São Paulo, 28 de outubro de 2021

Ao Sr. Emmanoel Campelo de Souza
Presidente do Comitê de Prestadoras de Pequeno Porte de Serviços de Telecomunicações - CPPP

10ª Reunião Ordinária do CPPP

A **TelComp – Associação Brasileira das Prestadoras de Serviços de Telecomunicações Competitivas**, pessoa jurídica de direito privado, com escritório na Av. Iraí, 438, conjunto 45, Moema, São Paulo – SP, inscrita no CNPJ sob o n° 03.611.622/0001-44, representando suas mais de 70 associadas, todas operadoras de telecomunicações, outorgadas pela Anatel, com atuação em todos os segmentos de mercado e em todo o país, apresenta seu relatório, conforme definido na 9ª Reunião do CPPP, sobre o tema a seguir

GT Ciber

A Anatel editou a Resolução nº 740, de 21 de dezembro de 2020, que "*Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações – R-Ciber*". Conforme explicitado pelo I. Relator do processo no Conselho Diretor da Agência, o objetivo do regulamento é promover a segurança cibernética nas redes e serviços de telecomunicações, o que se dará em uma linha de atuação eminentemente técnico-regulatória, integrada a um contexto de ações e esforços de diferentes esferas governamentais, adotando-se medidas proporcionais.

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

Dentre os dispositivos do regulamento, **o artigo 24 dispõe sobre a constituição do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica - GT-Ciber**, tendo entre suas atribuições: 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; e 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 (incisos II e III do art. 24).

A pretensão de criar o GT-Ciber estaria fundamentada, nos termos do voto do I. Relator, na latente característica multidisciplinar da segurança cibernética, que não poderia excluir das obrigações do regulamento agentes importantes da cadeia de telecomunicações.

Além da Resolução nº 740/2020, a Anatel aprovou, também, o Acórdão nº 692, de 21/12/2020, determinando, entre outras coisas, que o GT-Ciber, no prazo de 150 (cento e cinquenta) dias contados da sua instauração: ***i)*** remetesse à Superintendência de Planejamento e Regulamentação (SPR) contribuições à minuta de Resolução com proposta de incluir ou dispensar, total ou parcialmente, da incidência das obrigações em segurança cibernética outros agentes do setor de telecomunicações ainda não abrangidos pelo Regulamento; e, ***ii)*** paralelamente, avaliasse a viabilidade de modelagem complementar à estrutura prevista no Regulamento com vistas à constituição de entidade, ou designação de ente já existente, para creditação de conformidade em boas práticas de segurança cibernética, e, se entender pertinente, proponha as características de sua estruturação, financiamento e relacionamento com a Anatel.

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

O GT-Ciber, então, deu início às atividades, que passaram a ser discutidas em seus Grupos Ad Hoc e Subgrupos, assim definidos:

- Grupos Ad Hoc 1 (Agentes) e 2 (Entidade);
- Subgrupo Técnico de PSC e Gestão de IEC;
- Subgrupo Técnico de Compartilhamento de Informações e Boas Práticas;
- Subgrupo Técnico de Equipamentos, Fornecedores e Requisitos.

Os trabalhos desenvolvidos dentro dos grupos do GT-Ciber estão conduzidos e coordenados pela equipe técnica da Anatel em reuniões periódicas e possui representação das prestadoras NPPPs (TIM, Claro, OI, Telefônica e Sky) e das PPPs (TelComp).

Grupo Ad Hoc 1 – Agentes

O Grupo Ad Hoc 1 – Agentes teve por objetivo avaliar a proposta de incluir ou dispensar, total ou parcialmente, da incidência das obrigações em segurança cibernética previstas no R-Ciber, notadamente nos artigos 6º a 11 da Resolução nº 740/2020, os agentes do ecossistema de telecomunicações envolvidos direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços de telecomunicações, tendo o grupo se reunido e elaborado relatório de todo o processo de discussão.

Ao final das discussões do Grupo, foram apontados os posicionamentos, contribuições e fundamentos de cada membro participante, quais sejam, representantes de NPPPs e das PPPs, sendo que **não houve um consenso** sobre a extensão das obrigações determinadas nos artigos 6º ao 11 da Resolução nº 740/2020 a outros agentes, motivo pelo qual o GT-Ciber deveria dirimir os conflitos de posicionamento para encaminhar as conclusões finais à

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

Superintendência de Planejamento e Regulamentação (SPR), conforme determinado no item "*b.1.1)"* do Acórdão nº 692 de 21 de Dezembro de 2020.

Diante da falta de consenso registrada, conforme relatório SEI nº 7168767, a coordenação do mesmo, exercida pela Anatel, com amparo no § 5º do art. 24 do R-Ciber[1], trouxe sua contribuição, conforme 6.41 do referido Informe:

> *6.41. Como solução para promoção de uma modulação na abrangência das obrigações, sugeriu-se a adoção de uma classificação a incidência de obrigações sobre as prestadoras detentoras de ICT. Assim, sugere-se a criação de três classes de ICT em cuja incidência das obrigações estabelecidas nos arts6.º ao 11 do R-Ciber podem ser gradativamente exigidas. Essas classes podem ser assim descritas:*
>
> *I - Infraestruturas Críticas Classe I – Classe de infraestruturas críticas que, conforme a sua relevância ou nível de criticidade nas redes de telecomunicações, quando detidas por uma determinada prestadora, torna exigível as disposições estabelecidas nos arts. 6º, 7.º, 8.º, 9.º, 10 e do art. 11 do R-Ciber.*
>
> *II - Infraestruturas Críticas Classe II – Classe de infraestruturas críticas que, conforme a sua relevância ou nível de criticidade nas redes de telecomunicações, quando detidas por uma determinada prestadora, torna exigível as disposições estabelecidas no art. 6º, 8.º e do art. 11 do R-Ciber.*
>
> *III - Infraestruturas Críticas Classe III – Classe de infraestruturas críticas que, conforme a sua relevância ou nível de criticidade nas redes de telecomunicações, quando detidas por uma determinada prestadora, torna exigível as disposições estabelecidas no art. 8.º e 11 do R-Ciber.*

O entendimento sobre cada uma das infraestruturas abrangidas pela classificação encontra-se no item 6.47 do referido Informe:

[1] Resolução nº 740/2020.

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

6.47. Quanto à lista de ICT iniciais, sugere-se que sejam incluídas na Classe I, as seguintes infraestruturas (1) Cabo submarino com destino internacional; (2) Prestadores do SMP que detenham rede própria; (3) Rede de suporte para Transporte de tráfego interestadual em mercado de atacado. Explica-se que é considerado cabo submarino com destino internacional os cabos de fibra óptica que interligam qualquer parte do território nacional com uma parte de um território estrangeiro. Considera-se prestadora do SMP que detenha rede própria todas as prestadoras do SMP e as Autorizadas no RV-SMP que possuam qualquer elemento de rede uti lizado na prestação do seu próprio serviço. Considera-se rede de suporte para Trânsito de tráfego interestadual o serviço de comutação e/ou uso de rede interurbana de Prestadora de Serviço Telefônico Fixo Comutado – STFC para encaminhamento de chamadas entre Pontos de Interconexão, entre Áreas Locais distintas, desde que essas áreas estejam em unidades federativas estaduais distintas no território nacional.

Abaixo, temos o quadro resumo do que restou definido pela Agência sobre as obrigações relativas aos artigos 6º ao 11:

OBRIGAÇÕES		AGENTES				
		PROPOSTA				
		NPPP	PPP	PPPIC-I	PPPIC-II	PPPIC-III
Art. 4º	As condutas e procedimentos para a promoção da Segurança Cibernética (...) devem buscar assegurar **princípios.**	INCIDE	INCIDE	INCIDE	INCIDE	INCIDE
Art. 5º	As pessoas naturais ou jurídicas **envolvidas direta ou indiretamente na gestão ou no desenvolvimento** (...) de telecomunicações devem atuar em Segurança Cibernética observando as seguintes **diretrizes**:	INCIDE	INCIDE	INCIDE	INCIDE	INCIDE
Art. 6º	A empresa deve elaborar, implementar e manter uma **Política de Segurança Cibernética**	INCIDE	DISPENSADA	INCIDE	INCIDE	DISPENSADA
Art. 7º	A prestadora deve utilizar(...) produtos e equipamentos (...) provenientes de fornecedores que possuam política de segurança cibernética compatíveis com os princípios e diretrizes (...) e **realizam processos de auditoria independente periódicos.**	INCIDE	DISPENSADA	INCIDE	DISPENSADA	DISPENSADA
Art. 8º	A prestadora deve **alterar a configuração padrão de autenticação** dos equipamentos fornecidos em regime de comodato aos seus usuários.	INCIDE	INCIDE	INCIDE	INCIDE	INCIDE
Art. 9º	A prestadora deve **notificar à Agência e comunicar** às demais prestadoras e aos usuários, (...) os **incidentes relevantes** que afetem de maneira substancial a segurança das redes(...) e dos dados dos usuários	INCIDE	DISPENSADA	INCIDE	DISPENSADA	DISPENSADA
Art. 10.	A prestadora deve **realizar ciclos de avaliação de vulnerabilidades** relacionadas à Segurança Cibernética	INCIDE	DISPENSADA	INCIDE	DISPENSADA	DISPENSADA
Art. 11.	A prestadora deve enviar à Anatel **informações** sobre suas **Infraestruturas Críticas de Telecomunicações**	INCIDE	DISPENSADA	INCIDE	INCIDE	INCIDE

DS
LABDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

Sobre a decisão da Agência, as prestadoras Claro, Vivo, TIM e OI apresentaram recursos administrativos buscando reafirmar seu posicionamento de que as obrigações deveriam se estender a todas as empresas PPPs.

A TelComp, representando todas as PPPs e com a anuência das demais associações representativas, também apresentou recurso, a fim de modular alguns pontos da proposta trazida no Informe da Anatel que são cruciais para o cumprimento das obrigações pelas PPPs. Destacam-se os pedidos finais do recurso apresentado:

(i) que seja aplicada modulação quanto à aplicação das obrigações regulatórias às Prestadoras de Pequeno Porte (PPPs), para que sejam mais aderentes às situações concretas e apliquem-se de fato a infraestruturas críticas, notadamente aos itens (2) e (3) especificados para a Classe I[2];

(ii) que, no caso da aplicação da obrigação prevista no artigo 8° da Resolução nº 740/2020 para as PPPs, seja endereçado, imediatamente, a observação das particularidades da tecnologia e dos protocolos de autenticação empregados pelas prestadoras, de modo que o cumprimento do dispositivo regulatório não impacte a operação, não resulte em vulnerabilidades, mesmo que momentâneas, e que

[2] (2) Prestadores do SMP que detenham rede própria, ou seja: todas as prestadoras do SMP e as Autorizadas no RV-SMP que possuam qualquer elemento de rede utilizado na prestação do seu próprio serviço.

(3) Rede de suporte para Transporte de tráfego interestadual em mercado de atacado, assim considerada a comutação e/ou uso de rede interurbana de Prestadora de Serviço Telefônico Fixo Comutado – STFC para encaminhamento de chamadas entre Pontos de Interconexão, entre Áreas Locais distintas, desde que essas áreas estejam em unidades federativas estaduais distintas no território nacional.

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

seja possível de ser realizada pela prestadora, observadas as particularidades do serviço; e

(iii) que seja conferindo prazo mais extenso (até 18 meses) para a adoção de solução de autenticação prevista no artigo 8º da Resolução nº 740/2020.

Todos os recursos interpostos ainda estão pendentes de julgamento pela Agência.

Grupo Ad Hoc 2 – Entidade

O objetivo do Grupo foi avaliar a viabilidade de modelagem complementar à estrutura prevista no Regulamento com vistas à constituição de entidade, ou designação de ente já existente, para creditação de conformidade em boas práticas de segurança cibernética, e, se entender pertinente, proponha as características de sua estruturação, financiamento e relacionamento com a Anatel.

Após discussões e debates em reuniões dos representantes das NPPPS e PPPs **concluiu-se pelo não cabimento de constituição de entidade para creditar boas práticas de segurança cibernética**.

Subgrupo Técnico de Compartilhamento de Informações e Boas Práticas

O Subgrupo discute as questões relativas à implementação de boas práticas e compartilhamento de informações pelas prestadoras que têm tais obrigações previstas nos artigos 9º e 10 do R-Ciber.

Em reunião plenária, foi apresentada e aprovada a proposta relativa aos dispositivos na forma abaixo:

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

i) Artigo 9º da Resolução 740/2020:

I - Definição de incidentes relevantes para fins de notificação à Agência, a partir de lista exemplificativa de casos de reporte à Agência, sem prejuízo de demais casos que a prestadora julgue pertinente reportar. A lista abrange:

- Vazamentos de dados (dados corporativos ou de clientes);
- Ransomware bem-sucedido;
- Comprometimentos decorrentes de Ameaças Persistentes Avançadas (Advanced Persistent Threat - APT);
- Ataques de Negação de Serviço, considerando os seguintes parâmetros de tráfego e de quantidade de pacotes por segundo: igual ou superior a 50Gbps ou a 20Mpps;
- Problemas de roteamento (sequestro de prefixos, vazamento de rotas e/ou erros de configuração) que venham a ocasionar impacto na entrega de serviços aos clientes das prestadoras, órgãos ou entidades que operam na Internet; e
- Indisponibilidade de serviço causada por incidente de segurança cibernética.

Para os casos que envolvam mais de uma categoria da lista devem ser notificados apenas uma vez.

II - Comunicação aos usuários:

- Considerar-se-á atendida a obrigação de comunicação aos usuários, prevista no art. 9º do Regulamento, com a notificação ao titular de dados para cumprimento da LGPD. Essa notificação suprirá a necessidade de notificação adicional para fins de cumprimento do Regulamento de Segurança Cibernética;

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

- A notificação à ANPD não desobriga/não supre a necessidade de notificação da Anatel; e
- Sempre que houver notificação de consumidor como titular de dados, deve haver a notificação à Anatel (lista exemplificativa – vazamento de dados).

III - Forma de notificação à Agência:

- SEI – criação de área específica para tratamento dos processos. Processos individuais de acompanhamento – peticionamento eletrônico;
- Prazo razoável: prazo de 2 dias úteis, contados da data do conhecimento do incidente;
- Prazo adicional para atendimento do art. 17, § 1º (“A notificação do incidente relevante deve incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso”) - 60 dias.

IV - Definição de Incidentes Relevantes para fins de Compartilhamento entre Prestadoras, a partir de lista exemplificativa, sem prejuízo de outras informações relativas à Segurança Cibernética que a prestadora julgue compartilhar. A lista abrange:

- Compartilhamento de IoCs - Relevantes (ameaças telecomunicações);
- Compartilhamento de IoCs – Ramsonware;
- Compartilhamento de IoCs – Principais atacantes DDoS;
- Compartilhamento de IoCs - Servidores de DNS maliciosos; e
- Compartilhamento de IoCs – VoIP.

V – Forma de Compartilhamento:

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

- MISP – Criação de sharing group das prestadoras – eventos compartilhados por qualquer instância do grupo é enviada a todas instâncias;
- Atendimento do art. 18 – incentivo a demais prestadoras: criação de instâncias MISP para associações representativas das PPPs; criação de sharing group para cada uma dessas associações. Associações teriam suas instâncias participando do sharing group das prestadoras não PPPs e poderiam compartilhar os eventos recebidos nesse grupo com o seu. Eventualmente, casos compartilhados pelas PPPs poderiam ser anonimizados pela Associação, caso necessário, e vice-versa, e também compartilhados no grupo; e
- Compartilhamento do CERT.br para prestadoras atualmente vigente permanece inalterado.

VI – Prazo de Adaptação para as obrigações de notificação da Anatel, comunicação dos usuários e compartilhamento

- Prazo de 90 dias, contados da deliberação.

ii) Artigo 10 da Resolução 740/2021:

I - As prestadoras sobre as quais incida a obrigação contida no art. 10 do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, para atender ao disposto no parágrafo único deste artigo, devem apresentar para a Anatel os documentos abaixo relacionados:

- Relatório Executivo sobre o Processo de Gestão de Vulnerabilidades no âmbito da empresa abordando, no mínimo: (a) as atividades de avaliação que são realizadas; (b) os responsáveis pela avaliação; (c) quando aplicável, as empresas externas que realizam as avaliações, sua

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

qualificação e o escopo dos contratos; e, (d) um resumo executivo dos resultados encontrados;

- Os itens (c) e (d) podem ser excluídos dos relatórios da prestadora no caso de encaminhamento de relatório executivo da própria empresa externa; e
- Relatório Executivo de avaliação, realizada por empresa capacitada e independente, sobre os processos adotados pelas prestadoras, para identificar as vulnerabilidades nos elementos de infraestruturas publicamente acessíveis via Internet (TI), com o intuito de validar o processo de avaliação de vulnerabilidade praticado pela prestadora nestes elementos.

II - Forma de atendimento e periodicidade:

- Utilização do Sistema Eletrônico de Informações (SEI), com processos individuais de acompanhamento para cada prestadora;
- A entrega das informações dar-se-á anualmente, sempre no mês de abril, a fim de escalonar a entrega de informações ao GT-Ciber, referindo-se à(s) avaliação(ões) realizada(s) dentro do período dos últimos 12 (doze) meses. Excepcionalmente, a primeira entrega poderá ser até junho de 2022; e
- O Relatório Executivo sobre o Processo de Gestão de Vulnerabilidades no âmbito da empresa e os relatórios executivos de empresas externas mencionados nos itens 1 e 2 devem abranger as avaliações de vulnerabilidades realizadas a partir de 1° de janeiro de 2022 e, preferencialmente, também contemplar avaliações realizadas a partir de 1° de janeiro de 2021, caso possível.

DS
UABDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

Já a proposta de forma de envio de informações sobre as Infraestruturas Críticas de Telecomunicações, prevista no art. 11 do R-Ciber ainda não foi aprovada pelo GT-Ciber.

Subgrupo Técnico de Equipamentos, Fornecedores e Requisitos.

Este Subgrupo discute a implementação dos dispositivos que tratam dos equipamentos, fornecedores e requisitos, notadamente os do artigo 8º da Resolução nº 740/2020.

O atendimento ao art. 8º do R-Ciber foi objeto de debate em 7 reuniões do subgrupo e contou com representantes de:

- Prestadoras
- Indústria
- Setor acadêmico
- Laboratórios de ensaio
- Organismos de Certificação Designados
- Governo

Consenso do subgrupo quanto às medidas propostas para atendimento ao art. 8º:

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.

Equipamentos abrangidos:

- CPEs fornecidos em regime de comodato:

DS
LHBDS

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

- Equipamentos novos;
- Equipamentos já instalados ou em estoque.

Definição de CPE (conforme Ato 77/21):

- "3.3. Customer Premise Equipment (CPE): equipamento utilizado para conectar assinantes à rede do provedor de serviços de telecomunicações. Para fins de aplicação deste conjunto de requisitos, CPE deve ser considerado o equipamento associado aos serviços fixos de telecomunicações."

Aspectos de forma e procedimento:

Equipamentos novos:

- Mandatório: exigir nos processos de compra:

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

- Não mandatório:

✓ implementar acessos diferenciados às suas configurações para operadora e usuário;
✓ informações de segurança no aparelho.

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

DS
LHBDS

Equipamentos instalados/estoque:

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br

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

- Relatório sugere medidas:
- ✓ troca de equipamento
- ✓ troca de senha (vista técnica, canais digitais ou remotamente)

- Acompanhamento:
- ✓ 90 dias: prestadoras NPPP apresentem planejamento.
- ✓ NPPP deverá apresentar relatório semestral.

Conclusão:

Esperamos que estas considerações sejam eficientes para as análises deste Comitê e também para Anatel, de forma a que contribuam para os melhores encaminhamentos sobre tema tão importante para as telecomunicações.

Atenciosamente,

DocuSigned by:
Luiz Henrique Barbosa da Silva
78DB6418193D4D2...

Luiz Henrique Barbosa da Silva
Presidente-Executivo
TelComp – Associação Brasileira das Prestadoras
de Serviços de Telecomunicações Competitivas

Av. Iraí, 438 • 4° andar • cjs. 44 a 47 • Moema • São Paulo - SP • CEP 04082-001
Fone: 55 11 5533.8399 • www.telcomp.org.br