INFORME Nº 6/2020/ORCN/SOR

**PROCESSO Nº 53500.026122/2019-70**

**INTERESSADO: GERÊNCIA DE CERTIFICAÇÃO E NUMERAÇÃO, SUPERINTENDÊNCIA DE OUTOI RECURSOS À PRESTAÇÃO**

## 1. ASSUNTO

1.1. Proposta de Consulta Pública para aprovação de requisitos mínimos de segurança cibernética para equipamentos terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações, visando minimizar vulnerabilidades por meio de atualizações de *software/firmware* ou por meio de recomendações em configurações e em seus mecanismos de gerenciamento remoto.

## 2. REFERÊNCIAS

2.1. Lei Geral de Telecomunicações - LGT - Lei n.º 9.472, de 16 de julho de 1997;

2.2. Lei n.º 13.848, de 25 de junho de 2019;

2.3. Regulamento para Avaliação da Conformidade e Homologação de Produtos para Telecomunicações, aprovado pela Resolução n.º 715, de 23 de outubro de 2019;

2.4. Regimento Interno da Anatel, aprovado pela Resolução n.º 612, de 29 de abril de 2013;

2.5. Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética; e

2.6. Processo SEI n.º 53500.026122/2019-70.

## 3. AMPARO LEGAL DAS NORMAS TÉCNICAS

3.1. A presente proposta baseia-se no art. 19, Inciso XII, da Lei Geral de Telecomunicações, que estabelece a competência da Agência para expedir normas e padrões a serem cumpridos pelas prestadoras de serviços de telecomunicações quanto aos equipamentos que utilizarem.

3.2. Ademais, o desenvolvimento de normas técnicas respalda-se no Regulamento anexo à Resolução n.º 715/2019, o qual estabelece princípios gerais dos processos de avaliação da conformidade e homologação de produtos para telecomunicações, entre os quais: i) assegurar que os fornecedores dos produtos atendam a requisitos mínimos de qualidade para seus produtos; ii) assegurar o atendimento aos requisitos de segurança e de não agressão ao ambiente; e iii) assegurar que os produtos para telecomunicações comercializados no País, em particular aqueles ofertados pelo comércio diretamente ao público, possuam um padrão mínimo de qualidade e adequação aos serviços a que se destinam.

3.3. O instituto dos requisitos técnicos está previsto no art. 22 do Regulamento para Avaliação da Conformidade e Homologação de Produtos para Telecomunicações – Resolução n.º 715/2019:

> Art. 22. Os Procedimentos Operacionais e os Requisitos Técnicos são normas técnicas complementares, destinadas a operacionalizar a avaliação da conformidade de produtos para telecomunicações, na forma deste Regulamento.
>
> § 1º A atuação dos Organismos de Certificação Designados, dos Laboratórios de Ensaio e dos Requerentes à avaliação da conformidade de produtos para telecomunicações é vinculada às normas técnicas complementares previstas no **caput**.

§ 2º Os Procedimentos Operacionais e os Requisitos Técnicos são expedidos pela Superintendência competente, mediante Ato.

§ 3º A aprovação de Procedimentos Operacionais e Requisitos Técnicos deve ser precedida de Consulta Pública.

3.4. Havendo a necessidade de se avaliar a conformidade de produto de telecomunicações a ser comercializado no mercado brasileiro, a Resolução n.º 715/2019 estabeleceu a obrigatoriedade de edição de requisitos técnicos ou procedimentos operacionais.

## 4. AMPARO LEGAL DAS CONSULTAS PÚBLICAS

4.1. A Consulta Pública está fundamentada no Art. 59 do Regimento Interno da Anatel (Ref. 2.4):

*Art. 59. A Consulta Pública tem por finalidade submeter minuta de ato normativo, documento ou matéria de interesse relevante, a críticas e sugestões do público em geral.*

*§1º A Consulta Pública pode ser realizada pelo Conselho Diretor ou* ***pelos Superintendentes, nas matérias de suas competências.***

§ 2º A Consulta Pública será formalizada por publicação no Diário Oficial da União **com prazo não inferior a 10 (dez) dias**, devendo as críticas e as sugestões serem apresentadas conforme dispuser o respectivo instrumento deliberativo.

***Grifo nosso.***

4.2. A Lei n.º 13.848 (Ref. 2.2), de 25 de junho de 2019, dispõe sobre a duração mínima das consultas públicas, nos seguintes termos.

*§ 2º Ressalvada a exigência de prazo diferente em legislação específica, acordo ou tratado internacional, o período de consulta pública terá início após a publicação do respectivo despacho ou aviso de abertura no Diário Oficial da União e no sítio da agência na internet, e terá* ***duração mínima de 45 (quarenta e cinco) dias, ressalvado caso excepcional de urgência e relevância, devidamente motivado****.*

***Grifo nosso.***

4.3. Adicionalmente, o Tratado de Barreiras Técnicas (TBT) da Organização Mundial do Comércio (OMC) recomenda, na mesma linha, um período mínimo de 60 (sessenta) dias para consultas públicas.

*Before adopting a standard, the standardizing body shall allow a period of* ***at least 60 days*** *for the submission of comments on the draft standard by interested parties within the territory of a Member of the WTO. This period may, however, be shortened in cases where urgent problems of safety, health or environment arise or threaten to arise. No later than at the start of the comment period, the standardizing body shall publish a notice announcing the period for commenting in the publication referred to in paragraph J. Such notification shall include, as far as practicable, whether the draft standard deviates from relevant international standards.*

***Grifo nosso.***

## 5. ANÁLISE

### 5.1. DA CONTEXTUALIZAÇÃO

5.1.1. O presente processo objetiva estabelecer requisitos mínimos de segurança cibernética em produtos para telecomunicações, como parte de um plano geral da Anatel de desenvolver ações que possibilitem maior segurança cibernética nas telecomunicações.

5.1.2. Primeiramente, faz-se mister trazer à baila o conceito de segurança cibernética para a melhor compreensão do escopo do presente processo. Em que pese a definição se apresente de modo difuso, podem-se observar elementos centrais que a caracterizam.

5.1.3. A UIT (União Internacional das Telecomunicações) definiu segurança cibernética como “a coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, orientações, abordagens de gestão de risco, ações, treinamentos, melhores práticas, seguros e

tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e propriedades de usuários(as). A organização e as propriedades incluem dispositivos de computação conectados, funcionários(as) e colaboradores(as), infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade de informação transmitida e/ou armazenada no ambiente cibernético. A segurança cibernética busca garantir a obtenção e a manutenção das propriedades de segurança da organização e das propriedades do(as) usuários(as) contra riscos de segurança relevantes no ambiente cibernético". (ITU-CIBERSEG-2008)

5.1.4. De forma a enriquecer o conceito, foi colacionada uma definição mais voltada aos equipamentos e sistemas, *ipsis litteris*, em que a segurança cibernética constitui-se da prática de defender contra ataques maliciosos os computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados.

> *Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.*
>
> *- Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.*
>
> *- Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.*
>
> *- Information security protects the integrity and privacy of data, both in storage and in transit.*
>
> *- Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.*
>
> *- Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.*
>
> *- End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.*
>
> (fonte: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security)

5.1.5. De forma mais sucinta, pode-se entender a segurança cibernética como um conjunto de ações sobre pessoas, tecnologias e processos para proteção e prevenção contra ataques cibernéticos.

5.1.6. Vale, então, citar a mais recente iniciativa do Governo Federal no que atine à segurança cibernética nacional. Trata-se do Decreto n.º 10.222, de 5 de fevereiro de 2020 (Ref. 2.5), que criou a Estratégia Nacional de Segurança Cibernética, denominada E-Ciber.

5.1.7. O referida Estratégia traz em seu bojo uma visão geral sobre o cenário da segurança cibernética, sendo relevante também trazê-la para o âmbito deste processo.

> *A revolução digital está transformando profundamente nossa sociedade. Nas últimas duas décadas, bilhões de pessoas se beneficiaram do crescimento exponencial do acesso à internet, da rápida adoção dos recursos de tecnologia da informação e comunicação, e das oportunidades econômicas e sociais oriundas do ambiente digital.*
>
> *Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive a oferta de serviços por parte do Governo federal, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade.*
>
> *Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar*

*mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais. Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão.*

*[...]*

*A E-Ciber, além de preencher importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabelece ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto. Em primeiro lugar, verifica-se que há boas iniciativas gerenciais nessa área, entretanto, mostram-se fragmentadas e pontuais, o que dificulta a convergência de esforços no setor. Em segundo,* ***nota-se a falta de um alinhamento normativo****, estratégico e operacional, o que frequentemente gera retrabalho ou resulta na constituição de forças-tarefas para ações pontuais, que prejudicam a absorção de lições aprendidas e colocam em risco a eficácia prolongada dessas ações. Em terceiro, vê-se a existência de diferentes níveis de maturidade da sociedade em segurança cibernética, o que resulta em percepções variadas sobre a real importância do tema.*

***Grifo nosso.***

5.1.8. O referido decreto frisa em seu art. 2º que os órgãos e entidades da administração pública federal deverão realizar as ações de gestão que possibilitem a implementação das ações estratégicas definidas no E-Ciber, cada qual no seu âmbito de competência. Deste modo, no que pertine às competências desta Superintendência, mais especificamente no tocante à avaliação da conformidade de produtos para telecomunicações, observa-se a necessidade de realizar medidas regulatórias com vistas ao fomento da E-Ciber.

5.1.9. Ressalta-se que a Agência já iniciou o processo de estudo e construção do Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações por meio do processo 53500.078752/2017-68, em atenção ao item 58 da Agenda Regulatória para o biênio 2017-2018, aprovada pela Portaria n.º 491, de 10 de abril de 2017, e alterada pela Portaria n.º 1, de 2 de janeiro de 2018, ambas do Conselho Diretor.

*Item 58 - Análise sobre regulamentação de segurança das redes de telecomunicações*

*Elaboração de análises e estudos sobre a necessidade ou não de regulamentação que possibilite a implementação de medidas de proteção e segurança das redes e serviços das operadoras de telecomunicações. A segurança das redes é hoje um dos grandes problemas da nova economia digital. São diversos os países que vem enfrentando os problemas relacionados à segurança cibernética e realizando grandes investimentos na busca da disponibilidade, confidencialidade e integridade das informações no ambiente cibernético. Como os dados trafegam em redes de telecomunicações cabe à Anatel atuar dentro de suas competências a fim de garantir e fiscalizar a proteção dessa primeira linha de frente, a exemplo de outros reguladores como FCC (EUA), Anacom (Portugal), KISA (Coréia do Sul), Ofcom (Reino Unido) que atualizam constantemente suas diretrizes.*

5.1.10. Conforme explanado no AIR respectivo (SEI nº2843567), "o projeto busca abordar um tema sempre presente nas discussões acerca do futuro da internet e das redes de telecomunicações. Com o advento da Internet das Coisas (IoT), o tema ganha ainda mais relevância devido à ubiquidade dos dispositivos conectados à rede. Ainda, tal ação vai ao encontro das recentes diretivas de políticas públicas. A Estratégia Brasileirapara a Transformação Digital (E-Digital), fruto do Grupo de Trabalho Interministerial, instituído pela Portaria n.º 842, de 17 de fevereiro de 2017, do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), estabelece como um de seus eixos temáticos a “Confiança no Ambiente Digital” que é subdividido nos temas “Proteção de Direitos e Privacidade” e “Defesa e Segurança no Ambiente Digital”."

5.1.11. Vale citar que, como proposta de Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações, foi disponibilizada em Consulta Pública (CP 52/2018) uma Minuta de Resolução. Esta proposta prevê em seu art. 11, *ipsis litteris*, a implementação de ações futuras relacionadas à avaliação da conformidade e homologação de produtos para telecomunicações.

*Art. 11. Aspectos de segurança cibernética poderão ser levados em consideração nos*

*procedimentos relativos à avaliação da conformidade e homologação de produtos para telecomunicações, nos termos da regulamentação específica.*

5.1.12. Verifica-se, então, alinhamento da proposta de Resolução aos requisitos propostos no presente processo. Adicionalmente, observa-se também perfeito alinhamento à Estratégia Nacional de Segurança Cibernética (E-Ciber), que dispõe da seguinte forma:

> *2. A ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA*
>
> *[...]*
>
> *2.3. AÇÕES ESTRATÉGICAS*
>
> *[...]*
>
> *2.3.2. Estabelecer um modelo centralizado de governança no âmbito nacional*
>
> *Estabelecer um modelo centralizado de governança para o País, por meio da criação de um sistema nacional de segurança cibernética, com as seguintes atribuições:*
>
> *[...]*
>
> *- **estabelecer rotina de verificações de conformidade em segurança cibernética**, internamente, nos órgãos públicos e nas entidades privadas;*
>
> *[...]*
>
> *PARTE II*
>
> *ANÁLISE DOS EIXOS TEMÁTICOS*
>
> *[...]*
>
> *1. EIXOS TEMÁTICOS: PROTEÇÃO E SEGURANÇA*
>
> *1.1. Governança da Segurança Cibernética Nacional*
>
> *[...]*
>
> *Por oportuno, entende-se que a **certificação de produtos e de soluções em segurança cibernética é um objetivo a ser perseguido**, ao considerar a complexidade dos equipamentos e das ferramentas computacionais, que exigem elevado grau de especialização e de recursos tecnológicos à disposição, e de organismos estruturados e equipados para conduzi-la. Destaca-se que, antes de fomentar e desenvolver uma certificação própria, recomenda-se buscar alavancar os mecanismos de certificação existentes, para evitar a criação de barreiras comerciais.*
>
> *Entretanto, é crescente o entendimento, no meio produtivo, de que a **certificação de produtos - mais especificamente, de equipamentos - não se mostra algo simples**, uma vez que a certificação ocorre sobre o tipo, o modelo e o **firmware** de um equipamento, o que impede sua atualização de **firmware** ou que o fabricante disponibilize **patches** de segurança, sob pena de levar o produto a perder a certificação inicial.*
>
> *[...]*
>
> *Dentro dessa perspectiva, ressaltam-se três vertentes importantes: a medição da eficácia e da eficiência dos centros de tratamento e resposta aos incidentes computacionais, a elaboração de indicadores para medir o desempenho do País em segurança cibernética e o **estabelecimento de rotina de verificações de conformidade em segurança cibernética** dentro dos órgãos públicos e das entidades privadas, por eles conduzidas, de modo que seja possível estabelecer a correta relação entre os aspectos técnicos de tecnologia da informação, como análise de vulnerabilidades, relatórios técnicos de ameaças e relação de soluções em tecnologia, com os aspectos de negócio, como continuidade dos serviços prestados, riscos à imagem e processos de tomada de decisão. Entende-se, portanto, a verificação de conformidade como um processo natural, baseada em programas estabelecidos pelas próprias entidades públicas e privadas, que visa ao aprimoramento contínuo dos sistemas voltados à segurança cibernética.*
>
> *Destaca-se que as **verificações de conformidade devem ser planejadas com moderação, e devem ser baseadas em princípios de razoabilidade**, para que não levem as instituições públicas e privadas a empregarem tempo e grande soma de recursos em procedimentos excessivos de conformidade, em detrimento de seu uso para lidar com ameaças cibernéticas.*
>
> ***Grifo nosso.***

5.1.13. Atualmente, já é possível observar a dimensão do universo de produtos para Internet da Coisas (conhecida como IoT, do inglês *Internet of Things*), que engloba desde equipamentos mais simples como sensores e atuadores domésticos até sistemas mais complexos e críticos, como os sistemas de automação industrial ou os sistemas de transporte com veículos

autônomos.

5.1.14. Neste contexto, considerando a crescente interdependência entre as telecomunicações e os diversos setores da sociedade, e considerando que, com o advento da IoT, aumentar-se-á substancialmente a variedade de produtos e serviços conectados à internet, torna-se urgente e necessário criar instrumentos regulatórios que objetivem a mitigação das vulnerabilidades dos equipamentos que compõem as infraestruturas de redes e estações terminais de telecomunicações.

5.2. **DA PROPOSTA**

5.2.1. Os equipamentos para telecomunicações apresentam características técnicas diversificadas que variam de acordo com seus recursos de processamento, memória, interfaces e quanto às suas aplicações.

5.2.2. A depender do fim a que o equipamento para telecomunicação se destina, sua criticidade para o sistema o qual se conecta pode variar, necessitando do atendimento a requisitos de segurança cibernética mais simples ou rigorosos.

5.2.3. Diante do apontado, o estabelecimento de requisitos de segurança cibernética deve considerar esse ecossistema variado, devendo possuir ampla abrangência sem deixar de considerar as particularidades de cada produto e a criticidade de suas possíveis vulnerabilidades em relação à segurança do usuário e das redes de infraestrutura crítica da qual fazem parte ou se conectam. A exemplo dessas particularidades, podemos citar a virtualização de diversas funções de rede (por exemplo, *Software-Defined Networking* (SDN) e *Network Functions Virtualization* (NFV)), que serão amplamente utilizadas nas redes que darão o suporte ao 5G.

5.2.4. O Anexo 6.1 apresenta uma proposta de requisitos mínimos de segurança cibernética para manutenção da homologação de terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações. A aplicação de cada requisito contido na proposta deve levar em consideração as diferentes características técnicas (quantidade de memória, capacidade de processamento de dados, interfaces para usuário, interfaces de comunicação, etc.) de cada equipamento e os fins a que se destinam.

5.2.5. A proposta apresentada contempla requisitos que devem ser aplicados aos equipamentos e aos seus fornecedores e foi embasada em referências internacionais, tais como:

a) OECD - *Enhancing the Digital Security of Products - Draft Scoping Paper (November 2019)*.

b) IEEE - *Internet Technology Policy Community White Paper - Internet of Things (IoT) Security Best Practices (February 2017)*.

c) IETF - *Internet of Things (IoT) Security: State of the Art and Challenges* - RFC 8576.

d) LAC-BCOP-1 (May/2019) *–Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition*.

e) ENISA *-Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures (November 2017)*.

f) GSMA *IoT Security Guidelines – Complete Document Set*.

5.2.6. Ademais, a proposta de estabelecimento de requisitos de segurança cibernética está alinhada às atividades desenvolvidas pelo Grupo de Trabalho sobre Defesa do Consumidor e Segurança de Produtos (*Working Party on Consumer Product Safety*) da OCDE (Organização para a Cooperação e Desenvolvimento Econômico).

5.2.7. O interessado na homologação de um equipamento deverá demonstrar

conformidade por meio de declaração afirmando que o produto e seu fornecedor atendem os requisitos contidos na proposta e estar ciente que este o texto está sujeito a atualizações.

5.2.8. Considerando a diversidade de produtos para telecomunicações, o escopo de requisitos da declaração de conformidade deve considerar as diferentes características técnicas dos equipamentos (quantidade de memória, capacidade de processamento de dados, interfaces do usuário, interfaces de comunicação, etc.) e os fins a que se destinam.

5.2.9. Propõe-se que, durante as atividades de supervisão de mercado, a Agência possa avaliar os requisitos contidos neste documento por meio de procedimentos de ensaios orientados pelas melhores práticas, padronizadas internacionalmente, para avaliação de vulnerabilidades.

5.2.10. A fim de proteger os consumidores e garantir a integridade das infraestruturas das redes para telecomunicações do país, caso o equipamento para telecomunicação, ou seu fornecedor, apresente alguma desconformidade aos requisitos mínimos que possam afetar a segurança do usuário ou dos serviços para telecomunicações, a Agência notificará o responsável pela homologação a sanar a falha, sendo indicado um prazo adequado para esse fim, considerando-se o grau de risco da vulnerabilidade.

5.2.11. Decorrido o prazo sem que se verifique as adaptações necessárias ou a justificativa aceita pela Anatel para sua não implementação, a Agência suspenderá a homologação do produto, podendo indicar o recolhimento ou substituição do mesmo no mercado, garantidas as demais previsões regulamentares referentes ao direito do consumidor.

## 5.3. DA AVALIAÇÃO DE RISCOS

5.3.1. A proposta em questão visa a criação de um conjunto de requisitos mínimos de segurança cibernética para equipamentos terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações.

5.3.2. Foram identificados as seguintes opções de cenários para a ação regulatória:

a) **Cenário 1: Não estabelecimento de requisitos mínimos de segurança cibernética, mantendo os cenário atual.**

b) **Cenário 2: Estabelecimento de requisitos mínimos de segurança cibernética para certificação de produtos.**

c) **Cenário 3: Estabelecimento de procedimento de declaração de conformidade a requisitos mínimos de segurança cibernética para produtos de telecomunicações.**

5.3.3. A seguir, são apresentadas análise de impacto regulatório para os 3 (três) cenários mencionados:

5.3.3.1. **Cenário 1:** o não estabelecimento de requisitos mínimos de segurança implica que o próprio mercado irá regular e definir os níveis de segurança dos equipamentos para telecomunicações. Normalmente, grandes prestadores de serviços para telecomunicações têm o conhecimento técnico necessário e a consciência de que é preciso empregar em sua infraestrutura produtos que possuem níveis de segurança mais elevados, garantindo a confiabilidade dos serviços que prestam e a segurança dos dados de seus usuários. Contudo, prestadores de menor porte possuem, usualmente, orçamentos mais restritos e, às vezes, conhecimento técnico menos especializado. Tais empresas de menor capacidade podem optar, muitas vezes de forma inadvertida, em adquirir equipamentos com preços mais acessíveis e, possivelmente, com níveis de segurança inferiores. A mesma lógica se aplica aos equipamentos terminais de usuários, como telefones celulares, roteadores residenciais e câmeras de segurança. A falta de padrões mínimos de segurança pode expor os usuários, que normalmente não possuem

conhecimento técnico, a vazamentos de dados pessoais além de permitir que tais dispositivos possam vir a se tornar hospedeiros de *malwares* cuja finalidade seja executar ataques massivos de negação de serviço **DDoS** (*Distributed Denial of Service*), por exemplo.

a) **Vantagens:** menores custos regulatórios; simplificação da regulamentação; menor intervenção econômica.

b) **Desvantagens:** provável disponibilização, ao mercado consumidor (especializado ou não), de produtos com menores níveis de segurança cibernética e com maior potencial para sofrem com ataques como vazamento de dados pessoais e maiores probabilidades de incidência de ataques de DDoS às infraestruturas de telecomunicação e tecnologia da informação do país.

5.3.3.2. **Cenário 2:** o estabelecimento de requisitos mínimos de segurança cibernética para certificação de produtos exige que cada modelo de produto para telecomunicação seja submetido a testes previamente à sua homologação, a fim de verificar sua conformidade quanto aos requisitos de segurança cibernética. Considerando que diferentes equipamentos possuem diferentes características técnicas, capacidades de hardware/software e aplicações distintas (algumas altamente críticas e outras nem tanto), cada produto para telecomunicação deverá comprovar atendimento a um conjunto específico de requisitos. Essa grande variedade de equipamentos e aplicações exige uma análise mais complexa no ato da certificação, tornando o processo de homologação mais caro, complexo e moroso.

a) **Vantagens:** todo modelo de equipamento para telecomunicação deverá ser testado quanto a sua segurança cibernética previamente à sua disponibilização ao mercado consumidor garantindo que os produtos homologados estejam operando no estado da arte da segurança para tecnologia de segurança da informação.

b) **Desvantagens:** maiores custos regulatórios; maior intervenção econômica; processo de homologação mais complexo, demorado e dispendioso; maiores barreiras econômicas ao mercado.

5.3.3.3. **Cenário 3:** o estabelecimento de procedimento de declaração de conformidade a requisitos mínimos de segurança cibernética para produtos de telecomunicações visa apresentar aos fabricantes e aos fornecedores de equipamentos para telecomunicações um conjunto mínimos de critérios que devem ser atendidos pelo produto e pelo fornecedor para que a homologação de determinado equipamento seja expedida e se mantenha vigente. Neste cenário, os produtos não são submetidos a ensaios de certificação quanto ao requisitos de segurança cibernética. Contudo, no ato da solicitação da homologação, o fabricante/fornecedor declara conformidade aos requisitos mínimos de segurança, incluindo suas futuras atualizações. Durante o ciclo de vida do produto, caso fique evidente que o equipamento possua alguma vulnerabilidade que não esteja em conformidade com os requisitos definidos pela Anatel, a Agência poderá, após análise técnica, determinar a suspensão da homologação do equipamento até que as vulnerabilidades apontadas ou o potencial risco à segurança dos serviços para telecomunicações sejam sanadas.

a) **Vantagens:** menores custos regulatórios em comparação com o cenário 2; maior agilidade para homologação dos produtos, pois não são feitos ensaios de segurança cibernética no ato da certificação; menores barreiras econômicas ao comércio; possibilidade de acompanhamento dos produtos por meio da supervisão de mercado e da atuação preventiva da Anatel com a suspensão da homologação do produto a seu critério.

b) **Desvantagens:** possibilidade do fabricante/fornecedor declarar falsamente que o

produto atende aos requisitos de segurança; a avaliação do produto é feita *a posteriori*, no momento de um procedimento de fiscalização ou supervisão de mercado.

5.3.4. Analisando os 3 (três) cenários apresentados e ponderando as vantagens e desvantagens de cada um, a área técnica da Gerência de Certificação e Numeração desta Agência entende que o **Cenário 3** é o que apresenta um melhor balanceamento entre a garantia da segurança das redes e dos usuários sem representar grandes barreiras técnicas e econômicas à inserção de novos produto e tecnologias no país, sobretudo considerando o potencial aumento no número de produtos para telecomunicações a serem disponibilizados no mercado global nos próximos anos, resultante do desenvolvimento de soluções IoT e da implantação das redes móveis de quinta geração (5G).

5.3.5. Diante do exposto, propõe-se a disponibilização da Minuta de Ato (Anexo 6.1) em Consulta Pública, a fim de colher contribuição da sociedade na proposta de requisitos mínimos de segurança cibernética para equipamentos terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações.

5.3.6. Considerando a complexidade do tema, sugere-se que o documento fique disponível para análise popular em Consulta Pública pelo prazo de 60 dias.

## 6. DOCUMENTOS RELACIONADOS/ANEXOS

6.1. Minuta de Ato (SEI 4337576).

## 7. CONCLUSÃO

7.1. Diante da fundamentação, a Gerência de Certificação e Numeração da Anatel - ORCN submete à deliberação superior este Informe com vistas à apreciação pelo Superintendente de Outorga e Recursos à Prestação e consequente aprovação de proposta de Consulta Pública, nos moldes da Minuta de Ato (Anexo 6.1), com prazo de duração igual a 60 (sessenta) dias, em conformidade com o Art. 59 do Regimento Interno da Anatel, aprovado pela Resolução n.º 612, de 29 de abril de 2013, para a análise e contribuição do público em geral na proposta de "Requisitos Mínimos de Segurança Cibernética para Equipamentos para Telecomunicações".

Documento assinado eletronicamente por **Davison Gonzaga da Silva**, **Gerente de Certificação e Numeração**, em 17/03/2020, às 22:53, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da Portaria nº 912/2017 da Anatel.

A autenticidade deste documento pode ser conferida em http://www.anatel.gov.br/autenticidade, informando o código verificador **5162147** e o código CRC **DA0648B8**.