
ANATEL
Certificação / Homologação
Segurança Cibernética

Certificação e homologação de produtos

- Atualmente a Anatel exige a homologação de **170 tipos de produtos para telecomunicações**:
  - Telefones celulares, ERBs, roteadores, smartwatch, IoT, antenas, cabos fibras óptica, cabos metálicos, baterias de celular, carregadores de celular, centrais telefônicas, transmissores (TV, AM, FM), qualquer equipamento com wifi, bluetooth, etc.

- Cada um desses produtos possuem requisitos técnicos diferentes que são avaliados na certificação (https://www.gov.br/anatel/pt-br/regulado/certificacao/requisitos-tecnicos-para-certificações)

- Muitos desses produtos se conectam às redes de telecomunicações e, por esse motivo, estão expostos ameaças cibernéticas.

Cibersegurança em equipamentos de telecom.

- Equipamentos possuem características técnicas diversificadas (processamentos, memória, interfaces, etc...)
  - Sensor com comunicação sem fio
  - Telefones celulares
  - Equipamentos de *core* de rede
  - (...)

- Diversas aplicações
  - Automação industrial
  - Segurança pública/privada
  - Automação residencial
  - (...)

- Um equipamento pode ter diferentes tipos de aplicações com criticidades diferentes

Requisitos de Segurança Cibernética (Ato 77/21)

- Direcionados a equipamentos homologados pela Anatel:
  - Terminal com conexão à Internet; e
  - Infraestrutura de redes de telecomunicações.

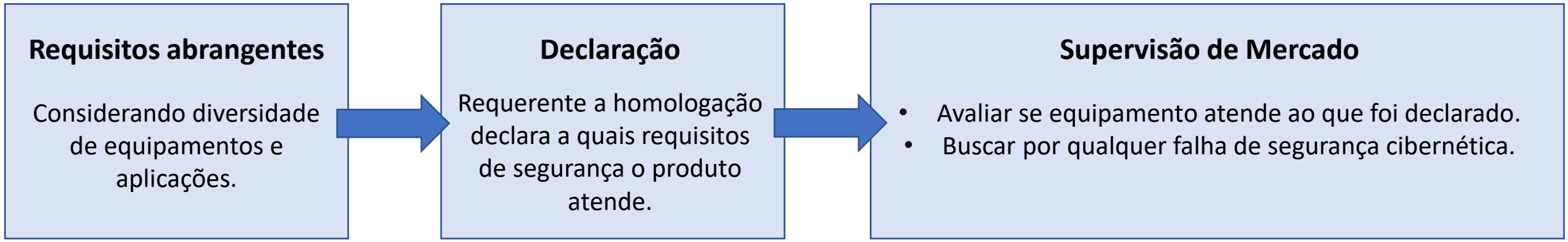
- Requerente à homologação irá declarar a quais requisitos seu equipamento atende.
  - A depender das características técnicas do equipamento e de sua aplicação.
  - Não existe obrigatoriedade em declarar atendimento a todos os requisitos.
  - Contudo, deve ser apresentada justificativa técnica para não atendimento de requisitos.

- Supervisão de mercado → Equip. inseguros terão sua homologação suspensa.

*Ato nº 77, de 05 de janeiro de 2021 (https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77)

Cibersegurança em equipamentos de telecom.

- **Modelo de avaliação adotado:**



- Durante a supervisão de mercado, caso seja identificado qualquer produto que coloque a segurança dos usuários ou das redes de telecomunicações em risco, sua homologação será suspensa.

- Homologação permanecerá suspensa até que falha de segurança seja sanada.

- **Requisitos do Ato 77/21 podem ser definidos como mandatórios para certificação de determinados equipamentos (com base em uma análise de riscos).**

Requisitos de Segurança Cibernética (Ato 77/21)

- **Requisitos para equipamentos:**
  - Quanto à atualização de *software/firmware* (4)
    Ex.: Possuir mecanismos automatizados e seguros para atualização de software/firmware que empregam métodos adequados de criptografia, autenticação e verificação de integridade.
  - Quanto ao gerenciamento remoto (2)
    Ex.: Possuir mecanismo para gerenciamento e administração remotos que empreguem métodos adequados de autenticação e criptografia.
  - Quanto à instalação e à operação (6)
    Ex.: Implementar rotinas simplificadas adequadas para sua instalação e configuração, evitando potenciais falhas de segurança não intencionais
  - Quanto ao acesso para configuração do equipamento (9)
    Ex.: Forçar, na primeira utilização, a alteração da senha inicial de acesso à configuração do equipamento.
  - Quanto aos serviços de comunicação de dados (4)
    Ex.: Estar desprovido de qualquer ferramenta de teste ou *backdoor* utilizados nos processos de desenvolvimento do produto e desnecessários à sua operação usual.
  - Quanto aos dados pessoais e dados pessoais sensíveis (4)
    Ex.: Possibilitar a utilização de métodos adequados de criptografia para a transmissão de dados sensíveis, incluindo informações pessoais.
  - Quanto à capacidade de mitigar ataques (3)
    Implementar mecanismos para validação do endereço de origem dos pacotes de dados, filtrando pacotes com endereço de origem falsificados (filtro *antispoofing*), em especial na transmissão de dados de saída (upload).

Requisitos de Segurança Cibernética (Ato 77/21)

- **Requisitos para fornecedores de equipamentos:**
  - Possuir uma política clara de suporte ao produto, especialmente em relação à disponibilização de atualizações de software/firmware para correção de vulnerabilidades de segurança.
  - Deixar claro para o consumidor até quando e em quais situações serão providas atualizações de segurança para o equipamento.
  - Garantir o provimento de 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.
  - Possuir implementados processos de Divulgação Coordenada de Vulnerabilidades baseados em boas práticas e recomendações reconhecidas internacionalmente.
  - (outros...)


ANATEL
GT-Ciber
Subgrupo de Equipamentos,
Fornecedores e Requisitos

Atribuições do Subgrupo Técnico

- Dentre as atribuições do GT-Ciber previstas na Res. 740/20, algumas estão relacionadas a:
    - Equipamentos;
    - Fornecedores de equipamentos; e
    - Requisitos para certificação de equipamentos.

- **Subgrupo de Equipamentos, Fornecedores e Requisitos** foi criado para tratar destes temas

Atribuições do Subgrupo Técnico

- Atribuições relacionadas a Equipamentos, Fornecedores e Requisitos (1/2):

  - **Acompanhar o surgimento de novas tecnologias e ameaças** para avaliar seu impacto na utilização segura e sustentável das redes e serviços de telecomunicações (Art. 24, IV do Anexo a Res. 740/20);

  - **Elaborar estudos e propor aprimoramentos na regulamentação** e nas decisões administrativas de âmbito setorial em matéria de Segurança Cibernética, inclusive nos procedimentos **relativos à avaliação da conformidade e homologação de produtos para telecomunicações** (Art. 24, VII);

  - Propor, ao Conselho Diretor, a determinação da **observância de requisitos técnicos** e da adoção de medidas específicas **na implementação, operação e manutenção das redes de telecomunicações** quanto à Segurança Cibernética, às prestadoras e demais agentes (Art. 24, XI);

Atribuições do Subgrupo Técnico

- Atribuições relacionadas a Equipamentos, Fornecedores e Requisitos (2/2):

  - Dispor sobre os aspectos e formas de atendimento da obrigação do **Art. 8º do R-Ciber** relacionada à **alteração da configuração padrão de autenticação dos equipamentos fornecidos em regime de comodato** aos usuários (Art. 24, XIII, f); e

  - Dispor sobre os aspectos de forma e procedimento relativos à obrigação da prestadora de utilizar, no âmbito de suas redes e serviços, **produtos e equipamentos de telecomunicações provenientes de fornecedores que possuam política de segurança cibernética** compatíveis com os princípios e diretrizes dispostos neste Regulamento e realizam processos de auditoria independente periódicos (art. 7, § 2°).

Atuações do Subgrupo em 2021

- **Estabelecimento das regras para atendimento ao Art. 8º do Regulamento:**

  "Art. 8º A prestadora deve alterar a **configuração padrão de autenticação** dos equipamentos fornecidos em regime de comodato aos seus usuários."

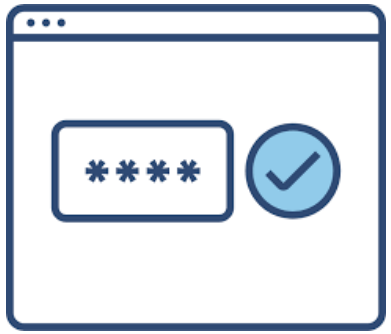
- **Proposta de requisitos mínimos de segurança cibernética para equipamentos CPE**

Alteração da configuração padrão de autenticação

"Art. 8º A prestadora deve alterar a **configuração padrão de autenticação** dos equipamentos fornecidos em regime de comodato aos seus usuários.

Parágrafo único. Cabe ao GT-Ciber estabelecer a **relação dos equipamentos abrangidos** e dispor sobre os aspectos de forma e procedimento relativos à medida de que trata o caput, observado o disposto no art. 24 deste Regulamento."

Configuração padrão de autenticação: login e senha fornecidos de fábrica utilizados para acesso às configurações do equipamento ou para acesso à rede sem fio e que são iguais entre muitas unidades de equipamentos ou que possuem um padrão de construção facilmente identificável.



Alteração da configuração padrão de autenticação

"Art. 8º A prestadora deve alterar a configuração padrão de autenticação dos equipamentos fornecidos em regime de comodato aos seus usuários.

Parágrafo único. Cabe ao GT-Ciber estabelecer a **relação dos equipamentos abrangidos** e dispor sobre os aspectos de forma e procedimento relativos à medida de que trata o caput, observado o disposto no art. 24 deste Regulamento."

Equipamentos abrangidos

- CPEs fornecidos em regime de comodato:
  - Equipamentos novos;
  - Equipamentos já instalados ou em estoque.

Alteração da configuração padrão de autenticação

"Art. 8º A prestadora deve alterar a configuração padrão de autenticação dos equipamentos fornecidos em regime de comodato aos seus usuários.

Parágrafo único. Cabe ao GT-Ciber estabelecer a **relação dos equipamentos abrangidos** e **dispor sobre os aspectos de forma e procedimento relativos à medida** de que trata o caput, observado o disposto no art. 24 deste Regulamento."

Novos:

Mandatório: exigir nos processos de compra:

- equipamentos sem senha padrão
- etiqueta com senha
- possibilidade de restaurar senha de fábrica

Prazo: até 6 meses para prestadoras adequarem seus processos de compra.

Instalados/Estoque:

- Prestadoras deverão adotar medidas para que, de forma gradual, reduzam o quantitativo de equipamentos vulneráveis em sua planta.

Medidas Sugeridas:

- troca de equipamento
- troca de senha (vista técnica, canais digitais ou remotamente)

Requisitos mínimos de seg. ciber. para equipamentos CPE

- **Proposta de requisitos mínimos de segurança cibernética para equipamentos CPE:**
  - Tipos de equipamentos:
    - *Cable* modem;
    - Modem XDSL;
    - ONU, ONT;
    - Roteadores Wi-Fi;
    - FWA SMP
    - Transceptores por satélite / Equipamentos para Estações Terrenas.
  - Será feita uma Consulta Pública para que a sociedade posso contribuir sobre essa proposta de requisitos mandatórios mínimos de segurança cibernética para equipamentos CPE


ANATEL
GT-Open RAN

GT - Open RAN

- Grupo de trabalho criado para estudar a tecnologia Open RAN:
  - Características da tecnologia;
  - Impactos (econômicos, técnicos, etc);
  - Benefícios;
  - Riscos.

- Participantes:
  - Indústria;
  - Operadoras de telecomunicações;
  - Setor acadêmico;
  - Laboratórios de ensaio;
  - Organismos de Certificação Designados.

GT - Open RAN

- **GT Open RAN** foi dividido em subgrupos:
  - Aspectos econômicos;
  - Aspectos regulatórios;
  - Interoperabilidade; e
  - Segurança.

- **OBJETIVO:** realizar estudo abrangente sobre Open-RAN nas diferentes dimensões citadas acima de forma a subsidiar a tomada de decisões da Agência com relação ao tema.

- **Subgrupo de segurança:**
  - Quais aspectos de segurança devem ser considerados além dos já definidos pelo 3GPP para as redes móveis;
  - Quais são os riscos adicionais ao se trabalhar com uma arquitetura aberta;
  - Formas de mitigar esses riscos.

Obrigado!

https://www.gov.br/anatel/pt-br

sor@anatel.gov.br

1331

@AnatelGovBR

@AnatelGovBR

Anatel

anatel_informa

anatelgovbr

@AnatelGovBR

APP Anatel Serviço Móvel

APP Anatel Consumidor