COMENTÁRIOS À CONSULTA PÚBLICA No 13 REFERENTE AOS REQUISITOS MÍNIMOS DE SEGURANÇA PARA EQUIPAMENTOS DE TELECOMUNICAÇÕES DA ANATEL

Maio de 2020

A Brasscom, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (TIC), entidade que congrega empresas fornecedoras de software, soluções e serviços de TIC e que tem como missão trabalhar em prol do desenvolvimento do setor, disseminando seu alcance e potencializando seus efeitos sobre a economia e o bem-estar social, parabeniza a ANATEL pela iniciativa de submeter à Consulta Pública a minuta de ato sobre requisitos mínimos de segurança para equipamentos de telecomunicações.

A garantia da segurança cibernética de um país está no cerne das medidas estruturantes que geram vantagens competitivas para incentivar a inovação e o desenvolvimento tecnológico de forma sustentável e crescente e é neste cenário que o Brasil necessita inserir-se.

Para promover abordagens de *security by design and default* é fundamental que se respeite a natureza de tais conceitos, ou seja, a preocupação de segurança como conceito estruturante do próprio desenvolvimento do produto e/ou serviço, evitando-se regimes de padronização e certificação prescritivos para a cibersegurança. Certificações e padronizações obrigatórias de segurança para o mercado podem inadvertidamente encorajar as empresas a investir apenas no cumprimento de padrões ou práticas estáticas definidas em norma ou processo determinado de certificação e que podem – em virtude da dinamicidade do setor de tecnologia – ficar desatualizadas em breves espaços de tempo.

Preocupa o olhar da regulamentação no sentido de certificar todo e qualquer equipamento utilizado pelo ecossistema com vistas específicas ao cumprimento de premissas de segurança cibernética na medida em que nessa temática, o objetivo é se ter um ecossistema seguro como um todo, não sendo a consideração da segurança de cada elemento desse conjunto de maneira individual a melhor maneira de se garantir a segurança cibernética sistêmica.

Uma abordagem de gerenciamento de risco equilibrada é essencial, honrando e encorajando os atores que já estão envolvidos com as melhores práticas adotadas pelo mercado para segurança, focando na construção de conhecimento e encorajando as melhores práticas para os atores que ainda estão evoluindo neste tema em suas organizações. Nesse sentido, a Brasscom defende ser fundamental que discussões relacionadas a requisitos mínimos de segurança, e à gestão de riscos relacionados à cibersegurança, são melhor endereçadas por meio de padrões flexíveis, globais, induzidos pelas relações de mercado e fomentados pela indústria, justamente pela sua natureza consensual e baseada nas melhores práticas.

Ademais, é importante ressaltar que existem diversas variáveis que podem direta ou indiretamente afetar os requisitos mínimos necessários. Por exemplo, o tipo de

equipamento e seus recursos, a finalidade de uso e o contexto no qual ele será implementado podem exigir requisitos mínimos diferentes, dependendo de uma vulnerabilidade específica, complexidade de um equipamento específico em toda a rede, capacidade da própria rede de fornecer determinadas proteções de segurança cibernética. Ou seja, entendemos que as discussões sejam norteadas pelo princípio de que abordagens prescritivas de "tamanho único" não necessariamente serão eficazes em endereçar todas as questões atreladas à temática de segurança cibernética.

Nesse sentido, sugerimos que a Agência segmente a edição de regulamentação específica sobre requisitos mínimos de segurança cibernética de modo a respeitar as características distintas de grupos de elementos de rede e dispositivos a ela conectados, para o objetivo maior da segurança seja atingido, sem a imposição de um ônus regulatório e de custo desnecessário e desproporcional a certos dispositivos cuja função e papel na rede é, na prática, de menor complexidade.

Sendo assim, a Brasscom agradece novamente a oportunidade de apresentar comentários à consulta pública e, abaixo, apresenta considerações específicas aos itens de discussão, bem como algumas alterações na minuta de ato, a fim de refletir a abordagem sobre o tema que mencionamos acima:

CONSIDERAÇÕES E SUGESTÕES DE ALTERAÇÕES DA MINUTA DE REGULAMENTAÇÃO

1. OBJETIVO

a) Exclusão expressa de dispositivos de IoT do escopo de aplicação do ato (item 1.1)

Redação original	Sugestão de redação
Estabelecer 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.	Estabelecer 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.
Justificativa Conforme explorado na parte introdutória de nossa contribuição, entendemos que a melhor política pública para garantir a segurança cibernética não é por meio da	

certificação individual de todo e qualquer elemento da rede, tendo em vista que tal abordagem poderá desconsiderar uma visão holística do funcionamento do sistema, e levar a imposição de custos muito altos em dispositivos de baixa complexidade. Portanto, de modo a equacionar essa questão, sugerimos que o texto da proposta de regulamento seja revisto de modo a se limitar, exclusivamente, a equipamentos de infraestrutura de rede de telecomunicações que possuam um papel com algum grau de complexidade na arquitetura da rede. Limitando o escopo de aplicação do ato em questão aos equipamentos de infraestrutura de redes de telecomunicações, vale ressaltar que essa camada da rede conta com uma enorme variedade de dispositivos, de diversos grupos e com funcionalidades diferentes. Entendemos, ainda, legítima a preocupação da Agência com a segurança do ecossistema como um todo. Sendo assim, sugerimos a constituição de um grupo de trabalho, composto por membros da Agência e da indústria, para empenhar esforços na discussão de item por item dos requisitos futuramente estabelecidos, tendo mente uma abordagem de gestação de risco, os custos, o perfil de cada classe de equipamento e, consequentemente, a viabilidade da incorporação de tais mecanismos em cada uma delas.

3. DEFINIÇÕES

a) Revisão da definição de backdoor (item 3.1.)

Redação original	Sugestão de redação
Backdoor: mecanismo não documentado contido no software/firmware do produto que possibilita acesso não autorizado ao equipamento. A presença de backdoors pode ser intencional ou acidental, podendo ser decorrente de erros de programação.	Backdoor: mecanismo não documentado contido no software/firmware do produto ~~que possibilita~~ com intenção de possibilitar acesso não autorizado ao equipamento. A presença de backdoors pode ser ~~intencional~~ maliciosa ou acidental, podendo ser decorrente de erros de programação.
Justificativa Por definição, um backdoor é sempre intencional, já que é criado com a intenção de permitir o acesso direto ao equipamento.	

Segundo o documento "Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition", que conta como referência no texto sob consulta, um backdoor não necessariamente é concebido para causar danos, na medida em que pode ter sido incluído durante o desenvolvimento do software/firmware e esquecido pelo programador. Dessa forma, sugerimos um pequeno ajuste na definição proposta para que fique mais aderente à definição técnica do termo.

b) Criar definição de "vulnerabilidade"

Sugestão de redação Vulnerabilidade: mecanismo não documentado contido no software/firmware do produto que pode permitir acesso não autorizado ao equipamento, ou mal funcionamento. A presença de vulnerabilidades pode ser acidental, podendo ser decorrente de erro de programação.
Justificativa Na medida em que o termo "vulnerabilidade" é mencionado diversas vezes ao longo do texto sob consulta, nós entendemos ser importante definir separadamente os conceitos de backdoor e vulnerabilidade, pois enquanto o primeiro é intencional, decorrentes das mais diversas motivações, inclusive criminosas ou de espionagem, o segundo pode ser apenas por erro de programação, sem más intenções. Além disso, esse conceito parece melhor aproximar da preocupação da Agência com o conjunto de requisitos identificados.

c) Revisão da definição de Customer Premise Equipment (item 3.2)

Redação original	**Sugestão de redação**
Customer Premise Equipment (CPE): equipamento utilizado para conectar assinantes à rede do provedor de serviços de telecomunicações.	Customer Premise Equipment (CPE): equipamento utilizado para conectar assinantes à rede do provedor de serviços de telecomunicações. <u>O termo não se aplica a sensores e dispositivos de propósito único e/ou recursos limitados,</u>

	normalmente referidos como dispositivos para Internet das Coisas ou IoT.

Justificativa

O conceito de Customer Premises Equipment refere-se usualmente a equipamentos de acesso como gateways domésticos, modems e roteadores.

Os dispositivos de IoT utilizam muitas outras características aquém daquelas tipicamente destinadas à CPEs. Por tal razão, sugerimos que a definição de CPE constante do regulamento seja revista para se delimitar aos conceitos utilizados como CPE, podendo, eventualmente, incluir outros elementos do core de rede, mas não devendo abranger dispositivos terminais e dispositivos de IoT em virtude das características simplificadas desse dispositivo. A segurança cibernética, nestes casos, deverá ser garantida por outros elementos da rede, dispensando o controle granular dos dispositivos colocados na ponta.

Quanto à eventualidade de se incluir outros elementos de core de rede, sugerimos que haja a elaboração de uma definição que englobe esses equipamentos, de forma clara e que proporcione uma interpretação objetiva. Da forma como apresentada a consulta pública, o texto se refere a equipamentos terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações, de maneira muito vaga, gerando incerteza e insegurança quanto a abrangência da obrigação estabelecida na norma.

d) Separação das definições de métodos adequados de criptografia, autenticação e integridade (item 3.5)

Redação original	Sugestão de redação
Métodos adequados de criptografia, autenticação e integridade: protocolos ou algoritmos de criptografia, autenticação e integridade, em suas versões atualizadas. A implementação deve permitir a seleção de conjuntos de criptografia e tamanhos de chave atualizados.	Métodos adequados de criptografia: protocolos ou algoritmos de criptografia documentadas pela IETF (Internet Engineering Task Force) e em suas versões atualizadas. A implementação deve permitir a seleção de conjuntos de criptografia e tamanhos de chave atualizados. Métodos adequados de autenticação: protocolos ou algoritmos de autenticação e integridade, em suas versões

	atualizadas. A autenticação deverá ser por senha segura, e não poderá ser definida no próprio código do hardware ou software, impedindo sua alteração. Métodos adequados de integridade: protocolos ou algoritmos de integridade dos dados, software, sistema operacional e firmware, em suas versões atualizadas.
Justificativa É importante uma definição em separado para criptografia, e a especificação que o método esteja padronizado e previsto por documento da IETF, conforme o documento "Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition" do LAC-BOP-1. Além disso, entendemos que, apesar de serem métodos complementares, é de suma importância que suas respectivas definições sejam concebidas separadamente, para permitir conceituação mais clara.	

4. REQUISITOS GERAIS

a) Revisar demonstração de conformidade e sua declaração (item 4.1)

Redação original	Sugestão de redação
a) que o equipamento e seu fornecedor atendem os requisitos contidos neste documento; e b) estar ciente que este documento está sujeito a atualizações.	a) que o equipamento e seu fornecedor atendem – no momento de homologação - os requisitos contidos neste documento; e b) estar ciente que ~~este documento~~ essa conformidade estará sujeita a atualizações, decorrente da evolução tecnológica e eventual atualização dos requisitos mínimos definidos pela Agência em regulamentação. O fabricante

	ou requerente do certificado de homologação da Anatel terá o prazo de 180 dias para se adequar, contados a partir da publicação do ato ou notificação da Agência.
Justificativa O setor das TIC é intrinsecamente disruptivo, onde novas tecnologias, dispositivos e soluções inovadoras são constantemente criados e aprimorados. Portanto, é natural que novas ameaças surjam com esses avanços, e é do próprio interesse das fabricantes tomar medidas para saná-las. Dito isto, sugerimos que a demonstração de conformidade e sua respectiva declaração sejam restritas ao âmbito do processo de homologação. Caso contrário, entendemos que a linguagem trazida pelo texto sob consulta, além de aumentar os custos de *compliance* por parte das empresas, pode exigir delas esforços desproporcionais em relação a algumas vulnerabilidades que não trazem riscos para os usos que o equipamento foi originalmente concebido a realizar, ao mesmo tempo que limita, do ponto de vista técnico e orçamentário, a capacidade de se mitigar vulnerabilidades relevantes.	

b) Revisão do escopo material de avaliação e identificação de vulnerabilidades (item 4.4)

Redação original	**Sugestão de redação**
Identificada, no produto homologado, qualquer vulnerabilidade relacionada a um ou mais requisitos de segurança cibernética, a Agência notificará o responsável pela homologação a sana-la, indicando prazo adequado para esse fim, considerando-se o grau de risco da vulnerabilidade.	Identificada, ~~no produto homologado~~ durante o processo de homologação de um produto, qualquer vulnerabilidade relacionada a um ou mais requisitos de segurança cibernética, a Agência ~~notificará~~ e o responsável pela homologação notificarão o fabricante do equipamento, o qual será responsável por sana-la, considerando-se o grau de risco da vulnerabilidade. O prazo fixado pela Anatel para saneamento da vulnerabilidade não será inferior a 180 dias.
Justificativa	

A Brasscom entende que os processos de avaliação e identificação de vulnerabilidades devem ser restritos no âmbito do processo de homologação do produto e não após a sua finalização. Isso porque a Brasscom entende que haverá uma certa dificuldade por parte das fabricantes em incluir internamente rotinas voltadas para processos de pós-venda via atualização do teste de conformidade, bem como daquelas direcionadas a providenciar respostas à Agência fora do processo de homologação. Além disso, reforçamos aqui nossa sugestão de criação de definição de "vulnerabilidade" para fins deste ato, conforme mencionamos anteriormente, e alertamos para a abrangência de seu conceito, na medida em que se trata de um mecanismo não documentado e acidental, que podem apresentar diferentes níveis de criticidade. Outro ponto importante é deixar claro que o fabricante do equipamento deve ser o responsável por sanar as eventuais vulnerabilidades identificadas em decorrência do ato fiscalizatório, e não o órgão responsável pela homologação. Por fim, a sugestão de prazo acima referida é compatível com os prazos de certificação de equipamentos usualmente utilizados pela Agência.

c) Revisão dos itens 4.4.1, 4.4.2. e 4.4.3.

Redação original	Sugestão de redação
4.4.1. 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.	4.4.1. Decorrido o prazo sem que se verifique as adaptações necessárias ou a justificativa aceita pela Anatel para sua não implementação, a Agência suspenderá <u>o processo de</u> homologação do produto, podendo indicar o recolhimento ou substituição do mesmo no mercado, garantidas as demais previsões regulamentares referentes ao direito do consumidor.
4.4.2. A suspensão da homologação do equipamento será mantida até que as vulnerabilidades apontadas sejam sanadas ou até que o potencial risco à segurança dos	4.4.2. A suspensão <u>do processo de</u> homologação do equipamento será mantida até que as vulnerabilidades apontadas sejam

serviços para telecomunicações seja mitigado, considerando-se o prazo máximo estabelecido na regulamentação vigente. 4.4.3. Após o prazo máximo determinado para sua suspensão, a homologação será cancelada, caso a vulnerabilidade não seja solucionada.	sanadas ou até que o potencial risco à segurança dos serviços para telecomunicações seja mitigado, considerando-se o prazo máximo estabelecido na regulamentação vigente. 4.4.3. Após o prazo máximo determinado para sua suspensão, o processo de homologação será cancelado, caso a vulnerabilidade não seja solucionada.
Justificativa Nós entendemos que os processos de avaliação e identificação de vulnerabilidades devem ser restritos ao âmbito do processo de homologação do produto e não após a sua finalização. Os ajustes propostos aqui são para refletir essa premissa que já pontuamos em relação ao item 4.4.	

5. REQUISITOS DE SEGURANÇA CIBERNÉTICA DOS EQUIPAMENTOS PARA TELECOMUNICAÇÕES

a) Revisão escopo de aplicação dos requisitos (item 5.1)

Redação original	Sugestão de redação
Equipamentos terminais que se conectam à Internet e equipamentos de infraestrutura de redes de telecomunicações, em suas versões finais destinadas à comercialização, devem:	~~Equipamentos terminais que se conectam à Internet e~~ equipamentos de infraestrutura de redes de telecomunicações, em suas versões finais destinadas à comercialização, devem:
Justificativa Alguns dos diversos requisitos listados abaixo são inviáveis de serem aplicados a todas as camadas da rede de telecomunicações. Dispositivos de IoT e equipamentos com interfaces mais simples, devido seu propósito único e/ou recursos limitados, não dispõem de uma granularidade que possibilite os usuários finais a mexer em sua interface, por exemplo.	

b) Revisão da característica atribuída à implementação de rotinas (subitem a) do item 5.1.2)

Redação original	Sugestão de redação
Implementar rotinas simplificadas para sua instalação e configuração, evitando potenciais falhas de segurança não intencionais.	Implementar rotinas ~~simplificadas~~ adequadas para sua instalação e configuração, evitando potenciais falhas de segurança não intencionais.
Justificativa Em virtude da complexidade da arquitetura das redes e CPEs, uma abordagem simplificada poderá, muitas vezes, comprometer a própria segurança cibernética que está se buscando garantir. Vale pontuar que as empresas de TIC têm cada vez mais se comprometido a implementar rotinas e estruturas que prezam pela segurança e integridades de seus equipamentos, bem como de suas informações.	

c) Exclusão de requisito de mecanismo de monitoramento de comportamentos não usuais (subitem c) do item 5.1.2)

Redação original	Sugestão de redação
Possuir mecanismo de monitoramento de comportamentos não usuais do software/firmware, alertando o usuário ou reiniciando-se automaticamente caso um comportamento suspeito seja detectado.	~~Possuir mecanismo de monitoramento de comportamentos não usuais do software/firmware, alertando o usuário ou reiniciando-se automaticamente caso um comportamento suspeito seja detectado.~~
Justificativa O requisito disposto acima é incompatível com a classe e sofisticação dos equipamentos CPE. Além disso, o alto custo atrelado à sua implementação faz com que nos pareça ser um requisito que deva ser exclusivamente estabelecido para equipamentos que compõem as camadas mais avançadas da infraestrutura de rede, e não na sua ponta.	

d) Exclusão de requisito de implementação de ferramenta de registro de atividades (logs) (subitem d) do item 5.1.2)

Redação original	Sugestão de redação
Implementar ferramenta de registro de atividades (logs) relacionadas à autenticação de usuários, alteração de configurações do sistema e funcionamento do sistema.	~~Implementar ferramenta de registro de atividades (logs) relacionadas à autenticação de usuários, alteração de configurações do sistema e funcionamento do sistema.~~
Justificativa A Brasscom sugere a exclusão desse dispositivo por dois motivos, sendo um técnico e outro jurídico: 1) Técnico - Na medida em que o fabricante do equipamento não tem controle nem visibilidade de como o usuário de seus equipamentos os utiliza, não caberia a ele registrar os logs de seu uso. 2) Jurídico - Eventual obrigação regulatória nesse sentido pode inclusive levar a questionamentos legais quanto ao descumprimento pelo fabricante do disposto no Marco Civil da Internet aprovado pela Lei nº 12.965/2014. Caso a preocupação da Anatel esteja voltada para o mapeamento de performance da máquina, para fins de identificação de vulnerabilidades em seu funcionamento, sugerimos que sejam feitas alterações na redação para limitar esse registro a comportamentos críticos da performance do equipamento e de seus softwares embutidos, com a anonimização de quaisquer dados pessoais.	

e) Exclusão de requisito quanto a credenciais e senhas iniciais no primeiro acesso ao equipamento (subitem a) do item 5.1.3)

Redação original	Sugestão de redação
Não utilizar credenciais e senhas iniciais para acesso às suas configurações que sejam iguais entre todos os dispositivos produzidos.	~~Não utilizar credenciais e senhas iniciais para acesso às suas configurações que sejam iguais entre todos os dispositivos produzidos.~~
Justificativa	

Equipamentos de baixo custo normalmente vêm com senha padrão comum a todos. Sugerimos a exclusão desse item, visto que o subitem c) já estabelece que seja forçada a alteração da senha de acesso à configuração do equipamento na primeira utilização.

f) Exclusão de requisitos relacionados aos dados sensíveis e informações pessoais (item 5.1.5)

Redação original	Sugestão de redação
Quanto aos dados sensíveis e informações pessoais: a) Possibilitar a utilização de métodos adequados de criptografia para transmissão e armazenamento de dados sensíveis, incluindo informações pessoais. b) Permitir que os usuários deletem facilmente seus dados pessoais armazenados, possibilitando o descarte ou a substituição do equipamento sem riscos de exposição de informações pessoais.	~~Quanto aos dados sensíveis e informações pessoais:~~ ~~a) Possibilitar a utilização de métodos adequados de criptografia para transmissão e armazenamento de dados sensíveis, incluindo informações pessoais.~~ ~~b) Permitir que os usuários deletem facilmente seus dados pessoais armazenados, possibilitando o descarte ou a substituição do equipamento sem riscos de exposição de informações pessoais.~~
Justificativa A Lei Geral de Proteção de Dados (LGPD), aprovada em agosto de 2018, já traz todos os balizadores referentes ao tratamento de dados pessoais, inclusive dos considerados sensíveis, e estabelece a Autoridade Nacional de Proteção de Dados como o órgão responsável pela aplicação da lei. Na medida em que os fabricantes de equipamentos já estão sujeitos a todas as regras estabelecidas na LGPD, sugerimos que esse item seja excluído do ato para evitar a duplicação de regras que potencialmente trariam insegurança jurídica a todos os players da cadeia.	

g) Revisão da periodicidade de atualizações de segurança (item 6.1.4)

Redação original	Sugestão de redação
Prover atualizações de segurança por, no mínimo, 2 (dois) anos após o lançamento	Prover atualizações de segurança ~~por, no mínimo, 2 (dois) anos~~ após o lançamento

do produto ou enquanto o equipamento estiver sendo distribuído ao mercado consumidor, sendo aplicável a opção que mais se estender.	do produto ~~ou~~ e enquanto o equipamento estiver sendo distribuído ao mercado consumidor~~, sendo aplicável a opção que mais se estender~~.
Justificativa Na medida em que há uma extrema variação entre as diversas categorias distintas de equipamento quanto à sua vida útil e necessidade de atualização, a Brasscom sugere que a Anatel proporcione aos fabricantes a flexibilidade de definir a periodicidade e prazo de atualizações de seus equipamentos, inclusive após a descontinuidade da oferta do produto no mercado.	

QUANTO AO PRAZO DE ENTRADA EM VIGOR (Art. 2º)

Redação original	Sugestão de redação
Este Ato entra em vigor 180 (cento e oitenta) dias após a data de sua publicação no Boletim de Serviços Eletrônico da Anatel.	Este Ato entra em vigor 365 (trezentos e sessenta e cinco) ~~180 (cento e oitenta)~~ dias após a data de sua publicação no Boletim de Serviços Eletrônico da Anatel.
Justificativa A Brasscom convida a Anatel a revisar o prazo de entrada em vigor do ato, e alterá-lo para 365 dias, para que as fabricantes de equipamentos possam adotar todas medidas necessárias para estarem em conformidade com o ato. Além disso, sugere que esses requisitos mínimos sejam discutidos recorrentemente, em parceria com a indústria, para garantir que estejam em consonância com as melhores práticas globais, a evolução tecnológica e o estado da arte.	