Resolução nº 740, de 21 de dezembro de 2020

Observação: Este texto não substitui o publicado no DOU de 24/12/2020.

O CONSELHO DIRETOR DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, no uso das atribuições que lhe foram conferidas pelo art. 22 da Lei nº 9.472, de 16 de julho de 1997, e pelo art. 35 do Regulamento da Agência Nacional de Telecomunicações, aprovado pelo Decreto nº 2.338, de 7 de outubro de 1997,

CONSIDERANDO os comentários recebidos em decorrência da Consulta Pública nº 52, de 24 de dezembro de 2018, publicada no Diário Oficial da União do dia 26 de dezembro de 2018;

CONSIDERANDO deliberação tomada em sua Reunião nº 894, de 17 de dezembro de 2020;

CONSIDERANDO o constante dos autos do Processo nº 53500.078752/2017-68,

RESOLVE:

Art. 1º Aprovar, na forma do Anexo, o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações.

Art. 2º Esta Resolução entra em vigor no dia 4 de janeiro de 2021.

EMMANOEL CAMPELO DE SOUZA PEREIRA

Presidente do Conselho, Substituto

ANEXO

REGULAMENTO DE SEGURANÇA CIBERNÉTICA APLICADA AO SETOR DE TELECOMUNICAÇÕES

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Seção I

Do Objeto

Art. 1º Este Regulamento tem por objetivo estabelecer 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.

Seção II

Da Abrangência

Art. 2º As disposições deste Regulamento aplicam-se a todas as prestadoras dos serviços de telecomunicações de interesse coletivo, ressalvadas as de Pequeno Porte, conforme conceito definido na regulamentação, observado o disposto neste artigo.

§ 1º O Conselho Diretor da Anatel poderá, motivadamente, incluir ou dispensar, total ou parcialmente, as prestadoras de serviços de telecomunicações de interesse coletivo ou restrito, independentemente do porte, empresas detentoras de direito de exploração de satélite para transporte de sinais de telecomunicações e demais empresas do ecossistema de telecomunicações envolvidos direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços de telecomunicações, da incidência das disposições deste Regulamento.

§ 2º Os princípios elencados no art. 4º e as diretrizes estabelecidas no art. 5º devem ser observados por todas as prestadoras dos serviços de telecomunicações, de interesse coletivo ou restrito, independentemente do porte, ainda que dispensadas do cumprimento das demais disposições deste Regulamento, bem como pelas demais pessoas naturais ou jurídicas envolvidas direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços de telecomunicações.

§ 3º A dispensa da incidência das disposições deste Regulamento não isenta, em qualquer caso, a prestadora do cumprimento de outras disposições legais e regulamentares.

Seção III

Das Definições

Art. 3º Para efeito deste Regulamento, além das definições constantes da regulamentação aplicável aos serviços de telecomunicações, são adotadas as seguintes:

I - Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

II - Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

III - Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

IV - Espaço Cibernético: espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC

e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente;

V - Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

VI - Infraestruturas Críticas de Telecomunicações: instalações, serviços, bens e sistemas, afetos à prestação de serviços de telecomunicações, que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade;

VII - Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

VIII - Interoperabilidade: característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente;

IX - Risco Cibernético: combinação das consequências de um evento associado a incidente futuro que detém o potencial de ocasionar comprometimento ou interrupção de um ou mais sistemas de tecnologia da informação, resultante de falhas ou brechas no sistema de segurança cibernética, e da probabilidade de ocorrência associada;

X - Segurança Cibernética: ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis; e,

XI - Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO II

DOS PRINCÍPIOS E DIRETRIZES EM SEGURANÇA CIBERNÉTICA

Seção I

Dos Princípios

Art. 4º As condutas e procedimentos para a promoção da Segurança Cibernética nas redes e serviços de telecomunicações devem buscar assegurar os seguintes princípios:

I - Autenticidade;

II - Confidencialidade;

III - Disponibilidade;

IV - Diversidade;

V - Integridade;

VI - Interoperabilidade;

VII - Prioridade;

VIII - Responsabilidade; e,

IX - Transparência.

Seção II

Das Diretrizes

Art. 5º As pessoas naturais ou jurídicas envolvidas direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços de telecomunicações devem atuar em Segurança Cibernética observando as seguintes diretrizes:

I - adotar normas e padrões, nacionais ou internacionais, e referências de boas práticas em Segurança Cibernética;

II - atuar com responsabilidade, zelo e transparência;

III - disseminar a cultura de Segurança Cibernética;

IV - buscar a utilização segura e sustentável das redes e serviços de telecomunicações;

V - identificar, proteger, diagnosticar, responder e recuperar de incidentes de Segurança Cibernética;

VI - buscar a cooperação entre os diversos agentes envolvidos com fins de mitigação dos riscos cibernéticos;

VII - respeitar e promover os direitos humanos e as garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação do usuário dos serviços de telecomunicações; e,

VIII - incentivar a adoção de conceitos de *security by design* e *privacy by design* no desenvolvimento e aquisição de produtos e serviços no setor de telecomunicações.

Parágrafo único. No cumprimento das diretrizes será observado o atendimento integral e tempestivo das solicitações apresentadas pela Agência.

CAPÍTULO III

DA SEGURANÇA CIBERNÉTICA NO ÂMBITO DAS REDES E SERVIÇOS DE TELECOMUNICAÇÕES E DA MITIGAÇÃO DE RISCOS EM INFRAESTRUTURAS CRÍTICAS

Seção I

Das Obrigações

Art. 6º A empresa deve elaborar, implementar e manter uma Política de Segurança Cibernética, nos termos da Seção II deste Capítulo.

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.

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.

Art. 9º A prestadora deve notificar à Agência e comunicar às demais prestadoras e aos usuários, conforme o caso e sem prejuízo de outras obrigações legais de comunicação, os incidentes relevantes que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários, nos termos da Seção III deste Capítulo.

Art. 10. A prestadora deve realizar ciclos de avaliação de vulnerabilidades relacionadas à Segurança Cibernética, nos termos da Seção IV deste Capítulo.

Art. 11. A prestadora deve enviar à Anatel informações sobre suas Infraestruturas Críticas de Telecomunicações, nos termos da Seção V deste Capítulo.

Seção II

Da Política de Segurança Cibernética

Art. 12. A Política de Segurança Cibernética dispõe sobre as condutas e procedimentos adotados para a promoção da Segurança Cibernética e mitigação de riscos das Infraestruturas Críticas de Telecomunicações.

Art. 13. A Política de Segurança Cibernética deve ser aderente aos princípios e diretrizes dispostos neste Regulamento, e ainda:

I - ser compatível com a base de clientes, a natureza e a complexidade dos produtos, serviços, atividades, processos e sistemas;

II - ser disseminada aos profissionais e colaboradores das áreas afetas, em seus diversos níveis, papéis e responsabilidades, resguardando-se o compartilhamento de informações sensíveis apenas para as pessoas que exerçam diretamente atividades de planejamento e execução da política, no que couber;

III - estabelecer estrutura interna responsável pela política, com a identificação de pessoas e áreas competentes, bem como ponto focal para contato em eventuais urgências;

IV - designar diretor responsável pela Política de Segurança Cibernética, o qual pode desempenhar outras funções na empresa, desde que não haja conflito de interesses;

V - ser aprovada pelo conselho de administração ou órgão de deliberação colegiado equivalente da empresa;

VI - ser periodicamente atualizada e revisada, sempre que necessário; e

VII - estar disponível à Anatel sempre que solicitada, juntamente com os documentos complementares e os comprovantes de sua aprovação interna pelo órgão competente.

Parágrafo único. Caso a estrutura de governança da Política de Segurança Cibernética seja única para o Grupo Econômico, deve ser identificada a empresa responsável, em níveis e funções, onde aplicável.

Art. 14. A Política de Segurança Cibernética deve contemplar, no mínimo:

I - os objetivos de Segurança Cibernética da empresa;

II - as normas e padrões, nacionais ou internacionais, e as referências de boas práticas em Segurança Cibernética adotados;

III - os procedimentos para a disseminação da cultura de Segurança Cibernética e capacitação dentro da empresa;

IV - o plano de ação com medidas para a conscientização e educação de seus usuários sobre aspectos de Segurança Cibernética;

V - os procedimentos relativos ao armazenamento seguro dos dados de seus usuários, nos termos da legislação e regulamentação;

VI - os procedimentos e controles adotados para a identificação e a análise das vulnerabilidades, das ameaças e dos riscos associados à Segurança Cibernética, às Infraestruturas Críticas de Telecomunicações e à continuidade dos serviços de telecomunicações;

VII - o mapeamento de possíveis riscos de incidentes e de eventos que possam afetar a segurança do armazenamento dos dados dos usuários;

VIII - a hierarquia das Infraestruturas Críticas de Telecomunicações;

IX - os procedimentos e controles adotados para mitigar as vulnerabilidades identificadas conforme os incisos VI, VII e VIII;

X - a avaliação do grau de dependência de fornecedores e a previsão de possíveis impactos operacionais e financeiros em razão dessa dependência;

XI - o plano de resposta a incidentes, definindo ações, recursos e responsabilidades; e,

XII - os procedimentos relativos ao compartilhamento de informações sobre incidentes relevantes e outras informações relativas à Segurança Cibernética.

Art. 15. A prestadora deve publicar, em sua página na Internet, com linguagem compreensível, extrato da sua Política de Segurança Cibernética contendo as informações não sensíveis.

Parágrafo único. Cabe ao GT-Ciber dispor sobre os aspectos de forma e procedimento relativos à publicação de que trata o **caput**, observado o disposto no art. 24 deste Regulamento.

Art. 16. A empresa deve, anualmente ou sempre que solicitado, apresentar à Anatel relatório sobre o acompanhamento de execução da Política de Segurança Cibernética.

Parágrafo único. Cabe ao GT-Ciber dispor sobre os aspectos de forma e procedimento para o relatório de acompanhamento de que trata o **caput**, observado o disposto no art. 24 deste Regulamento.

Seção III

Da Notificação e da Comunicação dos Incidentes Relevantes

Art. 17. A prestadora deve promover, junto à Anatel, a notificação dos incidentes relevantes que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários.

§ 1º A notificação do incidente relevante deve incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso.

§ 2º A notificação do incidente relevante não exime do atendimento de outras obrigações de comunicação previstas em leis, normas e regulamentos.

§ 3º Cabe ao GT-Ciber dispor sobre os aspectos de forma e procedimento para a notificação de que trata este artigo, observado o disposto no art. 24 deste Regulamento.

Art. 18. As prestadoras de serviços de telecomunicações devem adotar procedimento de compartilhamento de informações sobre incidentes relevantes e outras informações relativas à Segurança Cibernética de forma sigilosa e não discriminatória, sendo facultado o anonimato,

incentivando-se a participação de todas as prestadoras de serviços de telecomunicações e buscando a coordenação com as demais entidades relevantes.

Parágrafo único. Cabe ao GT-Ciber dispor sobre os aspectos de forma e procedimento para o compartilhamento de informações de que trata o **caput**, observado o disposto no art. 24 deste Regulamento.

Seção IV

Dos Ciclos de Avaliação de Vulnerabilidades Relacionadas à Segurança Cibernética

Art. 19. Os ciclos de avaliação de vulnerabilidades relacionadas à Segurança Cibernética devem ser realizados por entidade aferidora ou empresa capacitada e independente.

§ 1º Os resultados da avaliação de que trata **caput** devem ser submetidos à Anatel, onde serão tratados de forma sigilosa.

§ 2º Cabe ao GT-Ciber dispor sobre os aspectos de forma e procedimento para a realização dos ciclos de avaliação de vulnerabilidades e apresentação dos resultados mencionados neste artigo, observado o disposto no art. 24 deste Regulamento.

Seção V

Do Envio de Informações sobre Infraestruturas Críticas de Telecomunicações

Art. 20. A prestadora deve enviar informações sobre suas Infraestruturas Críticas de Telecomunicações, abrangendo, no mínimo, dados de rede e mapeamento geográfico das estruturas físicas e rotas.

Parágrafo único. Cabe ao GT-Ciber dispor sobre a identificação das Infraestruturas Críticas de Telecomunicações, observadas as diretrizes governamentais sobre a temática, bem como os aspectos de forma e procedimento relativos ao envio de informações de que trata o **caput**, observado o disposto no art. 24 deste Regulamento.

CAPÍTULO IV

DA ATUAÇÃO DA ANATEL E DO GRUPO TÉCNICO em segurança cibernética

Seção I

Da Atuação da Anatel em Segurança Cibernética

Art. 21. A Anatel promoverá o acompanhamento da Política de Segurança Cibernética das prestadoras, observando as diretrizes e os princípios dispostos neste Regulamento.

Art. 22. Aspectos de Segurança Cibernética devem ser considerados nos procedimentos relativos à avaliação da conformidade e homologação de produtos e equipamentos para telecomunicações, nos termos da regulamentação específica.

Art. 23. Sem prejuízo da adoção de outras medidas necessárias para o cumprimento do disposto neste Regulamento, a Anatel pode, motivadamente, determinar a observação de requisitos técnicos e a adoção de medidas específicas na implementação, operação e manutenção das redes de telecomunicações quanto à Segurança Cibernética.

Seção II

Do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestruturas Críticas

Art. 24. Fica constituído o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber), com as seguintes atribuições, entre outras estabelecidas neste Regulamento:

I - auxiliar a Anatel no acompanhamento da implantação da Política de Segurança Cibernética e da gestão das Infraestruturas Críticas pelas prestadoras;

II - propor, ao Conselho Diretor, condições de inclusão ou dispensa, total ou parcial, das prestadoras de serviços de telecomunicações de interesse coletivo ou restrito, independentemente do porte, empresas detentoras de direito de exploração de satélite para transporte de sinais de telecomunicações e demais empresas do ecossistema de telecomunicações envolvidos direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços de telecomunicações, da incidência das disposições deste Regulamento;

III - propor ações e iniciativas a serem adotadas pelas prestadoras dispensadas do cumprimento das obrigações estabelecidas neste Regulamento, de forma que os princípios e diretrizes nele dispostas sejam seguidos;

IV - acompanhar o surgimento de novas tecnologias e ameaças para avaliar seu impacto na utilização segura e sustentável das redes e serviços de telecomunicações;

V - avaliar e recomendar à Anatel a internalização de padrões, melhores práticas, ações e iniciativas em matéria de Segurança Cibernética de fóruns regionais e internacionais de telecomunicações, em colaboração com as Comissões Brasileiras de Comunicações (CBCs);

VI - interagir com as CBCs para construção e defesa dos posicionamentos brasileiros nos órgãos regionais e internacionais de telecomunicações nos temas referentes à Segurança Cibernética;

VII - 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;

VIII - incentivar ações de capacitação na matéria de Segurança Cibernética;

IX - interagir com outros órgãos e entidades no cumprimento das suas atividades, observada a competência de governança de atuação institucional da Anatel;

X - propor ações de conscientização em colaboração com as áreas responsáveis pela comunicação e relações com consumidores na Anatel;

XI - 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.

XII - dispor sobre a identificação das Infraestruturas Críticas de Telecomunicações, observadas as diretrizes governamentais sobre a temática;

XIII - dispor sobre os aspectos e formas de atendimento das obrigações relacionadas:

a) à publicação pela prestadora, na sua página na Internet, do extrato da Política de Segurança Cibernética;

b) à notificação e ao compartilhamento de informações sobre incidentes relevantes;

c) aos ciclos de avaliação de vulnerabilidades relacionadas à Segurança Cibernética e apresentação de resultados;

d) à apresentação do relatório de acompanhamento da execução da Política de Segurança Cibernética;

e) ao envio de informações sobre as Infraestruturas Críticas de Telecomunicações; e,

f) à alteração da configuração padrão de autenticação dos equipamentos fornecidos em regime de comodato aos usuários;

XIV - solicitar dados e informações das empresas abrangidas por este Regulamento;

XV - acompanhar o procedimento de compartilhamento de informações sobre incidentes relevantes adotado pelas prestadoras;

XVI - elaborar os procedimentos a serem adotados para a proteção do sigilo e a segurança das informações sensíveis, em posse da Anatel, relativas à Política de Segurança Cibernética; e

XVII - desempenhar outras atividades atribuídas pelo Conselho Diretor da Anatel.

§ 1º O GT-Ciber será coordenado por Superintendente designado por Portaria do Conselho Diretor da Anatel.

§ 2º O Superintendente Coordenador poderá organizar o GT-Ciber em subestruturas, de acordo com a conveniência e temática dos trabalhos.

§ 3º O GT-Ciber terá a participação das prestadoras com Poder de Mercado Significativo, definidas conforme a regulamentação específica sobre competição.

§ 4º O Superintendente Coordenador poderá franquear a participação dos representantes das prestadoras ou de suas associações e dos órgãos e entidades afetos, nos temas de interesse dessas empresas, órgãos e entidades.

§ 5º As discussões e deliberações no âmbito do GT-Ciber serão pautadas pelo diálogo e consenso, cabendo a decisão final ao Superintendente Coordenador.

§ 6º Cabe Recurso Administrativo da decisão proferida pelo Superintendente Coordenador do GT-Ciber ao Conselho Diretor da Anatel, conforme disposto no Regimento Interno da Anatel.

CAPÍTULO V

DAS SANÇÕES

Art. 25. A infração a este Regulamento sujeita os infratores às sanções administrativas previstas na Lei nº 9.472, de 16 de julho de 1997, bem como no Regulamento de Aplicação de Sanções Administrativas da Anatel.

Parágrafo único. Considera-se infração a este Regulamento a inobservância de comandos normativos quando não regularizadas em prazo razoável estabelecido pela Agência.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 26. A prestadora é integralmente responsável pelos ônus decorrentes da adoção e execução da Política de Segurança Cibernética e demais condutas e procedimentos exigidos neste Regulamento.

Art. 27. A prestadora deve se adequar ao disposto neste Regulamento em até 180 (cento e oitenta) dias da sua entrada em vigor.