# Ato nº 2436, de 7 de março de 2023

Publicado: Terça, 07 Março 2023 14:18 | Última atualização: Sexta, 17 Janeiro 2025 09:55 | Acessos: 25871

**Observação**: Este texto não substitui o publicado no Boletim de Serviço Eletrônico em 13/3/2023.

**O SUPERINTENDENTE DE OUTORGA E RECURSOS À PRESTAÇÃO DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES**, no uso das atribuições que lhe foram conferidas pela Portaria nº 419, de 24 de maio de 2013, e

CONSIDERANDO a competência dada à Agência pelos Incisos XIII e XIV do Art. 19 da Lei n.º 9.472/97 – Lei Geral de Telecomunicações;

CONSIDERANDO que os Requisitos Técnicos estabelecem os parâmetros e critérios técnicos verificados na Avaliação da Conformidade de um ou mais tipos de produto para telecomunicações, nos termos do art. 22 do Regulamento para Avaliação da Conformidade e Homologação de Produtos para Telecomunicações, aprovado pela Resolução nº 715, de 23 de outubro de 2019; e,

CONSIDERANDO o constante dos autos do processo nº 53500.032306/2022-74;

**RESOLVE:**

Art. 1º Aprovar os requisitos mínimos mandatórios de segurança cibernética para avaliação da conformidade de equipamentos CPE (*Customer Premises Equipment*), na forma do anexo a este Ato.

~~Art. 2º Este Ato entra em vigor em 10 de março de 2024.~~

Art. 2º Este Ato entra em vigor em 1º de julho de 2023, sendo mandatória a aplicação de seu anexo a partir de 10 de março de 2024. (Redação dada pelo Ato nº 7344, de 15 de junho de 2023)

VINICIUS OLIVEIRAA CARAM GUIMARÃES
Superintendente de Outorga e Recursos à Prestação

ANEXO AO ATO Nº 2436, DE 07 DE MARÇO DE 2023

**REQUISITOS MÍNÍNIMOS DE SEGURANÇA CIBERNÉTICA PARA AVALIAÇÃO DA CONFORMIDADE DE EQUIPAMENTOS CPE (*CUSTOMER PREMISES EQUIPMENT*)**

**1. OBJETIVO E ABRANGÊNCIA**

1.1. Estabelecer um conjunto de requisitos mínimos de segurança cibernética de aplicação mandatória para avaliação da conformidade dos seguintes equipamentos CPE de uso do público em geral empregados para conectar assinantes à rede do provedor de serviços de Internet:

a) *Cable* modem;

b) Modem xDSL;

c) ONU, ONT;

d) Roteador ou modem destinados ao acesso fixo sem fio (FWA - *Fixed Wireless Access*);

e) Roteador ou modem destinados ao acesso fixo à banda larga via satélite; e

f) Roteador ou ponto de acesso sem fio.

**2. REFERÊNCIAS NORMATIVAS**

2.1. Regulamento de Avaliação da Conformidade e de Homologação de Produtos para Telecomunicações, aprovado pela Resolução nº 715, de 23 de outubro de 2019;

2.2. Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020;

2.3. Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações, aprovados pelo Ato nº 77, de 05 de janeiro de 2021;

2.4. *NST Special Publication 800-63B - Digital Identity Guidelines - Authentication and Lifecycle Management;*

2.5. *Broadband Forum - TR-181 Issue-2;*

2.6. ISO/IEC 29147:2018 - *Information technology – Security techniques – Vulnerability disclosure;*

2.7. ISO/IEC 30111:2019 - *Information technology – Security techniques – Vulnerability handling processes;*

2.8. *The CERT Guide to Coordinated Vulnerability Disclosure;*

2.9. *FIRST Common Vulnerability Scoring System SIG, The Common Vulnerability Scoring System (CVSS);*

2.10. *Common Vulnerability Enumeration (CVE), The MITRE Corporation, CVE Program.*

**3. DEFINIÇÕES**

3.1. Aplicam-se as definições contidas nas referências normativas 2.1 a 2.3 adicionadas às seguintes:

3.1.1. Dicionário de senhas: arquivo que contém uma lista de palavras e frases comumente utilizadas como senha. O dicionário é composto por senhas obtidas em incidentes de vazamento de dados de autenticação que se tornaram públicos dos quais são extraídas informações estatísticas das senhas mais utilizadas por usuários. O dicionário pode conter, por exemplo, senhas de fácil memorização (ex.: 12345678, abcdefgh, abcde1234, qwerty123, senha12345) ou lista de senhas de associadas a um determinado contexto de aplicação ou de equipamento (ex.: admin123, password, root1234, router123, server123).

3.1.2. Público em geral: qualquer pessoa que utiliza e/ou tem acesso ao produto e que não possui conhecimento técnico especializado sobre o equipamento para telecomunicação e que tem interesse apenas no emprego das suas funcionalidades e no consumo dos serviços de telecomunicação.

~~3.1.3. Senha fraca: senha que não atende simultaneamente os seguintes critérios:~~ (Redação dada pelo Ato nº 45, de 02 janeiro de 2025)

~~a) possuir, no mínimo, 8 caracteres;~~

~~b) conter, pelo menos, uma letra maiúscula, uma letra minúscula, um número e um caractere especial.~~

3.1.3. Senha fraca: senha que não atende ao menos um dos seguintes critérios:

a) possuir, no mínimo, 8 caracteres;

b) conter, pelo menos, uma letra maiúscula, uma letra minúscula e um número.

**4. REQUISITOS PARA AS SENHAS PROVIDAS DE FÁBRICA**

4.1. Os requisitos desta seção aplicam-se às senhas para acesso à interface de configurações do equipamento e para acesso à rede sem fio definidas no processo fabril do equipamento.

4.2. As senhas não podem ser fracas, conforme critérios contidos no item 3.1.3.

4.3. O equipamento deve apresentar conformidade aos seguintes itens dos Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações (Referência 2.3):

a) Não utilizar credenciais e senhas iniciais para acesso às suas configurações que sejam iguais entre todos os dispositivos produzidos.

b) Não utilizar senhas iniciais que sejam derivadas de informações de fácil obtenção por métodos de escaneamento de tráfego de dados em rede, tal como endereços MAC - *Media Access Control*.

c) Não permitir o uso de senhas em branco ou senhas fracas.

4.4. Alternativamente ao atendimento dos requisitos especificados nos itens 4.2 e 4.3, o equipamento poderá forçar, na primeira utilização, a alteração da senha inicial de acesso à sua configuração, conforme Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações (Referência 2.3) e das senhas para acesso à rede sem fio.

4.4.1. Neste caso, a interface de configuração do equipamento deverá exigir que, no ato de sua primeira utilização/configuração ou após um *reset* para suas configurações iniciais de fábrica, o usuário defina novas senhas que atendam aos requisitos estabelecidos no item 5. A operação ou configuração do equipamento só poderá ser realizada após a definição de novas senhas.

4.5. As senhas devem constar em etiqueta no corpo do equipamento e devem ser restauradas sempre que for realizado o *reset* do equipamento para suas configurações iniciais de fábrica.

**5. REQUISITOS PARA AS SENHAS DEFINIDAS PELO USUÁRIO**

5.1. Os requisitos desta seção aplicam-se às funcionalidades do equipamento relacionadas às senhas definidas pelo usuário para acesso à interface de configurações do equipamento e para acesso à rede sem fio.

5.2. O equipamento deve apresentar conformidade aos seguintes requisitos:

a) Não permitir o uso de senhas em branco ou senhas fracas, conforme Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações (Referência 2.3).

b) Garantir que não sejam definidas senhas fracas, conforme critérios contidos no item 3.1.3.

c) O manual do produto, em meio físico ou digital, deve informar as quantidades mínima e máxima de caracteres permitidas para definição de senhas, além da regra para sua formação.

5.3. O equipamento deve implementar verificações que coíbam a definição de senhas fracas ou comumente utilizadas. A verificação pode ser feita por meio de comparação com dicionários de senha, sendo permitida a adoção de outra metodologia.

5.3.1. A metodologia adotada deverá ser informada pelo requerente da homologação ao agente responsável pela avaliação da conformidade do produto.

**6. DEMAIS REQUISITOS DE SEGURANÇA DO EQUIPAMENTO**

6.1. O equipamento deve apresentar conformidade aos seguintes itens dos Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações (Referência 2.3):

a) Possuir mecanismos de defesa contra tentativas exaustivas de acesso não autorizado (ataques de autenticação por força bruta).

b) Não utilizar credenciais, senhas e chaves criptográficas definidas no próprio código fonte do *software/firmware* e que não podem ser alteradas (*hard-coded*).

c) Proteger senhas, chaves de acesso e credenciais armazenadas ou transmitidas utilizando métodos adequados de criptografia ou *hashing*.

d) Implementar rotinas de encerramento de sessões inativas (*timeout*).

e) Ser fornecido com serviços de comunicação de dados (serviço associado a uma porta/port) não usualmente utilizados desabilitados, reduzindo sua superfície de ataque.

f) Facultar ao usuário a possibilidade de desabilitar funcionalidades e serviços de comunicação não essenciais à operação ou ao gerenciamento do equipamento.

6.2. O mecanismo de recuperação de senha, caso implementado no equipamento, deverá ser robusto contra tentativas de roubo de credenciais, conforme item dos Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações (Referência 2.3).

6.2.1. O mecanismo adotado deverá ser informado pelo requerente da homologação ao agente responsável pela avaliação da conformidade do produto.

**7. REQUISITOS QUE DEVEM SER ATENDIDOS PELOS FORNECEDORES DOS EQUIPAMENTOS**

7.1. Os fornecedores dos equipamentos que desempenham função de CPE relacionados em 1.1 devem demonstrar atendimento aos seguintes itens dos Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações (Referência 2.3):

7.1.1. Item 6.1.1 - Possuir uma política clara de suporte ao produto, especialmente em relação à disponibilização de atualizações de *software/firmware* para correção de vulnerabilidades de segurança.

7.1.1.1. A política pode estabelecer condições específicas conforme modelos, linhas ou categorias de produtos e deve descrever as coberturas gerais mínimas válidas para qualquer consumidor que adquirir o produto, seja pessoa física ou jurídica, e deve ser divulgada publicamente por meio de página na Internet.

7.1.1.2. Contratos de suporte com coberturas diferenciadas estão fora do escopo deste requisito.

7.1.2. Item 6.1.2 - Deixar claro para o consumidor até quando e em quais situações serão providas atualizações de segurança para o equipamento.

7.1.2.1. Este item deve compor a política especificada no item 7.1.1.

7.1.3. Item 6.1.4 - 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.

7.1.3.1. Durante este período, as atualizações devem ser providas sem custos adicionais ao consumidor.

7.1.4. Item 6.1.5 - Disponibilizar um canal de comunicação que possibilite aos seus clientes, usuários finais e terceiros notificarem vulnerabilidades de segurança identificadas nos produtos.

7.1.4.1. Este canal deve:

a) ser exclusivo para a notificação de vulnerabilidades; e

b) implementar comunicações seguras como, por exemplo: formulário web com uso de HTTPS, e-mail criptografado com PGP ou outro esquema de chave pública (a chave pública associada ao endereço de e-mail deve ser disponibilizada para que os interessados possam, se assim desejarem, enviar mensagens cifradas).

7.1.5. Item 6.1.6 - Possuir implementado processo de Divulgação Coordenada de Vulnerabilidades baseados em boas práticas e recomendações reconhecidas internacionalmente, tais como as referências 2.6 a 2.8 deste documento.

7.1.5.1. A Política de Divulgação Coordenada de Vulnerabilidade do fornecedor deve ser publicada em sua página na Internet e deve contemplar, no mínimo, os seguintes itens:

a) Os objetivos do fornecedor, suas responsabilidades, bem como o que ele espera de outras partes interessadas.

b) Como deseja ser notificado (ex.: e-mail, formulário em página na Internet) e os respectivos contatos (ex.: endereço de e-mail, URL de formulário web).

c) Detalhamento das opções de comunicação segura (ex.: chave PGP para e-mail, formulário seguro via HTTPS).

d) Quais informações o notificador deve incluir na notificação.

e) O que o notificador deve esperar após reportar uma vulnerabilidade como, por exemplo: reconhecimento do recebimento da notificação, reconhecimento da vulnerabilidade, atualizações na evolução do caso e seus respectivos prazos.

f) Orientação sobre o que está dentro e fora do escopo do processo de notificação, suas limitações, etc.

7.1.6. Item 6.1.7 e seus subitens - Disponibilizar um canal público de suporte, por meio de página na internet em língua portuguesa, para:

a) Informar sobre novas vulnerabilidades identificadas em seus produtos, medidas de mitigação e correções de segurança associadas, com no mínimo as seguintes informações:

- Identificador: código de identificação exclusivo para cada comunicado.

- Título: referência genérica e sucinta referente ao(s) produto(s) afetado(s) e à vulnerabilidade corrigida.

- Visão geral: breve resumo de alto nível sobre a vulnerabilidade para que os usuários possam entender os pontos principais e determinar rapidamente se o aviso é aplicável ao seu ambiente.

- Descrição: descrição com mais informações que permitam aos usuários entenderem como são afetados e avaliarem sua exposição. Não deve fornecer detalhes a ponto de permitir a exploração da vulnerabilidade.

- Produtos afetados: uma lista de produtos afetados conhecidos e suas versões.

- Impacto: informações que descrevam o impacto da vulnerabilidade (por exemplo, negação de serviço, execução de códigos maliciosos) e a criticidade da vulnerabilidade por meio de sistema de pontuação de severidade reconhecido internacionalmente (ex.: CVSS - Referência 2.7).

- Solução (ou Mitigação): informações sobre a ação que os usuários devem realizar para corrigir ou remediar a vulnerabilidade e seu impacto.

- Créditos: reconhecimento ao descobridor (notificador) por relatar a vulnerabilidade e/ou outros envolvidos no processo de solução.

- Histórico de Revisão: versão e data da publicação original. Pode conter um histórico de modificações se o boletim for atualizado posteriormente.

b) Manter histórico de: vulnerabilidades identificadas, medidas de mitigação e correções de segurança;

c) Permitir acesso a correções de segurança e/ou novas versões de software/firmware para seus produtos; e

d) Fornecer manuais e outros materiais com orientações relativas à configuração, atualização e uso seguro dos equipamentos.

7.1.6.1. A fim de garantir a agilidade na disponibilização de informações sobre vulnerabilidades identificadas em produtos, seu fabricante ou fornecedor poderá prover tais informações por meio de página de suporte global na internet em língua inglesa, desde que instruções para acessar tal canal de suporte global estejam disponíveis em português na página do fornecedor nacional.

7.2. A comprovação de conformidade ao conjunto de requisitos contidos em 7.1 poderá ser realizada mediante apresentação da Política de Segurança Cibernética do fornecedor que contemple e comprove atendimento à íntegra dos requisitos.