizada é uma pesquisa que baseia-se na aplicação de questionários e, posteriormente, na análise da maturidade em segurança cibernética do Setor de Tecnologia de Automação, em uma determinada área de sua atuação na Empresa X. Por questões de confidencialidade e de segurança das informações, a área de atuação, assim como a empresa permanecerão em sigilo.

O guia NIST CSF, discutido na subseção 2.9.1.1, propõe uma estrutura básica composta por quatro elementos: Funções, Categorias, Subcategorias e Referências Informativas, como pode ser observado na figura 28.

Figura 28 – Organização da estrutura básica do *framework* (NIST, 2018)

Em suma, as funções organizam atividades básicas de segurança cibernética e auxiliam uma organização a demonstrar seu gerenciamento de riscos de segurança cibernética, organizando as informações, possibilitando decisões de gerenciamento de riscos, tratando ameaças e aprimorando com base em atividades anteriores. As categorias, como podem ser vistas na figura 29, são as subdivisões de uma das funções em grupos de resultados de segurança cibernética de acordo com as necessidades programáticas e atividades específicas (NIST, 2018).

Já as subdivisões desmembram uma categoria em resultados específicos de atividades técnicas e/ou de gerenciamento, fornecendo um conjunto de resultados que ajudam a dar embasamento para a concretização dos resultados de cada categoria. Por fim, as referências informativas, discutidas na subseção 2.9, são itens específicas sobre normas, diretrizes e práticas comuns entre os setores de infraestrutura crítica que norteiam métodos para alcançar os resultados relacionados a cada subcategoria e, àquelas que são referenciadas com maior frequência no mundo da segurança cibernética, foram utilizadas durante o processo de desenvolvimento desta Estrutura (NIST, 2018).

Identificador Exclusivo de Função	Função	Identificador Exclusivo de Categoria	Categoria
ID	Identificar	ID.AM	Gerenciamento dos Ativos
		ID.BE	Contexto Empresarial
		ID.GV	Governança
		ID.RA	Avaliação de Risco
		ID.RM	Estratégia de Gerenciamento de Riscos
		ID.SC	Gerenciamento de Riscos da Cadeia de Suprimento
PR	Proteger	PR.AC	Gerenciamento de identidade e controle de acesso
		PR.AT	Conscientização e Treinamento
		PR.DS	Segurança de Dados
		PR.IP	Processos e Procedimentos de Proteção da Informação
		PR.MA	Manutenção
		PR.PT	Tecnologia Protetora
DE	Detectar ou Diagnosticar	DE.AE	Anomalias e Incidentes
		DE.CM	Monitoramento Contínuo de Segurança
		DE.DP	Processos de Detecção
RS	Responder	RS.RP	Planejamento de Resposta
		RS.CO	Comunicações
		RS.AN	Análise
		RS.MI	Mitigação
		RS.IM	Aperfeiçoamentos
RC	Recuperar	RC.RP	Planejamento de Recuperação
		RC.IM	Aperfeiçoamentos
		RC.CO	Comunicações

Figura 29 – Identificadores exclusivos de função e categoria (NIST, 2018)

Das 7 etapas que o guia *NIST CSF* sugere a organização seguir, seja para um novo programa de segurança cibernética, ou aperfeiçoar um programa existente, foram utilizadas as 5 primeiras nesse trabalho. NIST (2018) as define por: etapa 1 - priorizar e determinar o escopo; etapa 2 - orientar e identificar; etapa 3 - criar uma avaliação atual; etapa 4 - realizar uma avaliação de risco e etapa 5 - criar uma avaliação desejada.

Logo, na etapa 1, como os objetivos de negócio da organização X já são conhecidos e bem definidos, o guia foi adaptado à uma área exclusiva de atuação do Setor de Tecnologia de Automação da mesma. Consequentemente, após o escopo definido, na etapa 2 os agentes da pesquisa identificaram sistemas e ativos relacionados, os requisitos regulatórios e a abordagem geral de risco por intermédio da consulta aos *stakeholders* internos para identificar ameaças e vulnerabilidades aplicáveis aos sistemas e ativos.

Na etapa 3, os pesquisadores desenvolveram uma avaliação atual da área estudada, indicando quais resultados de categoria e subcategoria da estrutura básica estão sendo alcançados no momento. Na etapa 4, eles analisaram o ambiente operacional para identificar a probabilidade de uma ocorrência de segurança cibernética e o impacto que tal ocorrência poderia ter na organização, identificando os riscos emergentes e usando informações de ameaças cibernéticas de fontes internas e externas para obter uma melhor compreensão da probabilidade e do impacto de ocorrências de segurança cibernética.

Por fim, na etapa 5 eles criaram uma avaliação, descrevendo os resultados de segurança cibernética desejados e alcançados pelo setor. Essa avaliação foi obtida por meio de 3 opções ao responder o questionário: Atende; Não Atende; e Não se Aplica. Caso os itens da função (categoria e a subcategoria) do escopo do guia atendam em sua totalidade, os agentes da pesquisa marcaram a opção "Atende", caso contrário, "Não Atende". A opção "Não se Aplica"foi destinada àqueles itens dos quais referem-se estritamente à Empresa X e a setores distintos, visto que o foco desse trabalho é realizar uma análise sobre a maturidade cibernética do Setor de Tecnologia de Automação da Empresa X.

O escopo completo da ferramenta utilizada pode ser visualizado no Anexo A deste trabalho.

4 RESULTADOS

O estudo de caso realizado na subseção 3.2 apresentou os ciberataques *WannaCry*, *NotPetya/ExPetr*, *Stuxnet*, *DarkHotel* e *Mirai*, conhecidos por serem os mais famosos dos últimos anos, tal como os 2 ataques cibernéticos mais evidentes do Brasil até o momento, o ciberataque ao Superior Tribunal de Justiça (STJ) e à *JBS*. O resultado do estudo pode ser visualizado na tabela 13 a seguir.

Tabela 13 – Os Ataques Mais Famosos dos Últimos Anos

Ataque	***Malware***	**Resumo**
WannaCry	*Ransomware*	*Hackers* mantiveram os dados como reféns e exigiram resgate. Cerca de 230 mil computadores em 150 países foram atingidos, incluindo empresas com infraestruturas críticas e hospitais. As perdas causadas por esse crime cibernético estão estimadas em US$ 4 bilhões;
NotPetya/ExPetr	*Ransomware* e *Worms*	Os cibercriminosos direcionaram os ataques às empresas. É a epidemia mais cara da história, com prejuízo estimado a US$10 bilhões;
Stuxnet	*Worms*	Ciberataque mais conhecido. Foi direcionado para interromper o funcionamento das centrífugas de enriquecimento de urânio no Irã, atrasando o programa nuclear do país, danificando 20% delas e mais de 1000 computadores e sistemas de controle;
DarkHotel	*Spyware*	Uma rede de espionagem em redes *WiFi* de hotéis asiáticos, explorando vulnerabilidades em programas populares com *trojans* ocultos em mídias consumidas e *phishing* aos *e-mails* de empregados do Estado;
Mirai	*Worms*	Um exército zumbi com dispositivos *IoT*. Milhões de gravadores de vídeo, roteadores, câmeras IP, impressoras e outros equipamentos inteligentes, rastrearam uns aos outros, os infectando imediatamente. Por negação de serviço *DDoS*, inundaram a provedora *Dyn*, de serviços de DNS, com solicitações, deixando indisponíveis 85 sites e serviços populares no mundo;
Supremo Tribunal de Justiça	*Ransomware*	O mais grave e de maior impacto já dirigido contra uma instituição de Estado do Brasil. Criptografou todo o acervo de processos do tribunal, de *backups* de dados da corte e bloqueou o acesso às caixas de *e-mail*;
JBS	*Ransomware*	Afetou alguns dos seus servidores em três de suas unidades, tendo algumas de suas operações nos Estados Unidos, Canadá e Austrália interrompidas por 4 dias. A empresa pagou o equivalente a US$ 11 milhões em *bitcoins* para o resgate dos dados;

É interessante destacar que a segunda coluna "*Malware*"da tabela 13, apresenta o principal código malicioso utilizado em cada ataque. Não necessariamente o ataque utilizou apenas um desses códigos maliciosos, mas uma junção com outros métodos para ter seu ataque mais efetivo e desastroso. Dos 7 ataques estudados, sua grande maioria, precisamente 5 deles, utilizaram o *ransomware* como principal ferramenta para infectar, roubar dados, criptografá-los e exigir resgate.

O ataque *NotPetya/ExPetr* além de utilizar *ransomware* como código malicioso, utilizou *worms* para infectar redes de forma rápida e eficiente. Além desse ataque, os ciberataques *Stuxnet* e *Mirai* também utilizaram desse *malware* sua principal arma de ataque. Por fim, o ataque *DarkHotel* utilizou *spyware* como principal método de ataque para criar uma rede de espionagem e roubar dados confidenciais dos usuários de redes públicas de hotéis.

Os impactos causados por um ataque cibernético, como visto na tabela 13 são enormes, podendo ser irreversíveis para uma determinada organização. Com isso, após o estudo de caso realizado acima, foi introduzida a aplicação da ferramenta *NIST CSF Maturity Tool*, anteriormente registradas na subseções 2.9.1.2 e 3.3, sendo realizada internamente na Empresa X, em uma determinada área de atuação correspondente ao Setor de Tecnologia de Automação da organização. A pesquisa foi realizada com a utilização da ferramenta *NIST CSF Maturity Tool*, como discutido no item 2.9.1.2, a fim de realizar uma análise de maturidade no que tange a segurança cibernética do setor.

Em suma, as figuras 30, 31, 32 e 33, a seguir, representam os resultados alcançados. Na figura 30, estão registrados, em escala de 0 a 100%, o resultado alcançado em cada categoria estudada após o estudo completo da ferramenta (Anexo A).

Identificador Exclusivo de Função	Função	Identificador Exclusivo de Categoria	Categoria	Atende	Não Atende	Não se Aplica
ID	Identificar	ID.AM	Gerenciamento de Ativos	100%	0%	0%
		ID.BE	Contexto Empresarial	100%	0%	0%
		ID.GV	Governança	100%	0%	0%
		ID.RA	Avaliação de Risco	83%	17%	0%
		ID.RM	Estratégia de Gerenciamento de Riscos	100%	0%	0%
		ID.SC	Gerenciamento de Riscos da Cadeia de Suprimento	60%	20%	20%
PR	Proteger	PR.AC	Gerenciamento de identidade e controle de acesso	100%	0%	0%
		PR.AT	Conscientização e Treinamento	100%	0%	0%
		PR.DS	Segurança de Dados	75%	25%	0%
		PR.IP	Processos e Procedimentos de Proteção da Informação	67%	17%	17%
		PR.MA	Manutenção	100%	0%	0%
		PR.PT	Tecnologia Protetora	80%	0%	20%
DE	Detectar ou Diagnosticar	DE.AE	Anomalias e Incidentes	40%	60%	0%
		DE.CM	Monitoramento Continuo de Segurança	88%	13%	0%
		DE.DP	Processos de Detecção	20%	80%	0%
RS	Responder	RS.RP	Planejamento de Resposta	100%	0%	0%
		RS.CO	Comunicações	100%	0%	0%
		RS.AN	Análise	80%	20%	0%
		RS.MI	Mitigação	100%	0%	0%
		RS.IM	Aperfeiçoamentos	100%	0%	0%
RC	Recuperar	RC.RP	Planejamento de Recuperação	100%	0%	0%
		RC.IM	Aperfeiçoamentos	100%	0%	0%
		RC.CO	Comunicações	33%	0%	67%

Figura 30 – Resultado obtido após a aplicação da metodologia. Fonte: Autor.

Após a contabilização de cada categoria estudada, torna-se interessante transformar os dados encontrados nas colunas "Atende", "Não Atende" e "Não se Aplica" em gráficos, a fim de torná-los "palpáveis"a uma análise interna na empresa pesquisada e fornecer uma melhor visualização da maturidade atingida no setor.

Por intermédio da figura 31, das 108 subcategorias, ou itens, disponibilizadas no guia (Anexo A), é possível constatar que 80,56% desses itens são atendidos, 13,89% deste montante não são atendidos e apenas 5,55% deles são não aplicáveis à pesquisa.

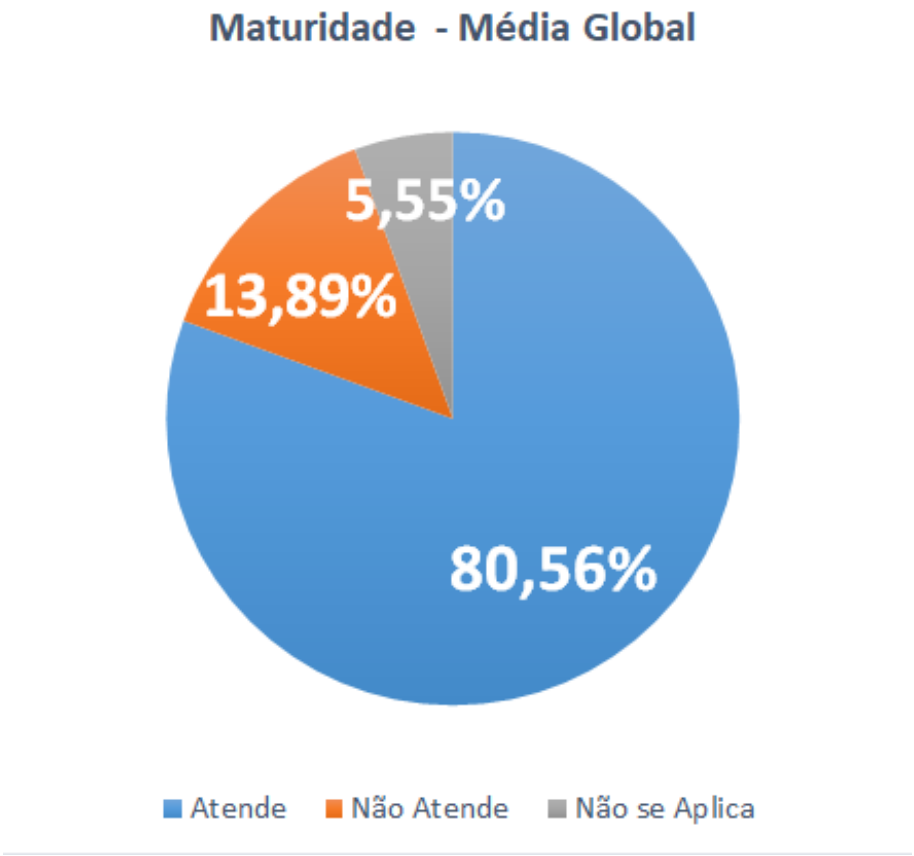


Figura 31 – Maturidade - Média Global obtida para as respostas: "Atende", "Não Atende" e "Não se Aplica". Fonte: Autor.

Na figura 32 pode-se visualizar o desempenho individualizado de cada categoria estudada. Em outras palavras as funções atingiram os seguintes percentuais:

- Identificar (ID): 91% dos itens atendidos, 6% não atendidos e 3% não aplicáveis;
- Proteger (PR): 87% dos itens são atendidos, 7% não atendidos e 6% não aplicáveis;
- Detectar ou Diagnosticar (DE): 49% dos itens atendidos, 51% não atendidos e nenhum não aplicável;
- Responder (RS): 96% dos itens atendidos, 4% não atendidos e nenhum não aplicável;
- Recuperar (RC): 79% dos itens são atendidos, nenhum item não atendido e 22% deles são não aplicáveis.

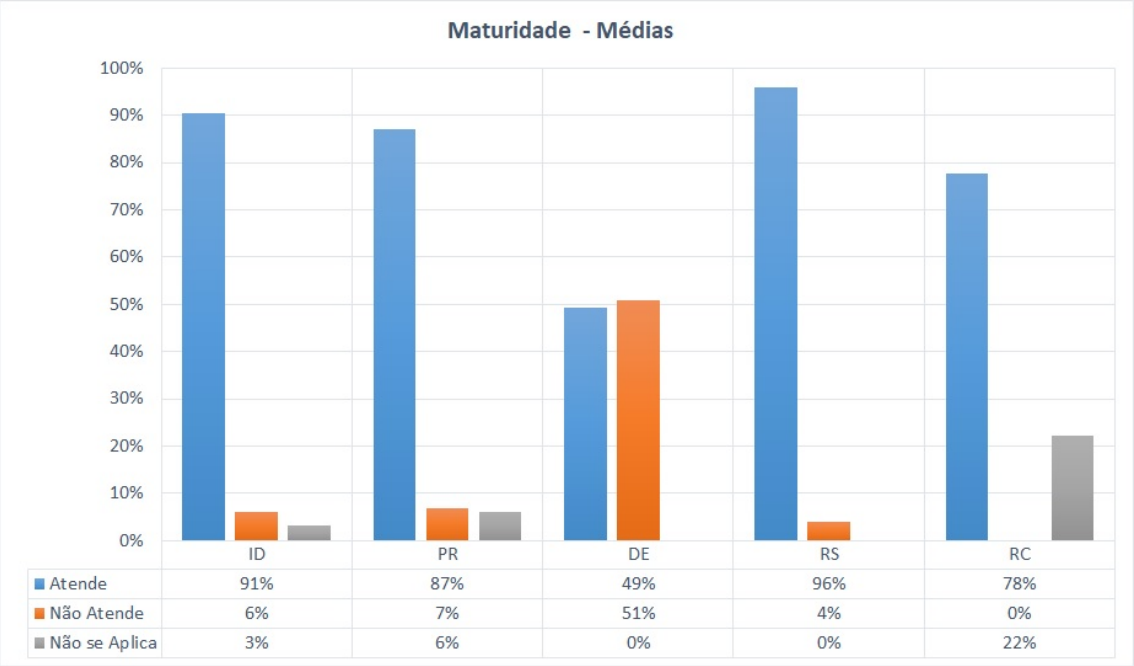


Figura 32 – Maturidade - Médias obtidas para as respostas 'Atende', 'Não Atende' e 'Não se Aplica' nas 5 funções do guia. Fonte: Autor.

A fim de avaliar o comportamento de cada categoria, foi gerado um gráfico que será apresentado a seguir, na figura 33, apresentando o comportamento dos itens atendidos mediante ao comportamento desejado. Para isso, foi considerado que o comportamento desejado da maturidade do Setor de Tecnologia de Automação é possuir maturidade igual ou superior a 80% nos itens atendidos. Intrinsecamente, ao se atingir no mínimo 80% nos itens atendidos, os itens não atendidos e não aplicáveis à pesquisa, de forma combinada, que de fato evidenciam vulnerabilidades na estrutura de segurança da organização, estarão sendo mitigados.

Dessa forma, evidencia-se que, das 23 categorias da estrutura, 6 delas não apresentam o comportamento desejado. São elas:

- Comunicações (RC.CO), na função Recuperar, com 33%. 67% dos itens são não aplicáveis;
- Processos e Detecção (DE.CP), na função Detectar ou Diagnosticar, com 20%. 80% dos itens não estão sendo atendidos;
- Anomalias e Incidentes (DE.AE), na função Detectar ou Diagnosticar, com 40%. 60% dos itens não estão sendo atendidos;
- Processos e Procedimentos de Proteção de Informação (PR.IP), na função Proteger, com 67%. 17% dos itens não estão sendo atendidos e 16% são não aplicáveis;
- Segurança de Dados (PR.DS), na função Proteger, com 75%. 25% dos itens não estão sendo atendidos;

- Gerenciamento de Riscos da Cadeia de Suprimento (ID.SC), na função Identificar, com 60%. 20% dos itens não estão sendo atendidos e 20% são não aplicáveis.

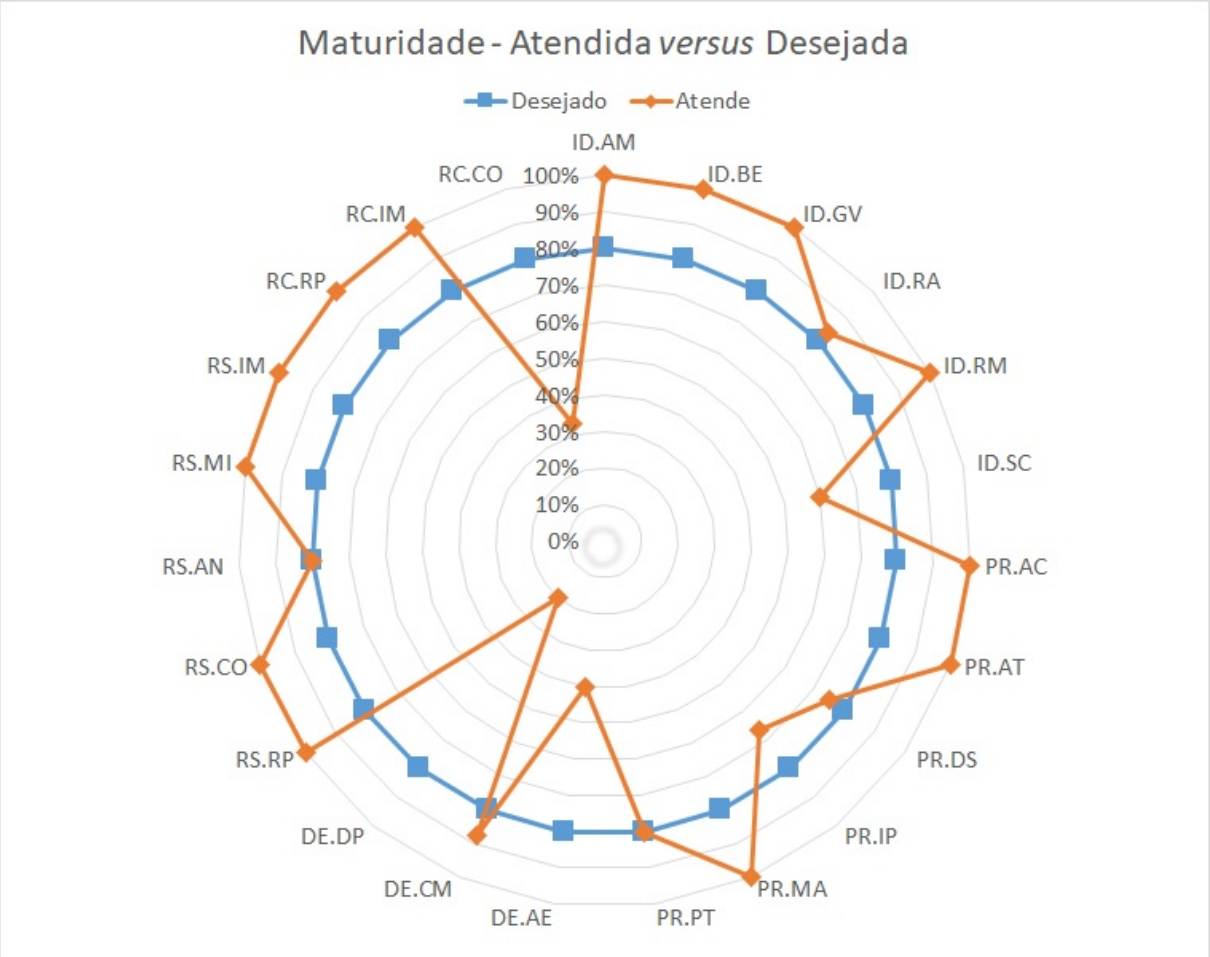


Figura 33 – Maturidade - Atendida *versus* Desejada. Fonte: Autor.

5 CONCLUSÃO

O estudo de caso realizado na seção 3.2 apresentou os 5 ciberataques mais famosos do mundo, do mesmo modo que os 2 ataques cibernéticos mais evidentes aqui no Brasil. Entende-se por "ciberataques mais famosos"aqueles que causaram danos financeiros e de infraestrutura significativos em suas vítimas e que, atualmente, servem de modelo para estudo e desenvolvimento de novas tecnologias de segurança.

Pôde-se verificar que os *hackers* nos ataques *WannaCry*, *NotPetya/ExPetr*, à empresa JBS e ao Supremo Tribunal de Justiça brasileiro, utilizaram *malwares* do tipo *ransomware* a fim de paralisar momentaneamente as operações das organizações, manter os dados capturados como reféns, criptografá-los e, por fim, exigir resgate às vítimas. Nos três primeiros casos, os criminosos obtiveram êxito, causando perdas estimadas de US$ 4 bilhões, US$ 10 bilhões e US$ 11 milhões, respectivamente.

Ademais, nos ataques *NotPetya/ExPetr*, *Stuxnet* e *Mirai*, foram utilizados *malwares* do tipo *worms* pelos criminosos, no intuito de infectar os sistemas, interromper a operação das organizações e danificar equipamentos, tornando seus serviços e operações indisponíveis. Além disso, trouxe prejuízo de US$ 10 bilhões, paralisação e danificação de centrífugas e computadores do programa nuclear iraniano, e indisponibilidade em 85 sites e serviços populares no mundo, respectivamente. Por fim, no ataque *DarkHotel* foi constatado um ataque de *spyware*, a fim de espionar empregados de Estado em hotéis asiáticos.

Os danos causados por alguns desses ataques poderiam ter sido evitados, caso os administradores de rede estivessem atentos ao uso contínuo de sistemas de computador e dispositivos desatualizados, à utilização de mídias removíveis em sistemas críticos e à falta de monitoramento seguro nas redes de acesso a internet.

Redes públicas não são consideradas as mais seguras, principalmente aquelas que recebem grandes fluxos de acessos e requisições, como as redes *WiFi* de cafés, hotéis e aeroportos, por exemplo. Mesmo assim, alguns usuários pensam que quando há algum tipo de autenticação, eles estão seguros. Entretanto, permanecem as orientações de segurança ao usuário. É importante que ele esteja atento aos sites que visita e às ligações, *sms* e *e-mails* recebidos. É recorrente que seja solicitada a instalação de uma atualização, aparentemente legítima, de um software popular, que receba um *e-mail* desconhecido com anexo ou *links* questionáveis, *sms* e ligações duvidosas, da mesma maneira que surja a percepção de lentidão na conexão, quando o usuário acessa uma rede infectada.

Os principais indícios citados anteriormente também podem surgir ao acessar uma rede confiável. Todavia, deve-se atentar aos *websites* visitados, se os *downloads* são seguros e de fontes confiáveis, se as mídias removíveis são seguras, se a rede é estável e sem lentidão,

e se o sistema está atualizado com as devidas correções de segurança implementadas pelos desenvolvedores do *software* e de sistemas operacionais.

Após o estudo do assunto segurança cibernética e ataques cibernéticos, tornou-se interessante aplicar uma metodologia prática (discutida na seção 3.3), voltada à aplicação de normas e métodos para a compreensão, gerenciamento e apresentação do risco de segurança cibernética em organizações - precisamente na indústria. Desse modo, utilizou-se a ferramenta *NIST CSF Maturity Tool* como pesquisa qualitativa que, além de estar baseada nas normas e metodologias do *framework NIST*, é gratuita e fornece uma gama de resultados aplicáveis aos *stakeholders* externos e internos à organização.

O estudo foi realizado internamente na Empresa X, como uma espécie de pesquisa, com a aplicação de questionários e, posteriormente, com uma análise da maturidade em segurança cibernética no Setor de Tecnologia de Automação da empresa.

Pode-se destacar que um ótimo resultado de média global foi alcançado, no qual 80,56% dos itens estudados foram atendidos, superando o índice desejado de 80%. Com relação às médias de cada função, apenas duas estiveram abaixo da média global: 'Detectar' com 49% e 'Recuperar' com 78% - esta última, esteve ligeiramente abaixo do média geral e foi influenciada pelos questionamentos relacionados à outro setor da organização.

Portanto, vale destacar que o setor de Tecnologia de Automação da Empresa X deve reavaliar suas políticas de segurança interna a fim de melhorar os índices dos itens atendidos abaixo do percentual desejado (80%). Isto inclui uma avaliação de riscos e gerenciamento de riscos na cadeia de suprimentos mais assertivos, incluindo documentações de vulnerabilidades e criando um processo de avaliação aos *stakeholders* externos a fim de priorizar aqueles que prezam pela segurança cibernética.

A empresa deve se atentar à segurança dos dados, garantindo que as informações e os registros sejam gerenciados de maneira consistente com a estratégia de risco da organização para proteger a confidencialidade, a integridade e a disponibilidade de informações. Além da proteção, deve-se preocupar com os processos e procedimentos de proteção das informações, garantindo que as políticas são mantidas e usadas para gerenciar a proteção de sistemas e ativos de informações. Por fim, é necessário garantir que anomalias e incidentes serão detectados, seu potencial impacto será compreendido e os processos de detecção serão mantidos e testados para garantir a conscientização sobre eventos anômalos.

Dessa forma, pode-se afirmar que um grande aliado no combate a ataques cibernéticos é a utilização de *frameworks* de segurança cibernética, seja o *NIST CSF Maturity Tool* ou qualquer um dos outros que foram apresentados na seção 2.9.

Além da utilização de *frameworks* de cibersegurança disponíveis, as principais dicas para se proteger de ataques cibernéticos de todos os tipos são: manter o software e o sistema operacional dos dispositivos atualizados; priorizar equipamentos e dispositivos que possuam

tecnologias e certificações de segurança; usar antivírus e *antimalwares* e os manter sempre atualizados; usar senhas fortes; nunca abrir anexos e *links* em *e-mails* desconhecidos e de *spams*; não efetuar *download* de sites não confiáveis; evitar usar mídias removíveis desconhecidas; usar *VPN* ao acessar redes *WiFi* públicas; realizar *backup* dos dados; não fornecer informações pessoais a desconhecidos; estar atento às *URL's* dos sites; entrar em contato com canais oficiais para confirmar pedidos suspeitos; e ficar atento ao extrato bancário.

Para trabalhos futuros, sugere-se a implementação da ferramenta *NIST CSF Maturity Tool* em todos os outros setores da Empresa X não abordados nesse trabalho, assim como aplicar uma outra abordagem de pontuação aos itens pesquisados. Em outras palavras, como orienta o criador da ferramenta, pode ser adotado o sistema de pontuação em uma escala de 0 a 5 (não necessariamente números inteiros) a cada subcategoria respondida. Ao final, será possível obter uma análise mais fiel à realidade do setor/empresa, além de mensurar assertivamente quais os índices estão abaixo do desejado, a fim de melhorá-los e determinar em qual nível de maturidade os setores da organização se encontram.

ANEXO A – ESTRUTURA *NIST CSF*

Guia NIST *Cybersecurity Framework* - NIST CSF, versão 1.1 (NIST, 2018).

Função	Categoria	Subcategoria	Referências Informativas
	Gerenciamento de Ativos (ID.AM): Os dados, pessoal, dispositivos, sistemas e instalações que permitem que a organização atinja objetivos de negócio são identificados e gerenciados de maneira consistente com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização.	**ID.AM-1:** Dispositivos físicos e sistemas dentro da organização são inventariados	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR. 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Plataformas de software e aplicações dentro da organização são inventariadas	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR. 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Comunicação organizacional e fluxos de dados são mapeados	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, 3-CA, CA-9, PL-8
		ID.AM-4: Sistemas de informação externos são catalogados	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Recursos (por exemplo, *hardware*, dispositivos, dados, tempo, pessoal e *software*) são priorizados com base em suas classificações, criticidade e valor para os negócios	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14 e SC-6
		ID.AM-6: Funções e responsabilidades de segurança cibernética para toda a força laboral e *stakeholders* de terceiros (por exemplo, fornecedores, clientes, parceiros) são estabelecidas	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Maturidade - Categoria ID.AM		
	Contexto Empresarial (ID.BE): A missão, objetivos, *stakeholders* e atividades da organização são compreendidos e priorizados; essas informações são usadas para informar funções, responsabilidades e decisões de gerenciamento de riscos da segurança cibernética.	**ID.BE-1:** O papel da organização na cadeia de suprimentos é identificado e comunicado	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: O lugar da organização na infraestrutura crítica e seu setor industrial é identificado e comunicado	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Cláusula 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: : Prioridades para missão organizacional, objetivos e atividades são estabelecidas e comunicadas	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** M-11, SA-14
		ID.BE-4: Dependências e funções críticas para a entrega de serviços críticos são estabelecidas	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Os requisitos de resiliência para apoiar a prestação de serviços críticos são estabelecidos para todos as condições operacionais (por exemplo, sob coerção/ ataque, durante a recuperação, operações normais)	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA- 14
	Maturidade - Categoria ID.BE		
	Governança (ID.GV): As políticas, procedimentos e processos para gerenciar e monitorar os requisitos regulatórios, jurídicos, de risco, ambientais e operacionais da organização são compreendidos e informam gerenciamento do risco de segurança cibernética.	**ID.GV-1:** A política organizacional de segurança cibernética é estabelecida e comunicada	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev.4** - 1 controles de todas as famílias de controle de segurança
		ID.GV-2: As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controles de todas as famílias de controle de segurança
		ID.GV-4: : Processos de governança e gerenciamento de riscos abordam os riscos de segurança cibernética	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Cláusula 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, 7-PM, PM-9, 10 PM, PM-11
	Maturidade - Categoria ID.GV		

Função	Categoria	Subcategoria	Referências Informativas
	Avaliação de risco (ID.RA): A organização entende o risco de segurança cibernética para operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais e indivíduos.	**ID.RA-1:** As vulnerabilidades dos ativos são identificadas e documentadas	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Informações sobre ameaças cibernéticas são recebidas de fóruns e fontes de compartilhamento de informações	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
		ID.RA-3: Ameaças internas e externas são identificadas e documentadas	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-4: Potenciais impactos no negócio e probabilidades são identificados na organização	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM- 9, PM-11
		ID.RA-5: Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar riscos	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Cláusula 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
		ID.RA-6: As respostas ao risco são identificadas e priorizadas	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 **NIST SP 800-53 Rev. 4** PM-9
	Maturidade - Categoria ID.RA		
	Estratégia de Gerenciamento de Riscos (ID.RM): As prioridades, restrições, tolerâncias de risco e suposições da organização são estabelecidas e usadas para apoiar as decisões de risco operacional.	**ID.RM-1:** Processos de gerenciamento de risco são estabelecidos, gerenciados e aprovados pelos *stakeholders* organizacionais	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001: 2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3
		ID.RM-2: Tolerância ao risco organizacional é determinada e claramente expressa	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: A determinação de tolerância ao risco da organização é permeada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53** AP 4 SA-14, PM-8, PM-9, PM-11
	Maturidade - Categoria ID.RM		
	Gerenciamento de Riscos da Cadeia de Suprimento (ID.SC): As prioridades, restrições, tolerâncias de risco e suposições da organização são definidas e utilizadas para apoiar as decisões de risco associadas ao gerenciamento do risco da cadeia de suprimentos. A organização definiu e implementou os processos para identificar, avaliar e gerenciar os riscos da cadeia de suprimentos.	**ID.SC-1:** Os processos de gerenciamento de riscos da cadeia de suprimentos cibernéticos são identificados, estabelecidos, avaliados, gerenciados e acordados pelos *stakeholders* da organização.	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
		ID.SC-2: Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernéticos	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização e do Plano de Gerenciamento de Riscos da Cadeia de Suprimentos Cibernéticos	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Fornecedores e parceiros terceirizados são avaliados sistematicamente por meio de auditorias, resultados de testes ou outras formas de avaliações para confirmar que estão cumprindo suas obrigações contratuais	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: O planejamento e o teste de resposta e recuperação são realizados com prestadores e fornecedores de serviços terceirizados	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR-7.3, SR 7.4

Função	Categoria	Subcategoria	Referências Informativas
		de serviços terceirizados	**ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, 3-IR, IR4, 6-IR, IR-8, IR-9
	Maturidade - Categoria ID.SC		
	Gerenciamento de Identidade, Autenticação e Controle de Acesso (PR.AC): O acesso a ativos físicos e lógicos e recursos associados é limitado a usuários, processos e dispositivos autorizados e é gerenciado de maneira consistente com o risco avaliado de acesso não autorizado a atividades e transações autorizadas.	**PR.AC-1:** Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: O acesso físico aos ativos é gerenciado e protegido	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: O acesso remoto é gerenciado	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Permissões de acesso e autorizações são gerenciadas, incorporando os princípios de menor privilégio e divisão de tarefas	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: As identidades são revisadas, vinculadas a credenciais e confirmadas em interações	**CIS CSC** 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013,** A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Usuários, dispositivos e outros recursos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Maturidade - Categoria PR.AC		
	Conscientização e Treinamento (PR.AT): Os funcionários e parceiros da organização são treinados sobre a conscientização sobre segurança cibernética e são treinados para executar suas obrigações e responsabilidades relacionadas à segurança cibernética, de acordo com os procedimentos e acordos relacionados.	**PR.AT-1:** Todos os utilizadores são informados a respeito e treinados	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Os usuários privilegiados compreendem suas funções e responsabilidades	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: *Stakeholders* terceirizados (por exemplo, fornecedores, clientes, parceiros) entendem suas funções e responsabilidades	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Executivos seniores compreendem suas funções e responsabilidades	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13

Função	Categoria	Subcategoria	Referências Informativas
PROTEGER (PR)		**PR.AT-5:** Os funcionários físicos e de segurança cibernética compreendem suas funções e responsabilidades	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	Maturidade - Categoria PR.AT		
	Segurança de Dados (PR.DS): As informações e os registros (dados) são gerenciados de maneira consistente com a estratégia de risco da organização para proteger a confidencialidade, a integridade e a disponibilidade de informações.	**PR.DS-1:** Os dados em repouso são protegidos	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Os dados em trânsito são protegidos	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Ativos são formalmente gerenciados durante a remoção, transferências e disposição	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: A capacidade adequada para garantir a disponibilidade é mantida	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: As proteções contra vazamentos de dados são implementadas	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Os mecanismos de verificação de integridade são usados para verificar o software, o *firmware* e a integridade das informações	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Mecanismos de verificação de integridade são usados para verificar a integridade do *hardware*	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Maturidade - Categoria PR.DS		
		PR.IP-1: Uma configuração básica de sistemas de tecnologia de informação/controle industrial é criada e mantida, incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev.** 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Um Ciclo de Vida de Desenvolvimento de Sistema para gerenciar sistemas é implementado	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Processos de controle de mudança de configuração estão em funcionamento	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: : Os Backups de informações são realizados, conservados e testados	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4

Função	Categoria	Subcategoria	Referências Informativas
	Processos e Procedimentos de Proteção da Informação (PR.IP): As políticas de segurança (que abordam a finalidade, o escopo, as funções, as responsabilidades, o compromisso de gerenciamento e a coordenação entre as entidades organizacionais), processos e procedimentos são mantidas e usadas para gerenciar a proteção de sistemas e ativos de informações.		**ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: As políticas e os regulamentos referentes ao ambiente operacional físico dos ativos organizacionais são cumpridos	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Os dados são destruídos de acordo com a política	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Os processos de proteção são aperfeiçoados	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 9, Cláusula 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: A eficácia das tecnologias de proteção é compartilhada	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e gerenciados	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Planos de recuperação e resposta são testados	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: A segurança cibernética está incluída nas práticas de recursos humanos (por exemplo, desaprovisionamento, triagem de pessoal)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maturidade - Categoria PR.IP		
	Manutenção (PR.MA): A manutenção e os reparos de componentes de sistemas de controle e informações industriais são executados de acordo com políticas e procedimentos.	**PR.MA-1:** Manutenção e reparo de ativos organizacionais são realizados e registrados, com ferramentas aprovadas e regulamentadas	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: A manutenção remota de ativos organizacionais é aprovada, registrada e realizada de maneira a impedir o acesso não autorizado	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	Maturidade - Categoria PR.MA		
	Tecnologia Protetora (PR.PT): As soluções de segurança técnica são gerenciadas para garantir a segurança e resiliência de sistemas e ativos,	**PR.PT-1:** Os registros de auditoria/registro são determinados, documentados, implementados e revisados de acordo com a política	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU Família
		PR.PT-2: As mídias removíveis são protegidas e seu uso é restrito de acordo com a política	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4

Função	Categoria	Subcategoria	Referências Informativas
	consistentes com políticas, procedimentos e acordos relacionados.	incorporado pela configuração de sistemas para fornecer apenas recursos essenciais	**ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Redes de comunicação e controle são protegidas	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Alguns mecanismos (por exemplo, *fail-safe, load balancing, hot swap*) são implementados para garantir que requisitos de resiliência funcionem em situações normais e adversas	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
	Maturidade - Categoria PR.PT		
DETECTAR (DE)	**Anomalias e Incidentes (DE.AE):** Atividade anômala é detectada e o impacto potencial dos eventos é compreendido.	**DE.AE-1:** Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53** Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: O impacto dos eventos é determinado	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Os limites de alerta de incidentes são estabelecidos	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Maturidade - Categoria DE.AE		
	Monitoramento Contínuo de Segurança (DE.CM): O sistema de informação e os ativos são monitorados para identificar incidentes de segurança cibernética e verificar a eficácia das medidas de proteção.	**DE.CM-1:** A rede é monitorada para detectar potenciais incidentes de segurança cibernética	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: O ambiente físico é monitorado para detectar possíveis eventos de segurança cibernética	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: A atividade dos colaboradores é monitorada para detectar possíveis eventos de segurança cibernética	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Código malicioso é detectado	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Código móvel não autorizado é detectado	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: A atividade de provedor de serviços externo é monitorada para detectar possíveis eventos de segurança cibernética	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4

Função	Categoria	Subcategoria	Referências Informativas
		DE.CM-7: O monitoramento de colaboradores não autorizados, conexões, dispositivos e software é executado	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Há realização de varreduras de vulnerabilidade	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	Maturidade - Categoria DE.CM		
	Processos de Detecção (DE.DP): Os processos e procedimentos de detecção são mantidos e testados para garantir a conscientização sobre eventos anômalos	**DE.DP-1:** Papéis e responsabilidades para a detecção são bem definidos para garantir a prestação de contas	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: As atividades de detecção cumprem todos os requisitos aplicáveis	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Os processos de detecção são testados	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Informações de detecção de incidente são comunicadas	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Processos de detecção são continuamente aperfeiçoados	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
	Maturidade - Categoria DE.DP		
	Planejamento de Respostas (RS.RP): Os processos e procedimentos de resposta são executados e mantidos para garantir a resposta a incidentes de segurança cibernética detectados.	**RS.RP-1:** Plano de resposta é executado durante ou depois de um incidente	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Maturidade - Categoria RS.RP		
	Comunicações (RS.CO): As atividades de resposta são coordenadas com *stakeholders* internos e externos (por exemplo, apoio externo de órgãos fiscalizadores).	**RS.CO-1:** Os colaboradores conhecem seus papéis e a sequência de operações quando uma resposta é necessária	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Os incidentes são informados de acordo com os critérios estabelecidos	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: As informações são compartilhadas de acordo com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Cláusula 7.4, Cláusula 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: A coordenação com os *stakeholders* ocorre de acordo com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: O compartilhamento voluntário de informações ocorre com os *stakeholders* externos para alcançar uma conscientização situacional mais ampla sobre segurança cibernética	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Maturidade - Categoria RS.CO		
		RS.AN-1: As notificações dos sistemas de detecção são analisadas	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5

Função	Categoria	Subcategoria	Referências Informativas
RESPONDER (RS)			**NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
	Análise (RS.AN): A análise é realizada para garantir resposta eficaz e dar apoio às atividades de recuperação.	**RS.AN-2:** O impacto do incidente é compreendido	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Há realização de investigações	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Os incidentes são categorizados de forma consistente com os planos de resposta	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Os processos são estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas para a organização a partir de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou pesquisadores de segurança)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Maturidade - Categoria RS.AN		
	Mitigação (RS.MI): As atividades são realizadas para impedir a expansão de um evento, atenuar seus efeitos e resolver o incidente.	**RS.MI-1:** Os incidentes são contidos	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Os incidentes são mitigados	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53** Rev. 4 IR-4
		RS.MI-3: As vulnerabilidades identificadas recentemente são mitigadas ou documentadas como riscos aceitos	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Maturidade - Categoria RS.MI		
	Aperfeiçoamentos (RS.IM): As atividades de resposta organizacionais são aperfeiçoadas pela incorporação de lições aprendidas de atividades anteriores de detecção/resposta.	**RS.IM-1:** Os planos de resposta incorporam as lições aprendidas	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: As estratégias de resposta são atualizadas	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Maturidade - Categoria RS.IM		
RECUPERAR (RC)	**Planejamento de Recuperação (RC.RP):** Os processos e procedimentos de recuperação são executados e mantidos para garantir a restauração de sistemas ou ativos afetados por incidentes de segurança cibernética.	**RC.RP-1:** O Plano de recuperação é executado durante ou após um incidente de segurança cibernética	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Maturidade - Categoria RC.RP		
	Aperfeiçoamentos (RC.IM): O planejamento e os processos de recuperação são aperfeiçoados pela incorporação de lições aprendidas em atividades futuras.	**RC.IM-1:** Planos de recuperação incorporam as lições aprendidas	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: As estratégias de recuperação são atualizadas	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Maturidade - Categoria RC.IM		
	Comunicações (RC.CO): As atividades de restauração são coordenadas com partes internas e externas (por exemplo, centros de coordenação, provedores de serviços de internet, proprietários de sistemas de ataque, vítimas, outras CSIRTs e fornecedores)	**RC.CO-1:** As relações públicas são gerenciadas	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Cláusula 7.4
		RC.CO-2: A reputação é reparada após um incidente	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Cláusula 7.4
		RC.CO-3: As atividades de recuperação são comunicadas aos *stakeholders* internos e externos, bem como às equipes executivas e de gestão.	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4
	Maturidade - Categoria RC.CO		

REFERÊNCIAS

ACCELLION. *Enhance Data Security and Privacy with SOC 2 Compliance*. 2018. [Online] Disponível em: https://www.accellion.com/sites/default/files/wysiwyg/governance-soc2-compliance-standards.jpg. Acesso em: 11/08/2021. Citado 2 vezes nas páginas 9 e 50.

ANATEL. *Segurança Cibernética*. 2021. [Online] Disponível em: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica. Acesso em: 21/06/2021. Citado na página 40.

ANSI. *ANSI*. 2018. [Online] Disponível em: https://www.fedramp.gov/. Acesso em: 15/08/2021. Citado 2 vezes nas páginas 9 e 55.

ANWAR, M. et al. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 2017. Elsevier, v. 69, p. 437–443, 2017. Citado na página 21.

BBC NEWS BRASIL. *Ataque de hackers à JBS: o que se sabe sobre grupo russo apontado como responsável pelo FBI*. 2021. [Online] Disponível em: https://www.bbc.com/portuguese/internacional-57344706. Acesso em: 20/08/2021. Citado na página 65.

BERNARDO, K. *Internet das coisas – Quais as oportunidades de negócios com IoT*. 2019. [Online] Disponível em: https://www.opus-software.com.br/internet-das-coisas-iot-oportunidades-de-negocios/. Acesso em: 10/07/2021. Citado 2 vezes nas páginas 9 e 28.

BOSCO, N. *Ataque de hackers ao STJ é o mais grave da história no país*. 2020. [Online] Disponível em: https://www.correiobraziliense.com.br/brasil/2020/11/4886936-ataque-de-hackers-ao-stf-e-o-mais-grave-da-historia-no-pais.html. Acesso em: 20/08/2021. Citado 2 vezes nas páginas 64 e 65.

BUG BUSTER. *5 ferramentas para acesso remoto*. 2020. [Online] Disponível em: https://bugbusters.com.br/2020/05/27/5-ferramentas-para-acesso-remoto/. Acesso em: 17/07/2021. Citado na página 38.

CANONGIA, C.; JUNIOR, R. M. Segurança cibernética: o desafio da nova sociedade da informação. *Parcerias Estratégicas*, 2010. v. 14, n. 29, p. 21–46, 2010. Citado 2 vezes nas páginas 21 e 40.

CASTELLS, M. *A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade*. [S.l.]: Zahar, 2003. Citado na página 27.

CERT.BR. *Cartilha de Segurança para a Internet. Códigos maliciosos (Malware)*. 2017. [Online] Disponível em: https://cartilha.cert.br/malware/. Acesso em: 17/07/2021. Citado 2 vezes nas páginas 11 e 43.

CIS. *CIS Controls Version 7 – What's Old, What's New*. 2021. [Online] Disponível em: https://www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/. Acesso em: 12/08/2021. Citado 2 vezes nas páginas 9 e 53.

CISQ. *CISQ*. 2021. [Online] Disponível em: https://www.it-cisq.org/. Acesso em: 14/08/2021. Citado 2 vezes nas páginas 9 e 54.

CISTERNELLI, E. *7 Cybersecurity Frameworks That Help Reduce Cyber Risk*. 2020. [Online] Disponível em: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk. Acesso em: 10/08/2021. Citado 5 vezes nas páginas 45, 48, 50, 51 e 52.

CITTÀ TELECOM. *Tudo sobre gerenciamento de redes*. 2016. [Online] Disponível em: https://www.cittatelecom.com.br/2016/06/gerenciamento-de-redes/. Acesso em: 03/07/2021. Citado 2 vezes nas páginas 9 e 23.

COACT. *Cyber Risk Management and Compliance Services*. 2020. [Online] Disponível em: https://coact.com/services/. Acesso em: 12/08/2021. Citado 2 vezes nas páginas 9 e 52.

COMER, D. E. *Redes de Computadores e Internet-6*. [S.l.]: Bookman Editora, 2016. Citado 6 vezes nas páginas 11, 23, 34, 37, 42 e 44.

CONVERGÊNCIA DIGITAL. *Hackers elegem o Brasil como alvo preferido na América Latina*. 2021. [Online] Disponível em: https://www.convergenciadigital.com.br/infoid=57318sid=18. Acesso em: 21/06/2021. Citado na página 20.

COSO. *Welcome to COSO*. 2021. [Online] Disponível em: https://www.coso.org/Pages/default.aspx. Acesso em: 13/08/2021. Citado 2 vezes nas páginas 9 e 53.

COSSETTI, M. C. *ExPetr/Petya/NotPetya: vírus é um Wiper e ainda pior que ramsonware*. 2017. [Online] Disponível em: https://www.techtudo.com.br/noticias/2017/06/expetrpetyanotpetya-virus-e-um-wiper-e-ainda-pior-que-ramsonware.ghtml. Acesso em: 18/08/2021. Citado na página 59.

COSSETTI, M. C. *Petya ou NotPetya? Novo ransomware usa mesma falha do WannaCry*. 2017. [Online] Disponível em: https://www.techtudo.com.br/noticias/2017/06/petya-ou-notpetya-novo-ransomware-usa-mesma-falha-do-wannacry.ghtml. Acesso em: 18/08/2021. Citado 2 vezes nas páginas 9 e 60.

COSTA, D. d. O. Crimes virtuais: uma breve análise da legislação brasileira sobre o tema. 2019. Centro Universitário CESMAC, 2019. Citado na página 56.

CRUZ, J. V. V. *O Futuro da Segurança Cibernética no Brasil: Papéis e Responsabilidades*. 2020. Monografia. Trabalho de Conclusão de Curso como exigência parcial para a aprovação no Curso de Aperfeiçoamento Militar. Escola de Formação Complementar do Exército. Salvador. Citado na página 21.

CZOSSECK, C.; OTTIS, R.; TALIHÄRM, A. Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 2011. IGI Global, v. 1, n. 1, p. 24–34, 2011. Citado na página 18.

DELOITTE. *Investimento em segurança cibernética pode acelerar a transformação digital no Brasil, aponta estudo da Deloitte*. 2021. [Online] Disponível em: https://www2.deloitte.com/br/pt/footerlinks/pressreleasespage/Release-Estrategias-Futuro-Cibernetico.html. Acesso em: 21/06/2021. Citado na página 21.

DIAS, J. C. S. *As 10 melhores frases de Tim Cook sobre privacidade e segurança*. 2015. [Online] Disponível em: https://www.kaspersky.com.br/blog/tim-cook-speaks-about-privacy-security/5372/. Acesso em: 11/06/2021. Citado na página 18.

DROZHZHIN, A. *VDarkHotel: campanha de espionagem em hotéis de luxo da Ásia*. 2014. [Online] Disponível em: https://www.kaspersky.com.br/blog/darkhotel-campanha-de-espionagem-em-hoteis-de-luxo-da-asia/4342/. Acesso em: 18/08/2021. Citado 4 vezes nas páginas 9, 61, 62 e 63.

FEDRAMP. *FedRAMP*. 2021. [Online] Disponível em: https://www.fedramp.gov/. Acesso em: 14/08/2021. Citado 2 vezes nas páginas 9 e 55.

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. [S.l.]: AMGH Editora, 2009. Citado 13 vezes nas páginas 9, 11, 23, 24, 25, 26, 27, 28, 29, 31, 33, 36 e 37.

FORTINET. *A América Latina sofreu mais de 41 bilhões de tentativas de ataques cibernéticos em 2020*. 2021. [Online] Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020. Acesso em: 21/06/2021. Citado na página 20.

G1. *JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA*. 2021. [Online] Disponível em: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml. Acesso em: 20/08/2021. Citado na página 65.

G1. *JBS sofre ataque hacker nas unidades dos EUA e da Austrália*. 2021. [Online] Disponível em: https://g1.globo.com/economia/agronegocios/noticia/2021/05/31/jbs-sofre-ataque-hacker-nas-unidades-dos-eua-e-da-australia.ghtml. Acesso em: 20/08/2021. Citado na página 65.

GALOYAN, A. *Segurança cibernética no Âmbito das Relações Internacionais*. 2019. Monografia. apresentada como um requisito para conclusão de curso de Relações Internacionais. Universidade de Brasília. Citado na página 21.

GEORGIADOU, A.; MOUZAKITIS, S.; ASKOUNIS, D. Working from home during covid-19 crisis: a cyber security culture assessment survey. *Security Journal*, 2021. Springer, p. 1–20, 2021. Citado na página 21.

GOMES, P. C. T. *Conheça os Principais Protocolos de Rede e Seus Usos*. 2019. [Online] Disponível em: https://www.opservices.com.br/protocolos-de-rede. Acesso em: 12/07/2021. Citado 3 vezes nas páginas 11, 29 e 30.

HAMANN, R. *Stuxnet: o vírus da pesada*. 2010. [Online] Disponível em: https://www.tecmundo.com.br/virus/5878-stuxnet-o-virus-da-pesada.htm. Acesso em: 18/08/2021. Citado na página 61.

IASME. *IASME Governance Audited*. 2020. [Online] Disponível em: https://iasme.co.uk/wp-content/uploads/2020/02/iasme-gov-audited-logo.png. Acesso em: 11/08/2021. Citado 2 vezes nas páginas 9 e 50.

IBM. *Estudo IBM: líderes brasileiros apontam áreas de investimento impulsionadas pela Covid-19*. 2020. [Online] Disponível em: https://www.ibm.com/blogs/ibm-comunica/estudo-ibm-lideres-brasileiros-apontam-areas-de-investimento-impulsionadas-pela-covid-19/. Acesso em: 21/06/2021. Citado na página 20.

IPERIUS BACKUP BRASIL. *Entendendo os conceitos entre os modelos TCP/IP e OSI*. 2019. [Online] Disponível em: https://www.iperiusbackup.net/pt-br/entendendo-os-conceitos-entre-os-modelos-tcpip-e-osi/. Acesso em: 11/07/2021. Citado 5 vezes nas páginas 11, 30, 32, 33 e 34.

ISACA. *COBIT*. 2021. [Online] Disponível em: https://www.isaca.org/resources/cobit. Acesso em: 13/08/2021. Citado 2 vezes nas páginas 9 e 53.

KASPERSKY. *O que é o ransomware WannaCry?* 2019. [Online] Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry. Acesso em: 17/08/2021. Citado 2 vezes nas páginas 57 e 59.

KELVIN. *Revisando o Stuxnet: Ataque Cibernético Israelense-Americano*. 2020. [Online] Disponível em: https://mdftechnology.com.br/revisando-o-stuxnet-ataque-cibernetico-israelense-americano/. Acesso em: 18/08/2021. Citado na página 61.

KOCHETKOVA, K. *Como você pode ajudar a não derrubar a Internet*. 2016. [Online] Disponível em: https://www.kaspersky.com.br/blog/attack-on-dyn-explained/6764/. Acesso em: 19/08/2021. Citado 3 vezes nas páginas 9, 63 e 64.

KOTTASOVÁ, I. *Como as ameaças russas fizeram da Estônia um país especialista em cibersegurança*. 2021. [Online] Disponível em: https://www.cnnbrasil.com.br/business/2021/06/19/como-as-ameacas-russas-fizeram-da-estonia-um-pais-em-especialista-ciberseguranca. Acesso em: 18/06/2021. Citado 2 vezes nas páginas 18 e 19.

KUROSE, J.; ROSS, K. *Redes de Computadores e a Internet: uma abordagem top-down*. [S.l.]: Pearson Education do Brasil Ltda.,, 2014. Citado 6 vezes nas páginas 9, 28, 34, 35, 36 e 37.

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a internet. *São Paulo: Person*, 2006. v. 28, 2006. Citado 2 vezes nas páginas 11 e 27.

LALLIE, H. S. et al. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 2021. Elsevier, v. 105, p. 102248, 2021. Citado na página 20.

LIMA, K.; RIGUES, R. *JBS pagou mais de R$ 55 milhões para solucionar ataque hacker*. 2021. [Online] Disponível em: https://olhardigital.com.br/2021/06/10/internet-e-redes-sociais/jbs-pagou-mais-de-r-55-milhoes-para-solucionar-ataque-hacker/. Acesso em: 20/08/2021. Citado 2 vezes nas páginas 65 e 66.

MACHADO DA COSTA, F. M. *PF investiga possível ataque hacker ao sistema do Supremo*. 2020. [Online] Disponível em: https://veja.abril.com.br/blog/radar/pf-investiga-possivel-ataque-hacker-ao-sistema-do-supremo/. Acesso em: 20/08/2021. Citado na página 65.

MASSERINI, J. J. *Free NIST CSF Maturity Tool*. 2019. [Online] Disponível em: https://johnmasserini.com/2019/01/28/free-nist-csf-maturity-tool/. Acesso em: 10/08/2021. Citado 4 vezes nas páginas 9, 47, 56 e 66.

MCAFEE. *9 Tipos de hackers e suas motivações*. 2019. [Online] Disponível em: https://www.mcafee.com/blogs/languages/portugues/9-tipos-de-hackers-e-suas-motivacoes/. Acesso em: 17/07/2021. Citado 3 vezes nas páginas 11, 40 e 41.

MELLO, D. *Home office foi adotado por 46% das empresas durante a pandemia*. 2020. [Online] Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia. Acesso em: 17/07/2021. Citado na página 37.

MICROSOFT AZURE. *O que é computação em nuvem?* 2015. [Online] Disponível em: https://azure.microsoft.com/pt-br/overview/what-is-cloud-computing/. Acesso em: 17/07/2021. Citado 3 vezes nas páginas 11, 38 e 39.

MONITOR MERCANTIL. *Trabalho remoto fez crescer tentativas de ciberataques*. 2021. [Online] Disponível em: https://monitormercantil.com.br/trabalho-remoto-fez-crescer-tentativas-de-ciberataques/. Acesso em: 21/06/2021. Citado na página 20.

MORELLI, M. *"É preciso diferenciar hacker de cibercriminoso"*. 2015. [Online] Disponível em: https://veja.abril.com.br/tecnologia/e-preciso-diferenciar-hacker-de-cibercriminoso/. Acesso em: 17/07/2021. Citado na página 42.

MUNDO+TECH. *10 ameaças cibernéticas em alta no primeiro semestre de 2020*. 2020. [Online] Disponível em: https://mundomaistech.com.br/seguranca/10-ameacas-ciberneticas-em-alta-no-primeiro-semestre-de-2020/. Acesso em: 17/07/2021. Citado na página 44.

MUTUNE, G. *23 Top Cybersecurity Frameworks*. 2019. [Online] Disponível em: https://cyberexperts.com/cybersecurity-frameworks/. Acesso em: 10/08/2021. Citado 9 vezes nas páginas 45, 48, 49, 50, 51, 52, 53, 54 e 55.

NASCIMENTO, M. B. *Qual a Diferença entre Modelo OSI e TCP/IP?* 2019. [Online] Disponível em: https://www.dltec.com.br/blog/redes/diferenca-entre-modelo-osi-e-tcp-ip/. Acesso em: 10/07/2021. Citado 2 vezes nas páginas 9 e 31.

NERC. *NERC CIP Standards*. 2021. [Online] Disponível em: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. Acesso em: 11/08/2021. Citado 2 vezes nas páginas 9 e 51.

NIST. *Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica*. 2018. [Online] Disponível em: https://www.uschamber.com/sites/default/files/intl$_n ist_f ramework_p ortugese_f inal f ull_w eb.pdf$. Acesso em: 10/08/2021. Citado 8 vezes nas páginas 9, 11, 45, 46, 67, 68, 69 e 79.

NOGUEIRA, L. *Conheça os maiores ciberataques da história do Brasil*. 2020. [Online] Disponível em: https://olhardigital.com.br/2020/11/06/seguranca/conheca-os-maiores-ciberataques-da-historia-do-brasil/. Acesso em: 19/08/2021. Citado 3 vezes nas páginas 9, 59 e 64.

NUNES, P. A definição de uma estratégia nacional de cibersegurança. *Nação e defesa*, 2012. v. 133, n. 5, p. 113–127, 2012. Citado na página 18.

PANZARINO, M. *Apple's Tim Cook Delivers Blistering Speech On Encryption, Privacy*. 2015. [Online] Disponível em: https://www.kaspersky.com.br/blog/tim-cook-speaks-about-privacy-security/5372/. Acesso em: 11/06/2021. Citado na página 18.

PATHCOM. *ISO 27001 27002*. 2018. [Online] Disponível em: https://www.pathcom.com/iso-27001-2-blue. Acesso em: 11/08/2021. Citado 2 vezes nas páginas 9 e 49.

PAUBOX. *What is HIPAA? Or is it HIPPA?* 2017. [Online] Disponível em: https://www.paubox.com/blog/what-is-hipaa/. Acesso em: 12/08/2021. Citado 2 vezes nas páginas 9 e 51.

PEREKALIN, A. *Você está protegido contra o WannaCry?* 2014. [Online] Disponível em: https://www.kaspersky.com.br/blog/stuxnet-as-origens/4391/. Acesso em: 18/08/2021. Citado na página 59.

PEREKALIN, A. *Você está protegido contra o WannaCry?* 2017. [Online] Disponível em: https://www.kaspersky.com.br/blog/wannacry-ransomware/7306/. Acesso em: 17/08/2021. Citado 2 vezes nas páginas 9 e 58.

RID, T.; BUCHANAN, B. Attributing cyber attacks. *Journal of Strategic Studies*, 2015. Taylor & Francis, v. 38, n. 1-2, p. 4–37, 2015. Citado na página 19.

SANTOS, A. H. O. *Principais Dispositivos de uma Rede de Computadores*. 2016. [Online] Disponível em: https://www.uniaogeek.com.br/principais-dispositivos-de-uma-rede-de-computadores-p1/. Acesso em: 17/07/2021. Citado na página 35.

SCHULTZ, F. *Segurança Cibernética: o que é e como ser um especialista no assunto*. 2020. [Online] Disponível em: https://milvus.com.br/seguranca-cibernetica-o-que-e/. Acesso em: 17/07/2021. Citado 3 vezes nas páginas 11, 40 e 43.

SCHULTZ, F. *Segurança no home office: trabalhe de casa sem riscos*. 2020. [Online] Disponível em: https://milvus.com.br/seguranca-home-office/. Acesso em: 17/07/2021. Citado na página 38.

SNOW, J. *Os ciberataques mais famosos dos últimos tempos*. 2018. [Online] Disponível em: https://www.kaspersky.com.br/blog/five-most-notorious-cyberattacks/11042/. Acesso em: 17/08/2021. Citado 6 vezes nas páginas 57, 59, 60, 61, 62 e 63.

SOUSA, L. B. Redes de computadores. *Dados Voz e Imagem*, 2009. 2009. Citado na página 23.

TANENBAUM, A. S. Redes de computadores. ed. *Campus-Tradução da Terceira Edição, Rio de Janeiro*, 2003. 2003. Citado na página 23.

VICENTIN, T.; LUCENA, A. *Vagas de emprego em home office crescem 309% em 2020*. 2021. [Online] Disponível em: https://olhardigital.com.br/2021/03/06/pro/vagas-de-emprego-em-home-office-crescem-309-em-2020/. Acesso em: 17/07/2021. Citado na página 37.

WOLOZIN, A. L. A ameaça invisível do terror cibernético. *Jornal do Brasil-Internacional*, 2009. A3, 2009. Citado na página 21.

ZETTER, K.; MODDERKOLK, H. *Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran*. 2019. [Online] Disponível em: https://media-mbst-pub-ue1.s3.amazonaws.com/creatr-uploaded-images/2019-08/1bef9bd0-cb54-11e9-afbb-41ba524c604d. Acesso em: 18/08/2021. Citado 2 vezes nas páginas 9 e 60.