PLANO SETORIAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

Setor de Telecomunicações – Versão 1.0

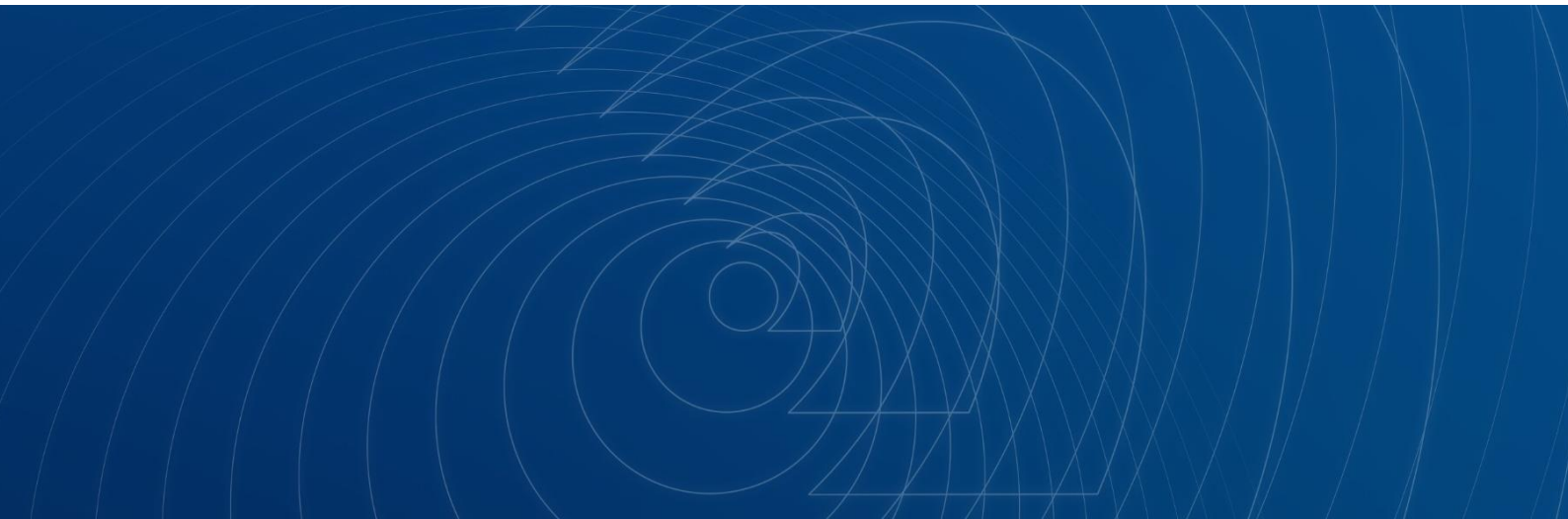
ANATEL
Agência Nacional de Telecomunicações

PLANO SETORIAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

Setor de Telecomunicações – Versão 1.0

Agência Nacional
de Telecomunicações

SAUS Quadra 06
Blocos C, E, F e H
CEP 70070-940
Brasília/DF



SUMÁRIO

1. APRESENTAÇÃO

O presente documento contém o Plano Setorial de Gestão de Incidentes Cibernéticos para o Setor de Telecomunicações, em atendimento ao Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

O Plano foi elaborado de forma colaborativa no âmbito do Setor de Telecomunicações, utilizando-se do fórum do Grupo de Estudos do Exercício do Guardião Cibernético 4.0 (EGC 4.0)1, bem como da estrutura do Subgrupo Técnico de Compartilhamento de Informações e Boas Práticas do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) da Agência e construído com base nas deliberações do GT-Ciber.

O GT-Ciber foi constituído pelo Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber), aprovado pela Resolução nº 740, de 21 de dezembro de 2020, da Agência, possuindo uma série de atribuições relacionadas ao acompanhamento da Política de Segurança Cibernética e Gestão de Infraestrutura Crítica; à elaboração das definições complementares para implementação do R-Ciber; à conscientização, capacitação, estudos e interação com as Comissões Brasileiras de Comunicações (CBCs); dentre outras.

Ressalta-se que a elaboração do Plano contou com a realização de evento presencial específico, no dia 21 de junho de 2022, na sede do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), em São Paulo, e contou com a participação de representantes da Anatel que integram o GT-Ciber; das prestadoras de telecomunicações participantes do EGC 4.0; do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br); do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov); do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República e de professores da Universidade Federal de Campina Grande e Universidade Estadual da Paraíba.

O Plano foi objeto de estudo e desenvolvimento do Grupo de Estudos do EGC 4.0 e será apresentado como resultado na Análise Pós-Ação do evento no dia 19 de agosto de 2022.

[1] O Exercício Guardião Cibernético é o maior exercício de defesa cibernética do hemisfério sul, o qual tem por objetivo criar um ambiente realista onde as infraestruturas críticas participantes precisam proteger seus sistemas de Tecnologia da Informação de ataques cibernéticos, contribuindo para o crescimento da resiliência cibernética das infraestruturas críticas do Brasil. A quarta edição será realizada de 16 a 19 de agosto de 2022.

2. REFERÊNCIAS

2.1 Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos - https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022;

2.2 Norma Complementar nº 05/IN01/DSIC/GSIPR, homologada pela Portaria nº 38, de 14 de agosto de 2009, do Diretor do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=17/08/2009&jornal=1&pagina=8&totalArquivos=108;

2.3 Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020 - https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740;

2.4 Plano Geral de Metas de Competição (PGMC), aprovado pela Resolução nº 600, de 8 de novembro de 2012, com alterações aprovadas pela Resolução nº 694, de 17 de julho de 2018 - https://informacoes.anatel.gov.br/legislacao/resolucoes/34-2012/425-resolucao-600;

2.5 Ato nº 6.359, de 18 de outubro de 2019 do Conselho Diretor da Agência, que declara quais empresas não são consideradas Prestadoras de Pequeno Porte – SEI nº 4773304;

2.6 Portaria Anatel nº 2.156, de 8 de dezembro de 2021, que aprova os procedimentos a serem adotados para a proteção do sigilo e a segurança das informações sensíveis relacionadas ao Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) e para o acompanhamento das obrigações do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber), aprovado pela Resolução nº 740, de 21 de dezembro de 2020;

2.7 Despacho Decisório nº 49/2021/COQL/SCO, de 10 de setembro de 2021, que trata da obrigação das prestadoras relacionada à notificação da Agência e à comunicação às demais prestadoras e aos usuários sobre os incidentes relevantes que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários;

2.8 Despacho Decisório nº 69/2022/COQL/SCO, de 12 de abril de 2022, que trata da obrigação das prestadoras relacionada à notificação de incidentes;

2.9 *Traffic Light Protocol* (TLP). *FIRST Standards Definitions and Usage Guidance*. Versão 2.0 - https://www.first.org/tlp/; e

2.10 *The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities* - https://resources.sei.cmu.edu/asset_files/TechnicalReport/2021_005_001_734796.pdf.

3. DEFINIÇÕES

Cabe trazer algumas definições do Decreto nº 10.748, de 16 de julho de 2021, do R-Ciber e do GT-Ciber:

1. Equipe de Coordenação Setorial (ETIR Setorial): "*equipe de prevenção, tratamento e resposta a incidentes cibernéticos das agências reguladoras, do Banco Central do Brasil ou da Comissão Nacional de Energia Nuclear ou das suas entidades reguladas responsáveis por coordenar as atividades de segurança cibernética e de centralizar as notificações de incidentes das demais equipes do setor regulado*", nos termos do art. 4º, II, do Decreto;

2. Equipes Principais (ETIRs Principais): "*equipes de prevenção, tratamento e resposta a incidentes cibernéticos de entidades, públicas ou privadas, responsáveis por ativos de informação, em especial aqueles relativos a serviços essenciais, cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade, nos termos do disposto no inciso I do parágrafo único do art. 1º do Anexo ao Decreto nº 9.573, de 22 de novembro de 2018*", nos termos nos termos do art. 4º, III, do Decreto;

3. Incidentes Relevantes para fins de compartilhamento: lista exemplificativa de casos de comunicação às demais prestadoras que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários, a qual abrange, nos termos do Despacho Decisório nº 49/2021/COQL/SCO, de 10 de setembro de 2021, os seguintes Indicadores de Comprometimentos (IoCs), sem prejuízo de outras informações relativas à segurança cibernética que a prestadora julgue pertinente compartilhar:

    - Compartilhamento de Indicadores de Comprometimentos (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.

4. Incidentes Relevantes para fins de notificação à Agência: lista exemplificativa de casos de reporte à Agência que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários, a qual abrange, nos termos do Despacho Decisório nº 49/2021/COQL/SCO, de 10 de setembro de 2021, os seguintes incidentes:

    - Vazamentos de dados (dados corporativos ou de clientes);
    - *Ransomwares* bem-sucedidos;

- 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.

5. Plano Setorial: "*planos que orientam as equipes nas agências reguladoras, no Banco Central do Brasil, na Comissão Nacional de Energia Nuclear ou nas suas entidades reguladas sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos inerentes ao setor específico*", nos termos do art. 4º, VII, do Decreto; e

6. Prestadora de Pequeno Porte (PPP): prestadoras que compõem "*grupo detentor de participação no mercado nacional inferior a 5% (cinco por cento) em cada mercado de varejo que atua*", nos termos do art. 4º, XV, do Plano Geral de Metas de Competição – PGMC, com redação dada pela Resolução nº 694, de 17 de julho de 2018.

4. CONTEXTO NORMATIVO

O Decreto nº 10.748, de 16 de julho de 2021, institui a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), a qual tem por finalidade "*aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação*".

A ReGIC será composta pelo CTIR Gov, pelas equipes de prevenção, tratamento e resposta a incidentes cibernéticos (ETIRs) dos órgãos e entidades da administração pública federal; equipes de coordenação setorial; e equipe principais.

O Decreto também traz atribuições às agências reguladora e à Anatel compete, nos termos do art. 13:

> I - instituir ou designar equipe de coordenação setorial, nos termos do disposto no inciso II do caput do art. 4º;
>
> II - apoiar as atividades de suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, nos termos do disposto no Decreto nº 9.637, de 2018;
>
> III - identificar as equipes principais das áreas prioritárias sob a sua regulação, nos termos do disposto no inciso III e IV do caput do art. 4º;
>
> IV - requerer às equipes principais identificadas, por meio da equipe de coordenação setorial, as notificações sobre os incidentes cibernéticos de maior impacto;
>
> V - notificar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, por meio da equipe de coordenação setorial, quanto aos incidentes cibernéticos de maior impacto, com base nas informações obtidas das equipes de prevenção, tratamento e resposta a incidentes cibernéticos das entidades sob a sua regulação;
>
> VI - analisar os riscos cibernéticos que deverão constar do plano setorial de gestão de incidentes cibernéticos específico;
>
> VII - estabelecer a sua forma de articulação com a equipe de coordenação setorial;
>
> VIII - identificar outras entidades, públicas ou privadas, relevantes para a segurança cibernética em sua área prioritária;
>
> IX - fornecer informações relativas às equipes de prevenção, tratamento e resposta a incidentes cibernéticos das entidades de que trata o inciso VIII, que deverão constar do plano setorial de gestão de incidentes cibernéticos; e
>
> X - identificar as infraestruturas críticas de suas áreas prioritárias que requeiram atenção em termos de segurança cibernética nacional.

Dessa forma, a Anatel, como Agência Reguladora, instituirá a ETIR Setorial com as seguintes competências, previstas no art. 14: elaborar o plano setorial de gestão de incidentes cibernéticos; e coordenar as atividades e centralizar as notificações de incidentes recebidas das demais ETIRs sob a sua coordenação. Ademais, também é atribuição da ETIR obedecer ao disposto nas normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Cabe aclarar que o presente Plano aborda tão somente a ETIR Setorial da Anatel, não contemplando a ETIR da Agência responsável pela prevenção, tratamento e resposta de incidentes cibernéticos da Anatel, como entidade que compõe a Administração Pública Federal. Destaca-se, por fim, que o Plano setorial se constitui como o elemento primordial da atuação da ETIR Setorial direcionando as suas atividades.

5. OBJETIVOS

Os objetivos da ReGIC estão descritos no art. 3º do Decreto nº 10.748, de 16 de julho de 2021:

I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;

III - divulgar informações sobre ataques cibernéticos;

IV - promover a cooperação entre os participantes da Rede; e

V - promover a celeridade na resposta a incidentes cibernéticos.

Especificamente para o Setor de Telecomunicações, além dos objetivos supracitados, corrobora-se especialmente a promoção das diretrizes de identificar, proteger, diagnosticar, responder e recuperar de incidentes de Segurança Cibernética, bem como de buscar a cooperação entre os diversos agentes envolvidos com fins de mitigação dos riscos cibernéticos, constantes do art. 5°, V e VI, do R-Ciber, também incentivando o compartilhamento de informações por todas as prestadoras de telecomunicações, independentemente do seu porte, em atendimento ao art. 18 do R-Ciber, e, assim, contribuindo para a segurança e resiliência das redes e serviços de telecomunicações, bem como para a proteção das suas Infraestruturas Críticas.

6. COMPOSIÇÃO

No setor de telecomunicação, a ETIR Setorial será instituída pela Anatel e composta por servidores integrantes dos seus quadros, a qual será estabelecida atendendo à Norma Complementar nº 05/IN01/DSIC/GSIPR, homologada pela Portaria nº 38, de 14 de agosto de 2009, do Diretor do Departamento de Segurança da Informação e Comunicações do GSI/PR, que disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.

A ETIR Setorial será instituída por instrumento próprio em apartado seguindo os trâmites administrativos da Agência, não integrando o presente plano. Além da ETIR Setorial, a rede do setor de telecomunicações será integrada pelas ETIRs Principais e por outras ETIRs interessadas do setor de telecomunicações.

A participação das ETIRs Principais é obrigatória e a identificação dessas equipes no setor de telecomunicações coincide, inicialmente, com as entidades sobre as quais as obrigações do R-Ciber recaem, atualmente as prestadoras dos serviços de telecomunicações de interesse coletivo que não são de pequeno porte, ou seja, pertencentes aos Grupos Econômicos Claro, Oi, Telefônica, Tim e Sky, nos termos do Ato nº 6.359, de 18 de outubro de 2019 do Conselho Diretor da Agência (SEI nº 4773304).

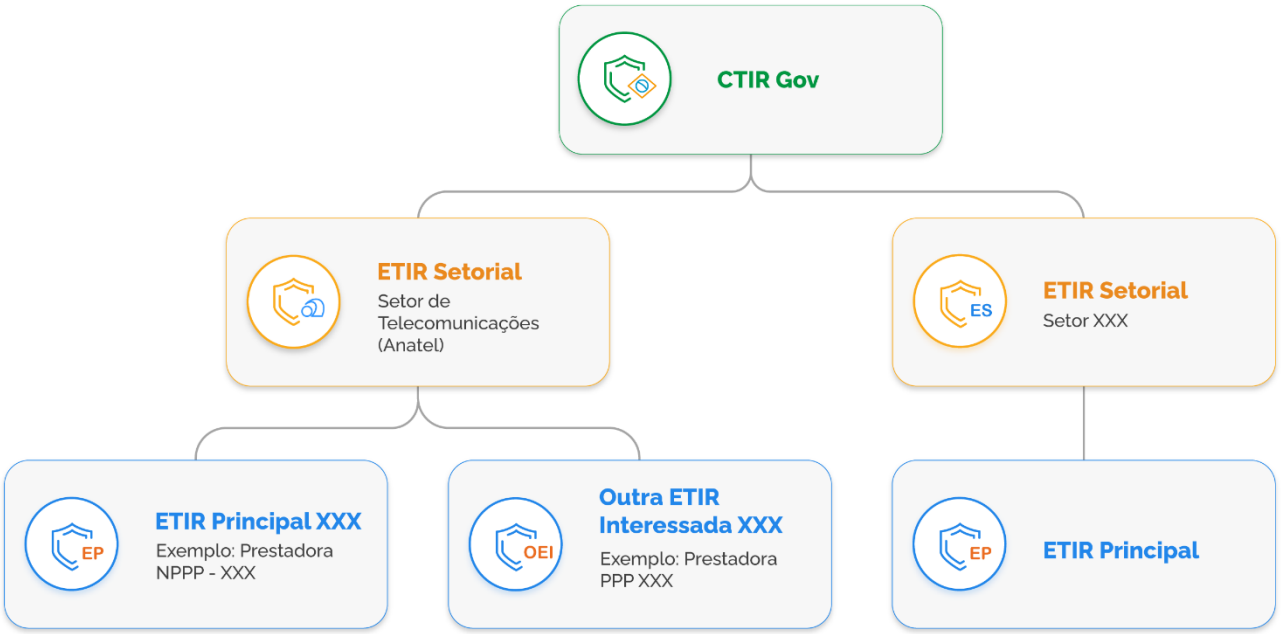
Eventual modificação na abrangência do R-Ciber (extensão das obrigações) automaticamente refletirá na condição de ETIR Principal. Por exemplo, se uma empresa passa a ser obrigada a cumprir arts. 6º ao 11 do R-Ciber, ela, automaticamente, passa a ser considerada como ETIR Principal, participando, portanto, obrigatoriamente da rede.

Demais ETIRs pertencentes ao setor regulado podem voluntariamente participar da rede do setor. Para tal, deverão solicitar à Coordenação Setorial o seu ingresso, a quem caberá a avaliação de ingresso, permanência e exclusão das ETIRs na rede.

As ETIRs integrantes do setor, sejam ETIRs Principais ou outras ETIRs interessadas, participarão da ReGIC por intermédio da ETIR Setorial, que se posicionará como elo entre a Rede e as equipes do setor de telecomunicações.

A adesão à organização setorial para participação na ReGIC exige como pré-requisitos a existência de uma ETIR formalizada e em operação no ente regulado, bem como a utilização de uma instância do *Open Source Threat Intelligence Platform* (MISP).

O fluxograma a seguir apresenta a organização de participação das ETIRs do Setor de Telecomunicações na ReGIC:



7. COMUNICAÇÃO

A comunicação entre a ETIR Setorial e demais ETIRs do setor de telecomunicações (ETIRs Principais e outras ETIRs interessadas) será realizada por diversos canais, incluindo a criação de um Fórum das ETIRs do setor e a utilização de e-mail, podendo ser criados outros canais conforme o andamento dos trabalhos.

Os procedimentos estabelecidos para notificação de incidentes relevantes à Agência e compartilhamento de incidentes relevantes entre prestadoras, construídos no âmbito do GT-Ciber em atendimento ao R-Ciber, permanecem inalterados, inclusive quanto aos procedimentos a serem adotados para a proteção do sigilo e a segurança das informações sensíveis relacionadas ao GT-Ciber e ao acompanhamento das obrigações do R-Ciber, aprovados pela Portaria Anatel nº 2.156, de 8 de dezembro de 2021.

O Fórum das ETIRs será abarcado pela estrutura existente do Subgrupo Técnico de Compartilhamento de Informações e Boas Práticas do GT-Ciber, o qual já se reúne com periodicidade adequada.

Cada ETIR participante deverá indicar 2 (dois) representantes à ETIR Setorial, existindo o compromisso de atualização tempestiva dos mesmos, além do canal oficial para acionamento da respectiva ETIR, inclusive com a previsão de contato para escalonamento.

Da forma semelhante, a ETIR Setorial criará e-mail específico para recebimento e encaminhamento de alertas, comunicados, agendamento de reuniões, etc.

O campo de assunto dos e-mails utilizará padrão a ser definido pelo Fórum das ETIRs, que também será responsável pela elaboração de outras definições relacionadas à operacionalização da ReGIC.

As comunicações (e-mails e documentos compartilhados por e-mail, em reuniões ou em outros canais de comunicação) utilizarão o padrão *Trafic Light Protocol* (TLP) do *Forum of Incident Reponse and Security Teams* (FIRST), a fim de permitir o adequado compartilhamento de informações, sendo que o Fórum das ETIRs detalhará e fomentará o uso do TLP.

As ETIRs Principais e outras ETIRs interessadas utilizarão chave pública disponibilizada pela ETIR Setorial para criptografar informações do conteúdo de e-mails e documentos designados como TLP:RED, TLP:AMBER+STRICT e TLP:AMBER.

As informações compartilhadas na Rede deverão ser sanitizadas pela Anatel antes do envio à ReGIC, a fim de proteger dados técnicos, operacionais e financeiros das empresas. Os critérios de sanitização serão definidos em comum acordo pelo Fórum das ETIRs.

8. COMPARTILHAMENTO DE INFORMAÇÕES

O MISP será a plataforma para compartilhamento de informações sobre ameaças e vulnerabilidades no setor de telecomunicações, destacando-se que essa plataforma já é utilizada pelas prestadoras que cumprem as obrigações do R-Ciber. O *Sharing Group* existente será ampliado para contemplar o ingresso das outras ETIRs interessadas do setor que desejem em participar desse ecossistema de compartilhamento.

Os IOCs compartilhados deverão compreender no mínimo aqueles já definidos no âmbito do GT-Ciber para cumprimento da obrigação das prestadoras relacionada à comunicação às demais prestadoras sobre os incidentes relevantes que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários, nos termos do art. 9º do R-Ciber. Os IOCs para compartilhamento com outros setores serão definidos pelo Fórum das ETIRs e revisados sempre que necessário.

Também será estabelecido compartilhamento de informações entre as ETIRs do setor e a ETIR Setorial, para o envio e recebimento de informações dos outros setores da REGIC, consoante orientações acordadas pelo Fórum das ETIRs.

9. NOTIFICAÇÃO DE INCIDENTES

A notificação de incidentes relevantes já é uma realidade no setor de telecomunicações desde novembro de 2021, quando foi esgotado o prazo de adaptação às definições elaboradas para cumprimento pelas prestadoras da obrigação relacionada à notificação da Agência sobre os incidentes relevantes que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários, prevista no art. 9º do R-Ciber e detalhada no Despacho Decisório nº 49/2021/COQL/SCO, de 10 de setembro de 2021.

Esse arcabouço existente será a base para a notificação de incidentes ao CTIR GOV e a ETIR Setorial fará a transposição das informações relevantes sobre os incidentes notificados à Agência para encaminhamento à REGIC, seguindo as regras de sanitização estabelecidas no âmbito do Fórum das ETIRs.

O Despacho Decisório nº 49/2021/COQL/SCO, de 10 de setembro de 2021, estabeleceu que a definição de incidentes relevantes para fins de notificação à Agência abrange vazamentos de dados (corporativos e pessoais). No entanto, somente os demais casos exemplificados na lista serão objeto de notificação (*ransomwares* bem-sucedidos; comprometimentos decorrentes de Ameaças Persistentes Avançadas; 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).

As outras ETIRs interessadas, que não estão obrigadas a notificar incidentes cibernéticos por força do R-Ciber, visando a colaboração na busca de maior segurança e resiliência das redes, poderão fazer notificação voluntária de seus incidentes, seguindo definições aprovadas pelo GT-Ciber e orientações da ETIR Setorial.

A notificação de incidentes deverá ser o mais célere possível, especialmente nos casos onde este possa auxiliar outros integrantes da ReGIC na proteção e resiliência das suas redes.

10. ANÁLISE DE RISCOS CIBERNÉTICOS

O art. 13, VI, do Decreto nº 10.748, de 16 de julho de 2021, determina que compete às agências reguladoras a análise dos riscos cibernéticos que deverão constar do Plano Setorial de Gestão de Incidentes Cibernéticos. Nesse ponto, cabe ressaltar que o R-Ciber prevê como conteúdo mínimo da Política de Segurança Cibernética (a ser elaborada, implementada e mantida pelas prestadoras obrigadas) os procedimentos e controles para a identificação dos riscos; mapeamento de possíveis riscos de incidentes; e procedimentos e controles adotados para a sua mitigação (art. 14, VI, VII e IX do R-Ciber).

Dessa maneira, a análise dos riscos do setor está contemplada nas Políticas supracitadas que são disponibilizadas à Agência para o processo de acompanhamento, com recente encerramento do ciclo de entregas à Agência, em atendimento à decisão do GT-Ciber.

Portanto, uma análise consolidada integrará versão posterior do Plano, após finalização do processo de acompanhamento do primeiro ciclo de entregas relacionadas às obrigações do R-Ciber.

11. OUTRAS ATIVIDADES

O Fórum das ETIRs, dentro da estrutura do Subgrupo Técnico de Compartilhamento de Informações e Boas Práticas do GT-Ciber, se reunirá periodicamente para tratar das melhorias possíveis nas atividades da rede; avaliar os resultados alcançados; realizar ajustes técnicos nas informações compartilhadas e reportadas; bem como propor encontros e capacitações que possam resultar em melhorias nas atividades de prevenção tratamento e mitigação de incidentes, e para minimizar os riscos cibernéticos.

Sempre que uma ameaça cibernética ou incidente afete mais de um participante da rede setorial, o Fórum das ETIRs poderá ser convocado para buscar ações conjuntas e de apoio mútuo na solução do problema compartilhado.

A ETIR Setorial e as ETIRs do setor poderão propor e realizar outras atividades que visem o aumento da segurança e resiliência das redes de telecomunicações.

12. OUTRAS DISPOSIÇÕES

Esse plano iniciará sua vigência com a instituição da ETIR Setorial pela Agência e sua implementação será de responsabilidade da ETIR Setorial, com suporte do GT-Ciber. Além disso, seu acompanhamento será atribuição do GT-Ciber e demais áreas competentes da Anatel.

PLANO SETORIAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

SETOR DE TELECOMUNICAÇÕES – VERSÃO 1.0

ANATEL

Agência Nacional de Telecomunicações