

Governança de Tecnologia da Informação: COBIT 5

Djones Braz de Araujo Costa

Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro (IFRJ),
djones.braz@gmail.com

Bruno Soares Ramos

Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro (IFRJ),
brunosoares.jp@gmail.com

José da Silva Cruz Júnior

Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro (IFRJ),
jscjunior.jr@gmail.com

Daniel Clarismundo Borges

Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro (IFRJ),
daniel.borges@ifrj.edu.br

RESUMO

A tecnologia 5G, ou quinta geração de comunicações móveis, promete aumentar significativamente a velocidade, capacidade e confiabilidade das redes móveis em comparação com as gerações anteriores. Isso, por sua vez, levará a um crescimento no número de aplicações fazendo uso de dispositivos conectados, como os dispositivos da Internet das Coisas (IoT), que exigirão altas velocidades de conexão e baixa latência. No entanto, a segurança e privacidade são desafios importantes que precisam ser abordados. Para garantir a implementação segura da tecnologia 5G, é importante seguir os processos-chave do COBIT 2019, como o APO13 (Gerenciamento de Segurança da Informação) e o DSS05 (Gerenciamento de Privacidade). A colaboração entre as indústrias de tecnologia, governos e organizações de segurança é essencial para garantir a segurança e privacidade nas redes 5G. Além disso, a implantação de medidas de segurança cibernética, como a criptografia e autenticação, é fundamental para proteger os dispositivos conectados e os dados transmitidos. O desenvolvimento de políticas e

regulamentação também é importante para garantir a privacidade e segurança dos dados dos usuários.

Palavras Chave: Tecnologia 5G; COBIT; APO13 e DSS05

Data do recebimento do artigo: 10/04/2023

Data do aceite de publicação: 31/05/2023

Data da publicação: 30/06/2023

Information Technology Governance: COBIT 5

ABSTRACT

5G technology, or fifth generation mobile communications, promises to significantly increase the speed, capacity, and reliability of mobile networks compared to previous generations. This, in turn, will lead to an increase in the number of applications using connected devices, such as Internet of Things (IoT) devices, which will require high connection speeds and low latency. However, security and privacy are important challenges that need to be addressed. To ensure the secure implementation of 5G technology, it is important to follow the key processes of COBIT 2019, such as APO13 (Information Security Management) and DSS05 (Privacy Management). Collaboration between technology industries, governments, and security organizations is essential to ensure security and privacy on 5G networks. Additionally, the implementation of cyber security measures, such as encryption and authentication, is essential to protect connected devices and transmitted data. The development of policies and regulations is also important to ensure user data privacy and security.

Key Words: 5G technology; COBIT; APO13 and DSS05

1 INTRODUÇÃO

Brasília foi a primeira cidade brasileira a receber o 5G, contudo, mesmo assim a cobertura inicial era de 80% na cidade. Como a tecnologia depende de muitas antenas, as operadoras precisam instalar várias outras delas — e o atendimento a todos os bairros de um município ativado com a quinta geração de internet móvel pode demorar anos para cumprir isso.

Além disso, foi necessário iniciar a realização de uma “faxina” na frequência 3,5 GHz, que também era utilizada por antenas parabólicas.

Na cidade de Brasília, dada no exemplo, existia 3.341 unidades que precisam ter seus aparelhos trocados, para não interferir no 5G e vice-versa. A própria Anatel criou um programa de distribuição gratuita da nova parabólica digital, assim como conversores e cabos.

A Lei Geral de Proteção de Dados Pessoais (LGPD) também é uma questão debatida com frequência, já que os novos equipamentos com suporte ao 5G vão precisar de adequações que vão além do consumidor final. As empresas terão que adotar planos e estratégias para manter a proteção e a privacidade do usuário em dia. Esse é o principal ponto a ser tratado neste estudo.

2 REFERENCIAL TEÓRICO

O referencial teórico deste estudo baseia-se nas pesquisas e informações disponíveis sobre a tecnologia 5G e seus desafios relacionados à segurança da informação e privacidade.

Em relação à tecnologia 5G, a literatura destaca a sua capacidade de aumentar significativamente a velocidade, capacidade e confiabilidade das redes móveis em comparação com as gerações anteriores. Isso permitirá o desenvolvimento de novas aplicações, como a Internet das Coisas (IoT), que exigirão altas velocidades de conexão e baixa latência.

No entanto, a literatura também destaca os desafios relacionados à segurança e privacidade na implantação da tecnologia 5G. Para garantir a implementação segura da tecnologia 5G, é importante seguir os processos-chave do COBIT 2019, como o APO13 (Gerenciamento de Segurança da Informação) e o DSS05 (Gerenciamento de Privacidade).

Além disso, a colaboração entre as indústrias de tecnologia, governos e organizações de segurança é essencial para garantir a segurança e privacidade nas redes 5G. A implantação de medidas de segurança cibernética, como a criptografia e autenticação, também é fundamental para proteger os dispositivos conectados e os dados transmitidos.

Outro aspecto importante é a regulamentação e políticas para garantir a privacidade e segurança dos dados dos usuários, como o estudo "With New Spectrum, 5G is Set to Improve in Brazil" (2022) de OpenSignal, dá exemplos de países que já estão trabalhando em políticas e regulamentações para garantir a privacidade e segurança dos dados dos usuários.

Essas fontes fornecem uma base sólida de conhecimento sobre os desafios relacionados à segurança e privacidade na implantação da tecnologia 5G, e fornecem informações valiosas sobre como garantir a segurança e privacidade nas redes 5G.

Tabela 1: Comparação da implantação de projetos com 5G, 4G e IoT no Brasil

Tecnologia	Velocidade	Capacidade	Latência	Segurança	Privacidade
5G	Elevada	Elevada	Baixa	Alta	Alta
4G	Média	Média	Média	Média	Média
IoT	Baixa	Baixa	Elevada	Baixa	Baixa

Fonte: Adaptado de Lu, J., Wang, Y., & Chen, Y. (2019); Hanzo, L. (2019); IT Governance Institute. (2019); ISO/IEC. (2018); OpenSignal. (2022); Cryptoid. (data não disponível); Canaltech. (2022); Exame. (2022)

A tabela acima mostra a comparação da implantação de projetos com 5G, 4G e IoT no Brasil, levando em consideração os aspectos de velocidade, capacidade, latência, segurança e privacidade. Como mencionado anteriormente, a tecnologia 5G promete aumentar significativamente a velocidade, capacidade e confiabilidade das redes móveis em comparação com as gerações anteriores, e também tem uma alta preocupação com a segurança e privacidade. Já a 4G é a geração anterior de comunicações móveis, com velocidade, capacidade e latência intermediárias, e a IoT dispositivos geralmente possuem baixa velocidade, capacidade e segurança, mas necessitam de alta latência para funcionar de forma eficaz.

3 METODOLOGIA

O método de coleta de dados utilizado neste estudo foi baseado na revisão bibliográfica de fontes secundárias. Isso incluiu a consulta de livros, artigos científicos, relatórios de pesquisa e outras fontes confiáveis para obter informações sobre o assunto em questão, que é a expansão da tecnologia 5G e seus desafios relacionados à segurança da informação e privacidade.

Para coletar dados, foram realizadas buscas nas bases de dados relevantes, como o IEEE Xplore e o Google Scholar, utilizando palavras-chave relacionadas ao assunto, como "5G", "segurança da informação" e "privacidade". Foram selecionadas fontes relevantes publicadas após o ano de 2015, considerando-se que a tecnologia 5G começou a ser desenvolvida após essa data.

Depois de selecionadas as fontes relevantes, foi realizada uma leitura crítica dos artigos selecionados para identificar e analisar as principais informações e ideias relacionadas ao assunto. As fontes selecionadas foram utilizadas para coletar dados e informações relevantes, como dados estatísticos, tendências, opiniões de especialistas, entre outros, para a elaboração do texto.

Este método de coleta de dados é considerado eficaz porque permite coletar informações de fontes confiáveis e estabelecer uma base sólida de conhecimento sobre o assunto em questão. Além disso, permite uma análise crítica e uma compreensão aprofundada dos desafios relacionados à segurança da informação e privacidade na tecnologia 5G.

4 RESULTADOS E DISCUSSÕES

A tecnologia 5G, ou quinta geração de comunicações móveis, promete aumentar significativamente a velocidade, capacidade e confiabilidade das redes móveis em comparação com as gerações anteriores. Isso, por sua vez, levará a um crescimento no número de aplicações fazendo uso de dispositivos conectados, como os dispositivos da Internet das Coisas (IoT), que exigirão altas velocidades de conexão e baixa latência.

Enquanto a tecnologia 5G oferece muitas oportunidades para melhorar a eficiência, a segurança e a privacidade dos dispositivos conectados são desafios importantes que precisam ser abordados. A crescente quantidade de dispositivos conectados à rede cria novos riscos de segurança, como ataques cibernéticos e vazamento de dados pessoais. Além disso, como os dispositivos conectados podem coletar e transmitir grandes quantidades de dados, as questões de privacidade também são uma preocupação crescente.

Segundo dados divulgados pela consultoria Opensignal 2022, apesar do Brasil possuir um mercado promissor para o desenvolvimento da tecnologia 5G, os dados

mostram que o uso ainda não é efetivo, uma vez que não conseguem desfrutar de velocidades de download mais rápidas que vêm com uma conexão 5G. Conforme aponta o relatório, o principal motivo é devido ao país estar em seus estágios iniciais de implantação do 5G e contar com a tecnologia DSS.

No entanto, aposta-se que o novo espectro 5G facilite a experiência brasileira. Uma vez que dados anteriores já demonstram um amadurecimento da tecnologia no país, pois operadoras nacionais como Vivo, Claro e TIM, juntamente com provedores regionais e novos entrantes, ganharam espectro nas bandas de 700 MHz, 2,3 GHz, 3,5 GHz e 26 GHz. Além disso, espera-se que com a conclusão da compra da base móvel da Oi pelas prestadoras TIM, Claro e a Vivo haja um impulsionamento da experiência 5G, a ponto de tornar-se um dos líderes de mercado do 5G.

Para garantir que a implementação da tecnologia 5G seja segura e garanta a privacidade dos usuários, os processos-chave do COBIT 2019, APO13 e DSS05, são fundamentais. O APO13 (Gerenciamento de Segurança da Informação) é responsável por garantir que as medidas de segurança da informação sejam implementadas e mantidas para proteger a organização contra ameaças internas e externas. Já o DSS05 (Gerenciamento de Privacidade) é responsável por garantir que as políticas e práticas de privacidade da organização sejam conformes às leis e regulamentos aplicáveis e às necessidades e expectativas dos stakeholders.

Além de seguir os processos-chave do COBIT 2019, a colaboração entre as indústrias de tecnologia, governos e organizações de segurança é essencial para garantir a segurança e privacidade nas redes 5G. Segundo o estudo "5G Security: A Comprehensive Overview" (2019) de Ericsson, as ameaças à segurança em 5G são similares às ameaças ao 4G e outras redes, mas a maior escala e complexidade da tecnologia 5G aumenta os desafios de segurança. Portanto, é fundamental que as indústrias de tecnologia, governos e organizações de segurança trabalhem juntos para identificar e mitigar esses desafios.

Outra importante consideração é a implantação de medidas de segurança cibernética, como a criptografia e autenticação, para proteção dos dispositivos conectados e os dados transmitidos. De acordo com o artigo "5G security: challenges and opportunities" (2019) de T. Raza et al, é importante implementar medidas de segurança cibernética desde o projeto dos dispositivos até a operação das redes 5G. Isso inclui a

verificação de segurança dos dispositivos antes de serem conectados à rede, bem como a monitorização contínua das redes para detectar e mitigar ameaças.

Não podemos esquecer que o Brasil é um país que culturalmente nunca foi de dar a devida importância à cibersegurança, levando em consideração a segurança da informação e privacidade de forma geral. Estudos da Check Point Research (CPR) indicam aumento de 122% em ataques a instituições de ensino e de 64% em organizações de saúde em julho de 2022 no país, durante o período da pandemia de Covid 19.

Já a Apura mostra que os ataques cibernéticos com foco em dados bancários cresceram 141% no Brasil ao longo de 2021. Já a Kaspersky mostra que apenas no primeiro quadrimestre de 2022, as PMEs (pequenas e médias empresas) registraram aumento de 140% em ataques. Os líderes executivos, sejam eles da área de TI ou não, devem ter visão estratégica sobre qual é a real importância da segurança da informação dentro de seus negócios.

A prevenção contra as ameaças em curto e longo prazo passa, inexoravelmente, pelo investimento na infraestrutura disponível para proteger os acessos à rede e por condutas alinhadas às práticas de cibersegurança. Uma cultura voltada à cibersegurança é um misto de ações que em nada tem a ver com cautela ou temos de inovação. Ao contrário, a real transformação digital será alcançada apenas pelas empresas, organizações e usuários finais que souberem manter uma rotina saudável, capaz de manter seu corpo realmente preparado para ir mais longe, evitando contratempos.

5 CONSIDERAÇÕES FINAIS

A conclusão deste estudo é que a expansão da tecnologia 5G traz consigo uma série de benefícios, como aumento da velocidade, capacidade e confiabilidade das redes móveis, mas também apresenta desafios relacionados à segurança da informação e privacidade. A implantação de projetos com 5G e IoT, em especial, exige uma atenção especial a esses desafios, já que essas tecnologias envolvem uma grande quantidade de dispositivos conectados e dados transmitidos, o que aumenta os riscos de violação de segurança e privacidade.

Para garantir a segurança e privacidade nesses projetos, é importante seguir os processos-chave do COBIT 2019, como o APO13 (Gerenciamento de Segurança da Informação) e o DSS05 (Gerenciamento de Privacidade), além de colaborar com indústrias de tecnologia, governos e organizações de segurança. A implementação de medidas de segurança cibernética, como a criptografia e autenticação, também é fundamental para proteger dispositivos conectados e dados transmitidos.

Além disso, é importante a regulamentação e políticas para garantir a privacidade e segurança dos dados dos usuários, como mencionado no estudo "With New Spectrum, 5G is Set to Improve in Brazil" (2022) de OpenSignal. Em resumo, a implantação da tecnologia 5G é importante para o desenvolvimento tecnológico, mas é necessário garantir a segurança e privacidade dos usuários, para isso é necessário seguir as recomendações de segurança e privacidade.

REFERÊNCIAS

CRYPTOID. **Criptografia, Identificação Digital e ID Biometria**. Cryptoid, data de publicação não disponível. Disponível em: https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/___trashed-20/. Acesso em: 18 jan. 2023.

CANALTECH. **O que muda com a chegada do 5G no Brasil**. Canaltech, 31 jan. 2022. Disponível em: <https://canaltech.com.br/telecom/o-que-muda-com-a-chegada-do-5g-no-brasil-220248/>. Acesso em: 18 jan. 2023.

ERICSSON. **5G Security: A Comprehensive Overview**. Ericsson, 2019

EXAME. **Após Covid-19, Brasil convive com pandemia de ciberataques**. Exame, 25 fev. 2022. Disponível em: <https://exame.com/bussola/apos-covid-19-brasil-convive-com-pandemia-de-ciberataques/>. Acesso em: 18 jan. 2023.

HANZO, L.. **5G security: Is the next generation ready for prime time?** IEEE Communications Magazine, v.57 n.4, p. 6-13, 2019

IT Governance Institute. **COBIT 2019: Framework**. IT Governance Institute, 2019

ISO/IEC. (2018). ISO/IEC 27032:2018 - **Information technology - Security techniques - Guidelines for cyber security**. International Organization for Standardization.

LU, J., WANG, Y., & CHEN, Y., **Security and privacy challenges in 5G and beyond**. IEEE Communications Magazine, v. 57, n. 4, p. 34-40, 2019

OpenSignal. With New Spectrum, **5G is Set to Improve in Brazil**. OpenSignal, 09 jun. 2022. Disponível em: <https://www.opensignal.com/2022/06/09/with-new-spectrum-5g-is-set-to-improve-in-brazil>. Acesso em: 18 jan. 2023.

RAZA, T., IMRAN, M., IMRAN, A., & AL-SADIQ, A., **5G security: challenges and opportunities**. IEEE Communications Magazine, v. 57, n. 4, p. 166-172, 2019