Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Unidade Acadêmica de Engenharia Elétrica

Amanda Barbosa Silva

Estudo sobre Arquitetura de Segurança Cibernética em Rede 5G

Campina Grande, Paraíba, Brasil

Amanda Barbosa Silva

Estudo sobre Arquitetura de Segurança Cibernética em Rede 5G

Trabalho de Conclusão de Curso submetido à Coordenação do Curso de Engenharia Elétrica da Universidade Federal de Campina Grande – Campus de Campina Grande como parte dos requisitos necessários para a obtenção do grau de Bacharel em Ciências no Domínio da Engenharia Elétrica.

Área de Concentração: Telecomunicações

Edmar Candeia Gurjão, Dr.
Orientador

Campina Grande, Paraíba, Brasil
7 de abril de 2022

Amanda Barbosa Silva

Estudo sobre Arquitetura de Segurança Cibernética em Rede 5G

Trabalho de Conclusão de Curso submetido à Coordenação do Curso de Engenharia Elétrica da Universidade Federal de Campina Grande – Campus de Campina Grande como parte dos requisitos necessários para a obtenção do grau de Bacharel em Ciências no Domínio da Engenharia Elétrica.

Aprovado em _____ / _____ / _____.

Professor Dr. Leocarlos Bezerra da Silva Lima
Universidade Federal de Campina Grande - UFCG
Avaliador

Professor Dr. Edmar Candeia Gurjão
Universidade Federal de Campina Grande - UFCG
Orientador

Campina Grande, Paraíba, Brasil, em 7 de abril de 2022

Dedico este trabalho a minha avó Terezinha
Limeira de Sousa, *in memoriam*.

Agradecimentos

A Deus, por me dar a saúde e a força necessárias para ultrapassar os obstáculos encontrados durante essa jornada.

Aos meus pais, Masé e Amazan, por todo o esforço e dedicação a mim concedidos ao longo de toda a minha vida, além da educação e ensinamentos necessários à minha formação.

A minha irmã, Teresa, pelo apoio e incentivo nesse período.

A Bruno Dantas, pela parceria, estímulo e força durante esse processo.

A esta instituição, todo o seu corpo docente e de funcionários, que proporcionaram as condições necessárias para que eu alcançasse meus objetivos.

Ao meu orientador, Edmar Gurjão, por todo o tempo que dedicou a me ajudar durante o processo de realização deste trabalho.

Aos meus amigos, sempre presentes na minha vida, que ajudaram a tornar essa caminhada mais leve.

Enfim, a todos que fizeram parte, direta ou indiretamente, desta etapa da minha vida, o meu muito obrigada!

Resumo

Ao longo dos anos, observou-se um crescimento na troca de dados, acompanhando a evolução das Tecnologias da Informação e Comunicação e das gerações de tecnologias móveis, o que tornou a informação um ativo fundamental para a indústria e para a sociedade como um todo. Tendo em vista esses avanços, é primordial que se garanta a segurança da informação, seguindo os princípios que a norteiam. Nesse contexto, o presente trabalho faz um estudo sobre a Segurança Cibernética das redes 5G, apresentando os mecanismos de segurança projetados em sua arquitetura. Destaca-se que, apesar dos esforços para uma troca de informação segura, ainda há vulnerabilidades presentes na rede e propõe-se uma análise destas para que se possam avaliar e prevenir os riscos de futuros ataques.

Palavras-chaves: Tecnologias da Informação e Comunicação; Segurança Cibernética; Redes 5G.

Abstract

Over the years, there has been a considerable growth in data exchange, accompanying the evolution of Information and Communication Technologies, as well as the generations of mobile technologies, which made information a fundamental asset for the industry and for the society as a whole. Bearing in mind these advances, it is essential to ensure the security of information, following the principles which guide it. In this context, the present work accomplishes a study about 5G networks Cyber Security, presenting the mechanisms of security designed into its architecture. Highlighting that, despite of the efforts to a safe information exchange, there are still vulnerabilities present in the network. Therefore, it is proposed to carry out their analysis, in order to enable an evaluation and a prevention of the risks of future attacks.

Keywords: Information and Communication Technologies; Cyber Security; 5G networks.

Sumário

Lista de símbolos e abreviaturas

1G Primeira Geração de Tecnologia Móvel 8

2G Segunda Geração de Tecnologia Móvel 8

3G Terceira Geração de Tecnologia Móvel 8

3GPP *3rd Generation Partnership Project* 10

4G Quarta Geração de Tecnologia Móvel 8

5G Quinta Geração de Tecnologia Móvel 2

5G-NSA *Non-Standalone* 10

5G-SA *Standalone* 10

5GC 5G Core 10

AKA *Authentication and Key Agreement* – Autenticação e Acordo de Chave 14

AMF *Access and mobility Management Function* – Função de Gerenciamento de Acesso e Mobilidade 13

ANs *Access Networks* – Rede de Acesso 9

ARPF *Authentication credential Repository and Processing Function* – Função de Repositório e Processamento de Credenciais de Autenticação 13

AUSF *Authentication Server Function* – Função Servidor de Autenticação 13

DDoS *Distributed Denial of Service* – Negação de Serviço Distribuída 5

DoS *Denial of Service* – Negação de Serviço 5

EAP *Extensible Authentication Protocol* – Protocolo de Autenticação Extensível 15

EPC *Evolved Packet Core* 10

GSI/PR Gabinete de Segurança Institucional da Presidência da República 6

HSS *Home Subscriber Server* – Servidor de Assinante Doméstico 14

IA Inteligência Artificial 2

IMSI *International Mobile Subscriber Identity* – Identidade Internacional do Assinante Móvel 10

IoT *Internet of Things* – Internet das Coisas 2

IPUPS *Inter-PLMN User Plane Security* 12

ME *Mobile Equipment* – Equipamento Móvel 11

MITM *Man in the Middle* – Homem no meio 10

MNOs *Mobile Network Operators* – Operadoras de Redes Móveis 9

NFs *Network Functions* – Funções de Rede 12

NFV *Network Functions Virtualization* – Virtualização das Funções de Rede 16

O&M *Operations and Management* – Operações e Gerenciamento 14

PLMN *Public Land Mobile Network* – Rede Móvel Terreste Pública 12

SBA *Service-Based Architecture* – Arquitetura Baseada em Serviço 12

SDN *Software Defined Networks* – Redes Definidas por Software 16

SEAF *Security Anchor Function* – Função de Ancoragem de Segurança 13

SEPP *Security Edge Protection Proxy* 12

SIDF *Subscription Identifier De-concealing Function* – Função de Desocultação do Identificador de Assinatura 13

SNs *Serving Networks* – Rede Servidora 14

stc *Saudi Telecom Company* 9

SUCI *Subscriber Concealed Identifier* – Identificador Oculto do Assinante 13

SUPI *Subscriber Permanent Indentifier* – Identificador Permanente do Assinante 13

TICs Tecnologias da Informação e Comunicação 1

Tríade CIA *Confidentiality, Integrity and Availability* – Confidencialidade, Integridade e Disponibilidade 4

UDM *Unified Data Management* – Gerenciamento de Dados Unificado 13

UDR *Unified Data Repository* – Repositório de Dados Unificado 13

UE *User Equipment* – Equipamento do Usuário 11

UP *User Plane* – Plano de Usuário 12

USIM *Universal Subscriber Identity Module* – Módulo de Identidade do Assinante Universal 13

VNFs *Virtualized Network Functions* – Função de Rede Virtualizada 16

Lista de Figuras

Capítulo 1

Introdução

A Segurança Cibernética protege sistemas, computadores e servidores contra ameaças e ataques cibernéticos e deve ser implementada desde a segurança das redes físicas e dos aplicativos até a educação do usuário final [1].

É crescente a importância da Internet para instituições e pessoas que a utilizam para atividades profissionais, sociais e pessoais, mas, embora seja bastante útil, há indivíduos que atacam os dispositivos conectados à rede, desrespeitando a privacidade, tornando os serviços inoperantes ou executando outro tipo de ação. A área de segurança estuda os tipos de ameaças e como é possível defender os sistemas ou criar arquiteturas menos vulneráveis a esses riscos [2].

O mundo vem se tornando cada vez mais conectado e, nos últimos dois anos, com a pandemia de Covid-19, observou-se um crescimento digital que antecipou todas as estimativas de produção e troca de dados [1]. O avanço das Tecnologias da Informação e Comunicação (TICs) fez crescer, em larga escala, os ataques cibernéticos, que são considerados o desafio do século.

Existe uma grande variedade de ameaças e novos ataques ainda mais destrutivos que podem surgir a todo instante. Isso tornou a Segurança Cibernética imprescindível à manutenção e preservação das infraestruturas críticas de um país, tais como saúde, energia, defesa, transporte, telecomunicações, da própria informação, entre outras [3].

Segundo Fernando Siqueira [4], Arquiteto de Cibersegurança Sênior e Especialista Global em Segurança 5G da IMB Security América Latina, a chegada da quinta geração da tec-

nologia das redes celulares, o 5G, proporcionará capacidades como ultra velocidade, baixa latência e aumento na quantidade de dispositivos conectados por metro quadrado, resultando em novas experiências, aceleradas por tecnologias como a Inteligência Artificial (IA) e a Automação.

No entanto, a aceleração das tecnologias pelo 5G mudará a forma como se costuma abordar a segurança do sistema, já que, diferentemente do que acontece nas gerações anteriores, essa rede não se limitará a clientes individuais. Não se trata apenas de ter uma rede móvel com taxas mais altas ou funções mais robustas em *smartphones*. Uma maior conectividade de pessoas e atividades produtivas aumenta os riscos de falhas e, principalmente, as ameaças. Surge um elemento que demanda bastante atenção: o risco cibernético [4], [5].

A tecnologia 5G deverá transformar o que se conhece em relação ao oferecimento de serviços. A Internet das Coisas (IoT – do inglês, *Internet of Things*), veículos conectados, realidade aumentada e virtual, entre outros, demandarão que a rede e os dados possam ser acessados de forma veloz em qualquer local, assim, é preciso muito preparo, pois o 5G será também uma tecnologia revolucionária para a prática de crimes cibernéticos [4], [5].

1.1 Objetivos

Neste trabalho de conclusão de curso, objetiva-se entender como deve ser implementada a segurança da informação na rede 5G, analisando o que está normatizado e o que deve ser aperfeiçoado.

1.1.1 Objetivos específicos

Para se alcançar o objetivo geral, devem-se cumprir os seguintes objetivos específicos.

1. Estudar os sistemas 5G, observando sua arquitetura e padrões;
2. Analisar os aspectos de segurança propostos para as redes 5G.

1.2 Organização do Trabalho

No capítulo 1, foi feita uma breve introdução acerca dos assuntos abordados neste trabalho e foram apresentados os objetivos de sua realização, bem como a estrutura em que ele se apresenta.

No capítulo 2, serão abordados os conceitos de Segurança da Informação e os pilares que devem ser seguidos para que esta seja garantida.

No capítulo 3, será apresentada a evolução das tecnologias móveis, com foco na revolução trazida pela atual geração, o 5G. Também será feito um estudo acerca dos mecanismos de segurança projetados para o 5G e das vulnerabilidades ainda encontradas na rede.

No capítulo 4, serão ressaltadas as principais conclusões do trabalho, além de uma proposição para trabalhos futuros.

Capítulo 2

Segurança da Informação

A informação já pode ser considerada como principal bem de muitas instituições e, seja ela manipulada de forma eletrônica ou não, sua preservação se tornou obrigatória [6]. A Segurança Cibernética se torna mais importante à medida que o mundo se conecta cada vez mais.

Cherdantseva e Hilton (2013) [7] definem a segurança da informação como uma área multidisciplinar de estudo e profissional que busca o desenvolvimento e a aplicação de medidas para manter a informação e os sistemas de informações livres dos diversos tipos de ameaças.

Por mais que se empreendam esforços visando à segurança da sociedade e dos interesses do Estado, as vulnerabilidades e ameaças crescem na sociedade da informação. Sendo assim, é essencial garantir a confidencialidade, a integridade e a disponibilidade (tríade CIA – do inglês, *Confidentiality, Integrity and Availability*) da informação.

2.1 Traíde CIA

A tríade CIA representa os três pilares que conduzem a Segurança da Informação e que, juntos, asseguram sua confiabilidade.

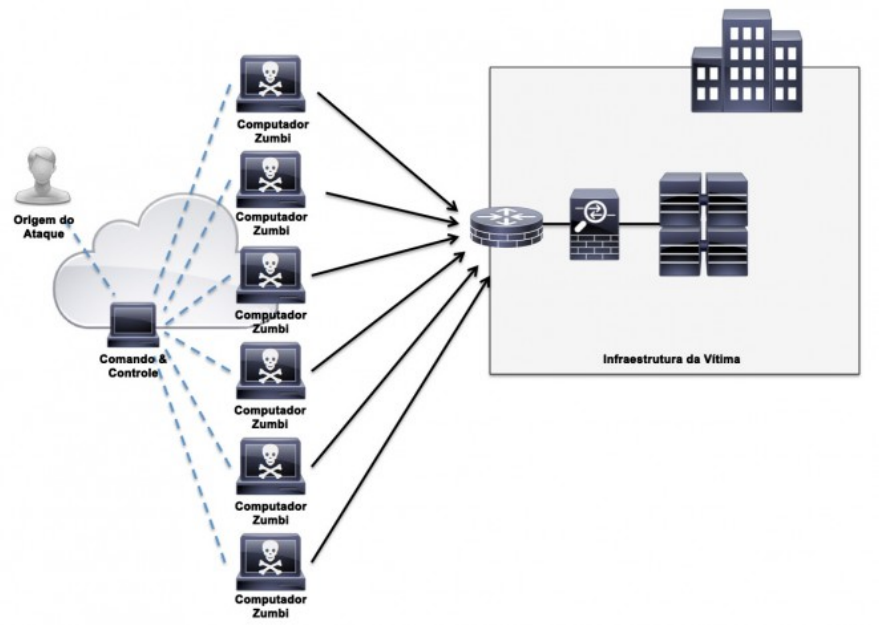
A **confidencialidade** deve garantir que sujeitos e sistemas não autorizados não tenham nenhum acesso à informação, esteja ela armazenada, em processamento ou em trânsito. Esse princípio pode ser violado de forma intencional, por meio de ataques, captura de tráfego,

entre outros, ou de forma não premeditada, por imperícia ou desatenção [6]. Os ataques à confidencialidade podem ser evitados com o uso de criptografia, prova de identidade e verificação em duas etapas [8].

A **integridade** refere-se à confiança que se pode ter sobre a informação e deve impedir que a informação armazenada, em processamento ou em trânsito seja modificada por sujeitos não autorizados ou que modificações não autorizadas sejam feitas por sujeitos autorizados. Uma informação que não sofreu alteração da transmissão à recepção é considerada íntegra [6]. Baumann, Cavin e Schmid (2006) [9] definem duas categorias de integridade: integridade de fonte e integridade de dados; a primeira garante que uma informação vem realmente do remetente correto, enquanto a segunda se refere à garantia de que a informação não foi manipulada em algum momento anterior ao acesso pelo destinatário pretendido. Modificação, falsificação, repetição e retração de dados são formas de ataque à integridade, que pode ser garantida com a utilização de funções hash ou soma de verificação [8]. Função hash é um algoritmo matemático que resume um dado grande em um pequeno dado de tamanho fixo; a verificação da integridade se dá pela comparação dos resumos obtidos do dado emitido e do dado recebido [10]. De forma semelhante, a soma de verificação compara dois conjuntos de dados e, caso não coincidam, conclui-se que os dados podem ter sido alterados ou corrompidos [11].

A **disponibilidade** é o aspecto da segurança da informação que garante que um sujeito ou sistema autorizado terá acesso a ela quando e onde for necessário, o que é possível com a manutenção dos equipamentos, atualização de softwares, reparos de hardwares e criação de backups [8]. A maior ameaça à disponibilidade são os ataques DoS (*Denial of Service*) e DDoS (*Distributed Denial of Service*) [6]. Segundo Kurose e Ross (2013) [2], o ataque de recusa de serviços (DoS) "torna uma rede, hospedeiro ou outra parte da infraestrutura inutilizável por usuários verdadeiros", mas, se a taxa de acesso do servidor for muito grande, é possível que uma fonte única de ataque não consiga causar danos ao servidor ou que um roteador identifique e bloqueie o tráfego do ataque antes de ele chegar ao servidor; o ataque DoS distribuído (DDoS) é gerado por múltiplas fontes, como mostrado na Figura 2.1.

Figura 2.1: Ataque de Recusa de Serviço Distribuído (DDoS)



Fonte: Hammer (2016) [12].

2.2 Segurança Cibernética

O espaço cibernético é o espaço não físico composto por canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação, em que as pessoas podem se comunicar de diferentes maneiras [3] e [13].

O Glossário de Segurança da Informação, elaborado pelo Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) [13], define Segurança Cibernética como:

> Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Alguns termos que dizem respeito à segurança da informação devem ser considerados [6]:

- Vulnerabilidade: refere-se às fragilidades das quais um atacante pode se aproveitar, comprometendo o funcionamento de um sistema ou serviço;

- Ameaça: representa o meio pelo qual uma vulnerabilidade pode ser explorada. A pessoa (*hacker*), o processo ou o evento natural que se utiliza de uma vulnerabilidade é um agente de ameaça;
- Risco: é a possibilidade de um agente de ameaça explorar uma vulnerabilidade;
- Proteção: forma de se prevenir o risco, como os antivírus, por exemplo;
- Incidente: quando um agente de ameaça consegue causar danos a um sistema por meio de uma vulnerabilidade. Neste caso, um (ou mais) dos princípios da tríade CIA foi(ram) violado(s).

Comumente, um agente de ameaça faz um reconhecimento inicial para coletar informações sobre vulnerabilidades dos dispositivos, sistemas e identidades dos alvos e, a partir daí, dispara ataque(s) que, em caso de sucesso, violará(ão) um (ou mais) princípio(s) da tríade CIA.

Capítulo 3

A Rede 5G

A quinta geração de tecnologia móvel, o 5G, traz mais do que uma maior largura de banda, ela proporciona características como maior velocidade, menor latência e mais dispositivos conectados simultaneamente.

A evolução das redes móveis promoveu mudanças importantes. A primeira geração (1G) tinha tecnologia analógica e ofertava somente serviço de voz; o serviço de mensagens de texto foi oferecido a partir da segunda geração (2G), que passou a ser digital e permitia acesso a e-mail. Com a terceira geração (3G), além dos serviços oferecidos no 2G, ocorreu a transição para a banda larga, sendo possível o acesso a aplicativos, redes sociais, sites, e o celulares passaram a contar com sistemas operacionais, ficando conhecidos como *smartphones*. A quarta geração (4G) surgiu com tecnologia de serviços semelhante à encontrada no 3G, porém visando a alcançar maiores taxas [14].

O 5G chega com o objetivo de modificar a arquitetura da rede de acesso, com a transição de um único serviço de acesso (conectividade de banda larga) para serviços mais robustos e computação de borda, em que os dados são processados e armazenados onde são gerados, diminuindo a necessidade de um data center remoto e proporcionando respostas mais rápidas. Essa geração deve oferecer suporte para aplicativos de missão crítica (como veículos autônomos, por exemplo) e IoT, possibilitando não somente o acesso à Internet por meio dos *smartphones*, mas também muitos dispositivos autônomos operando em conjunto [15].

No tocante à segurança, segundo a chefe de Comunicações e Relações com Analistas da 5G Americas, Vicki Livingston [16], o fato de o 5G suportar diversas redes de acesso (ANs

– do inglês, *Access Networks*), incluindo 2G, 3G, 4G e Wi-Fi, significa que todos os desafios de segurança podem ser herdados pela nova geração.

Livingston [16] ressalta ainda que o 5G possui a primeira arquitetura móvel projetada para suportar diversos casos de uso específico, cada um com exigências exclusivas de segurança cibernética. É imprescindível que os agentes de ameaça não consigam acessar dados, invadir dispositivos IoT ou realizar ataques DDoS em cenários de cidades inteligentes, que gerenciam recursos e ativos por meio de dados coletados por diferentes tipos de sensores eletrônicos.

Ainda nesse contexto, a Saudi Telecom Company (stc) e a Nokia [17] destacam que a variedade de casos de uso do 5G aumentará a complexidade da proteção da rede; as vulnerabilidades da rede podem causar consequências mais graves que nas gerações anteriores. A Tríade CIA precisa evoluir para atender a redes dinâmicas, múltiplos agentes envolvidos na prestação de serviços, grande diversidade de dispositivos (inclusive IoT), usuários e aplicativos. A grande quantidade de dispositivos conectados implica que a rede pode ser exposta a ataques maciços caso esses dispositivos sejam infectados por um invasor para realizar ataques DDoS, por exemplo.

Uma técnica bastante utilizada para reduzir os riscos de segurança em empresas é a segmentação de rede, que divide uma rede em diversas sub-redes menores e possibilita que cada uma delas tenha serviços e controles de segurança exclusivos. Com o advento do 5G, surge o conceito de fatiamento de rede, que oferece às operadoras móveis meios de segmentação que não eram possíveis nas gerações anteriores [16] e [18].

Alguns aspectos de segurança para as redes 5G já propostos no domínio de órgãos de padronização internacionais são [19]:

- confidencialidade e integridade dos dados, que têm sua proteção garantida por meio da criptografia, obrigatória para o tráfego de dados no 5G;
- autenticidade, com mecanismos de autenticação mútua reforçados, evitando que usuários se conectem a redes falsas e possibilitando a verificação da identidade de usuários conectados a redes autênticas;
- políticas de segurança, tendo em vista que muitos dos serviços das operadoras de redes móveis (MNOs – do inglês, *Mobile Network Operators*) poderão estar alocados, por

exemplo, em nuvens públicas, o que determina uma grande mudança em relação aos controles de segurança que as MNOs precisarão praticar;

- disponibilidade da rede, que garante o acesso aos recursos de rede sempre que solicitado por usuários legítimos, mantendo a eficácia da rede.

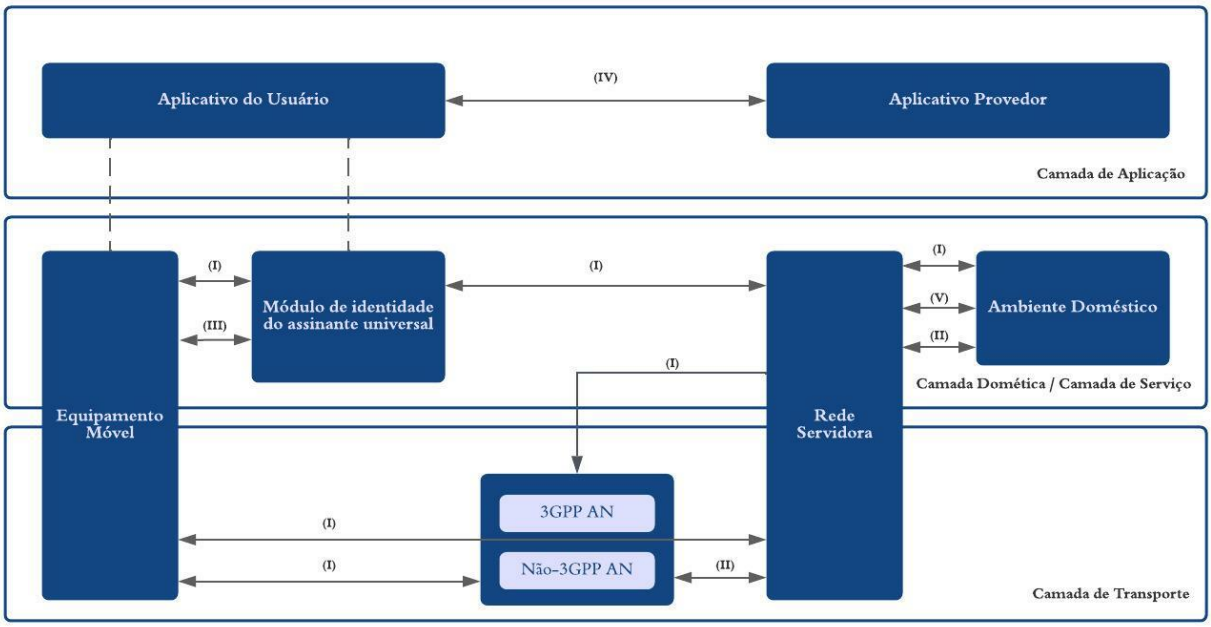
A *3rd Generation Partnership Project* (3GPP), entidade responsável pelas especificações para tecnologia móvel, trata da segurança conectando sete organizações de desenvolvimento de padrões de telecomunicações. O padrão 3GPP estabelece duas implementações diferentes de redes 5G que são importantes para a Segurança Cibernética: o 5G *Non-Standalone* (5G-NSA), em que o núcleo de rede EPC (*Evolved Packet Core*) é usado para conexões 4G e 5G, e o 5G herda todas as vulnerabilidades da geração anterior, como rastreamento da Identidade Internacional do Assinante Móvel (IMSI – do inglês, *International Mobile Subscriber Identity*) - número que identifica exclusivamente todos os usuários de uma rede celular -, ataque do homem no meio (MITM – do inglês, *Man in the Middle*) - em que dados trocados entre duas partes são manipulados por um atacante sem que as vítimas percebam - e problemas de integridade e confidencialidade quando o usuário está em *roaming* - conectado a uma rede em que é visitante, pertencente ou não à mesma operadora; e o 5G *Standalone* (5G-SA), em que as conexões 4G são feitas usando o EPC e as conexões 5G, no núcleo de rede conhecido como 5G Core (5GC), aprimorando os mecanismos de segurança e tratando essas vulnerabilidades, mas trazendo novos desafios às MNOs que operam as redes 5G-SA [16], [19], [20], [21] e [22].

3.1 Arquitetura de Segurança do 5G

As arquiteturas e protocolos de segurança e privacidade em sistemas 3GPP são responsabilidade do Grupo de Trabalho SA3, que publicou a especificação técnica 33.501 [23], na qual estabelece a arquitetura, recursos, mecanismos e procedimentos de segurança praticados no 5G.

A arquitetura de segurança 3GPP 5G engloba vários elementos e conceitos de arquitetura de segurança, mostrados na Figura 3.1.

Figura 3.1: Visão Geral da Arquitetura de Segurança



Fonte: 3GPP (adapatada) [23].

A Figura 3.1 ilustra os seguintes domínios de segurança:

I Segurança de Acesso à Rede: mecanismos de segurança que permitem que o equipamento do usuário (UE – do inglês, *User Equipment*) – qualquer dispositivo usado diretamente por um usuário final para se comunicar, como celular ou tablet – autentique e acesse a rede (incluindo acesso 3GPP e acesso não-3GPP), protegendo as interfaces de rádio;

II Segurança de Domínio de Rede: mecanismos de segurança que permitem que os nós da rede troquem dados de sinalização e dados do usuário com segurança;

III Segurança de Domínio do Usuário: mecanismos de segurança que tornam possível o acesso seguro do usuário ao equipamento móvel (ME – do inglês, *Mobile Equipment*);

IV Segurança de Domínio do Aplicativo: mecanismos de segurança que permitem que aplicativos de domínio do usuário e do provedor troquem mensagens com segurança (A especificação técnica 33.501 não aborda esse aspecto da segurança);

V Segurança de domínio da Arquitetura Baseada em Serviço (SBA — do inglês, *Service-Based Architecture*): mecanismos de segurança que permitem que as funções de rede (NFs — do inglês, *Network Functions*) da arquitetura SBA se comuniquem com segurança dentro do domínio de rede de serviço e com outros domínios de rede;

VI Visibilidade e configuração da segurança: mecanismos que permitem ao usuário ser informado se um recurso de segurança está em operação ou não (informação para o usuário, não mostrada na Figura 3.1).

É importante ressaltar que a Figura 3.1 apresenta uma visão geral da arquitetura de segurança projetada pelo 3GPP, porém os principais elementos de segurança da rede real não são mostrados, assim como a relação destes com outros componentes da arquitetura do 5G [24]. Os recursos de segurança inseridos na rede e especificados pelo 3GPP são descritos nas seções a seguir.

3.2 Perímetro de Rede

O perímetro de rede separa a rede interna e seus dispositivos de outras redes e da Internet. Além da rede interna, um usuário e os dispositivos conectados a ela acessam redes externas e a Internet, por isso, é necessário controlar ameaças que possam ultrapassar esse perímetro. Com a segurança de perímetro, é possível garantir que a rede interna não seja exposta a ataques que sejam originados fora dela [25].

Para a segurança de perímetro do 5GC, são introduzidos o *Security Edge Protection Proxy* (SEPP) e o *Inter-PLMN User Plane Security* (IPUPS), no perímetro da Rede Móvel Terrestre Pública (PLMN — do inglês, *Public Land Mobile Network*). O SEPP atua como um *gateway* de segurança nas interconexões entre as redes domésticas e as redes visitadas, protegendo a PMLN contra vulnerabilidades em processos de *roaming*, com conexões criptografadas e autenticadas. O SEPP também previne ataques *bidding down*, em que o UE e as entidades de rede acreditam, respectivamente, que o outro lado não suporta um recurso de segurança, quando na verdade ambos suportam [16] e [24]. O IPUPS tem a função de proteger as mensagens do plano de usuário (UP — do inglês, *User Plane*), associando sessões de UP com sessões de plano de controle e descartando sessões inválidas do UP se não

houver correspondência.

3.3 Segurança do 5GC

A proteção do 5GC se dá a partir das seguintes funções adicionadas à rede:

- Função Servidor de Autenticação (AUSF — do inglês, *Authentication Server Function*), que fornece (i) autenticação de UEs, por meio da Função de Gerenciamento de Acesso e Mobilidade (AMF — do inglês, *Access and mobility Management Function*), mediante as credenciais fornecidas pelo Gerenciamento de Dados Unificado (UDM — do inglês, *Unified Data Management*); (ii) criptografia para tráfego seguro de informações na atualização do UE; (iii) fornecimento de parâmetros de segurança em processos de *roaming* [26];

- Função de Repositório e Processamento de Credenciais de Autenticação (ARPF — do inglês, *Authentication credential Repository and Processing Function*), que conserva as credenciais de autenticação, espalhadas pelo Módulo de Identidade do Assinante Universal (USIM — do inglês, *Universal Subscriber Identity Module*) do lado do UE. As informações do assinante são armazenadas no repositório de dados unificado (UDR — do inglês, *Unified Data Repository*) e usadas pelo UDM para, por exemplo, gerar credenciais de autenticação, identificar os usuários, etc. [27];

- Função de Desocultação do Identificador de Assinatura (SIDF — do inglês, *Subscription Identifier De-concealing Function*), que decifra a identidade fornecida pelo Identificador Oculto do Assinante (SUCI — do inglês, *Subscriber Concealed Identifier*) para obter a IMSI, que, no 5G-SA é chamada de Identificador Permanente do Assinante (SUPI — do inglês, *Subscriber Permanent Indentifier*). O 5G exige criptografia de todo o tráfego de dados e, sempre que a IMSI precisa ser trocada pela rede, o SUCI é transmitido pelas interfaces de rádio. Apenas a SIDF tem acesso à chave privada e somente um elemento da rede doméstica pode solicitar a SIDF, o que resolve problemas de rastreamento de IMSI [19],[24] e [28];

- Função de Ancoragem de Segurança (SEAF — do inglês, *Security Anchor Function*),

que permite a autenticação do dispositivo que se move entre diferentes ANs ou redes servidoras (SNs – do inglês, *Serving Networks*) sem a necessidade de um método de autenticação completo – por exemplo, Autenticação e Acordo de Chave (AKA — do inglês, *Authentication and Key Agreement*), que permite autenticação mútua entre o UE e a rede. Dessa forma, reduz-se a carga de sinalização no Servidor de Assinante Doméstico (HSS — do inglês, *Home Subscriber Server*) da rede doméstica em diversos serviços de mobilidade [16].

3.4 Requisitos de Segurança da Estação Rádio Base (gNB)

As estações rádio base 5G nativas são chamadas de gNB e o 3GPP define alguns requisitos de como devem ser configuradas com segurança pelos sistemas de Operações e Gerenciamento (O&M — do inglês, *Operations and Management*). O não seguimento desses requisitos pode fazer com que as configurações da gNB e do software sejam modificadas por invasores. Tais requisitos incluem [24]:

- Confidencialidade, integridade e proteção contra partes não autorizadas da comunicação entre sistemas O&M e a gNB;
- Execução em ambiente seguro do processo de inicialização, para que suas partes sensíveis sejam protegidas;
- Suporte, pela gNB, do mecanismo de inscrição de certificados (que é especificado na TS 33.310 [1]). A utilização desse mecanismo é considerada opcional, pois fica a critério das operadoras.

3.5 Proteção da SBA

A arquitetura baseada em serviço do 5G é basicamente uma estrutura em que o plano de controle e os repositórios de dados da rede são implementados por NFs interconectadas.

[1] Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310 version 10.4.0 Release 10) <https://www.etsi.org/deliver/etsi_ts/133300_133399/133310/10.04.00_60/ts_133310v100400p.pdf>

Todas as NFs podem se comunicar entre si, o que requer proteção da confidencialidade e da integridade das mensagens trocadas e um mecanismo de autenticação e autorização robusto [24].

3.6 Estrutura de Autenticação

Para se garantir a segurança de qualquer rede, é imprescindível a autenticação mútua entre a rede móvel e seus usuários, assim como a utilização de chaves criptográficas para a proteção de dados do usuário. O 3GPP define os seguintes mecanismos de autenticação:

- Autenticação primária: autenticação mútua dos dispositivos móveis e da rede. É normalmente implementada no registro inicial, quando um dispositivo é ligado pela primeira vez, por exemplo. O 5G-AKA é o principal protocolo de autenticação, que oferece autenticação mútua entre UE e a rede. No 5GC, utilizando os serviços de UDM e ARPF, a AUSF realiza a autenticação da rede principal com o UE. Ao mesmo tempo, a SIDF recupera o SUPI do SUCI. A SEAF atua na SN e toma como base as informações recebidas da AUSF da rede doméstica. As redes 5G suportam o Protocolo de Autenticação Extensível (EAP – do inglês, *Extensible Authentication Protocol*), que oferece flexibilidade para autenticar redes de acesso 3GPP e não-3GPP [24] e [29];

- Autenticação secundária: é executada na configuração de conexões de UP, para navegar na Internet, por exemplo. Redes de transmissão de dados externas ao domínio da operadora móvel, como as Wi-Fi, são autenticadas pela autenticação secundária. Esta realiza a autenticação entre o UE e a rede externa e seu uso é opcional. Algumas operadoras a utilizam para permitir a autenticação independente de operadores de rede externa antes de o UE se conectar com a rede externa utilizando o EAP para solicitá-la [24] e [29].

3.7 Vulnerabilidades da Rede 5G

A rede 5G foi projetada com uma arquitetura de segurança bastante robusta para garantir sua confiabilidade, porém o sistema da nova geração não é inviolável. Os avanços

tecnológicos e as novas áreas de atuação do 5G permitem também o surgimento de novas vulnerabilidades que requerem atenção dos profissionais da área de segurança.

- Compatibilidade com as gerações anteriores [29]: como já mencionado, o 5G poderá operar no modo NSA, herdando, assim, as vulnerabilidades já presentes nas outras gerações;

- Fatiamento de rede: se, por um lado, o fatiamento de rede isola cada fatia, que tem seus próprios requisitos de segurança, o que, teoricamente, faz com que o comprometimento de uma dessas fatias não atinja as demais, por outro, isso torna a proteção da rede como um todo mais complexa, uma vez que será necessária a configuração de um número maior de redes, o que aumenta também a possibilidade de uma falha na segurança geral da rede [29].

- Redes Definidas por Software (SDN – do inglês, *Software Defined Networks*) e Virtualização das Funções de Rede (NFV – do inglês, *Network Functions Virtualization*): a tecnologia SDN permite que uma entidade lógica de software faça o controle externo de dados, tornando o controle de rede diretamente programável, sendo possível a introdução de novos serviços ou alterações à rede 5G [30], e as funções virtuais de rede (VNFs – do inglês, *Virtualized Network Functions*) são máquinas virtuais que implementam funcionalidades de rede em software em vez de em dispositivos físicos especializados, permitindo que as operadoras gerenciem e ampliem seus recursos por meio de aplicativos virtuais em locais em que antes se utilizavam estes dispositivos físicos [31], [32] e [33]. A transição para SDN/NFV provoca uma mudança na estrutura de rede e o surgimento de novos elementos, trazendo novos riscos: (i) redução da isolação, pois, com a NFV, os componentes podem se comunicar diretamente; (ii) compartilhamento de recursos, pois componentes não relacionados podem compartilhar os mesmos recursos de hardware e um ataque em qualquer função virtual pode atingir outras máquinas virtuais que operem no mesmo servidor físico; (iii) problemas de controle de acesso, pois pode não haver o controle correto da distribuição de credenciais e chaves, possibilitando o acesso de um invasor [29].

- Dispositivos IoT: a segurança desses dispositivos ainda é fraca, pois raramente eles

são atualizados e também não se costuma alterar as senhas de fábrica [29].

Buscando a mitigação dessas vulnerabilidades nas redes 5G, é fundamental que as operadoras trabalhem inicialmente na segurança das gerações anteriores. Devem-se analisar as informações que atravessam o perímetro de rede, para bloquear tráfego ilegítimo.

A arquitetura SBA, com SDN, NFV e fatiamento de rede, possibilita a rápida adequação das redes ao mercado, mas torna difícil o gerenciamento completo. Sendo assim, é importante que se realizem auditorias de segurança periodicamente para detecção de vulnerabilidades e correta configuração e aplicação das políticas de segurança.

Capítulo 4

Considerações Finais

O crescente avanço das TICs consolidou a informação como um dos recursos mais importantes para empresas e para a sociedade em geral, sendo assim, garantir a sua segurança é indispensável. A evolução tecnológica abre espaço também para maliciosos que visam a atacar as redes e obter vantagens sobre seus usuários legítimos. O surgimento de uma nova geração de tecnologia, com recursos inovadores, faz com que apareçam também novas ameaças cibernéticas.

Ao longo desse trabalho de conclusão de curso, estudaram-se as características da segurança da informação, bem como a revolução trazida pelo 5G, analisando-se os recursos de segurança propostos para a arquitetura desta geração. Porém, por mais que a segurança tenha sido levada bastante em consideração nas especificações do 5G, é possível observar que algumas vulnerabilidades ainda estão presentes na rede. É preciso avaliá-las e buscar meios de solucioná-las.

Propõe-se, para trabalho futuros, a geração, por meio de simulação, de cenários de ataques à rede 5G, a fim de se fazer uma análise mais concreta dos possíveis riscos ainda enfrentados pela atual geração, assim chegando a formas de mitigá-los.

Referências bibliográficas

1 INDÚSTIRA, Portal. *Cibersegurança: o que é, importância e como se qualificar*. 2020. <https://www.portaldaindustria.com.br/industria-de-a-z/ciberseguranca/#:~:text=Se%20antes%20da%20pandemia%20de,e%20troca%20de%20dados%20cibern%C3%A9ticos/>, acesso em 2022-03-15.

2 KUROSE, Keith W. Ross; tradução Daniel Vieira; revisão técnica Wagner Luiz Zucchi James F. *Redes de computadores e a internet uma abordagem top-down*. 6. ed. São Paulo - SP: Pearson Education do Brasil, 2013. ISBN 978-85-430-1443-2.

3 CANONGIA, Claudia; JUNIOR, Raphael Mandarino. Segurança cibernética: o desafio da nova sociedade da informação. *Parcerias Estratégicas*, PE, v. 14, n. 29, p. 21–46, Julho 2010. <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>.

4 SIQUEIRA, Fernanda. *Pensando em segurança cibernética para a era 5G*. 2021. <https://www.ibm.com/blogs/ibm-comunica/seguranca-cibernetica-5g/>, acesso em 2022-03-10.

5 E-VAL. *Quais são os desafios da tecnologia 5G para a proteção de dados da empresa?* 2021. <https://www.evaltec.com.br/quais-sao-os-desafios-da-tecnologia-5g-para-a-protecao-de-dados-da-empresa/#:~:text=N%C3%A3o%20se%20trata%20apenas%20de,grande%20diversidade%20de%20novos%20servi%C3%A7os>, acesso em 2022-03-11.

6 LIMA, de Almeida André. *VoIP: Segurança da Informação*. 2021. <https://www.teleco.com.br/tutoriais/tutorialvoipsip/pagina_3.asp>, acesso em 2022-02-08.

7 CHERDANTSEVA, Yulia; HILTON, Jeremy. A reference model of information assurance & security. *2013 International Conference on Availability, Reliability and Security*, IEEE, v. 2, n. 3, p. 546–555, Setembro 2013. <https://ieeexplore.ieee.org/document/6657288>.

8 ACADEMY, Cisco Networking. *Cybersecurity*. 2022. <https://skillsforall.com/career-path/cybersecurity>, acesso em 2022-28-01.

9 BAUMANN, Rainer; CAVIN, Stéphane; SCHMID, Stefan. Voice over ip-security and spit. *Swiss Army, FU Br*, Citeseer, v. 41, n. 1, p. 1–34, Janeiro 2006. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.6329&rep=rep1&type=pdf>.

10 PISA, Pedro. *O que é hash?* 2012. <https://www.techtudo.com.br/noticias/2012/07/o-que-e-hash.ghtml>, acesso em 2022-03-20.

11 TECHLIB. *Definição de soma de verificação*. 2020. <https://techlib.wiki/definition/checksum.html#:~:text=Uma%20soma%20de%20verifica%C3%A7%C3%A3o%20%C3%A9,garantir%20que%20eles%20sejam%20iguais.>, acesso em 2022-03-20.

12 HAMMER, Wolfgang. *Was ist eine DDoS Attacke?* 2016. <https://www.a1blog.net/2016/02/03/was-ist-eine-ddos-attacke/>, acesso em 2022-03-29.

13 FEDERAL, Governo. *Gabinete de Segurança Institucional*. 2022. <https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao->, acesso em 2022-03-21.

14 MOTA, Vitor Luiz Gomes; CARVALHO, Roberta; CORREA, Carina; RENNA, Roberto Brauer Di; MAGRI, Vanessa; FERREIRA, Tadeu; CASTELLANOS, Pedro; MATOS, Leni. Evolução da tecnologia de telefonia móvel e estudo e caracterização de um sistema móvel 5g de quinta geração. *Engevista*, Engevista, v. 21, n. 1, p. 154–175, Fevereiro 2019. <https://periodicos.uff.br/engevista/article/view/27028/16398>.

15 SYSTEMSAPPROACH. *5G Mobile Networks: A systems Approach*. 2022. <https://5g.systemsapproach.org/intro.html>, acesso em 2022-02-20.

16 LIVINGSTON, Vicki. *What's the answer for 5G security?* 2019. <https://www.techtarget.com/searchsecurity/opinion/Whats-the-answer-for-5G-security>, acesso em 2022-02-24.

17 NOKIA. *5G Security Risks and Mitigation Measures*. 2021. <https://www.nokia.com/sites/default/files/2021-05/Whitepaper-5G-security-Nokia-STC-March-31-2021.pdf>, acesso em 2022-03-29.

18 VMWARE. *Por que a segmentação de rede: benefícios da segmentação de rede*. 2018. <https://www.vmware.com/br/topics/glossary/content/network-segmentation.html#:~:text=Segmenta%C3%A7%C3%A3o%20de%20rede%20%C3%A9%20uma,exclusivos%20a%20cada%20sub%2Drede>, acesso em 2022-01-27.

19 INATEL. *OperRan a Conexão do futuro*. 2020. <https://inatel.br/cxsc/downloads-docman/geral/18-white-paper-openran>, acesso em 2022-02-11.

20 WIKIPEDIA. *International mobile subscriber identity*. 2022. <https://pt.wikipedia.org/wiki/International_mobile_subscriber_identity>, acesso em 2022-03-22.

21 WIKIPEDIA. *Ataque man-in-the-middle*. 2022. <>, acesso em 2022-03-22.

22 WIKIPEDIA. *Itinerância*. 2022. <>, acesso em 2022-03-2.

23 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.9.0 Release 16). Etsi. Provença-Alpes-Côte d'Azur: 3GPP, 2022. ISBN ETSI TS 133 501.

24 ENISA. *Security in 5G Specifications - Controls in 3GPP*. 2021. <https://www.enisa.europa.eu/publications/security-in-5g-specifications>, acesso em 2022-03-21.

25 ALLEASY. *Segurança de Perímetro: Entenda como é e como fazer*. 2018. <https://www.alleasy.com.br/2018/05/30/seguranca-de-perimetro-como-e-como-fazer/>, acesso em 2022-03-23.

26 SILVA, JPL; NERY, SWL; SILVA, R; OLIVEIRA-JR, AC; CARDOSO, KV; BOTH, CB. Entendendo o núcleo 5g na prática, através de uma implementaçao de código aberto. *XXXVIII Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*, SBRT, v. 1, n. cs.NI, p. 3460572, Novembro 2020. <https://www.researchgate.net/publication/344860721_Entendendo_o_nucleo_5G_na_pratica_atraves_de_uma_implementacao_de_codigo_aberto>.

27 PRASAD, Anand R; ARUMUGAM, Sivabalan; SHEEBA, B; ZUGENMAIER, Alf. 3gpp 5g security. *Journal of ICT Standardization*, River Publishers, v. 6, n. 1, p. 137–158, Abril 2018. <https://journals.riverpublishers.com/index.php/JICTS/article/view/6449/5205>.

28 SILVA, Sergio Henrique; MIERS, Charles Christian. Análise de mecanismos de autenticação de dispositivos em redes móveis 5g para internet industrial (iiot) categorizada por mmtc, embb e urllc. *Anais da XIX Escola Regional de Redes de Computadores*, SBC, v. 1, n. 19, p. 91–96, Janeiro 2021. <https://doi.org/10.5753/errc.2021.18548>.

29 5G Security Issues. positive-tech.com. São Paulo: 3GPP, 2022. ISBN <https://www.gsma.com/membership/wp-content/uploads/2019/11/5G-Research_A4.pdf>.

30 HUSSAIN, Alifya. *5G SDN and NFV*. 2020. <https://medium.com/@alifyahussain/5g-sdn-and-nfv-e411dbe927b1>, acesso em 2022-03-25.

31 FUTURECOM. *O que é Network Function Virtualization? Como NFV se relaciona com SDN?* 2019. <https://digital.futurecom.com.br/especialistas/o-que-e-network-function-virtualization-como-nfv-se-relaciona-com-sdn>, acesso em 2022-03-25.

32 ERICSSON. *Network Functions Virtualization (NFV)*. 2020. <https://www.ericsson.com/en/nfv>, acesso em 2022-03-25.

33 SOUSA, Nathan F Saraiva de; PEREZ, Danny A Lachos; ROSA, Raphael V; SANTOS, Mateus AS; ROTHENBERG, Christian Esteve. Network service orchestration: A survey. *Computer Communications*, Elsevier, v. 142, n. 143, p. 69–94, Junho 2019. <https://doi.org/10.1016/j.comcom.2019.04.008>.