**Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestruturas Críticas (GT-Ciber)**

**Subgrupo Técnico de Equipamentos, Fornecedores e Requisitos**

# Política de Segurança Cibernética de fornecedores de produtos e equipamentos de telecomunicações para as prestadoras

## 1. Introdução

A Agência Nacional de Telecomunicações (Anatel) publicou em dezembro de 2020 o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Aprovado pela Resolução nº 740, de 21 de dezembro de 2020, o regulamento estabelece uma série de condutas e procedimentos para a promoção da segurança nas redes e serviços de telecomunicações, incluindo a Segurança Cibernética e a proteção das Infraestruturas Críticas de Telecomunicações.

Dentre as definições do regulamento consta a constituição do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestruturas Críticas (GT-Ciber) com objetivo de fomentar discussões sobre segurança cibernética nas redes de telecomunicações e auxiliar na implementação das medidas definidas no regulamento.

O GT-Ciber foi dividido em subgrupos técnicos, sendo um focado em equipamentos para telecomunicações, seus fabricantes/fornecedores e nos requisitos técnicos para certificação. Tal subgrupo foi denominado Subgrupo Técnicos de Equipamentos, Fornecedores e Requisitos.

A este subgrupo foram incumbidas as seguintes atribuições:

- 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, inciso IV do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações);

- 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);

- Dispor sobre os aspectos e formas de atendimento da obrigação 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 no Regulamento e que realizam processos de auditoria independente periódicos (Art. 7, § 2).

Este relatório trata das definições do subgrupo técnico relativas à forma e aos procedimentos relacionados à medida estabelecida no Art. 7º do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações aprovado pela Resolução nº 740, de 21 de dezembro de 2020.

O tema foi debatido nas reuniões do subgrupo técnico realizadas nos dias 27/01/2022, 17/02/2022, 14/04/2022, 28/04/2022, 19/05/2022, 23/06/2022, 21/07/2022 e 11/08/2022, 01/06/2023 e 15/06/2023, resultando na proposta de texto contida no corpo deste documento.

## 2. Referências Normativas

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

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

Lista de Referência de Produtos para Telecomunicações, aprovada pelo Ato nº 7280, de 26 de novembro de 2020 ou por outro documento normativo que venha a substituí-lo.

## 3. Definições

**Auditoria:** processo de verificação sistemática de evidências físicas ou documentais que demonstram as atividades desenvolvidas pelo fabricante ou fornecedor de produtos de telecomunicações em atendimento à Política de Segurança Cibernética definida neste documento. Este processo deve ser realizado por entidade e profissionais habilitados, conforme condições estabelecidas neste documento.

**Auditoria de manutenção:** auditoria com a finalidade de comprovação da manutenção das atividades desenvolvidas pelo fabricante ou fornecedor de produtos de telecomunicações em atendimento à Política de Segurança Cibernética.

**Auditoria complementar:** auditoria focada em itens da Política de Segurança Cibernética que sofreram revisão ou que foram introduzidos ou nas alterações que foram implementadas pelo fabricante no processo de desenvolvimento e fabricação de produtos desde a última auditoria. Tem o propósito de demonstrar a manutenção da conformidade dos processos do fornecedor com a Política de Segurança Cibernética vigente. O relatório da Auditoria complementar é tratado como um adendo ao Relatório de Auditoria do Fornecedor do Produto de Telecomunicações resultante da última auditoria realizada no fornecedor, não afetando sua data de validade.

Fornecedor: é o solicitante da homologação do equipamento para telecomunicações, podendo ser o próprio fabricante nacional do equipamento ou o representante nacional de um fabricante estrangeiro.

Aplicam-se, adicionalmente, as definições contidas nos documentos listados nas referências normativas.

## 4. Objetivos

Este documento visa apresentar as definições do subgrupo técnico quanto aos aspectos de forma e procedimentos relativos ao cumprimento da obrigação especificada no Art. 7º do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, qual seja:

> "Art. 7º A prestadora deve 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.
>
> § 1º Os resultados do processo de auditoria mencionado no caput devem estar disponíveis para a Anatel a qualquer momento, sempre que requisitados.
>
> § 2º Cabe ao GT-Ciber dispor sobre os aspectos de forma e procedimento relativos à medida de que trata o caput, observado o disposto no art. 24 deste Regulamento.

O referido artigo objetiva promover a segurança digital das redes de telecomunicações e de seus usuários exigindo que as prestadoras de serviços utilizem produtos e equipamentos provenientes de fornecedores que possuam política de segurança cibernética e que passam por auditorias periódicas que avaliam o alinhamento de seus processos internos a essa política, com enfoque nos processos de manufatura e seus controles, não abrangendo a avaliação direta da segurança cibernética de equipamentos para telecomunicações específicos.

Conforme estabelecido em seu parágrafo segundo, caberá ao GT-Ciber estabelecer parâmetros mínimos da política de segurança cibernética do fornecedor e o procedimento de auditora aplicável ao atendimento ao Art. 7º.

## 5. Política de Segurança Cibernética do Fornecedor

A Política de Segurança Cibernética do fornecedor de produtos e equipamentos de telecomunicações para as prestadoras deve indicar que seus produtos são projetados, desenvolvidos e fabricados com a observância dos princípios de *security by design*, *privacy by design* e *security by default*, visando:

a) A autenticidade, a confidencialidade e a integridade dos dados transmitidos, processados e armazenados pelos equipamentos;
b) A disponibilidade dos serviços e dos dados sustentados pelos equipamentos.

Adicionalmente, a Política de Segurança Cibernética do fornecedor deve contemplar, no mínimo, os seguintes requisitos do item 6 do Anexo ao Ato nº 77, de 05 de janeiro de 2021:

> "6. REQUISITOS PARA FORNECEDORES DE EQUIPAMENTOS PARA TELECOMUNICAÇÕES

6.1. Requisitos para fornecedores de equipamentos terminais que se conectam à Internet e de equipamentos de infraestrutura de redes de telecomunicações:

> 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.
>
> 6.1.2. Deixar claro para o consumidor até quando e em quais situações serão providas atualizações de segurança para o equipamento.
>
> 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.
>
> 6.1.5. Disponibilizar um canal de comunicação que possibilite aos seus clientes, usuários finais e terceiros reportarem vulnerabilidades de segurança identificadas nos produtos.
>
> 6.1.6. Possuir implementados processos de Divulgação Coordenada de Vulnerabilidades baseados em boas práticas e recomendações reconhecidas internacionalmente.
>
> 6.1.7. 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;
> >
> > 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."

As seguintes ressalvas aos requisitos do item 6 do Ato 77/21 se aplicam à estruturação da Política de Segurança Cibernética do fornecedor de equipamentos de telecomunicações para as prestadoras:

a) A distribuição de equipamentos ao mercado consumidor citada no item 6.1.4 do Ato 77/21 refere-se somente aquelas unidades de produtos disponibilizadas ao mercado nacional pelo requerente da homologação. Não contempla unidades remanescentes na cadeia do comércio após a data do fim da distribuição do produto pelo requerente da homologação.
b) Considerando que as prestadoras possuem equipes técnicas com conhecimento especializado sobre a instalação, a configuração e a utilização dos equipamentos por elas adquiridos, considera-se suficiente que o canal de suporte especificado no item 6.1.7 do Ato 77/21 seja em inglês.

## 6. Auditoria do fornecedor

O fornecedor, para as prestadoras, de produtos e equipamentos de telecomunicações que se enquadrem na abrangência definida no item 8 deste documento deve ser submetido a processos de auditoria independentes, composto por uma auditoria inicial seguida por auditorias de manutenção. Ambas visam comprovar a aplicação da política de segurança cibernética em seus processos internos. Tanto a auditoria inicial, quanto as de manutenção terão validade de 2 anos.

Os procedimentos de auditoria poderão ser realizados de acordo com melhores práticas e padrões técnicos reconhecidos internacionalmente.

Caso o fornecedor da prestadora seja o representante nacional de um fabricante estrangeiro, a auditoria dos seguintes itens da política deve ser realizada mediante apresentação de documentação ou evidências relacionadas aos processos do fabricante:

a) observância dos princípios de *security by design*, *privacy by design* e *security by default*; e
b) itens 6.1.6 e 6.1.7 do Ato 77/21.

Para os demais itens da política, a avaliação da auditoria poderá ser realizada sobre documentação ou evidências relacionadas aos processos do representante nacional ou do fabricante estrangeiro.

Durante o prazo de validade da auditoria, caso os processos de projeto, de desenvolvimento ou de fabricação de produtos do fornecedor sofram alterações, auditorias complementares deverão ser realizadas para comprovar aderência entre os processos do fornecedor e a Política de Segurança Cibernética. Caso a Anatel determine a alteração do conteúdo da Política de Segurança Cibernética do fornecedor, o instrumento que aprovará tal alteração determinará, também, a necessidade ou prazo para realização da auditoria complementar. As auditorias complementares não resultarão em alteração do prazo de validade da auditoria vigente.

As auditorias poderão ser conduzidas por:

a) um dos Organismos de Certificação Designados (OCD) pela Anatel habilitados pela Agência para esta atividade;
b) por qualquer empresa independente que possua acreditação concedida por entidade membro do IAF (*International Accreditation Forum*) com escopo que contemple os itens da política definida no item 5 deste documento; ou
c) por entidades que integram esquemas de certificação desenvolvidos por organismos ou fóruns de normatização técnica internacionalmente reconhecidos que contemplem os itens da política definida no item 5 deste documento.

O procedimento de auditoria deve resultar em relatório(s) que descreva(m) a avaliação de cada item da política do fornecedor e sua conformidade ou não. Caso o procedimento de auditoria ateste total aderência do fornecedor à Política de Segurança Cibernética, o responsável pela condução da auditoria emitirá um atestado de conformidade em favor do fornecedor.

Previamente ao fim da validade do atestado de conformidade vigente, o fornecedor deverá realizar auditoria de manutenção, da qual resultará novo atestado de conformidade comprovando a continuidade de atendimento, por parte do fornecedor, aos itens da Política de Segurança Cibernética definida no item 5 deste documento.

O fornecedor deverá apresentar o atestado de conformidade à prestadora previamente à celebração de contratos de fornecimento dos produtos e equipamentos previstos na abrangência definida no item 8 deste documento. O fornecedor poderá, a seu critério, manter o atestado de conformidade público em sua página na internet.

Para o caso de contratos de fornecimento já firmados e vigentes, com duração residual acima de 4 anos, o fornecedor deverá comprovar conformidade com a política e com as auditorias previstas no Art. 7º do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações a partir de 2 anos a contar da entrada em vigor do procedimento proposto neste documento.

A Anatel, por meio da superintendência competente, irá publicar Ato contendo diretrizes para auditores e fornecedores de equipamentos quanto ao processo de auditoria, referenciando melhores práticas e padrões internacionais como orientadores dos processos de auditoria.

## 7. Atuação das prestadoras

A aquisição pela prestadora de produtos e equipamentos que se enquadrem na abrangência definida no item 8 deste documento estará condicionada à comprovação, pelo fornecedor, de que possui Política de Segurança Cibernética em conformidade com a definida no item 5 e que realiza as auditorias descritas no item 6 deste documento, conforme prevê no Art. 7º do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações

Os novos contratos ou prorrogações e renovações contratuais deverão conter condições que visam garantir que, durante sua vigência, o fornecedor manterá conformidade com à política e com às auditorias definidas neste documento.

Para o caso de contratos de fornecimento já firmados e vigentes, com duração residual acima de 4 anos, a prestadora deverá garantir que o fornecedor estará em conformidade com a política e com as auditorias previstas no Art. 7º do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações a partir de 2 anos a contar da entrada em vigor do procedimento proposto neste documento.

É suficiente, para fins de comprovação de conformidade do fornecedor à política e às auditorias, a apresentação do atestado de conformidade previsto no item 6 deste documento. As prestadoras deverão requerer aos fornecedores a disponibilização dos atestados previamente à celebração dos contratos.

Durante a vigência do contrato, caso fique comprovado pela prestadora que seu fornecedor deixou de apresentar conformidade à política e aos procedimentos de auditoria, novos produtos e equipamentos deste fornecedor não poderão ser adquiridos pela prestadora,

cabendo a esta avaliar, com base em análise de riscos, a manutenção ou retirada dos equipamentos deste fornecedor instalados em sua rede de telecomunicações.

Os resultados dos processos de auditoria dos fornecedores contratados pela prestadora devem estar disponíveis para a Anatel a qualquer momento, sempre que requisitados à prestadora, a quem cabe garantir a disponibilidade dessas informações à Agência em um prazo de até 20 (vinte) dias úteis após demandadas.

## 8. Abrangência

As prestadoras abrangidas pelo art. 7º do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações deverão exigir que seus fornecedores de produtos e equipamentos de telecomunicações relacionados no Anexo I deste documento, a serem utilizados no âmbito de suas redes e serviços, comprovem conformidade com a Política de Segurança Cibernética e com os procedimentos de auditoria descrito nos itens 5 e 6 deste documento.

A lista contida no Anexo I foi elaborada com base na Lista de Referência de Produtos para Telecomunicações (referência 2.3) e poderá ser atualizada a qualquer momento pela Anatel para que passe a contemplar novos produtos e tecnologias, endereçando, assim, vulnerabilidades identificadas em produtos atualmente não incluídos na lista. A alteração da lista será precedida de discussão com entidades interessadas a fim de avaliar os impactos da inclusão de um novo produto.

No caso de atualização do Anexo I, será concedido prazo razoável, a ser debatido entre os interessados, para que prestadoras, fornecedores e demais entidades envolvidas se adequem ao novo texto.

## 9. Entrada em vigor

A partir de 12 meses da publicação do Ato contendo as diretrizes para auditores e fornecedores de equipamentos quanto ao processo de auditoria, especificado no item 6 deste documento, em toda e qualquer aquisição de produtos e equipamentos que se enquadrem na abrangência definida no item 8, as prestadoras deverão garantir que seus fornecedores de produtos e equipamentos de telecomunicações possuam uma Política de Segurança Cibernética alinhada com o item 5 deste documento e que realizem as auditorias previstas no item 6.

**ANEXO I**

**RELAÇÃO DE PRODUTOS ABRANGIDOS PELO ART. 7º DO REGULAMENTO DE SEGURANÇA CIBERNÉTICA APLICADA AO SETOR DE TELECOMUNICAÇÕES**

| FAMÍLIA DE PRODUTOS | TIPO DE PRODUTO |
|---|---|
| **CENTRAIS DE COMUTAÇÃO** | Central de Comutação digital |
| | Central de Comutação e Controle – CCC |
| | Central Privada de Comutação Telefônica - CPCT |
| **EQUIPAMENTOS DE RF (EXCETO RADIODIFUSÃO)** | Femtocélula |
| | Femtocélula Residencial |
| | Transceptor de Radiação Restrita |
| | Transceptor para Estação Rádio Base |
| **EQUIPAMENTOS ÓPTICOS** | OLT – Terminação de Linha Óptica |
| | ONU – Unidade de Rede Óptica |
| | ONT – Terminação de Rede Óptica |
| | Terminal de Linhas Ópticas |
| | Terminal de Linhas Ópticas com Multiplex Integrado |
| **EQUIPAMENTOS PARA COMUNICAÇÃO DE DADOS** | Equipamento de Rede Dados - Ambiente do Usuário |
| | Equipamento para Interconexão de Redes |
| | Equipamento de Rede Dados (exceto para ambiente do usuário) |
| | Plataforma Multi-serviço |
| **EQUIPAMENTOS TERMINAIS** | Equipamento Terminal de Usuário de TV por Assinatura (SeAC) |
| | Modem Digital ADSL |
| | Modem Digital HDSL ou MSDSL |
| | Modem Digital SHDSL |
| | Modem Digital VDSL |
| | Modem Digital VDSL2 |
| | Modem para TV a Cabo (Cable Modem) |
| **EQUIPAMENTOS TERMINAIS IP (COM FIO E SEM FIO)** | ATA – Adaptador para Telefone Analógico (com e sem fio) |