MINISTÉRIO DAS COMUNICAÇÕES
Assessoria Especial de Assuntos Parlamentares e Federativos

OFÍCIO Nº 29624/2023/MCOM

Brasília/DF, assinado nesta data.

A Sua Excelência o Senhor
Deputado **LUCIANO BIVAR**
Primeiro-Secretário
Mesa Diretora da Câmara dos Deputados
Palácio do Congresso Nacional - Praça dos Três Poderes
CEP 70160-900 - Brasília/DF

Assunto: Resposta ao Ofício 1ª Sec/RI/E/nº 293, de 2023 - Requerimento de Informação (RIC) nº 1820/2023.

Senhor Primeiro-Secretário,

1. Faço referência ao Ofício 1ª Sec/RI/E/nº 293, de 2023, pelo qual V. Exa. encaminha a este Ministério das Comunicações (MCOM) cópia do Requerimento de Informação (RIC) nº 1820/2023 (10996379), de autoria do Deputado Federal Marcos Pereira (REPUBLICANOS/SP), que requer desta Pasta informações "sobre a ocorrência de fraudes nos processos que envolvem a portabilidade de celulares, prática conhecida no mercado como SIM SWAP."

2. Em atendimento ao expediente referenciado, encaminho a Nota Informativa nº 589/2023/GPR-ANATEL (11040217), que fornecem informações e esclarecimentos pertinentes ao mencionado Requerimento de Informação.

3. Permaneço à disposição para esclarecimentos adicionais, caso necessário.

Atenciosamente,

JUSCELINO FILHO
Ministro de Estado das Comunicações

Documento assinado eletronicamente por **José Juscelino dos Santos Rezende Filho**, **Ministro de Estado das Comunicações**, em 06/10/2023, às 15:00 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://super.mcom.gov.br/sei/verifica, informando o código verificador **11145062** e o código CRC **CA0587AE**.

Anexos:

- Plano Tático da Anatel 2023-2024 (11040143);
- Plano Estratégico da Anatel 2023-2027 (11040152);
- Manual Operacional da Portabilidade (11040167);
- Informe nº 540/2022/COGE/SCO (11040169);
- Informe nº 274/2023/COGE/SCO (11040183).

INFORME Nº 274/2023/COGE/SCO

PROCESSO Nº 53500.062890/2023-73

INTERESSADO: CÂMARA DOS DEPUTADOS, MARCOS PEREIRA, MINISTÉRIO DAS COMUNICAÇÕES

1. ASSUNTO

1.1. Informações ao Excelentíssimo Senhor Ministro de Estado das Comunicações sobre a ocorrência de fraudes nos procedimentos de Portabilidade de terminais do Serviço Móvel Pessoal.

2. REFERÊNCIAS

2.1. Lei n.º 9.472, de 16 de julho de 1997, Lei Geral de Telecomunicações (LGT);

2.2. Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998;

2.3. Regulamento Geral de Portabilidade, aprovado pela Resolução nº 460, de 19 de março de 2007;

2.4. Regulamento do Serviço Móvel Pessoal – SMP, aprovado pela Resolução n.º 477, de 7 de agosto de 2007;

2.5. Regulamento de Fiscalização Regulatória, aprovado pela Resolução nº 746, de 22 de junho de 2021;

2.6. Condições para a Portabilidade de Código de Acesso (CPCA), Anexo ao Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998;

2.7. Manual Operacional da Portabilidade (MOP).

3. HISTÓRICO

3.1. Em 12 de junho de 2023, a Anatel recebeu o Ofício nº 19600/2023/MCOM, por meio do qual o Ministério das Comunicações (MCOM) apresenta requerimento de informações para subsidiar resposta ao Excelentíssimo Senhor Deputado Federal Marcos Pereira, que indaga sobre a ocorrência de fraudes nos procedimentos de Portabilidade. O MCOM encaminhou cópia do Requerimento de Informações (RIC) n.º 1820/2023 solicitando que fossem apresentados os esclarecimentos necessários sobre o mencionado tema.

4. ANÁLISE

4.1. Trata-se de atendimento a Requerimento de Informações apresentado para a Agência Nacional de Telecomunicações por intermédio do Ministério da Comunicações para prestação de informações sobre eventuais fraudes nos procedimentos de Portabilidade. Por meio do RIC n.º 1820/2023, apresentado pelo Excelentíssimo Senhor Deputado Federal Marcos Pereira foram apresentadas as seguintes questões:

> a) Como as operadoras têm cumprido as orientações da ANATEL sobre a segurança da portabilidade?
>
> b) Quais são os outros meios confiáveis de identificação mencionados no artigo 46, § 3º da Resolução 750/22 que as operadoras estão utilizando para cumprir essa exigência? A ANATEL considera esses meios confiáveis? Quem é responsável por determinar quais meios são considerados confiáveis para a identificação?
>
> c) Existem estudos estatísticos realizados pela ANATEL que investigam a preferência dos usuários em relação ao acesso aos serviços de portabilidade?

d) Existem estudos realizados pela ANATEL que demonstram empiricamente a confiabilidade dos meios de identificação autorizados pelos regulamentos para a portabilidade?

e) A ANATEL tem fiscalizado as fraudes de SIM SWAP relacionadas à portabilidade? Houve sanções aplicadas às operadoras pela inobservância do artigo 46, § 3º da Resolução 750/22? Em caso positivo, quais foram as penalidades?

f) Quais são as bases técnicas, regulamentares, e legais para a ANATEL adotar a confirmação por SMS na portabilidade? Qual é a norma da ANATEL que regulamenta o envio de SMS como etapa de confirmação do processo de portabilidade?

g) Considerando que a notícia1 repercutida pela ANATEL fala de expansão gradual da prática de confirmação via SMS aos demais DDDs do país a partir de abril de 2023, qual é a abrangência atual e qual é a data prevista para a universalidade da abrangência?

h) Há estudos da ANATEL que demonstrem a confiabilidade deste meio de identificação ou que reportem uma redução no número de fraudes de SIM SWAP?

i) A ANATEL incentiva as operadoras a melhorar seus métodos de autenticação para prevenir o acesso não autorizado aos números dos clientes? Em caso positivo, de que forma?

j) Quais são as ações em curso ou previstas para reforçar e aperfeiçoar a proteção dos usuários?

k) A ANATEL atua em parceria com as autoridades de segurança pública e as operadoras para combater o SIM SWAP via portabilidade? Em caso positivo, de que forma?

l) A ANATEL e as empresas de telefonia móvel têm algum projeto de implementação de autenticação biométrica para verificação de identidade mais rigorosa para os clientes? Há intercâmbio de ideias entre as operadoras para discutir iniciativas como essa?

m) Existe por parte do Ministério das Comunicações interesse em implementar campanhas educativas e alertas de segurança com o intuito de criar uma maior conscientização por parte da população em relação aos cuidados com golpes SIM SWAP via portabilidade?

4.2. Inicialmente, faremos considerações iniciais nas questões relacionadas a golpes e fraudes. O sequestro de terminais pode acontecer mediante duas técnicas fraudulentas:

4.2.1. *SIM swap*, em que os criminosos se apresentam com documentos falsificados nos pontos de atendimento da prestadora de serviços da vítima e, se passando por esta, solicitam a migração da linha para outro chip, com ou sem a cooptação de colaboradores das prestadoras.

4.2.2. Fraude nos procedimentos de portabilidade, em que os criminosos se apresentam em prestadora distinta da original requerendo a portabilidade e falseando a identificação do titular.

4.3. Em ambos os casos, o resultado é que o criminoso consegue a posse do serviço contratado pela vítima, até que ela perceba uma falha em seus serviços e reclame junto à prestadora.

4.4. O tempo decorrente entre a fraude e a recuperação dos serviços é utilizado para a prática de crimes ou obtenção de informações importantes que são enviadas para as vitimas por meio do seu telefone celular, tais como segundo fator de autenticação em sistemas, senhas ou *Personal Identification Numbers* (PIN). Os criminosos podem, alternativamente, tomar posse de diversas contas em redes sociais e, até, em casos de insegurança extrema, reunir condições para acessar as contas bancárias das vitimas.

4.5. Destacamos que, em razão da importância do tema, existe, em curso processo de fiscalização da Anatel em face das operadoras, avaliando os tipos de fraudes, suas quantidades e as ações adotadas em resposta, entre outros aspectos.

4.6. Adicionalmente, a Anatel instaurou, dentro do GT-SEG, grupo com instituições de segurança pública e operadoras de telefonia que é liderado pela Agência, um subgrupo técnico (SGT-

Fraudes), com o objetivo de identificar as principais fraudes e dar-lhes tratamento. Representantes das instituições financeiras, da Febraban e Banco Central também integram esse subgrupo.

4.7. Em relação ao *SIM swap*, a Agência, em sua apuração, constatou que as operadoras têm conduzido ações de prevenção e mitigação. Para a mitigação do *SIM swap*, são realizadas operações de reprogramação dos *SIM cards* originais, de modo a retornar os acessos para seus autênticos consumidores. No que tange à prevenção, são utilizadas técnicas para melhorar a identificação dos consumidores, como avaliações de documentos pessoais e avaliações em bancos de dados próprios, biometria de face e restrição de acesso a programações para colaboradores específicos. Também são realizadas parcerias para dificultar as operações criminosas mediante a prestação de informações sobre substituição de *SIM cards* para empresas de telecomunicações com empresas do sistema financeiro.

4.8. Quando se encerra a possibilidade de um modelo de fraude, os criminosos atualizam suas práticas delituosas; o uso da portabilidade como canal para essas práticas foi uma consequência do esgotamento de modelos anteriores. As regras para esse procedimento exigem procedimentos operacionais que viabilizam a correta identificação dos requisitantes, mediante processos de habilitação e de autenticação de dados cadastrais. Para robustecer os procedimentos, a Anatel requereu das prestadoras a implementação de um novo procedimento introduzindo um Segundo Fator de Autenticação, a ser apresentado nos próximos itens.

Como as operadoras têm cumprido as orientações da ANATEL sobre a segurança da portabilidade?

4.9. O disciplinar da Portabilidade é encontrado no anexo ao Regulamento de Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998 e alterado pela Resolução nº 750, de 15 de março de 2022, na forma de Condições para a Portabilidade de Código de Acesso (CPCA) e no Manual de Procedimentos de Portabilidade (MOP). O MOP foi editado por força da regulamentação e exige a existência de procedimentos técnico-operacionais elaborados pelo conjunto das prestadoras, a Entidade Administradora da Portabilidade (EA) e a própria Agência, conjuntamente, no âmbito do Grupo de Implementação da Portabilidade (GIP).

4.10. No que diz respeito à segurança, é importante destacar, no que concerne à integralidade do objeto do presente documento, o disposto no texto do art. 65-M, do Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998 (RST), abaixo transcrito:

> Art. 65-M. As prestadoras devem adotar as medidas técnicas e administrativas necessárias e disponíveis para prevenir e cessar a ocorrência de fraudes relacionadas à prestação do serviço e ao uso das redes de telecomunicações, bem como para reverter ou mitigar os efeitos destas ocorrências.

4.11. Ou seja, por força de regulamento, é obrigação das prestadoras a atuação consistente no sentido de prevenção e cessação de fraudes. Da mesma forma, cabe à Anatel o acompanhamento e controle do cumprimento dessa obrigação.

4.12. No cumprimento de suas competências, a Anatel realiza continuamente o monitoramento da portabilidade, mediante o acesso direto ao Portal Interativo da Portabilidade e sistemas acessórios disponibilizados pela EA, e realiza o acompanhamento, quando necessário, de situações específicas a serem tratadas junto às prestadoras de serviços. Os indicadores relativos à portabilidade são publicados na página da Agência, no endereço https://informacoes.anatel.gov.br/paineis/portabilidade .

4.13. Os ajustes contratuais entre as partes (EA e prestadoras), para regularização mediante a edição da Lei Geral de Proteção de Dados (LGPD) foram objeto de acompanhamento pela Agência por meio do Procedimento n.º 53500.014648/2022-11, instaurado especificamente para esta finalidade.

Quais são os outros meios confiáveis de identificação mencionados no artigo 46, § 3º da Resolução 750/22 que as operadoras estão utilizando para cumprir essa exigência? A ANATEL considera esses meios confiáveis? Quem é responsável por determinar quais meios são considerados confiáveis para a identificação?

4.14. Conforme discussões empreendidas no âmbito do Grupo Executivo Antifraude de Telecomunicações (GEAFT), as prestadoras utilizam a identificação pessoal dos contratantes, mediante apresentação de documentos pessoais, e utilizam processos de biometria facial e análise de dados e

informações durante a jornada de atendimento.

4.15. A Anatel não realiza avaliações prévias sobre a confiabilidade dos meios adotados pelas prestadoras. A regulamentação exige que as operadoras utilizem métodos seguros, e a escolha destes é prerrogativa e responsabilidade das empresas. Não obstante, acaso o método escolhido pela prestadora se demonstre vulnerável, a Agência pode atuar e exigir providências.

4.16. As discussões sobre as fraudes são empreendidas no âmbito de grupos técnicos constituídos de representantes das prestadoras para esta finalidade. A Anatel participa das discussões conforme verifique conveniência e oportunidade.

Existem estudos estatísticos realizados pela ANATEL que investigam a preferência dos usuários em relação ao acesso aos serviços de portabilidade?

4.17. A Anatel monitora continuamente a atividade das prestadoras a fim de que sejam assegurados os direitos dos usuários, inclusive à portabilidade, fomentada pela disponibilização de ofertas e vantagens comerciais para os consumidores. É importante destacar que a portabilidade tem valor distinto para diferentes usuários: aqueles que utilizam um número como forma de contato com clientes veem nesse instrumento a permanência de seus contatos comerciais. Por outro lado, existem serviços onde o número sequer é divulgado e às vezes pode ser desconhecido, como no caso dos dispositivos de rastreamento de veículos - situação em que a portabilidade agrega pouco valor.

4.18. Em qualquer caso, o importante para a Anatel é que os consumidores que desejarem a portabilidade tenham seu direito assegurado pelas prestadoras, cabendo à Agência monitorar o processo, por meio das ações relatadas no portal, e, conforme o planejamento interno, também podem ser empreendidas atividades de fiscalização de campo.

Existem estudos realizados pela ANATEL que demonstram empiricamente a confiabilidade dos meios de identificação autorizados pelos regulamentos para a portabilidade?

4.19. Como mencionado, a Anatel não autoriza ou desautoriza previamente os meios de identificação de usuários para a portabilidade ou para as demais contratações de serviços. Não obstante, a utilização de meios seguros é exigência normativa, cabendo às prestadoras a tomada das decisões de escolha e substituição dos processos conforme se confirma ou refuta a segurança. É importante destacar, ainda, que o conceito de confiabilidade pode variar; um exemplo é o do reconhecimento facial por *selfie*, outrora considerado seguro, mas que recentemente teve vulnerabilidades identificadas.

A ANATEL tem fiscalizado as fraudes de SIM SWAP relacionadas à portabilidade? Houve sanções aplicadas às operadoras pela inobservância do artigo 46, § 3º da Resolução 750/22? Em caso positivo, quais foram as penalidades?

4.20. A regulamentação da Anatel exige que as prestadoras tomem providencias para a prevenção, cessação, reversão e mitigação das fraudes. Para as ocorrências concretas, faz-se necessário analisar e avaliar os procedimentos de combate utilizados pela prestadora e, no caso de insuficiência de procedimentos, há possibilidade de aplicação de sanções.

4.21. Os procedimentos para a solicitação da portabilidade requerem dois processos: primeiro, a habilitação do solicitante, momento em que este apresenta a documentação pertinente; posteriormente, a autenticação, quando a titularidade do solicitante sobre o serviço é verificado junto à prestadora doadora.

4.22. Este processo de habilitação, por força do § 3º do art. 46 do CPCA, deve ser realizado presencialmente ou por meio seguro. Ademais, é fixado no inciso II do art. 49 da mesma norma, um prazo de 1 (um) dia útil para a eventual recusa da solicitação de portabilidade, que pode ocorrer devido a dados incorretos ou incompletos. A qualquer momento entre a solicitação e a efetivação da portabilidade, que ocorre 3 (três) dias úteis após a solicitação, o procedimento pode ser frustrado.

4.23. Caso, mesmo assim, ocorra uma portabilidade indevida, existe um procedimento de restituição, que permite o retorno dos serviços para a prestadora doadora e que considera o menor tempo possível. Esse procedimento, denominado "portabilidade de estorno", é de simples execução e utiliza prazos reduzidos, de forma que, ao ser inserido um bilhete desta natureza, seu agendamento é

alocado na primeira janela de portabilidade disponível; assim, o terminal retorna ao consumidor legítimo em prazos muito curtos.

4.24. A exploração do procedimento de portabilidade para o sequestro de terminais mediante fraude foi identificada pela Anatel, que atuou junto às prestadoras para tratar essa questão. Um acordo setorial entendeu pertinente introduzir um Segundo Fator de Autenticação, mecanismo que possibilite verificar a posse do terminal pelo solicitante da portabilidade. Logo após a autenticação pela prestadora doadora, são enviadas mensagens de texto (SMS) para o terminal objeto da portabilidade, questionando o usuário sobre o reconhecimento desta solicitação; caso o usuário não reconheça a solicitação e responda negativamente, o pedido é cancelado.

4.25. Sobre a aplicação de sanções por infração ao artigo 46, § 3º da Resolução 750/22, cabe informar que, até o presente momento, não foram instaurados processos sancionatórios em relação à tais ocorrências de fraudes na portabilidade. A Agência estabeleceu prazos para inserir a regra do segundo fator de autenticação e, atualmente, realiza fiscalização geral sobre fraudes, para avaliar a segurança das práticas das operadoras.

Quais são as bases técnicas, regulamentares, e legais para a ANATEL adotar a confirmação por SMS na portabilidade? Qual é a norma da ANATEL que regulamenta o envio de SMS como etapa de confirmação do processo de portabilidade?

4.26. O Segundo Fator de Autenticação da portabilidade utiliza o serviço de mensagens SMS para verificar a posse do terminal pelo solicitante do procedimento. As tentativas de sequestro do terminal ocorrem exatamente pelo fato de o fraudador não ter a posse do aparelho, pelo que o envio da mensagem impede o sucesso da sua tentativa de sequestro do terminal.

4.27. Para a adoção da regra foi introduzida uma alteração no MOP, nos termos abaixo:

> 1.25. Processo de dupla autenticação de Portabilidade Numérica
>
> 1.25.1. Os usuários pessoas físicas (PF) de Prestadoras do Serviço Móvel Pessoal (SMP), receberão uma mensagem via SMS (*Short Message Service*) após a abertura e autorização do bilhete de portabilidade pela Prestadora Doadora. O usuário deverá necessariamente estar em posse de um aparelho telefônico com a referida linha ativa.
>
> 1.25.1.1. A continuidade da portabilidade será condicionada à resposta positiva desta mensagem pelo usuário.
>
> 1.25.1.2. Caso o usuário responda a mensagem negando a continuidade da portabilidade numérica referida, o bilhete será cancelado pela EA.
>
> 1.25.1.3. Caso o usuário não responda a mensagem dentro do tempo-limite (parametrizado) o bilhete entrará em conflito.
>
> 1.25.1.4. A prestadora Receptora poderá enviar uma nova mensagem ao usuário que ficar silente, assim que ultrapassado o tempo limite configurado.
>
> 1.25.2. Os usuários pessoas jurídicas (PJ) de Prestadoras do Serviço Móvel Pessoal (SMP), quando solicitada a portabilidade e tiver a quantidade limite de terminais (parametrizável) definida pelo GTOP, receberão uma mensagem via SMS (*Short Message Service*) após a abertura e autorização do bilhete de portabilidade pela Prestadora Doadora. O usuário deverá necessariamente estar em posse de um aparelho de telefonia com a referida linha ativa.
>
> 1.25.2.1. A continuidade da portabilidade será condicionada à resposta positiva desta mensagem pelo usuário.
>
> 1.25.2.2. Caso o usuário responda a mensagem negando a continuidade da portabilidade numérica referida, o bilhete será cancelado pela EA.
>
> 1.25.2.3. Caso o usuário não responda a mensagem dentro do tempo-limite (parametrizado) o bilhete entrará em conflito.
>
> 1.25.2.4. A prestadora Receptora poderá enviar uma nova mensagem ao usuário que ficar silente, assim que ultrapassado o tempo limite configurado.
>
> 1.25.3. Quando ultrapassada a quantidade limite de terminais pessoal jurídica (PJ), definida pelo GTOP, será enviado para o usuário um SMS informativo sobre o pedido de portabilidade numérica referido.

Considerando que a notícia repercutida pela ANATEL fala de expansão gradual da prática de

confirmação via SMS aos demais DDDs do país a partir de abril de 2023, qual é a abrangência atual e qual é a data prevista para a universalidade da abrangência?

4.28. Atualmente, o Segundo Fator de Autenticação está operacional para os clientes pessoa física nas regiões Centro-Oeste e Norte e, ainda, nos estados do Paraná e Santa Catarina. Conforme a programação, este Segundo Fator de Autenticação estará disponível em todo o território nacional até o dia 28 de agosto de 2023.

Há estudos da ANATEL que demonstrem a confiabilidade deste meio de identificação ou que reportem uma redução no número de fraudes de SIM SWAP?

4.29. As avaliações da Anatel consideraram os cenários observados com base nos dados da Agência, as informações obtidas no relacionamento com o GAECO-SP e a experiência internacional quanto aos desafios de identificação de usuários. Todas as considerações constam do Informe nº 540/2022/COGE/SCO, que segue anexo a este Informe (Anexo II, SEI 10625577).

A ANATEL incentiva as operadoras a melhorar seus métodos de autenticação para prevenir o acesso não autorizado aos números dos clientes? Em caso positivo, de que forma?

4.30. A Anatel exige, por força de normatização, que as prestadoras procedam com a cessação, prevenção, reversão e mitigação das fraudes. Esta é a interpretação do art. n.º 65-M, como transcrito:

> Art. 65-M. As prestadoras devem adotar as medidas técnicas e administrativas necessárias e disponíveis para prevenir e cessar a ocorrência de fraudes relacionadas à prestação do serviço e ao uso das redes de telecomunicações, bem como para reverter ou mitigar os efeitos destas ocorrências.
>
> Parágrafo único. Na implementação de ações coordenadas de combate à fraude, os custos e os benefícios devem ser compartilhados entres as prestadoras participantes, considerando-se o porte da empresa.

4.31. Ademais, como será mencionado a seguir, a Anatel constituiu Grupos de Trabalhos específicos, com partição de *stakeholders* voltados ao suporte à segurança pública e ao combate a fraudes.

Quais são as ações em curso ou previstas para reforçar e aperfeiçoar a proteção dos usuários?

4.32. Conforme mencionado, a Anatel empreende, atualmente, procedimento de fiscalização em face das operadoras para identificar as principais fraudes cometidas, suas quantidades e as ações de mitigação realizadas pelas empresas. A recente criação de grupo de trabalho antifraude composto pela Agência, empresas de telecomunicações e instituições financeiras, para a identificação das pautas prioritárias, também foi citada como ação em curso, e o estreitamento do relacionamento da Anatel com órgãos de segurança pública, buscando atuação conjunta no combate às fraudes, também tem sido empreendida.

4.33. Para além dessas medidas, ressaltamos que a prevenção de fraudes é objeto do Planejamento Estratégico da Agência, cuja cópia segue no Anexo III (SEI 10625579). Nesse sentido, a *Iniciativa 17: Zelar pela prevenção contra fraudes no ecossistema digital* tem como objetivo estratégico a promoção da conscientização e a segurança digital dos usuários. Esperam-se, como resultados da iniciativa, a redução de golpes/estelionatos digitais e o aumento da confiança dos usuários na tecnologia.

A ANATEL atua em parceria com as autoridades de segurança pública e as operadoras para combater o SIM SWAP via portabilidade? Em caso positivo, de que forma?

4.34. Nos termos do art. 65-N do Regulamento de Serviços de Telecomunicações, foi constituído o Grupo Técnico de Suporte à Segurança Pública (GT-Seg), que busca auxiliar a Anatel no acompanhamento da implantação de políticas relacionadas à segurança pública. Este grupo técnico é formado pela própria Agência, pelas prestadoras de serviços e pelas forças de segurança, conforme a temática dos subgrupos técnicos:

4.34.1. O SGT-Celular Legal cuida do impedimento de terminais roubados, furtados, extraviados e identifica terminais não homologados e parte dos adulterados com a mesma finalidade de produzir o impedimento;

4.34.2. O SGT-Sittel cuida das atividades relacionadas à quebra do sigilo telefônico e telemático;

4.34.3. O SGT-Localização trabalha com as atividades relacionadas aos Serviços de Emergência, sendo sua constituição voltada para a elaboração das condições técnicas de fornecimento da localização de terminais em chamadas de emergência;

4.34.4. O SGT-Fraudes tem uma atuação de coordenação de ações de combate e prevenção a fraudes relacionadas à prestação de serviços de telecomunicações.

4.35. No caso específico da portabilidade existe uma área técnica específica, na Gerência de Controle de Obrigações Gerais (COGE) da Agência, que cuida do monitoramento e acompanhamento deste procedimento. Informa-se, por oportuno, que os mesmos servidores atuam nestas frentes, em aproveitamento da sinergia de ações.

A ANATEL e as empresas de telefonia móvel têm algum projeto de implementação de autenticação biométrica para verificação de identidade mais rigorosa para os clientes? Há intercâmbio de ideias entre as operadoras para discutir iniciativas como essa?

4.36. As principais prestadoras do Serviço Móvel Pessoal (SMP) já utilizam procedimentos de identificação biométrica dos seus contratantes de serviços. Existem procedimentos de identificação biométrica presenciais, utilizados no atendimento em lojas, e procedimentos de identificação biométrica remota, utilizada para casos específicos, como em atividades relacionadas ao bloqueio de estações roubadas ou furtadas ou para o cadastramento de linhas da modalidade pré-paga, com acompanhamento especial destacado para esta matéria.

Existe por parte do Ministério das Comunicações interesse em implementar campanhas educativas e alertas de segurança com o intuito de criar uma maior conscientização por parte da população em relação aos cuidados com golpes SIM SWAP via portabilidade?

4.37. A Anatel realiza, em conjunto com instituições públicas e privadas, atividades de conscientização de usuários. No que diz respeito à conscientização sobre o sequestro de terminais mediante fraude nos procedimentos de portabilidade, foram veiculadas campanhas utilizando o Movimento #FiqueEsperto, iniciativa apoiada por 16 (dezesseis) instituições, à saber: ABBC; Abranet; Abrint; Anatel; Associação Neo; Banco Central do Brasil; CACB; Câmara e-net; CGI.br; Conexis; Febraban; Internet Societ - Capítulo Brasil; NIC.br; Proteste; Telcomp; e Whatsapp.

4.38. O movimento veicula, periodicamente, mensagens de alerta para os consumidores de serviços digitais sobre os principais golpes e fraudes identificados pelos entes envolvidos. A veiculação das mensagens ocorre pela distribuição de SMS para toda a base de terminais móveis, distribuição de e-mails para toda a base de consumidores cadastrado,; e veiculação de *stories* nas redes sociais dos apoiadores do movimento.

4.39. Para além de tais iniciativas, informa-se que a inserção de segundo fator de autenticação no procedimento de portabilidade também é acompanhada de campanhas de informação aos consumidores.

5. ANEXOS

5.1. Anexo I - Manual Operacional da Portabilidade (MOP) (SEI nº 10625576);

5.2. Anexo II - Informe n.º 540/2022/COGE/SCO (SEI nº 10625577);

5.3. Anexo III - Planejamento Estratégico da Anatel 2023-2027 (SEI nº 10625579);

5.4. Anexo IV - Plano Tático da Anatel 2023-2024 (SEI nº 10625581).

6. PROPOSIÇÃO

6.1. Propõe-se o encaminhamento de cópia deste Informe nº 274/2023/COGE/SCO para a ARI, em atenção ao Ofício nº 717/2023/ARI-ANATEL.

Documento assinado eletronicamente por **Gustavo Santana Borges**, **Superintendente de Controle de Obrigações**, em 31/07/2023, às 16:20, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da Portaria nº 912/2017 da Anatel.

A autenticidade deste documento pode ser conferida em http://www.anatel.gov.br/autenticidade, informando o código verificador **10631797** e o código CRC **2E5A3C04**.

Referência: Processo nº 53500.062890/2023-73 SEI nº 10631797

INFORME Nº 540/2022/COGE/SCO

PROCESSO Nº 53500.310843/2022-61

INTERESSADO: CLARO S.A., OI S.A. - EM RECUPERACAO JUDICIAL, TIM CELULAR S.A., TELEFO BRASIL S.A., ALGAR TELECOM S/A, SERCOMTEL CELULAR S.A., SURF TELECOM S.A., DATORA MO TELECOMUNICACOES S.A

1. ASSUNTO

1.1. Introdução de segundo fator de autenticação da Portabilidade.

2. REFERÊNCIAS

2.1. Lei n.º 9.472, de 16 de julho de 1997, Lei Geral de Telecomunicações (LGT);

2.2. Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998;

2.3. Regulamento Geral de Portabilidade, aprovado pela Resolução nº 460, de 19 de março de 2007;

2.4. Regulamento do Serviço Móvel Pessoal – SMP, aprovado pela Resolução n.º 477, de 7 de agosto de 2007;

2.5. Regimento Interno da Anatel, aprovado pela Resolução n.º 612, de 29 de abril de 2013;

2.6. Regulamento de Fiscalização Regulatória, aprovado pela Resolução nº 746, de 22 de junho de 2021;

2.7. Condições para a Portabilidade de Código de Acesso (CPCA), Anexo ao Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998;

2.8. Manual Operacional da Portabilidade (MOP).

3. HISTÓRICO

3.1. Em 17 de março de 2022 a Anatel solicitou reunião com as prestadoras de serviços para tratar de fraudes relacionadas ao sequestro de terminais mediante exploração dos procedimentos de Portabilidade.

3.2. Em 03 de maio, 09 de maio, 08 de junho, 22 de junho, 29 de junho, 10 de agosto, 24 de agosto, 11 de outubro e 26 de outubro de 2022 foram realizadas reuniões de trabalho para planejamento de atividades para a implementação de alterações nos procedimentos de Portabilidade, com o objetivo de prevenir a ocorrência das fraudes.

4. ANÁLISE

4.1. Trata-se de Processo de Acompanhamento e Controle instaurado nos termos do art. 79 do Regimento Interno da Anatel, aprovado pela Resolução n.° 612, de 29 de abril de 2013 (RI-Anatel), cuja finalidade é subsidiar a Agência com informações relevantes para os seus processos decisórios; analisar o desempenho das prestadoras de serviços de telecomunicações; estimular a melhoria contínua da prestação dos serviços de telecomunicações visando soluções para as inconformidades detectadas; atuar na busca da reparação ou minimização de eventuais danos à prestação dos serviços de telecomunicações ou aos seus usuários. No caso específico, cuida-se de análise referente aos procedimentos para efetivação da Portabilidade de Códigos de Acesso de Usuários do Serviço Móvel Pessoal, onde se verifica a ocorrência de fraudes consistentes no sequestro dos terminais.

4.2. O presente processo possui fundamentação, ainda, no art. 15 do Regulamento de Fiscalização Regulatória, aprovado pela Resolução nº 746, de 22 de junho de 2021 (RFR), abarcando o

conjunto de medidas destinadas ao acompanhamento, monitoramento, análise e verificação do cumprimento da legislação e da regulamentação e das condições de prestação dos serviços.

4.3. Destaca-se que tal acompanhamento se insere na Temática "Enfrentamento de Golpes", incluída na Lista Institucional de Temas Priorizados de Fiscalização Regulatória para o Ciclo 2023/2024 (SEI nº 9333872), aprovada pela Comissão de Gestão Executiva (CGE).

4.4. Inicialmente, consignamos a competência desta unidade e, para tanto, buscamos amparo no também no RI-Anatel, que dispõe sobre a organização e o funcionamento da Agência Nacional de Telecomunicações – Anatel, em observância ao disposto nos arts. 19, inciso XXVII e 22, inciso X, da Lei nº 9.472, de 16 de julho de 1997, Lei Geral de Telecomunicações (LGT). A atuação desta Superintendência de Controle de Obrigações (SCO), no presente caso, é lastreada no que é estabelecido no art. 158, *in verbis,* de onde destacamos os incisos I e IV:

> **Art. 158.** A Superintendência de Controle de Obrigações tem como competência:
>
> **I -** acompanhar e controlar as obrigações das detentoras de concessão, permissão e autorização para exploração de serviços de telecomunicações, de autorização de uso de radiofrequência, de autorização de uso de numeração e de direito de exploração de satélite definidas nos instrumentos regulatórios pertinentes e nos respectivos contratos, termos e atos;
>
> (...)
>
> **IV -** instaurar, instruir e decidir Procedimento de Apuração de Descumprimento de Obrigações e Procedimento de Acompanhamento e Controle;
>
> (...)

4.5. Em decorrência das atividades de monitoramento realizadas pela Gerência de Controle de Obrigações Gerais (COGE) sobre os procedimentos de Portabilidade e de combate e prevenção de fraudes, a Anatel demandou reuniões com as prestadoras de serviços, para tratar de casos de sequestro de terminais com a utilização dos procedimentos de Portabilidade. O registro das reuniões, que se iniciaram em 03 de maio 2022, estão relatados nos documentos SEI nº 9062444, 9062452, 9064616, 9064628, 9062461, 9062469, 9062478, 9373653, 9373707 e 9381162.

4.6. O sequestro de terminais pode acontecer mediante duas técnicas fraudulentas: (1) o Sim Swap, ou (2) fraude nos procedimentos de Portabilidade. Difere o primeiro do segundo o fato do sequestro ocorrer na mesma prestadora da vítima ou em prestadora distinta. Assim, os criminosos, se fazendo passar pela vítima, apresentam-se com documentos falsificados nos pontos de atendimento das prestadoras e solicitam a recuperação de serviços supostamente roubados ou furtados, ou com interesse em contratar serviços com o uso da Portabilidade. Em ambos os casos o resultado é que o criminoso consegue a posse do serviço contratado pela vítima, até que esta última perceba uma falha em seus serviços, reclame junto à prestadora e seja providenciado o reparo.

4.7. O tempo decorrente entre a fraude e a recuperação dos serviços é suficiente para a prática de crimes ou posse pelos criminosos de informações importantes que são enviadas para as vitimas por meio do seu telefone celular, tais como: segundo fator de autenticação em sistemas, senhas ou *Personal Identification Numbers* (PIN). Os criminosos podem, também, tomar posse de diversas contas em redes sociais e, até, em casos de insegurança extrema, alcançar condições para acessar contas bancárias das vitimas.

4.8. No que tange às soluções tem-se que o Sim Swap ocorre pela exploração de vulnerabilidade de processos internos das prestadoras de serviços e de responsabilidade individual de cada uma delas. Decerto que, neste caso, o acompanhamento da Anatel se faz necessário, entretanto, as soluções são prerrogativas individuais que devem considerar os próprios procedimentos internos da prestadoras para avaliar as melhores soluções. De outra forma, o procedimento de Portabilidade é matéria regulada pela Agência, parte por regulamentação e parte em manual de procedimentos. Assim, verifica-se a necessidade de atuação para este caso.

4.9. Antes de adentrar na proposta em curso para solucionar a questão, passa-se a uma explicação do arcabouço normativo relacionado. Ressalte-se, inicialmente, a competência estabelecida no inciso XIV do art. 19 da LGT que possibilita que a Agência expeça normas e padrões que assegurem a operação integrada.

4.10. Nos termos das Condições para a Portabilidade de Código de Acesso (CPCA), Anexo ao Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998, o processo de Portabilidade inclui a autenticação e a habilitação. O texto normativo substituiu o antigo art. 49 do Regulamento Geral de Portabilidade, aprovado pela Resolução nº 460, de 19 de março de 2007.

4.11. Estes são os exatos termos:

> **Art. 45.** A fase de **autenticação** do Processo de Portabilidade é caracterizada pela **conferência dos dados do usuário**, que são **encaminhados à Prestadora Doadora** por meio da Entidade Administradora.
>
> **§ 1º** Os dados referidos no caput são os seguintes:
>
> **a)** nome completo;
>
> **b)** número do documento de identidade ou número do registro no cadastro do Ministério da Fazenda, no caso de pessoa natural;
>
> **c)** número do registro no cadastro do Ministério da Fazenda, no caso de pessoa jurídica;
>
> **d)** código de acesso; e,
>
> **e)** nome da Prestadora Doadora.
>
> **§ 2º** A Prestadora Doadora terá, no máximo, 1 (um) dia útil para conferência e confirmação dos dados do usuário.
>
> **§ 3º** Caso não ocorra a autenticação pela Prestadora Doadora em observância aos prazos e condições estipulados neste Anexo, as razões para tal devem ser enviadas à Prestadora Receptora por meio da Entidade Administradora.
>
> **Art. 46**. Após a fase de autenticação, não havendo condições para recusa da Solicitação de Portabilidade, a Prestadora Receptora deve agendar a **habilitação** do usuário e o procedimento para ativação e desativação dentro do Período de Transição.
>
> **§ 1º** A Prestadora Receptora é responsável pela atualização das etapas do Processo de Portabilidade junto ao usuário, tanto nas situações de efetivação da Portabilidade quanto nas condições de recusa.
>
> **§ 2º** A ativação na Prestadora Receptora e a desativação na Prestadora Doadora devem ocorrer de forma a minimizar a interrupção da prestação do serviço de telecomunicação.
>
> **§ 3º A habilitação na Prestadora Receptora deve ser feita presencialmente, ou utilizando outros métodos seguros de identificação, mediante apresentação de documentos que comprovem os dados informados quando da Solicitação de Portabilidade.**
>
> **§ 4º** Nos prazos estabelecidos no regulamento de cada serviço, a Prestadora Receptora deve entregar ao Usuário Portado cópia do documento de adesão e do Plano de Serviço ao qual será vinculado.

4.12. O escólio da regra pretende assegurar que o consumidor solicitante da Portabilidade seja corretamente identificado, à partir da apresentação de documentos pessoais e de mandato (pessoa jurídica), e que seja apto a realizar o pedido. A partir das informações é verificada a titularidade sobre o serviços junto à Prestadora Doadora e pela conferência de documentos averiguada a identificação do mesmo. Convém esclarecer que a habilitação, quando realizada de modo não presencial, deve ser realizada de forma a assegurar a identificação do consumidor solicitante, com nível de segurança semelhante ao processo presencial.

4.13. Não obstante, observa-se que estes procedimentos tem sido abusados, seja com a finalidade fraudulenta, seja com finalidades comerciais associados à competição nos mercados.

4.14. O volume fraudes está contido nas Portabilidades Indevidas e que pode ser representado pela quantidade de Portabilidades Estornadas. Explica-se.

4.15. Nos termos do item 7.1 do Manual Operacional da Portabilidade (MOP) o estorno aplica-se quando é solicitada a Portabilidade de forma fraudulenta, equivocada ou ocorrer uma autenticação indevida que resulte na migração irregular. Assim, a quantidade de Bilhetes de Portabilidade (BP) estornados representa uma parte das fraudes com utilização abusiva da Portabilidade. Importante destacar que a análise quantitativa não é suficiente para separar as fraudes de problemas regulares de autenticação. A experiência nos mostra, inclusive, que a quantidade de fraudes neste universo é de

pequena monta. Mas os dados que ilustram a quantidade de estornos representam o tamanho do problema a ser enfrentado. Saliente-se que mesmo as Portabilidades ocorridas com problemas naturais de autenticação e sem a finalidade fraudulenta também constituem problemas para os usuários e podem ser amenizadas com os mesmos procedimentos de prevenção de fraudes ora em implementação.

4.16. Assim, seguem tabelas ilustrativas da quantidade de BP estornados. A Figura 01 demonstra os resultados apurados entre os meses de abril e setembro do ano de 2022, de BP de estorno abertos com a visão Prestadora Doadora. A Figura 02 demonstra os resultados apurados entre os meses de abril e setembro do ano de 2022, de BP de estorno, com a visão da Prestadora Receptora.

BILHETES DE PORTABILIDADE ESTORNADOS PRESTADORA DOADORA						
PRESTADORA	SET	AGO	JUL	JUN	MAI	ABR
DATORA	-	1	1	-	-	-
SURF	**56**	**539**	**1.157**	**818**	**346**	**354**
AMERICANET	**22**	**27**	**20**	**17**	**27**	**14**
ALGAR	6	7	-	2	4	4
BRT MOVEL	-	-	-	1	5	9
TELECALL	4	7	4	14	21	34
VIVO	**1.447**	**1.187**	**1.053**	**1.126**	**1.105**	**1.197**
CLARO	**670**	**618**	**730**	**596**	**941**	**892**
OI MOVEL	1	2	2	2	13	18
TIM MOVEL	**1.536**	**1.381**	**1.100**	**1.407**	**1.591**	**1.140**
SERCOMTEL	-	-	-	-	-	-
TOTAL ESTORNADO	3.742	3.769	4.067	3.983	4.053	3.662
EFETIVADAS	912.228	931.096	849.087	822.014	841.472	750.928

Figura 01

BILHETES DE PORTABILIDADE ESTORNADOS PRESTADORA RECEPTORA						
PRESTADORA	SET	AGO	JUL	JUN	MAI	ABR
DATORA	-	-	-	-	-	-
SURF	-	-	-	-	-	-
AMERICANET	1	1	4	1	-	-
ALGAR	3	3	1	2	4	3
BRT MOVEL	29	48	63	47	138	65
TELECALL	-	-	3	-	-	-
VIVO	**812**	**1.035**	**1.360**	**1.045**	**1.422**	**907**
CLARO	**2.582**	**2.288**	**2.082**	**2.371**	**2.123**	**2.135**
OI MOVEL	122	143	109	115	115	236
TIM MOVEL	193	251	444	401	251	315
SERCOMTEL	-	-	1	1	-	1
TOTAL ESTORNADO	3.742	3.769	4.067	3.983	4.053	3.662
EFETIVADAS	912.228	931.096	849.087	822.014	841.472	750.928

Figura 02

4.17. Explica-se que os BP de estorno demonstram a Portabilidade realizada para corrigir um equívoco acontecido, nele figurando inversamente as Prestadoras Doadora e Receptora comparativamente à Portabilidade indevida. A visão conforme a Prestadora Doadora (Figura 01) reflete a ocorrência de um equívoco na Portabilidade, na quantidade demonstrada na tabela, de responsabilidade das prestadoras listadas. Ou seja, as prestadoras listadas foram responsáveis por gerar solicitações de Portabilidade que vieram a ser consideradas indevidas. Já a visão Prestadora Receptora reflete as prestadoras responsáveis de prestação de serviços original do consumidor e, também, por autenticar, dando sua anuência, para a perfectibilizaçãdo da Portabilidade indevida.

4.18. Sem entrar no mérito da eventual culpa pela ocorrência da Portabilidade indevida, posto que esta avaliação depende de maiores informações referentes aos motivos que ensejaram a mesma, verifica-se nos números apresentados que elas estão ocorrendo. Neste sentido, verifica-se oportunidade

para o aprimoramento dos procedimentos de autenticação. Isto porque os procedimentos para a reversão da ocorrência das fraudes e dos demais problemas de autenticação não tem sido suficientes para satisfação da sociedade, carecendo a criação de procedimentos de prevenção e mitigação dos problemas descritos.

4.19. Em setembro de 2021 a *Federal Communications Commission* (FCC) propôs uma consulta pública - Notice of Proposed Rulemaking FCC 21-102 - Protecting Consumers from SIM Swap and PortOut Fraud, anexada (SEI n.º 9391032), com a finalidade de criar regras para a a prevenção da ocorrência de Sim Swap e Portabilidades fraudulentas. A agência reguladora americana registrou que os telefones celulares são essenciais na vida dos americanos que os utiliza não apenas para a realização de chamadas. A FCC reconhece que os serviços são utilizados para o gerenciamento da vida financeira, acesso de contas bancárias e de corretagem, pagamentos usando uma ampla gama de aplicativos de serviços, dentre outros. E acrescenta que quando se faz login em determinados sites ou aplicativos, ou é necessário redefinir uma senha, geralmente se recebe a mesma pelo envio de uma mensagem de texto para o telefone celular informado. Neste sentido, o uso dos telefones celulares revestem-se de singular necessidade de proteção contra eventuais sequestros com a utilização das técnicas.

4.20. A FCC indicou a existência de seis tipos de informações utilizadas pelas prestadoras para autenticar seus clientes: (1) Informações Pessoais: incluindo endereço, endereço de e-mail, data de nascimento; (2) Informações da conta: últimos 4 dígitos do número do cartão de pagamento, data de ativação, data do último pagamento e valor; (3) Informações do dispositivo: IMEI (número de série do dispositivo), ICCID (número de série do SIM); (4) Informações de uso: números de telefone recentes chamados; (5) Conhecimento: PIN ou senha, respostas a perguntas de segurança; e (6) Posse: senha de uso único enviada por mensagem de texto ou e-mail.

4.21. Avaliando o mesmo problema a *Australian Communications and Media Authority* (ACMA) emitiu em 2020 o *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard*, anexado (SEI n.º 9391047), contendo regras com o objetivo de: (a) impedir a Portabilidade não autorizada de números de serviços móveis; (b) reduzir os danos causados aos clientes pela Portabilidade não autorizada de números de serviços móveis; e (c) exigir que os prestadores de serviços de transporte contratados tomem medidas razoáveis para confirmar que a pessoa que solicita uma Portabilidade: (i) seja titular dos direitos de uso do número do serviço móvel a ser portado; e (ii) tenha acesso direto e imediato a um dispositivo móvel associado a esse número.

4.22. A ACMA determinou verificações adicionais a serem realizadas previamente à Portabilidade, para todos os usuários, exigindo: (a) confirmar que o solicitante tem acesso direto e imediato a um dispositivo móvel usado em associação com o número do serviço móvel a ser portado; (b) uso de um código de verificação único que é enviado via mensagem SMS e do qual o prestador de serviço recebe confirmação imediata por mensagem SMS de que o cliente, ou o representante autorizado do cliente, recebeu o código de verificação exclusivo; (c) uso de uma ou mais formas de dados biométricos; ou (d) quando um grande cliente empresarial confirmando a solicitação pelo representante autorizado e que a pessoa solicitante tem acesso direto e imediato ao número principal associado a empresa.

4.23. Conforme se depreende da comparação entre os modelos americano e australiano os procedimentos de identificação de usuário são semelhantes ao processo de habilitação vigente no Brasil. Nos EUA são fornecidas informações pessoais e de uso do serviço e do terminal, conhecidos do verdadeiro titular do serviço (1 a 4). Na Austrália, da mesma forma, são verificadas informações pertinentes à identificação pessoal (a; c; e, d).

4.24. Por outro lado, verifica-se, em ambas as nações, exigências de verificação de posse do terminal não utilizados ainda no Brasil. No mercado americano a proposta prevê o conhecimento de informações de segurança (5 e 6) enviadas para o consumidor (e-mail) ou para o terminal (SMS) e no modelo australiano interação pessoal e de máquina (envio e controle de recepção por meio de SMS). O modelo de Portabilidade nacional estará alinhado aos modelos americano e australiano após a implementação de um segundo fator de autenticação em execução.

4.25. Neste sentido, esta área técnica vem realizando reuniões com as prestadoras de serviço no sentido de introduzir o segundo fator de autenticação nos procedimentos de Portabilidade. Já foi

acordado um procedimento para acrescentar o envio e recebimento de confirmação, por meio de SMS, para os consumidores da categoria pessoa física. O procedimento é representado pela Figura 03, extraído do registro da reunião ocorrida no dia 03 de maio de 2022 (SEI n.º 9062444).

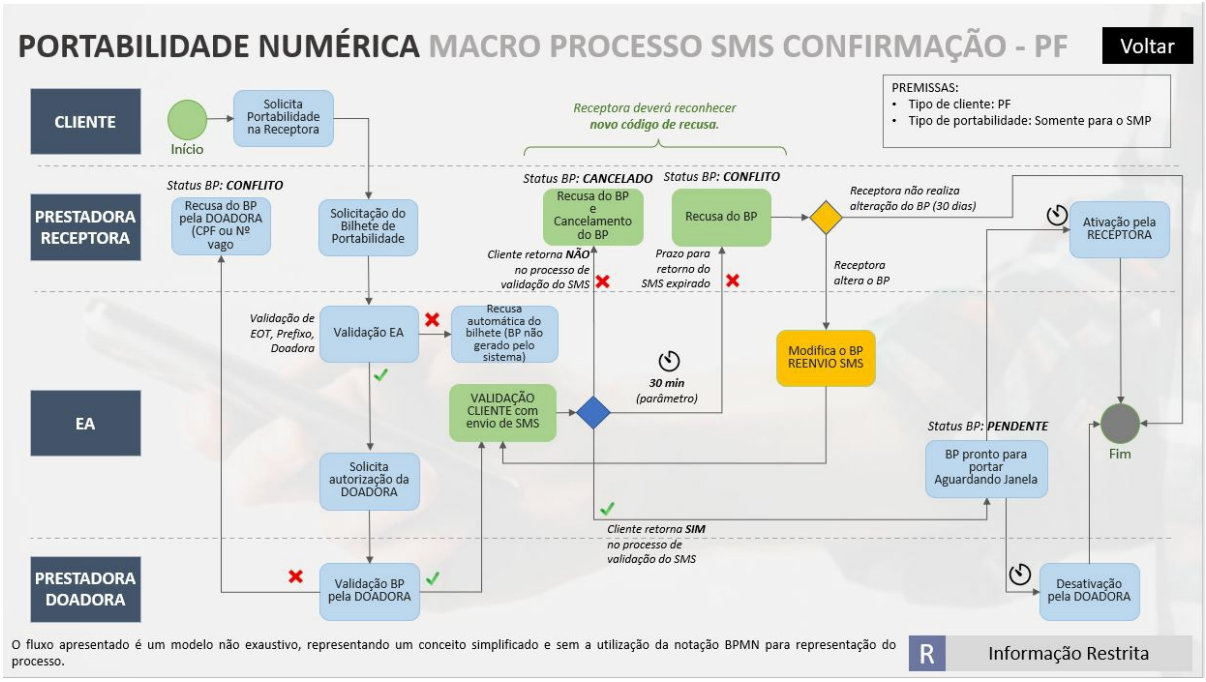


Figura 03

4.26. Não obstante, verifica-se que o cronograma proposto pelas prestadoras consome um tempo de execução desmedido considerando a ocorrência de fraudes e os prejuízos decorrentes das mesmas para as prestadoras de serviços e para a sociedade. Em detalhes o cronograma é apresentado na Figura 04, extraído do registro da reunião ocorrida no dia 26 de outubro de 2022 (SEI n.º 9381162), e registra a disponibilização operacional do segundo fator de autenticação apenas em 21 de abril de 2023.

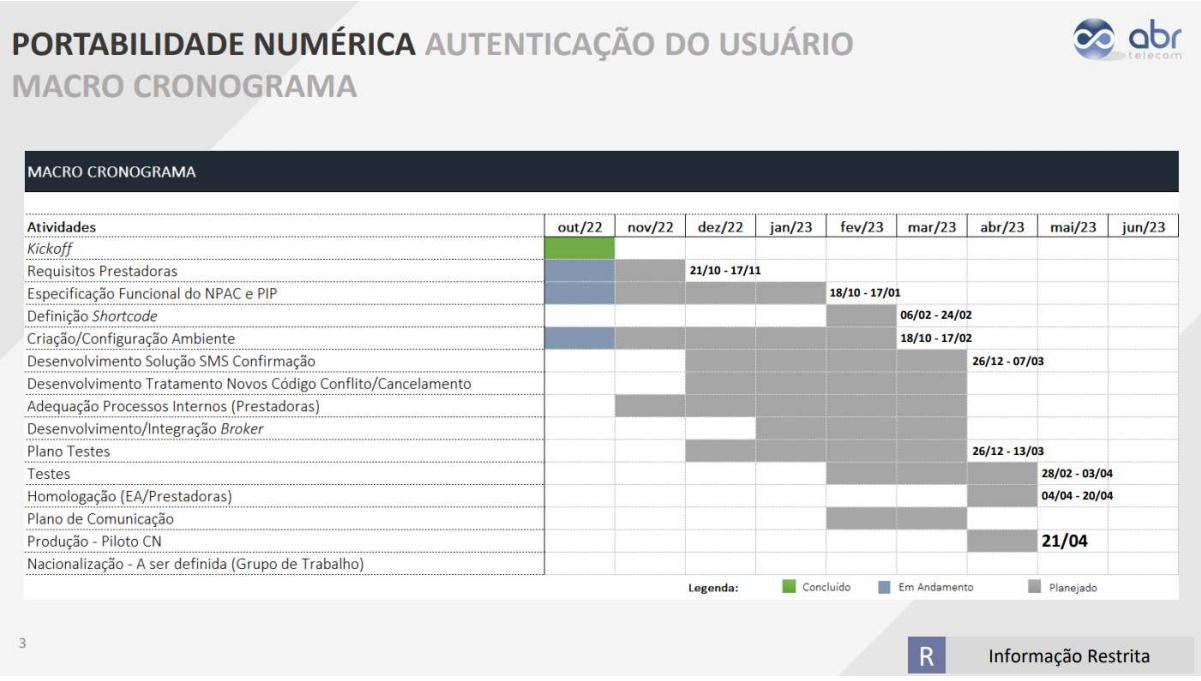


Figura 04

4.27. Registre-se que os esforços para otimização do cronograma foram solicitados pelo grupo técnico para as prestadoras, restando esgotadas as negociações com o prazo indicado alhures. Registre-se que o prazo indicado no cronograma é demasiado extenso considerando a ocorrência de fraudes, no entanto, necessário considerando a complexidade das atividades de implementação, bem como o envolvimento de diversos agentes com atuação conjunta e sincronizada para alcançar a a implementação segura.

4.28. Em demonstração da necessidade de urgência no aprimoramento dos procedimentos registra-se reunião convocada pelo Grupo de Atuação Especial de Combate ao Crime Organizado no Estado de São Paulo (GAECO) Ministério Público Federal (SEI n.º 9374211) que dá notícias de que as agências internacionais de segurança (FBI e Enisa) deram alerta para este tipo de fraude, e apontam esta como a principal ameaça da atualidade. O GAECO ainda aponta que as descobertas recentes da Europol indicam a participação de organizações criminosas neste tipo de crime, com grandes operações relacionadas ao cibercrime e lavagem de dinheiro. Na referida reunião a Anatel informou que já estaria tomando providências para introdução do segundo fator de autenticação (SEI n.º 9390947), conforme os acordos que vem empreendendo com as prestadoras.

4.29. Em demonstração da complexidade indica-se que o sistema *Number Portability Administration Center* (NPAC) é responsável pela efetivação de todos os procedimento de Portabilidade, de ativação de Códigos não Geográficos nas redes e, atualmente, da migração de consumidores entre as redes da Oi S.A. - Em Recuperação Judicial (Oi) e da Claro S.A. (Claro) Tim S.A. (Tim) e Telefônica Brasil S.A. (Vivo) por decorrência de processo de aquisição da primeira pelas últimas. Ademais o ambiente do NPAC é conectado a aproximadamente 300 (trezentas) prestadoras de serviços que necessitam ajustar seis sistemas aos novos procedimentos. O NPAC é responsável por 30.000 (trinta mil) Portabilidades diárias e aproximadamente a mesma quantidade de migrações de usuários da Oi.

4.30. Saliente-se que as providências que estão sendo acordadas com as prestadoras não constituem mera liberalidade das mesmas. Cuida-se de atendimento ao comando normativo estabelecido no art. 65-M do Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998 (RST), que institui obrigações de tomada de providências quando identificada a ocorrência de fraudes, conforme se verifica *in verbis*:

> **Art. 65-M.** As prestadoras devem adotar as medidas técnicas e administrativas necessárias e disponíveis para prevenir e cessar a ocorrência de fraudes relacionadas à prestação do serviço e ao uso das redes de telecomunicações, bem como para reverter ou mitigar os efeitos destas ocorrências.

4.31. Assim, a colaboração das prestadoras no que diz respeito a proposição de medidas não exime a atuação da Anatel. Em acréscimo, as providências em adoção não eximem as prestadoras de sua responsabilidade na eventual exploração dos procedimentos de Portabilidade em operações fraudulentas.

4.32. Entende-se que os procedimentos atualmente estabelecidos na regulamentação e no MOP seriam suficientes para prevenir a ocorrências das fraudes quando executadas com exímio pelas prestadoras. Neste sentido, o segundo fator de autenticação em implementação adiciona uma camada de segurança aos procedimentos com o objetivo de assegurar a identificação das eventuais tentativas mais facilmente. É justificada a introdução deste segundo fator de autenticação dada a capacidade dos criminosos na criação de situações que contornam estes procedimentos vigentes.

4.33. Tendo em vista o interesse acrescentar a camada de segurança para a prevenir exploração dos procedimento de Portabilidade e o conflito de interesses relativamente ao prazo de implementação, resta necessário o pronunciamento formal da Superintendência de Controle de Obrigações acerca caso.

DAS MEDIDAS DE FISCALIZAÇÃO REGULATÓRIA

4.35. O tema objeto nos presentes autos e o tratamento a ele dado deve se inserir nas regras previstas no RFR. Tal regulamento busca, dentre outros pontos, estabelecer o conjunto de regras sistematizadas da Agência a respeito da adoção de regulação responsiva, reorganizando e coordenando toda a atuação de enforcement da Agência.

4.36. Deste modo, considerando que o objetivo do presente processo é justamente o cumprimento de obrigações previstas no RST, relacionados a procedimentos adotados na Portabilidade de Código de Acesso dos Usuários, cabe avaliar qual a medida mais adequada a ser aplicada no presente momento .

4.37. Deste modo, tendo ocorridas discussões necessárias, com a realização de reuniões com os interessados, e formado o convencimento por parte desta Superintendência sobre o conteúdo e forma

de adimplemento das obrigações em análise, resta estabelecer as definições necessárias para o efetivo cumprimento das obrigações e aprimoramento da prestação do serviço aos usuários.

4.38. Sendo assim, dentre as disposições do referido regulamento, está a divisão das atividades de enforcement em etapas de: (i) planejamento, (ii) acompanhamento e (iii) controle. Cada uma dessas etapas é definida no instrumento e obedecem a um conjunto de normas que padronizam a atuação da Agência. Por oportuno, veja-se as definições do RFR:

> Art. 4º Para efeito deste Regulamento, além das definições constantes na regulamentação aplicável aos serviços de telecomunicações, são adotadas as seguintes:
> I - Acompanhamento: atividade de acesso, obtenção e averiguação de dados e informações, incluindo aquela realizada mediante Inspeção, com as finalidades de reunir evidências para a apuração do cumprimento de obrigações e conformidades e de promover melhorias preventivas na prestação dos serviços;
>
> (...)
>
> VI - Controle: atividade destinada à aplicação de medidas corretivas de condutas em desacordo com a legislação e a regulamentação;
>
> (...)
>
> Art. 8º O planejamento de Fiscalização Regulatória objetiva programar e priorizar as medidas necessárias para atuação da Anatel, promovendo o alinhamento dos objetivos, recursos e esforços, mediante aplicação de metodologia de priorização.

4.39. As atividades aqui desenvolvidas se enquadram na etapa de acompanhamento, uma vez que buscam avaliar e monitorar o cumprimento da legislação e, portanto, se subsumem ao previsto no caput do art. 15:

> Art. 15. O processo de acompanhamento abarca o conjunto de medidas destinadas ao acompanhamento, monitoramento, análise e verificação do cumprimento da legislação e da regulamentação e das condições de prestação dos serviços, incluindo aquela realizada mediante Inspeção, bem como de medidas de prevenção e de reparação.

4.40. De modo diverso, a definição regulamentar da fase planejamento estabelece que ele envolve as atividades de estabelecer prioridades e alinhamento das iniciativas de fiscalização ao objetivos, recursos e esforços da Agência, enquanto o controle corresponde ao conjunto de medidas destinadas à reação perante condutas em desacordo com a legislação e a regulamentação.

4.42. Para além da hipótese de simples arquivamento, a conclusão da fase de acompanhamento da fiscalização regulatória pode ocasionar a composição de base de dados para reavaliação e, também, imposição ao administrado de medidas preventivas ou reparatórias ou de medidas de controle, elencadas nos arts. 43 e 55, respectivamente.

4.44. Tendo em vista toda a celeuma estabelecida sobre o modo de cumprimento da obrigação, ficam inviabilizadas as alternativas de encerramento por simples arquivamento e também de composição de base de dados para reavaliação no próximo ciclo. Todo o debate formado exige pronunciamento formal da SCO acerca do modo de cumprimento da obrigação de garantir a segurança nas operações de portabilidade de código de acessos dos usuários realizadas pelas prestadoras.

4.46. Considerando as exigências de proporcionalidade e gradação, reafirmadas com o RFR, não convém por ora estabelecer medidas de controle. Verifica-se que os atores envolvidos têm comparecido às discussões e colaborado para a solução, de acordo com suas visões e interesses. Assim, por exclusão, cabe a análise da imposição de medidas preventivas ou reparatórias que objetivem a mitigação da ocorrência de fraudes até a implementação completa do segundo fator de autenticação na realização da portabilidade pelas prestadoras.

4.49. De acordo com o art. 42 do RFR, a Anatel poderá determinar a adoção de medidas preventivas ou reparatórias que visem a prevenir condutas de forma tempestiva, cessar ou reduzir o impacto aos consumidores e ao setor. Dentre as medidas previstas no regulamento, estão:

a) divulgação de informações;

b) orientação aos administrados;

c) notificação para regularização;

d) plano de conformidade;

e) medida cautelar; e,

f) demais medidas que vierem a ser adotadas de acordo com a legislação vigente.

4.51. No presente caso, a medida mais adequada é a orientação aos administrados, que tem o objetivo de instrui-los acerca de normas, procedimento, documentação comprobatória, da implementação e da observância de melhores práticas para o atendimento da regulamentação de forma efetiva e eficaz, nos termos do art. 49 do RFR.

4.53. Importante destacar a indicação realizada no âmbito técnico e registrada no item 1.7 da Ata de Reunião - 26.10.2022 (SEI.º 9381162) onde a Anatel solicitou que as prestadoras estudassem o aprimoramento dos procedimentos de habilitação e autenticação, que constitui o primeiro fator de autenticação, promovendo ações de melhorias que pudessem prevenir a ocorrências de fraudes. Em atenção ao pedido da Anatel as prestadoras, no âmbito do Grupo de Implementação da Portabilidade - Subrgrupo Operacional (G-TOP), avaliaram o pedido e apresentaram, por meio de e-mail do coordenador (SEI .º 9493140), anexado, uma proposta para a distribuição de Short Mesages Service (SMS) informativo ao consumidores. Segundo a proposta as mensagens seriam enviadas pela Prestadora Doadora, quando identificadas solicitações, alertando para a ocorrência de Portabilidade e eventual risco de fraude. Esta implementação seria disponibilizada até o dia 12 de dezembro de 2022. O G-TOP informou, ainda, que a utilização de SMS Classe 0, seria reavaliada no mês de janeiro de 2023.

4.54. Assim, diante do lapso temporal extenso para a implementação do segundo fator de autenticação, sugere-se que as prestadoras passem a expedir mensagens para todos os consumidores solicitantes de Portabilidade, conforme proposto, informando à respeito da identificação de um Bilhete de Portabilidade. É importante que a mensagem disponibilize orientações sobre as providências serem tomadas em caso de improcedência do pedido, indicando a procurar a prestadora dos serviços.

4.56. Esta medida demanda a adoção de medidas técnicas externas ao NPAC, bem como a preparação de das forças de atendimento para responder às demandas, mas que podem ser implementadas rapidamente. Conforme a proposta do G-TOP há possibilidade de implementação imediata, sendo que os consumidores passariam a receber as mesmas à partir de 12 de dezembro de 2022. Não obstante, foi informado que as discussões sobre a utilização do SMS Classe 0 seriam retomadas somente em janeiro de 2023. À despeito de eventuais dificuldades operacionais para a implementação deste tipo de mensagem neste momento, não se vislumbra dificuldade para a continuidade dos estudos técnicos, de forma a redundar na utilizazação do SMS Classe 0 no curso do mês de janeiro de 2023. Assim, sugere-se acatar a proposição do G-TOP, e aprimorá-la , orientando a dar continuidade nos estudos de viabilidade do uso de SMS classe 0, com o objetivo de verificada a viabilidade, empregue seu uso até o dia 31 de janeiro de 2022.

4.59. Em resumo do exposto verifica-se que os procedimentos alhures propostos para implementação do segundo fator de autenticação estão alinhados com a melhor prática internacional e, portanto, também tem o condão de atender às necessidades nacionais. Por outro lado o tempo de execução proposto excede às expectativas da Agência e da sociedade no que diz respeito ao alcance da maior segurança das operações, no entanto, é necessário para assegurar uma implementação segura. A implementação do segundo fator de autenticação será concluida em abril de 2023 o que exige a expedição de orientação às prestadoras para a adoção de medidas para reforçar os procedimentos de habilitação e autenticação dos BP, com o objetivo de frustrar a ocorrência das fraudes. O envio de mensagens informativas sobre a identificação de Bilhetes de Portabilidade, com orientações de medidas a serem tomadas em caso de improcedência do pedido serão implementadas até o dia 12 de dezembro de 2022. A utilização de SMS Classe 0 deve continuar sendo avaliada pelas prestadoras com o objetivo de eventual implementação até o dia 31 de janeiro de 2023. As atividades de implementação deste segundo fator de autenticação no procedimento de Portabilidade e das medidas de informações aos consumidores não exime as prestadoras da responsabilidade pela ocorrência de fraudes, devendo, quando identificadas, ser objeto de apuração pela Anatel.

4.60. De tudo o exposto sugere-se, com amparo no disposto no art. 49 do RFR a expedição de orientação para as prestadoras para que deem prosseguimento com a implementação das atividades acordadas nas reuniões técnicas até o dia 23 de abril de 2023 e que adotem todas as medidas adicionais acima sugeridas e aprovadas pela Agência, dando continuidade aos estudos para a utlização do SMS Classe 0. Adverte-se, entretanto, que as providências em adoção não eximem as prestadoras de sua responsabilidade em caso de eventual ocorrência da fraude.

5. ANEXOS

5.1. Notice of Proposed Rulemaking FCC 21-102 - Protecting Consumers from SIM Swap and PortOut Fraud (SEI n.º 9391032);

5.2. Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard (SEI n.º 9391047);

5.3. Ofício n.º 5957/2022/GAECO-MPF/SP do Grupo de Atuação Especial de Combate ao Crime Organizado no Estado de São Paulo (SEI n.º 9374211);

5.4. Memória de Reunião com o Grupo de Atuação Especial de Combate ao Crime Organizado no Estado de São Paulo (SEI n.º 9390947);

5.5. E-mail - Reunião do G-TOP (SEI n.º 9493140).

6. PROPOSIÇÃO

6.1. De tudo o exposto, propõe-se a expedição de Despacho Decisório por parte da Superintendência de Controle de Obrigações (SCO) com o seguintes teor:

6.1.1. Expedir às prestadoras do Serviço Móvel Pessoal **Orientação aos Administrados,** prevista no arts. 43, II e 49 do RFR, de que a obrigação relacionada à utilização de métodos seguros de identificação, previstas no art. 46, §3º das Condições de Portabilidade de Código de Acesso, anexo ao Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998, será atendida de forma adequada e satisfatória com o uso do segundo fator de autenticação, conforme apresentado em reuniões realizadas pelas próprias prestadoras.

6.1.1.1. Fixar o prazo máximo de 23 de abril de 2023 para a implementação da solução de segundo fator de autenticação em todas as solicitações de portabilidade, apresentando em reuniões de ponto de controle mensais com esta Superintendência, relatório sobre a execução do projeto, bem como aspectos relacionados à comunicação à sociedade de suas funcionalidades;

6.1.2. Expedir às prestadoras do Serviço Móvel Pessoal **Orientação aos Administrados,** prevista no arts. 43, II e 49 do RFR, para que providenciem a expedição de mensagens, para todos os terminais objeto de solicitações de Portabilidade, informando à respeito da identificação de uma Bilhete de Portabilidade e orientando-os a procurar a sua prestadora em caso de improcedência do pedido.

6.2.2.1. Fixar que as providências para o envio de SMS deve ser iniciada imediatamente e que as mensagens devem ser encaminhadas para os consumidores solicitantes de Portabilidade à partir de 12 de dezembro de 2022.

6.2.3. Expedir às prestadoras do Serviço Móvel Pessoal **Orientação aos Administrados,** prevista no arts. 43, II e 49 do RFR, para que deêm continuidade nos estudos para a utilização do SMS Classe 0, com o objetivo de empregar este tipo de mensagem até o dia 31 de janeiro de 2023.

6.2.4. Informar às prestadoras que as atividades de implementação ora acordadas não as exime de responsabilidade por eventuais ocorrências de fraudes e que, sendo identificada pela Anatel, serão objeto de apuração em autos próprios.

6.3. Propõe-se notificar as partes interessadas, mediante o encaminhamento do presente Informe, que na sua totalidade, faz parte das orientações ora expedidas.

Documento assinado eletronicamente por **Gustavo Santana Borges**, **Superintendente de Controle de Obrigações**, em 30/11/2022, às 09:54, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da Portaria nº 912/2017 da Anatel.

A autenticidade deste documento pode ser conferida em http://www.anatel.gov.br/autenticidade, informando o código verificador **9271950** e o código CRC **4FBD80E9**.

Referência: Processo nº 53500.310843/2022-61 SEI nº 9271950

plano estratégico 2023-27

ANATEL

CONEXÃO:

NOSSO PRESENTE PARA O FUTURO.

plano estratégico 2023-27

Novembro, 2022

DESTAQUES

Nova identidade institucional

Página 39

PROPÓSITO

Conectar o Brasil para melhorar a vida de seus cidadãos

VALORES

Inovação
Segurança Regulatória
Foco em resultados e efetividade
Construção Participativa

MISSÃO

Promover o desenvolvimento da conectividade e da digitalização do Brasil em benefício da sociedade

VISÃO

Ser uma instituição ativa na transformação digital no país, promovendo mercados dinâmicos com serviços de qualidade

DESTAQUES

Novo mapa estratégico

Página 41

PROPÓSITO

Conectar o Brasil para melhorar a vida de seus cidadãos

VALORES

Inovação
Segurança Regulatória
Foco em resultados e efetividade
Construção participativa

MISSÃO

Promover o desenvolvimento da conectividade e da digitalização do Brasil em benefício da sociedade

VISÃO

Ser uma instituição ativa na transformação digital no país, promovendo mercados dinâmicos com serviços de qualidade.

OBJETIVOS ESTRATÉGICOS DE RESULTADO

1 Promover a **conectividade** e a **prestação de serviços** de comunicação com qualidade para todos

2 Estimular **mercados dinâmicos e sustentáveis** de serviços de comunicação e conectividade

3 Fomentar a transformação digital junto à sociedade em condições de equilíbrio de mercado

4 Garantir atuação de **excelência** com **foco nos resultados** para a sociedade

OBJETIVOS ESTRATÉGICOS DE PROCESSOS

Infraestrutura e Qualidade

1A Viabilizar o acesso físico e a qualidade dos serviços a todos

1B Viabilizar a expansão e a implantação da infraestrutura da rede de base

1C Garantir o cumprimento de obrigações regulatórias

1D Proteger as infraestruturas críticas da conectividade

Dinamismo de Mercado

2A Garantir a adequabilidade da definição do mercado

2B Garantir equidade no acesso e nas regras aplicáveis aos agentes

2C Promover uso eficiente dos recursos escassos

2D Promover a atratividade e a sustentabilidade do setor pela modernidade da regulação

2E Promover o acesso econômico dos usuários

Modernidade, transformação digital, inovação e sociedade

3A Promover a conscientização e a segurança digital dos usuários e demais agentes

3B Fomentar aplicações e modelos de negócio inovadores

3C Promover a modernização da tecnologia de forma isonômica e transparente

Gestão interna

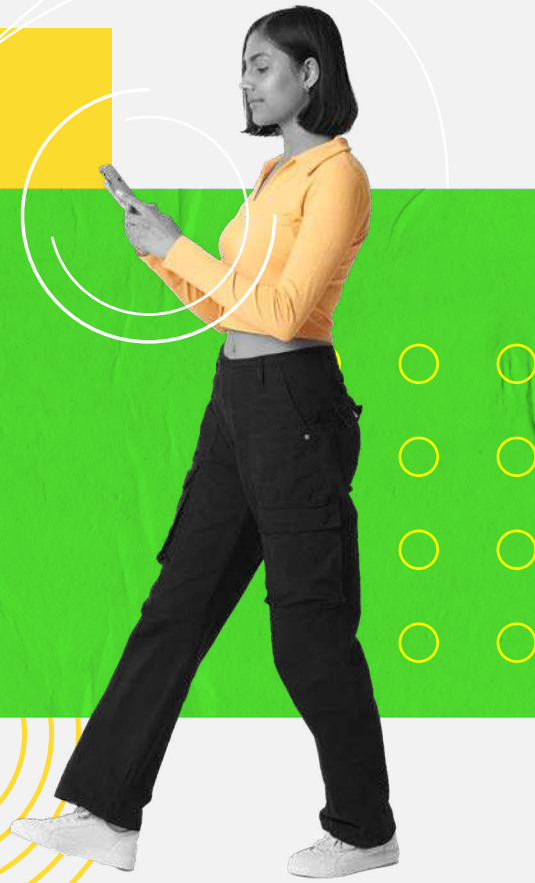
4A Promover a oxigenação e capacitação de servidores

4B Garantir a transparência e a gestão interna adequada

4C Garantir a adequabilidade da infraestrutura interna e das TICs

ÍNDICE

Figuras e Tabelas



INTRODUÇÃO

O Plano Estratégico da Agência Nacional de Telecomunicações para o período de 2023-2027 contém os fundamentos basilares da atuação regulatória com a finalidade de garantir que o propósito da Agência permaneça aderente aos anseios da sociedade, estando em sintonia com os principais instrumentos de planejamento governamental, refletidos no Plano Plurianual (PPA), nas políticas públicas de telecomunicações e na Estratégia Federal de Desenvolvimento para o Brasil (EFD).

Conectar o Brasil para melhorar a vida de seus cidadãos é o propósito que movimenta continuamente a Anatel no sentido de criar as condições necessárias para ampliar a conectividade e modernizar as infraestruturas de telecomunicações, de forma a contribuir com o desenvolvimento nacional, a digitalização da sociedade e com a redução das desigualdades sociais e regionais.

A conectividade é a potência que está movendo a era digital. Novas tecnologias são desenvolvidas em um ritmo intenso e têm impacto em diversos segmentos da economia desde a comunicação, o mercado de trabalho, a educação, a medicina, as relações comerciais, o sistema produtivo agrícola e industrial, bem como a gestão das cidades, do meio ambiente e de recursos naturais.

Isso exigirá cada vez mais que a Anatel realize o acompanhamento mais atento das evoluções tecnológicas, explorando novas ideais e estando aberta a contribuições e às inovações de mercado, sem, contudo, deixar de assegurar a estabilidade e a agilidade necessária na regulação do setor da conectividade para que se atraia os investimentos para proporcionar o seu pleno desenvolvimento e a população possa usufruir dos benefícios das novas tecnologias.

Por isso, a estratégia da Anatel está baseada nos valores da inovação, da segurança regulatória e do foco em resutados para a sociedade, tendo sido construída a partir da análise de cenários prospectivos, das incertezas críticas e das tendências que deverão moldar as telecomunicações e os usos da conectividade no médio e longo prazos.

A definição da estratégia da Agência para os próximos anos contida neste Plano levou em consideração o posicionamento estratégico resiliente aos cenários com maior probabilidade de ocorrerem, a avaliação de riscos, o estabelecimento de metas alcançáveis e a promoção da boa governança e de sua comunicação a fim de garantir a transparência dos resultados almejados.

O Plano está estruturado por um conjunto de objetivos estratégicos, metas e iniciativas, tendo o foco em resultados voltados à promoção da conectividade à internet e do desenvolvimento de mercados dinâmicos, bem como da prestação de serviços de comunicação com qualidade para todos.

Por fim, considera-se que este Plano Estratégico contribuirá para aperfeiçoar a gestão estratégica da Anatel, com o olhar voltado para o futuro, mas atenta aos desafios presentes, com o intuito de manter as pessoas conectadas, promover o acesso à informação, gerar novos modelos de negócios em meio digital e, assim, pavimentar os caminhos para que o Brasil possa ser reconhecido pelo avanço tecnológico na transformação digital e pelos benefícios proporcionados à sua população.

1. A AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

Criada pela Lei Geral de Telecomunicações – LGT –, Lei nº 9.472/1997, a Agência Nacional de Telecomunicações – Anatel – foi a primeira Agência Reguladora a ser instalada no Brasil, em 5 de novembro daquele mesmo ano. É vinculada ao Ministério das Comunicações e integra a Administração Pública Federal indireta, estando submetida a regime autárquico especial, que se caracteriza pela ausência de tutela ou de subordinação hierárquica, pela autonomia funcional, decisória, administrativa e financeira e pela investidura a termo de seus dirigentes e estabilidade durante os mandatos.

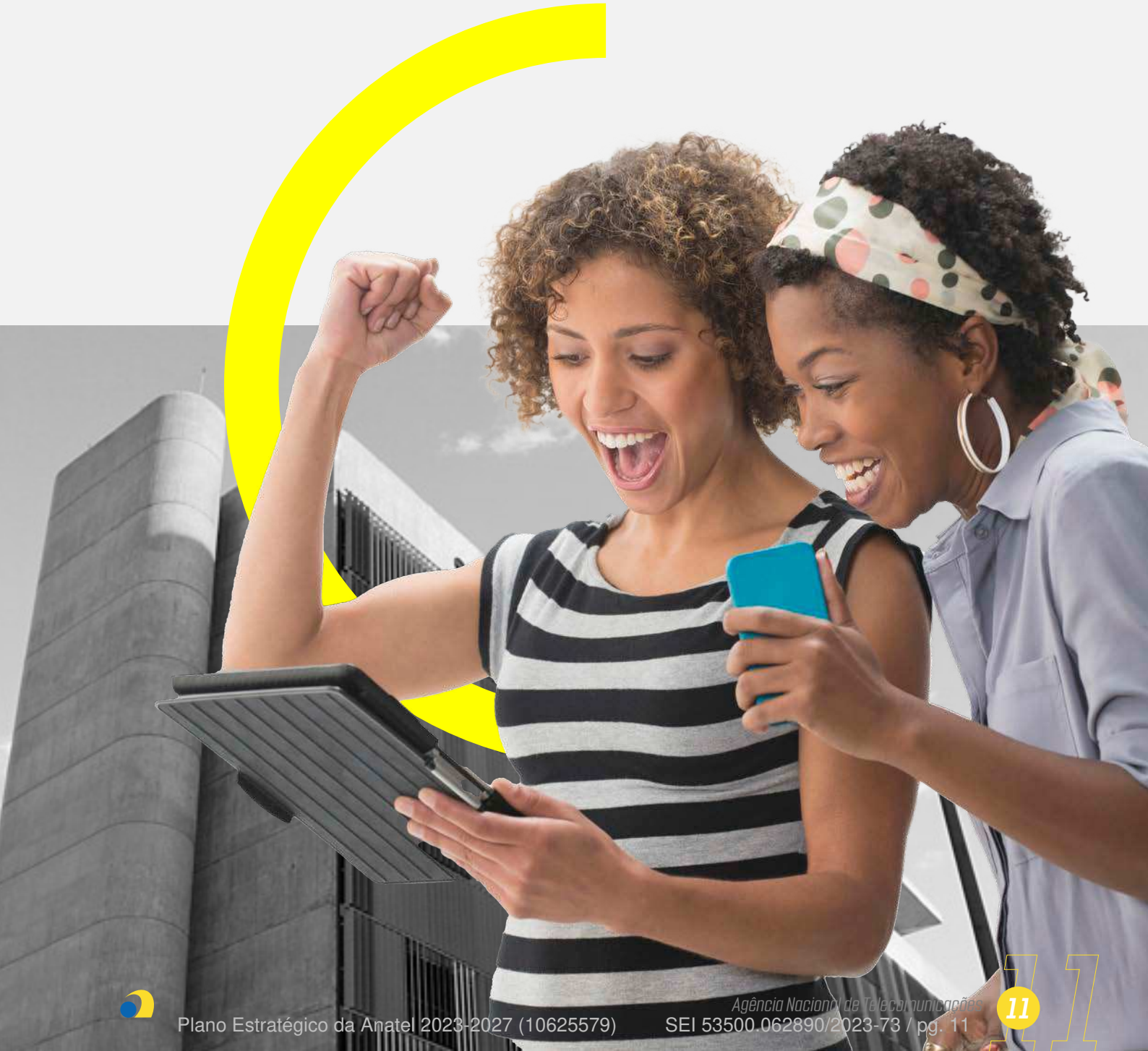
A Anatel é o órgão regulador responsável pela organização da exploração dos serviços de telecomunicações, o que inclui, entre outros aspectos, o disciplinamento e a fiscalização da execução, comercialização e uso dos serviços e da implantação e funcionamento de redes de telecomunicações, bem como da utilização dos recursos de órbita e espectro de radiofrequências.

Compete à Agência adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras. No rol de suas atribuições legais, destacam-se:

- implementar, em sua esfera de atribuições, a política nacional de telecomunicações;
- representar o Brasil nos organismos internacionais de telecomunicações sob a coordenação do Poder Executivo;
- expedir normas quanto à outorga, prestação e fruição dos serviços de telecomunicações, editando atos de outorga e extinção de direito de exploração dos serviços;
- fiscalizar a prestação dos serviços de telecomunicações, aplicando sanções e realizando intervenções;
- controlar, acompanhar e proceder a revisão de tarifas e homologar reajustes;
- administrar o espectro de radiofrequências e o uso de órbitas, expedindo as respectivas normas;
- expedir ou reconhecer a certificação de produtos, observados os padrões e as normas por ela estabelecidos;
- compor administrativamente conflitos de interesses entre prestadoras de serviço de telecomunicações;

- reprimir infrações dos direitos dos usuários;
- exercer relativamente às telecomunicações as competências legais em matéria de controle, prevenção e repressão das infrações da ordem econômica, ressalvadas as pertencentes ao Conselho Administrativo de Defesa Econômica (Cade); e
- reavaliar, periodicamente, a regulamentação com vistas à promoção da competição e à adequação à evolução tecnológica e de mercado.

A Anatel tem sede em Brasília e representações em todas as capitais brasileiras, por meio das quais mantém contato próximo com a sociedade e instituições locais. As atividades são exercidas pelo Conselho Diretor, oito superintendências e um superintendente-executivo, além de oito órgãos de assessoramento, e são orientadas por este Plano Estratégico alinhado ao planejamento plurianual do Governo Federal e às políticas públicas setoriais.



2. ORIENTAÇÕES ESTRATÉGICAS DO GOVERNO E POLÍTICA SETORIAL

Estratégia Federal de Desenvolvimento para o Brasil (EFD)

A Estratégia Federal de Desenvolvimento para o Brasil relativa ao período de 2020 a 2031 (EFD 2020-2031), instituída por meio do Decreto nº 10.531, de 26 de outubro de 2020, foi concebida com objetivo de definir a visão de longo prazo para a atuação das entidades da Administração Pública Federal. Trata-se de importante documento para uniformizar os cenários macroeconômicos nos planos setoriais do País, a partir da identificação dos desafios para o Brasil no período de 2020 a 2031, bem como da definição das orientações que nos permitirão deslocar em direção ao futuro desejado.

A Estratégia Federal de Desenvolvimento para o Brasil está organizada em cinco eixos: econômico, institucional, infraestrutura, ambiental e social. Para cada um deles, foram instituídos diretrizes, índices-chave e respectivas metas-alvo, desafios e orientações que deverão ser alcançados ao final do período.

Nos eixos econômico, infraestrutura e social estão elencados os principais desafios relacionados à conectividade, infraestrutura de telecomunicações e internet. Cuida-se, assim, de um referencial para formulação de políticas públicas, no sentido de se construir a visão de futuro de País, integrando-as em seus diversos campos de atuação: educação, saúde, robótica, pesquisa e desenvolvimento, indústria, comércio, entre outros.

As orientações de desenvolvimento relacionadas ao setor de telecomunicações podem ser visualizadas nas tabelas a seguir:

Tabela 1: Eixo Econômico

DIRETRIZ: Alcançar o crescimento econômico sustentado e a geração de empregos, com foco no ganho de produtividade, na eficiência alocativa e na recuperação do equilíbrio fiscal.

DESAFIO 1.3.2. Aumentar a produtividade da economia brasileira.

Para o desenvolvimento da economia digital do País, as orientações são:

- ampliar o acesso da população à internet e às tecnologias digitais, com qualidade de serviço e economicidade;
- incentivar o desenvolvimento da economia digital, aumentando o apoio à difusão de tecnologias emergentes (interconectividade, automação, energias, nanotecnologia, novos materiais e biotecnologias e edição gênica, por exemplo) e as suas aplicações no País; e
- propiciar as condições necessárias para que os setores produtivo e público utilizem dados abertos para a geração de valor econômico, a melhoria dos serviços e a criação de empregos, por meio de análise de dados, big data/analytics, inteligência artificial e outras aplicações tecnológicas.

Fonte: Governo Federal do Brasil

Tabela 2: Eixo Infraestrutura

DIRETRIZ: Fomentar o desenvolvimento da infraestrutura, com foco no ganho de competitividade e na melhoria da qualidade de vida, assegurando a sustentabilidade ambiental e propiciando a integração nacional e internacional.

DESAFIO 3.3.1. Ampliar os investimentos em infraestrutura.

Para a modernização dos serviços de telecomunicações, as orientações são:

- garantir regras e instrumentos para suportar políticas e programas de expansão da infraestrutura de banda larga, o que inclui, entre outros, conectividade para as Regiões Norte e Nordeste, comunicação por satélite, governo eletrônico, data centers, redes móveis com tecnologia 5G ou superior e backhaul de fibra óptica para todos os Municípios do País, com padrões de qualidade e custo compatíveis com as referências internacionais;
- estimular a pesquisa e o desenvolvimento tecnológico e produtivo, a atualização constante dos serviços de tecnologia da informação e comunicação - TIC, a inteligência artificial, a segurança cibernética e a distribuição de tecnologias digitais, de forma a acompanhar a fronteira econômica mundial;
- preservar a estabilidade, a segurança cibernética e a funcionalidade da rede de internet, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo uso de boas práticas, com respeito aos direitos dos cidadãos;
- reduzir o gap digital entre a população brasileira, promovendo o acesso aos serviços de TIC em condições econômicas que viabilizem o uso e a fruição dos serviços;
- aperfeiçoar os sistemas de comunicação dos serviços de segurança pública, defesa nacional, inteligência e outras atividades críticas de Estado, com alta capacidade de tráfego e disponibilidade; e
- modernizar e aperfeiçoar o sistema brasileiro de radiodifusão.

Fonte: Governo Federal do Brasil

Tabela 3: Eixo Social

DIRETRIZ: Promover o bem-estar, a família, a cidadania e a inclusão social, com foco na igualdade de oportunidades e no acesso a serviços públicos de qualidade, por meio da geração de renda e da redução das desigualdades sociais e regionais.

DESAFIO 5.3.1. Ampliar o acesso à educação, a permanência nesta e principalmente a sua qualidade.

Para a modernização dos serviços de telecomunicações, as orientações são:

- ampliar a infraestrutura de conectividade nas escolas e estimular o uso pedagógico de tecnologias digitais na sala de aula e no ensino à distância.

DESAFIO 5.3.4. Reduzir a proporção da população abaixo da linha de pobreza e as desigualdades sociais.

Para o aproveitamento das potencialidades regionais para a geração de renda, as orientações são:

- priorizar planos e estratégias regionais que maximizem a criação de infraestrutura de conectividade e acesso à internet.

Fonte: Governo Federal do Brasil

Assim, a EFD 2020-2031 deve ser compreendida como um planejamento de longo prazo que apresenta questões macro para o desenvolvimento nacional e que deve ser traduzida em programas, projetos e ações de todos os entes da federação.

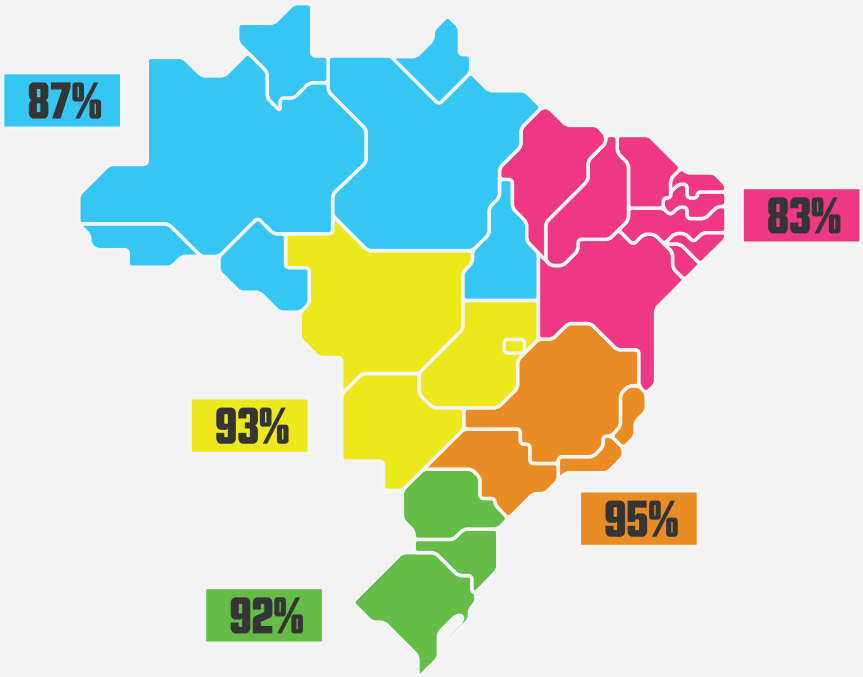
Plano Plurianual 2020-2023

O Plano Plurianual (PPA) é o instrumento de planejamento orçamentário que se destina a organizar e a viabilizar a atuação pública, orientando o Estado e a sociedade no sentido de cumprir os fundamentos e os objetivos da República. Por meio dele, são declarados o conjunto das políticas públicas do governo para o próximo período de quatro anos e os caminhos que serão trilhados para viabilizar as diretrizes, objetivos e metas previstas, visando à construção de um país melhor.

O PPA 2020-2023 foi aprovado pela Lei nº 13.971/2019 e, na condição de estratégia global do governo federal, encontra-se os desafios relativos às telecomunicações concentrados no Programa Temático 2205: "Conecta Brasil", cujo objetivo é promover o acesso universal e ampliar a qualidade dos serviços de comunicações do país (Objetivo 1185).

O Programa enfatiza como público-alvo da política pública toda a população, destacando como beneficiários: (i) populações em localidades remotas, (ii) localidades com prestação inadequada ou inexistente e (iii) populações em situação de vulnerabilidade. Sublinham-se, ainda, os critérios de priorização a serem utilizados, a saber: as Regiões Norte e Nordeste e o Indicador de Vulnerabilidade (IPEA).

Figura 4: Metas regionalizadas de acesso à internet em banda larga para os domicílios brasileiros



Fonte: Governo Federal do Brasil

Esse Objetivo traz como meta "Ampliar o acesso à internet em banda larga para os domicílios brasileiros de 74,68% para 91,00%", além das metas regionalizadas, conforme mapa acima:

Nesse diapasão, a Anatel permanece se preparando e agindo, tanto para contribuir com o alcance das metas finais deste PPA, ao término de 2023, quanto para dar continuidade, nos próximos planos plurianuais e no presente Plano Estratégico, ao progresso atingido no setor de telecomunicações, aproveitando as oportunidades de ampliação de acesso aos diversos serviços, de evolução das tecnologias de informação e comunicação e de expansão da indústria setorial, com o intuito de diminuir desigualdades regionais e sociais e promover a inclusão digital, a inovação e o desenvolvimento econômico e tecnológico do Brasil.

Políticas Públicas de Telecomunicações

O Decreto nº 9.612, de 17 de dezembro de 2018, estabeleceu os objetivos e as diretrizes para as políticas públicas de telecomunicações, abrangendo, entre outros aspectos, a organização da exploração dos serviços de telecomunicações, o desenvolvimento industrial e tecnológico do setor e a inclusão digital da população.

2.0.1 Objetivos e público-alvo das políticas de telecomunicações

A Administração Pública Federal deve observar os seguintes objetivos gerais das políticas públicas de telecomunicações:

- promover (i) o acesso às telecomunicações em condições econômicas que viabilizem o uso e a fruição dos serviços, especialmente para a expansão do acesso à internet em banda larga fixa e móvel, com qualidade e velocidade adequadas e a ampliação do acesso à internet em banda larga em áreas onde a oferta seja inadequada, tais como áreas urbanas desatendidas, rurais ou remotas; (ii) a inclusão digital, para garantir à população o acesso às redes de telecomunicações, sistemas e serviços baseados em tecnologias da informação e comunicação - TIC, observadas as desigualdades sociais e regionais; e (iii) um mercado de competição ampla, livre e justa;

- proporcionar um ambiente favorável à expansão das redes de telecomunicações e à continuidade e à melhoria dos serviços prestados;

- garantir os direitos dos usuários dos serviços de telecomunicações;

// estimular (i) a pesquisa e o desenvolvimento tecnológico e produtivo; e (ii) as medidas que promovam a integridade da infraestrutura de telecomunicações e a segurança dos serviços que nela se apoiam; e

// incentivar a atualização tecnológica constante dos serviços de telecomunicações.

O Decreto nº 9.612 enfatiza ainda que as políticas públicas relativas à inclusão digital objetivam fomentar e implantar a infraestrutura, os serviços, os sistemas e as aplicações baseados em TIC, necessários para o acesso às redes de telecomunicações pela população: (i) de localidades remotas; (ii) de localidades com prestação inadequada ou inexistente desses serviços; ou (iii) em situação de vulnerabilidade social; o que reforça a preocupação da Administração Pública Federal com as parcelas da população brasileira ainda não atendidas ou precariamente atendidas pelos serviços de telecomunicações.

Ainda de acordo com o normativo federal, o Ministério das Comunicações é o responsável pela formulação de políticas, diretrizes, estratégias, ações e mecanismos de monitoramento e acompanhamento, papel estabelecido por meio do PPA; enquanto a Anatel, qualquer que seja o seu posicionamento estratégico, é a responsável pela implementação e execução da regulação do setor de telecomunicações, em conformidade com as políticas estabelecidas por aquele Ministério.

2.0.2 Diretrizes da política pública

Em conformidade com o Decreto nº 9.612/2019, as ações e providências adotadas pela Anatel na implementação das políticas públicas em telecomunicações devem observar as seguintes diretrizes:

- promoção da concorrência e da livre iniciativa, da gestão eficiente de espectro de radiofrequência, de forma a ampliar a qualidade e expandir os serviços de telecomunicações, em especial a conectividade em banda larga, da regulação assimétrica, com vistas, em especial, à expansão da oferta de serviços em áreas onde eles inexistem ou à promoção da competição no setor, da simplificação normativa, da qualidade dos serviços baseada na experiência do usuário, de forma a incentivar a transparência nas ofertas e os mecanismos de comparação entre prestadoras e da proteção física e lógica das infraestruturas críticas de telecomunicações;

- estímulo aos negócios inovadores e que desenvolvam o uso de serviços convergentes, à expansão e ao compartilhamento de infraestrutura e à redução sistemática dos riscos cibernéticos;

- adoção de procedimentos céleres para a resolução de conflitos;

- regulação de preços de atacado conforme modelo que considere o incentivo ao investimento agregado setorial na modernização e na ampliação de redes de telecomunicações;

- harmonização da regulamentação setorial às normas gerais sobre relações de consumo; e dos procedimentos e das exigências referentes à exploração de satélite brasileiro e à execução do serviço de telecomunicações que utilize satélite às práticas internacionais;

- incentivo à autorregulação e mecanismos correlatos; e

- realização de levantamentos periódicos e sistematizados das infraestruturas de transporte e de acesso em operação.

A implementação de políticas públicas pela Anatel serve à constante atualização das bases para a organização dos serviços de telecomunicações, com fundamentação na competição e na ampliação do acesso e com vistas à evolução da sociedade da informação característica deste século.

Por fim, ressalta-se o tratamento expresso dado pelo Decreto nº 9.612, com alterações introduzidas pelo Decreto nº 10.799, de 17 de setembro de 2021, quanto aos compromissos de expansão e de prestação dos serviços de telecomunicações fixados pela Anatel em função da celebração de termos de ajustamento de conduta, de outorga onerosa de autorização de uso de radiofrequência e de atos regulatórios em geral, devendo ser direcionados às seguintes iniciativas:

// I - expansão das redes de transporte de telecomunicações de alta capacidade, com prioridade para: (i) cidades, vilas, áreas urbanas isoladas e aglomerados rurais que ainda não disponham dessa infraestrutura; e (ii) localidades com projetos aprovados de implantação de Cidades Conectadas;

// II - expansão da cobertura de redes de acesso móvel, em banda larga, priorizado o atendimento de cidades, vilas, áreas urbanas isoladas, aglomerados rurais e rodovias federais que não disponham desse tipo de infraestrutura;

// III - expansão das redes de acesso em banda larga fixa, com prioridade para setores censitários, conforme classificação do Instituto Brasileiro de Geografia e Estatística, sem oferta de acesso à internet por meio desse tipo de infraestrutura; e

// IV- prestação temporária de serviço de banda larga fixa ou móvel com o objetivo de promover o acesso à internet, para uso individual ou coletivo, de pessoas físicas ou jurídicas estabelecidas em ato do Ministério das Comunicações.

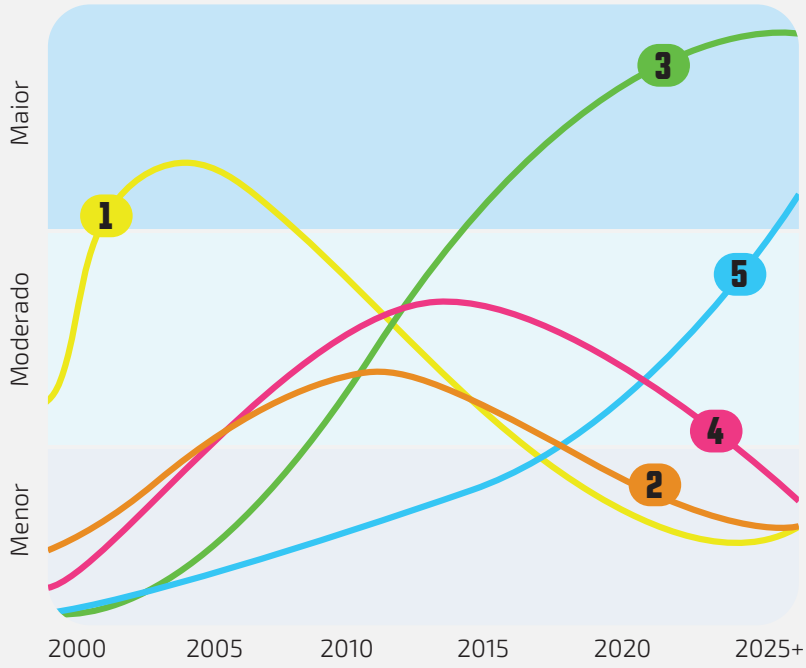
3. CONTEXTUALIZAÇÃO E DESAFIOS DA CONECTIVIDADE

Panorama atual da conectividade

Desde sua criação em 1997, a Anatel vem atuando ativamente na promoção do acesso de qualidade às infraestruturas de telecomunicações no país, sendo que, nesse período, o seu foco esteve em torno da universalização do acesso, da promoção da competição e do zelo pela qualidade dos serviços.

Ao longo desse tempo, os serviços de telecomunicações e os usos de conectividade mudaram conforme a queda da importância dos usos tradicionais da conectividade e a ascensão de novos usos, nomeadamente de serviços ligados à comunicação via internet. Há hoje quatro principais serviços de interesse coletivo: o Serviço de Comunicação Multimídia (SCM), o Serviço Móvel Pessoal (SMP), o Serviço Telefônico Fixo Comutado (STFC) e o Serviço de Acesso Condicionado (SeAC), que se destacam pelas diferentes evoluções em termos de relevância econômica e maturidade tecnológica no país.

Figura 5: A importância dos serviços de telecomunicações no cenário brasileiro



1 Telefonia Fixa (STFC)
Com a mudança nos hábitos da população, vem perdendo relevância e deve se tornar cada vez mais um serviço de nicho (ex. apenas empresas).

2 TV por Assinatura (SeAC)
Tendência atual é de que perca relevância com o crescimento de serviços de streaming.

3 Telefonia móvel (SMP) | Dados
Grande crescimento nos últimos anos deve-se manter como o mais relevante no país, impulsionado pelo 5G.

4 Telefonia móvel (SMP) | Voz
Grande expansão inicial, porém redução nos últimos anos conforme se popularizou a comunicação por áudio através de aplicações online (ex. Whatsapp).

5 Banda Larga Fixa (SCM)
Tendência constante de crescimento, vem ganhando relevância no país e deve assumir papel de destaque cada vez maior com a expansão de invetimentos feitos conforme metas impostas a concessionárias do STFC e vencedores do leilão do 5G.

Observa-se que os serviços tradicionais de conectividade (serviço de voz fixo, o serviço de voz móvel e a televisão por assinatura) tiveram, no geral, uma redução de adesão dos últimos anos.

Ao avaliar os números de acessos, as receitas por unidade e as receitas operacionais líquidas desses três setores, constata-se um decréscimo nesses indicadores, evidenciando a redução da sua relevância para conectividade.

Figura 6: Evolução dos acessos de telecomunicações

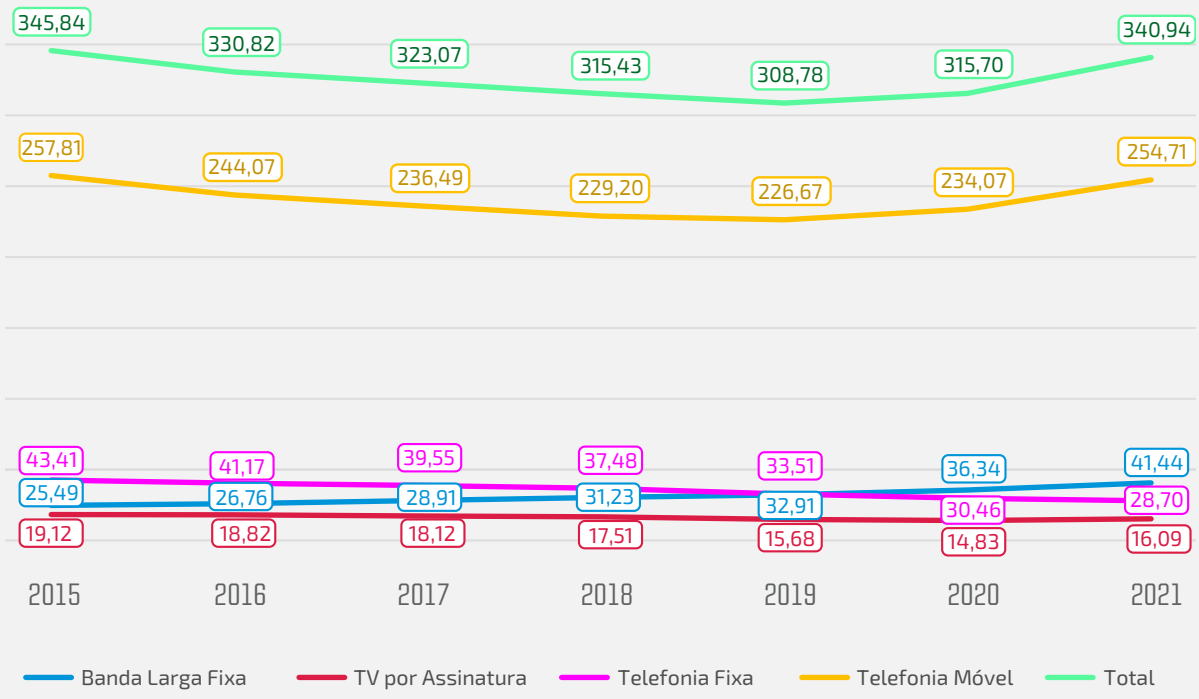
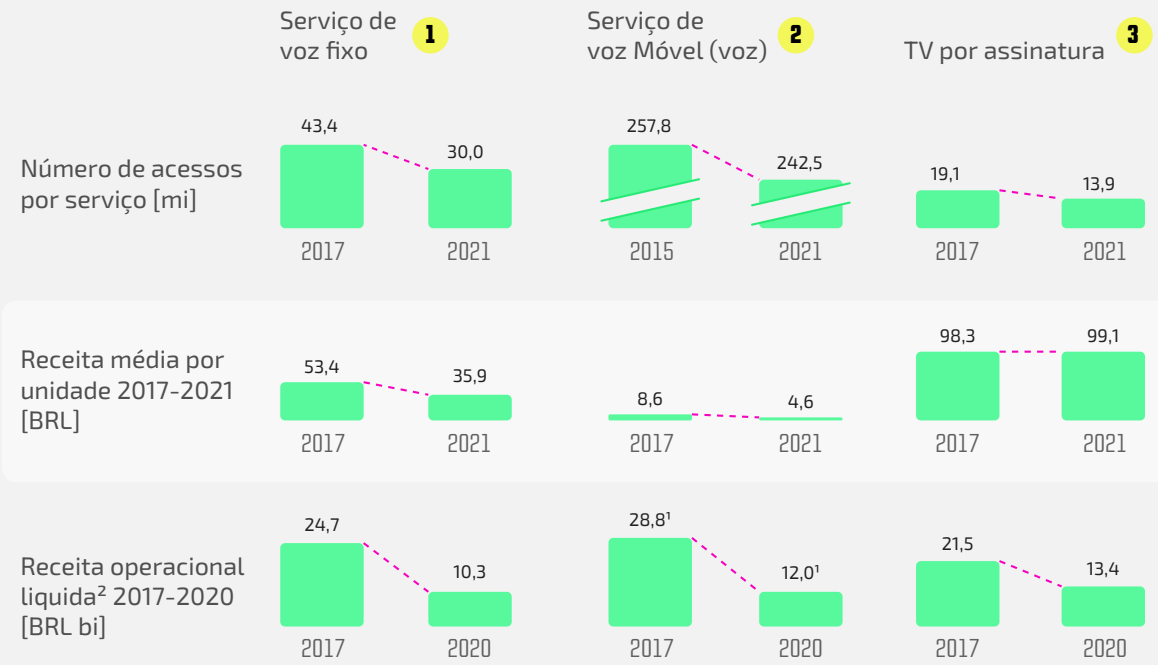


Figura 7: Panorama dos usos tradicionais de conectividade



1 Receita operacional do serviço de voz móvel é bruta, calculada com base na proxy de preço por minuto e número de minutos saintes

O serviço de voz fixo (STFC) tem reduzido a sua relevância na comunicação, sendo substituído, em ampla escala, pelo serviço de voz móvel (SMP) ou por alternativas digitais. Atualmente, os planos corporativos e vendas conjuntas (pacotes/combos) de serviços de conectividade são responsáveis por grande parte dos contratos de STFC.

O serviço de voz móvel também tem sofrido com o processo progressivo de substituição pelo serviço de voz por meio da rede de dados ou plataformas de videoconferência, fato este observado a partir da média do tempo de uso da telefonia móvel por usuário, que segue tendência de retração desde 2017.

A redução da relevância da televisão por assinatura, por sua vez, ocorre, principalmente, devido à competição com os serviços de streaming e vídeos online.

3.0.1 Serviço de Comunicação Multimídia

O Serviço de Comunicação Multimídia (SCM ou banda larga fixa) apresentou em 2021 crescimento de 14,0% em relação ao ano anterior, um acréscimo de 5,1 milhões de novos acessos em serviço, representando o principal serviço de telecomunicações para a oferta de acesso fixo à internet em banda larga e encerrou o ano de 2021 com 41,4 milhões de acessos em serviço.

Figura 8: Evolução dos acessos de banda larga fixa [Milhões]

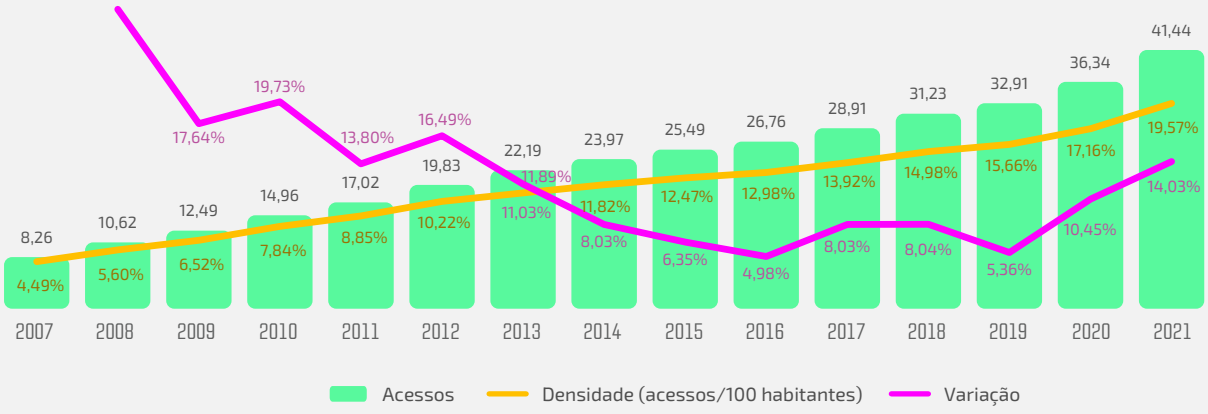
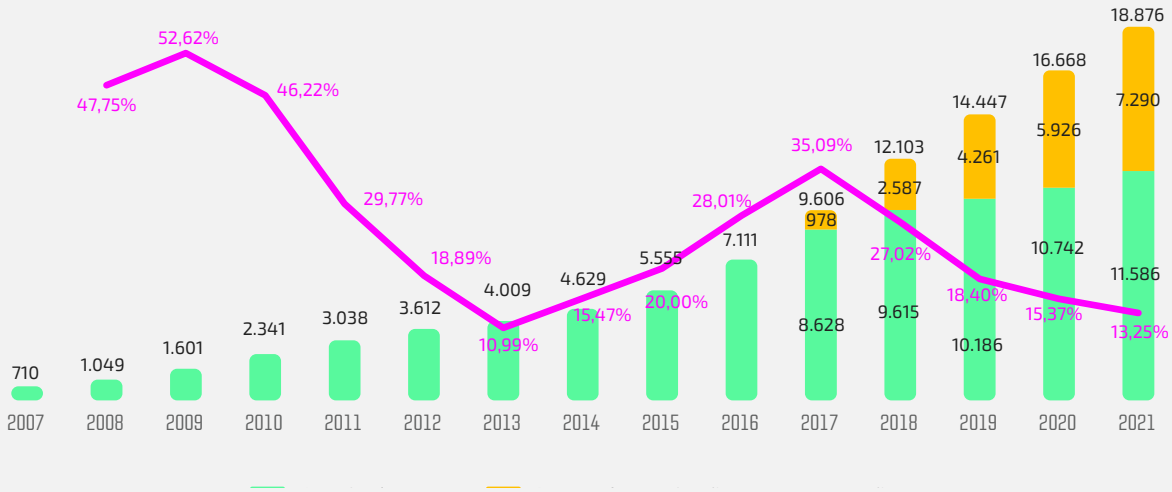


Figura 9: Evolução do número de prestadoras de banda larga fixa



Com crescimento de 13,2% em relação a 2020, o Brasil fechou 2021 com pouco menos de 18,9 mil empresas que fornecem o Serviço de Comunicação Multimídia (SCM ou banda larga fixa), com destaque para o crescimento das prestadoras isentas de autorização, modalidade existente desde 2017.

Em relação à dinâmica competitiva nos mercados, notam-se diferenças expressivas na comparação com outros serviços de telecomunicações. Isso se dá em função do crescimento significativo das prestadoras de pequeno porte, PPPs, tal que em 2021, 51,7% do mercado nacional era detido pelas 3 principais prestadoras e 46,7% era detido por prestadoras de pequeno porte.

Ainda quanto ao papel desempenhado pelas PPPs no cenário nacional, é possível constatar que desempenham um papel central de expansão do acesso com qualidade ao SCM, explorando regiões menos atrativas para as grandes prestadoras. Além disso, a tecnologia de fibra óptica responde por 85,9% das conexões dentre as PPPs, enquanto entre as grandes prestadoras está presente em cerca de 42,3% das conexões.

3.0.2 Serviço Móvel Pessoal

Na telefonia móvel, o Brasil encerrou 2021, com 254,7 milhões de acessos do Serviço Móvel Pessoal (SMP), número 8,8% maior que o do final de 2020. Nos últimos 12 meses, as grandes operadoras – aquelas que possuem ao menos 5% do mercado – tiveram incremento de 21,7 milhões de acessos, enquanto as prestadoras de pequeno porte diminuíram sua base em 1,1 milhão de acessos.

Em 2021, a tecnologia LTE, usada para a oferta do 4G, seguiu em expansão, sendo esse resultado devido, entre outros fatores, às obrigações estabelecidas pela Anatel nas licitações realizadas para a prestação do SMP por meio dessa tecnologia. No final do período, 5.540 municípios eram atendidos com 3G e 5.446 municípios também com 4G. O desafio para os próximos anos será aumentar a penetração, oferta e adoção de tecnologias de suporte à banda larga móvel, atingindo uma proporção cada vez maior de municípios.

3.0.3 Serviço de Telefonia Fixa Comutado

No Brasil, havia em 2021 aproximadamente 28,7 milhões de acessos em serviço na telefonia fixa, o que representa uma redução de 5,8% em relação a 2020. Conforme últimos dados disponibilizados pela União Internacional de Telecomunicações (UIT), o Brasil ocupa a 64° posição no cenário internacional, com 14,4 assinantes por grupo de 100 habitantes. A queda no número de acessos de telefonia fixa demonstra a substituição do STFC por outras modalidades de serviços, principalmente pelo Serviço Móvel Pessoal (SMP) e pelo Serviço de Comunicação Multimídia (SCM).

Futuramente, todo o segmento passará por um grande desafio e, possivelmente, por transformações significativas com o fim do prazo das concessões do setor em 2025.

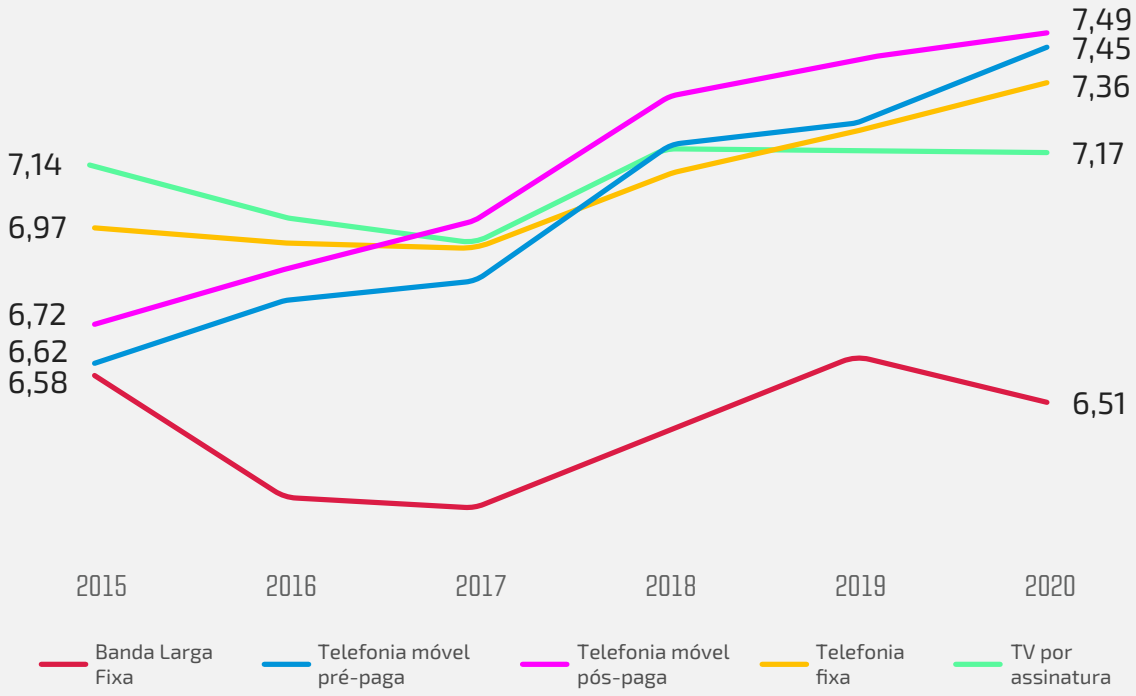
3.0.4 Serviço de Acesso Condicionado

A exemplo do que ocorreu com o serviço de telefonia fixa, a TV por assinatura também registrou redução da base de assinantes em 2021. O SeAC passa por uma perda de relevância recente devido, entre outros fatores, ao crescimento de serviços de *streaming* de vídeo oferecidos por OTTs. Atualmente, existe uma tendência de perda de interesse dos consumidores pela TV por assinatura em oposição ao crescimento da demanda por dados e por serviços de *streaming*.

O número de acessos do SeAC alcançou 16,1 milhões no final de 2021, porém o aumento de 8,5% relativo a 2020 é consequência do acréscimo de aproximadamente 2,5 milhões acessos, via satélite e sem assinatura paga, que começaram a ser acompanhados pela Anatel no período.

Na avaliação dos serviços de telecomunicações, nota-se melhoria expressiva da satisfação dos consumidores com serviços de telefonia móvel e telefonia fixa, além de certa estabilidade na satisfação quanto à TV por assinatura e à banda larga fixa, comparando-se às notas consolidadas de satisfação geral por serviço no país entre os anos de 2015 e 2020.

Figura 10: Evolução da nota consolidada de Satisfação Geral com os serviços de telecomunicações no país



Pesquisa de Satisfação e Qualidade Percebida, em que
0 = totalmente insatisfeito;
10 = totalmente satisfeito,
sendo as notas definidas a partir da consolidação de todas as operadoras e Unidades Federativas pesquisadas

Em termos de qualidade dos serviços oferecidos à população, houve significativa melhora da velocidade de conexão de internet e da utilização da tecnologia 4G (dominante no Brasil), a partir da expansão da fibra óptica nos municípios do país..

Neste sentido observa-se que mesmo com diversas ações da Anatel visando aprimorar a qualidade da prestação dos serviços nos últimos anos, ainda persiste a necessidade de avanços a fim de promover a ampliação do acesso aos serviços de telecomunicações e a satisfação do consumidor, cada vez mais exigente quanto à qualidade desejada e dependente de telecomunicações para a realização de atividades cotidianas.

Desafios da Anatel

3.0.5 Tendências externas

Na análise de ambiente externo foram identificadas quatro tendências principais que atuarão como alavancas de transformação do setor, gerando desafios e oportunidades para a atuação institucional nos próximos anos: (i) introdução e expansão gradual de novas tecnologias de 5G; (ii) crescimento dos serviços OTT (over-the-top); (iii) cibersegurança e privacidade de dados pessoais; e (iv) demanda por uma regulação mais ágil, responsiva e articulada por parte da Anatel. Além dessas tendências, uma incerteza crítica com potenciais impactos sobre a atividade regulatória da Anatel surge no horizonte temporal: a possível assunção de atribuições relativas à regulação dos serviços postais, num cenário de privatização da Empresa Brasileira de Correios e Telégrafos (ECT) e aprovação do marco legal do Sistema Nacional de Serviços Postais.

O 5G será catalisador de uma revolução digital em termos de suas aplicações, tendo um grande impacto sobre a oferta e fruição de serviços. Indústria, energia, segurança pública, medicina e entretenimento são exemplos de setores em que o 5G terá grande impacto.

Nos próximos anos, espera-se a manutenção da tendência de crescimento acelerado dos serviços chamados OTT. O crescimento desses serviços tem produzido um intenso debate regulatório global, cujo cerne concentra-se no equilíbrio entre seus benefícios aos consumidores e a sustentabilidade dos investimentos necessários ao processo de expansão dos serviços de telecomunicações.

No Brasil, a ascensão dos serviços OTT traz consigo desafios principalmente no que tange ao relacionamento entre seus

ofertantes e o órgão regulador de telecomunicações, em função das restrições legais ao escopo de atuação da Agência; e à existência de possíveis divergências entre as normas que regem a oferta de conteúdos por radiodifusão, TV por assinatura e OTT.

A cibersegurança e privacidade dos dados pessoais são temas cada vez mais relevantes, devido, entre outros fatores, ao crescimento na quantidade de ataques cibernéticos reportados no Brasil e no mundo. Nesse contexto, a Anatel aprovou normativo instituindo diretrizes e requisitos para elaboração de Políticas de Segurança Cibernética por empresas do setor de telecomunicações (Resolução Anatel nº 740, de 21 de dezembro de 2020), com foco na obrigatoriedade de adoção de normas, padrões e boas práticas no desenvolvimento e gestão das redes que suportam a prestação dos serviços de telecomunicações.

Sob o ponto de vista da atividade de regulação, agências reguladoras do mundo todo e de diferentes setores têm se deparado com a necessidade, cada vez mais premente, de adotar uma regulação ágil e responsiva, acompanhando o ritmo de inovação do mercado e buscando a cooperação regulatória, na medida em que novos produtos e serviços convergem, combinando características de mais de um setor. Esse cenário requer que as autoridades regulatórias envolvidas estejam prontas para atuar de forma conjunta e articulada.

Por fim, a possível assunção de atribuições relativas à regulação dos serviços postais, num cenário de privatização dos Correios e aprovação do marco legal do Sistema Nacional de Serviços Postais, deve ser considerada. Nesse contexto hipotético, a Anatel receberia atribuições típicas de órgão regulador dos serviços postais, com competências para implementar, regular e fiscalizar a política postal brasileira, caso permaneçam os termos da proposição legislativa em trâmite no Congresso Nacional (PL 591/2021).

3.0.6 Aspectos da gestão interna

Nos últimos anos, a Agência buscou aumentar seu foco em resultados, todavia, ainda há espaço para melhorias na regulação, haja vista que a convergência tecnológica irá exigir que a regulação seja colaborativa e multidisciplinar, demandando uma abordagem mais principiológica e com voz ativa dos agentes de mercado.

Há de se salientar também todo o esforço concentrado na iniciativa de simplificação e atualização regulatória e as iniciativas de regulação responsiva até então implementadas.

A gestão das tarefas já está consolidada e madura dentro da Agência, mas será essencial adaptá-las para suportar as mudanças que a tecnologia trará para a regulação. Com a estrutura atual implementada em 2013, houve grande evolução na gestão dos processos, havendo ainda grande potencial para automação e digitalização de atividades.

As aplicações de inteligência de dados ainda são pouco utilizadas, havendo espaço para maior aproveitamento, avançando também no mapeamento de atividades dentro das áreas, para uma visão mais precisa do que poderá ser automatizado. As atividades de fiscalização contarão cada vez mais com iniciativas e parcerias que impulsionarão a automação dos processos e a autorregulação.

Em face de tais expectativas, entende-se que a Agência evoluiu de forma bastante expressiva em uma série de temas ligados à gestão interna e a sua forma de atuação nos últimos anos, de modo que há, majoritariamente, apenas refinamentos a serem endereçados.

Por fim, com relação aos pontos a endereçar mencionados acima, ressaltam-se a necessidade de oxigenação do quadro da Agência, o aprimoramento dos métodos de avaliação de desempenho individual e o robustecimento da inteligência institucional, a fim de que a Anatel seja plenamente capaz de acompanhar o ritmo de inovação tecnológica e de transformação setorial.

Cenários prospectivos da conectividade

A avaliação de cenários prospectivos constitui o eixo fundamental para a proposição de um posicionamento estratégico institucional que seja resiliente às volatilidades, incertezas, complexidade e ambiguidades características do ambiente.

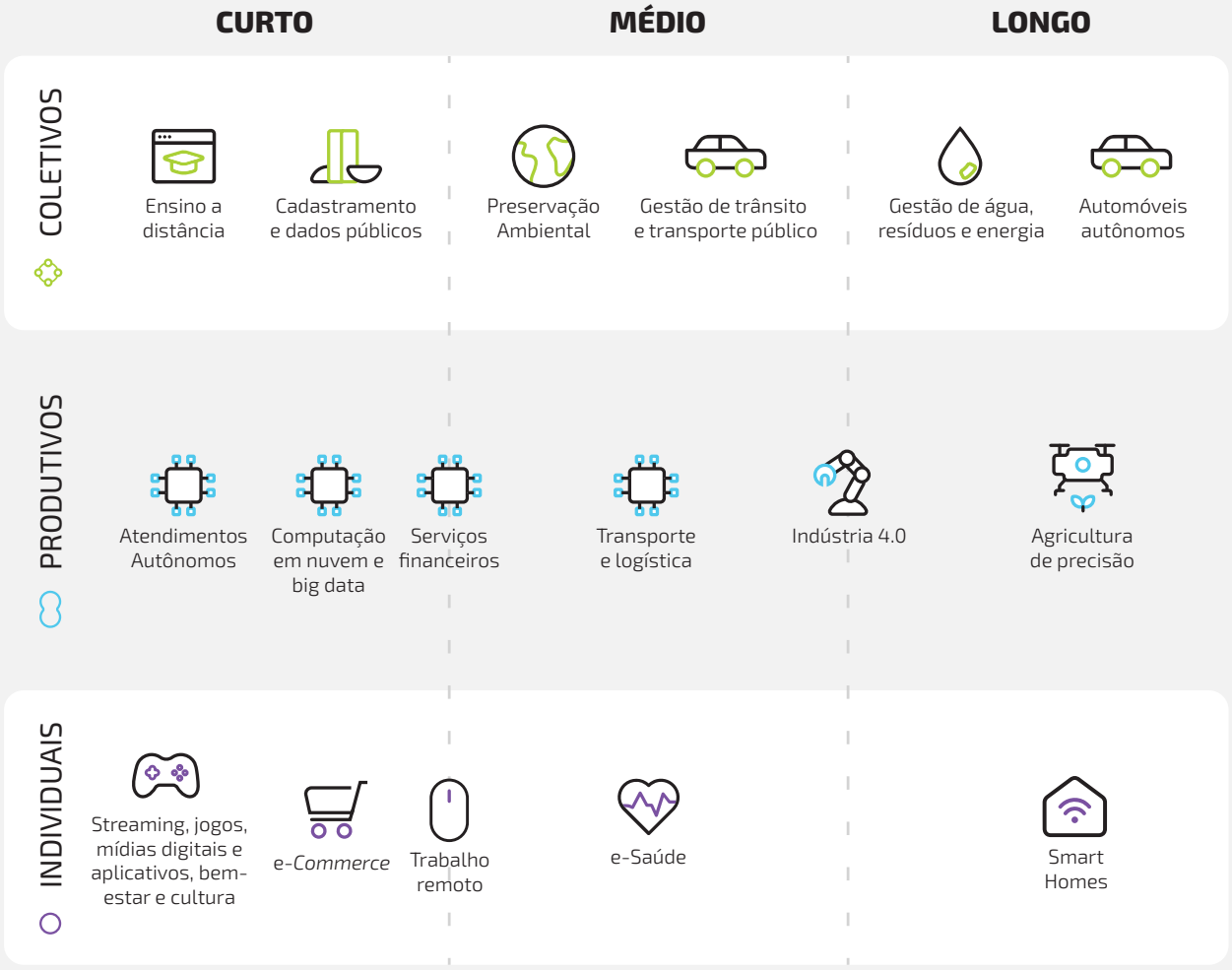
O desenvolvimento da conectividade exigirá requisitos regulatórios e de infraestrutura que acompanharão a mudança da dinâmica do mercado. A adoção das tecnologias futuras nos níveis coletivo, produtivo e individual é, em grande parte, dependente da recuperação econômica, do próprio desenvolvimento tecnológico e da formulação de políticas públicas orientadas a esse desenvolvimento.Essas tecnologias futuras comporão a evolução da economia digital caracterizada por ecossistemas que eliminarão as fronteiras setoriais tradicionais.

A visão de futuro da conectividade pode ser dividida nas perspectivas da demanda e da oferta, sendo que nesta última consideram-se duas camadas principais: uma relacionada à infraestrutura física e outra, às plataformas e ecossistemas nas quais se desenvolvem os usos da conectividade.

3.0.7 Os usos futuros da conectividade

Os usos coletivos são tipificados como aqueles de tecnologia de rede num contexto de sociedade como um todo, considerando a convivência e a interação entre os indivíduos. Os usos produtivos são definidos como aqueles relacionados à produção econômica na sociedade, e os individuais como aqueles relacionados às tecnologias que impactam no dia a dia de forma mais pessoal e na manutenção e melhoria do estilo de vida das pessoas.

Figura 11: Usos futuros da conectividade



Fonte: ANATEL; Roland Berger

Por exemplo, maiores velocidades de conexão poderão permitir a universalização da educação através do ensino a distância, com ganhos de qualidade de vídeo e facilitação da interação por meio de menores latências na conectividade entre alunos e professores, possibilitando também a integração entre o ensino digital e físico no ensino híbrido, culminando na aplicação de metodologias de ensino inovadoras no Brasil.

Na gestão pública, estarão inseridas as questões de disponibilização de informações à sociedade de forma digital, como as relacionadas com saúde, anúncios, clima, informações de turismo, assim como o cadastramento de dados públicos, documentações oficiais digitalizadas e um sistema único de fácil acesso por diversos órgãos governamentais, permitindo a disponibilização de serviços públicos por vias digitais.

Nos usos produtivos, considera-se como foco central para os próximos anos: a agricultura de precisão, os serviços financeiros e a implementação da indústria 4.0, sendo que neste último caso vislumbra-se a integração entre máquinas e funcionários, em um modelo de tomada de decisões em tempo real, com foco na conexão da cadeia produtiva e acompanhamento de máquinas e qualidade de produção por meio de uma multiplicidade de sensores.

No quesito de bem-estar e lazer, podem-se observar aspectos como *streaming*, jogos, mídias sociais e aplicativos com usos crescentes de rede, com a adoção cada vez mais ampla por parte da população, possibilitada por um aumento do acesso e por uma melhora da qualidade da rede.

A realidade aumentada e a realidade virtual têm o potencial de mudar significativamente a forma como interagimos com esportes, com o cuidado do bem-estar individual e como buscamos lazer.

Por fim, no uso doméstico, há possibilidade de controlar remotamente os domicílios, por meio, por exemplo, de um ecossistema digital de segurança e do acionamento de produtos de linha branca, como geladeiras, máquinas de lavar, entre outros.

3.0.8 Desenvolvimento da economia digital e a dinâmica da conectividade

Nesta nova economia digital, em que os dados são o grande produto que passa nas infraestruturas de telecomunicações, o conceito de telecomunicações assume uma perspectiva mais ampla de conectividade na qual passam a atuar outros tipos de agentes que reconfiguram os tradicionais mercados de atacado e varejo. Por exemplo, atualmente as pessoas continuam utilizando o serviço de voz, ou de voz e imagem, mas priorizam uma comunicação por meio da internet com a mediação de plataformas digitais. Esses atores mencionados podem ser atacadistas ou varejistas. Então, tem-se uma segunda camada de conectividade - caracterizada pelas plataformas que atuam dentro dos serviços de internet, possibilitando os serviços da conectividade - que de certa forma condiciona, como no passado condicionavam as telecomunicações, o desenvolvimento dos mercados. As plataformas atuantes no contexto digital atuam em diversos setores produtivos e mudam fundamentalmente a forma como os serviços são oferecidos, formando ecossistemas digitais compostos por diversos agentes que oferecem soluções multisetoriais.

Algumas plataformas e os ecossistemas digitais constituem-se, já hoje, infraestruturas e serviços de interesse coletivo - serviços dos quais as pessoas dependem no seu cotidiano - e têm como regulação exclusiva a autorregulação, que pode comportar falhas envolvendo direitos e garantias, inovação, competição e ainda os direitos dos consumidores.

Por outro lado, observa-se que a cadeia de valor da conectividade nos últimos anos deixou de ter grande foco no setor de fornecimento de acesso à conectividade (i.e infraestrutura de comunicações), passando a ser muito superior nas atividades que utilizam a camada de serviços de conectividade, como o comércio digital, as redes sociais e os *e-services*.

De forma a evidenciar essa alteração na cadeia de valor, considerando esse conceito alargado da conectividade, desde a infraestrutura até os serviços digitais, constata-se que, em 2017, as telecomunicações (aqui expressando os serviços de rede fixa e móvel) representava 33% do valor dessa cadeia, ao passo que, em 2020, ela passou a representar 22%. E isso não ocorreu pela mera ausência de crescimento da conectividade: o oferecimento de serviços de rede móvel e fixa gerou um volume maior de receitas do que nos setores tradicionais, porém, relativamente aos demais setores, houve um encolhimento relativo da relevância da conectividade.

Os setores de interface dos usuários, compostos pelos *smartphones* e dispositivos conectados, são setores que cresceram fortemente (73,6%), mas principalmente o setor dos serviços digitais teve um crescimento de mais de duas vezes, considerando o *e-commerce*, a propaganda digital, a mídia e os *e-services*. Isso é uma importante alteração, uma vez que molda a dinâmica do mercado e influencia a tomada de decisões dos agentes diretamente ligados aos elementos da cadeia de valor em processo em encolhimento. Isso ocorre porque a perda de relevância na cadeia de valor atrai menos investimentos e, por outro lado, setores em expansão atraem mais.

Do lado da oferta de conectividade, o desenvolvimento harmonioso da economia digital no Brasil obrigará a atenção regulatória em diversas matérias, como: a abertura de API (interface a programação de aplicações) de plataformas, a transparência de algoritmos, a identificação eletrônica de usuários, a portabilidade de dados e o controle do seu armazenamento.

Conjuntamente, do lado da demanda serão necessárias ações para o desenvolvimento da cibersegurança, para a proteção de dados dos consumidores, para a capacitação de indivíduos e para o incentivo à inovação e ao desenvolvimento setoriais.

3.0.9 Novos requisitos das infraestruturas físicas de suporte à conectividade

No Brasil, a demanda por velocidade nos acessos digitais tem crescido e continuará crescendo em razão da digitalização do país. Os novos usos de conectividade, tal como os serviços de telemedicina, precisarão de grande velocidade de rede para a transmissão de imagens de alta definição e a comunicação de sistemas.

Também será necessária a capacidade de múltiplas conexões para conectar o número enorme de sensores que a indústria 4.0 vai requerer. Além disso, para atender às necessidades de competitividade futura do agronegócio, adotando uma agricultura de precisão, e para atender aos carros autônomos, sem problemas significativos de segurança, serão necessárias grandes coberturas geográficas, incluindo locais remotos, com condições de latência baixíssimas.

Para a obtenção dessas características centrais da rede (velocidade, capacidade, cobertura e latência) em níveis suficientes para o desenvolvimento pleno dos novos usos da conectividade e dos ecossistemas a eles associados, será necessário um grande volume de investimentos e de modo permanente. No cerne disso se encontra o desenvolvimento do 5G e de *full gigabits networks* (redes de alta capacidade) com níveis suficientes de qualidade, o que exigirá extensos investimentos.

Para suprir essa demanda, será necessária a construção de redes sustentáveis, modificando *backbone*, *backhaul* e os acessos finais da rede, observando-se os cinco principais atributos para uma infraestrutura de longo prazo: escalabilidade, confiança, qualidade, simplicidade e elementos de sistemas de conectividade.

3.0.10 Cenário-alvo para a estratégia da Anatel

Para a elaboração dos cenários futuros mais prováveis, foram consideradas as tendências e incertezas identificadas e os fatores que influenciam a estratégia da Anatel no curto, médio e longo prazos.

Sob o contexto da análise de tendências e incertezas que deverão moldar os potenciais futuros da conectividade, estabeleceram-se, como dimensões-chave para os cenários prospectivos, o nível de acesso/conectividade (oferta) e o ritmo de digitalização da economia (demanda).

Quanto ao nível de conectividade, consideraram-se os seguintes quesitos qualitativos:

a. flexibilidade de compartilhamento de infraestrutura através de aspectos como mercado secundário de espectro e tecnologias como o OpenRAN;

b. evoluções na tributação e a reação dos principais agentes às novas regras;

c. intenção de investimento em infraestrutura de telecomunicações e *compliance* com compromissos firmados em editais e planos de universalização;

d. evolução da P&D de novas tecnologias que otimizem o potencial de uso do 5G e permitam velocidades fixas mais elevadas e menores custos de investimento; e

e. recuperação econômica do país e seu impacto na renda e investimentos.

Quanto ao ritmo de digitalização, foram apreciados os seguintes elementos qualitativos na análise dos cenários:

a. evolução da regulação, implantação e massificação das novas tecnologias prospectivas no âmbito individual, coletivo e produtivo;

b. nível de confiança da população na rede, dadas a cibersegurança e a proteção de dados;

c. nível de capacitação digital da população;

d. evolução da interoperabilidade das diferentes redes e portabilidade de dados;

e. alterações em regulações e padrões que impactem no acesso *e-ids* (Sistemas de Detecção de Intrusão), transparência de algoritmos, abertura de APIs, dentre outros; e

f. evolução do poder de mercado e relevância de grandes plataformas, tanto as focadas em B2B *(business to business)* quanto em B2C *(business to customer)*.

O cenário ideal é o que se denominou “Brasil no G20 Digital”. Trata-se de um país que desenvolve todo o seu potencial econômico-social com uma pujante economia digital. Nele, cria-se um mercado que é dinâmico tanto do ponto de vista da oferta (porque há vários agentes que utilizam os meios disponíveis, sejam eles tangíveis ou intangíveis, para endereçar as necessidades crescentes dos usuários) quanto da demanda, em que os usuários demandam mais devido a um processo de retroalimentação – quanto maior a conectividade, maior o crescimento da conectividade, os usuários confiam mais nos sistemas, enxergam valor neles e têm os meios necessários para adotar as tecnologias de fronteira.

Entende-se que o futuro da conectividade trará muitas questões a serem decididas pelo Brasil, e a Anatel precisará estar preparada para as tendências e transformações observadas no setor, para potenciais falhas de mercado e para a eventual necessidade de regulação nesse mundo emergente.

Diante do cenário-base identificado, considera-se que os pilares deste Plano Estratégico sustentarão o direcionamento da Anatel e ditarão os rumos que almeja.

4. DECLARAÇÃO DA ESTRATÉGIA

Identidade Institucional

A declaração da identidade institucional estabelece o conjunto próprio de características que identifica a Anatel: a razão de sua existência, os ideais cultivados que amoldam os comportamentos; como pretende cumprir com seus objetivos; o papel atual exercido e o futuro desejado. Essas características são, respectivamente, o propósito, os valores, a missão e a visão que orientam o planejamento estratégico e a gestão cotidiana das atividades das equipes, auxiliando na tomada de decisões.

A Identidade Institucional da Agência é representada visualmente a seguir:

Figura 12: Identidade Institucional da Anatel

PROPÓSITO

Conectar o Brasil para melhorar a vida de seus cidadãos

VALORES

Inovação
Segurança Regulatória
Foco em resultados e efetividade
Construção Participativa

MISSÃO

Promover o desenvolvimento da conectividade e da digitalização do Brasil em benefício da sociedade

VISÃO

Ser uma instituição ativa na transformação digital no país, promovendo mercados dinâmicos com serviços de qualidade

4.0.1 Propósito

"Conectar o Brasil para melhorar a vida de seus cidadãos": a razão de existir da Anatel está ligada com a conectividade no Brasil e o impacto de sua atuação é contribuir para melhorar a vida dos brasileiros, sendo a regulação um instrumento que suportará esse progresso.

4.0.2 Valores

"***Inovação***": na medida em que as tecnologias avançam em uma velocidade crescente, a Anatel fomenta a sua atuação com medidas inovadoras para que a sociedade usufrua dos benefícios da evolução tecnológica.

"Segurança regulatória": traz estabilidade ao setor e o fiel cumprimento às normas e aos contratos vigentes, sendo elemento básico e fundamental para avalizar os investimentos necessários da conectividade.

"Foco em resultados e efetividade": essência de uma atuação eficaz e pragmática, permeando todas as atividades, finalísticas e de gestão, a Anatel está preparada para fazer o que deve ser feito da forma mais eficiente possível, com respeito aos recursos dos contribuintes, buscando o impacto positivo para a sociedade.

"Construção participativa": soluções regulatórias que buscam incorporar os pontos de vista, os anseios e a experiência dos mais diferentes atores governamentais, privados e da sociedade civil envolvidos ou afetados pelo ambiente da conectividade, são mais legítimas e eficientes."

4.0.3 Missão

"***Promover o desenvolvimento da conectividade e da digitalização do Brasil em benefício da sociedade":*** a Agência promove a reflexão contínua sobre o papel da conectividade para impulsionar o desenvolvimento econômico e social do Brasil, reduzindo as desigualdades regionais, sendo a força motriz da transformação digital do Brasil e a catalizadora da adoção das novas tecnologias pelo país.

4.0.4 Visão

"***Ser uma instituição ativa na transformação digital no país, promovendo mercados dinâmicos com serviços de qualidade"***: a agência visa ser reconhecida como uma instituição independente e imparcial que contribui para transformação digital do país e regula o setor em benefício da sociedade, tornando o mercado dinâmico, atraindo e ampliando os investimentos e garantindo a qualidade dos serviços oferecidos a todos.

Mapa Estratégico / Figura 13

PROPÓSITO

Conectar o Brasil para melhorar a vida de seus cidadãos

VALORES

Inovação
Segurança Regulatória
Foco em resultados e efetividade
Construção participativa

MISSÃO

Promover o desenvolvimento da conectividade e da digitalização do Brasil em benefício da sociedade

VISÃO

Ser uma instituição ativa na transformação digital no país, promovendo mercados dinâmicos com serviços de qualidade.

OBJETIVOS ESTRATÉGICOS DE RESULTADO

1 Promover a **conectividade** e a **prestação de serviços** de comunicação com qualidade para todos

2 Estimular **mercados dinâmicos e sustentáveis** de serviços de comunicação e conectividade

3 Fomentar a transformação digital junto à sociedade em condições de equilíbrio de mercado

4 Garantir atuação de **excelência** com **foco nos resultados** para a sociedade

OBJETIVOS ESTRATÉGICOS DE PROCESSOS

Infraestrutura e Qualidade

1A Viabilizar o acesso físico e a qualidade dos serviços a todos

1B Viabilizar a expansão e a implantação da infraestrutura da rede de base

1C Garantir o cumprimento de obrigações regulatórias

1D Proteger as infraestruturas críticas da conectividade

Dinamismo de Mercado

2A Garantir a adequabilidade da definição do mercado

2B Garantir equidade no acesso e nas regras aplicáveis aos agentes

2C Promover uso eficiente dos recursos escassos

2D Promover a atratividade e a sustentabilidade do setor pela modernidade da regulação

2E Promover o acesso econômico dos usuários

Modernidade, transformação digital, inovação e sociedade

3A Promover a conscientização e a segurança digital dos usuários e demais agentes

3B Fomentar aplicações e modelos de negócio inovadores

3C Promover a modernização da tecnologia de forma isonômica e transparente

Gestão interna

4A Promover a oxigenação e capacitação de servidores

4B Garantir a transparência e a gestão interna adequada

4C Garantir a adequabilidade da infraestrutura interna e das TICs

O Mapa Estratégico sintetiza o processo do planejamento estratégico da Anatel, contemplando a sua identidade institucional e o conjunto de objetivos estratégicos, com vistas a facilitar a compreensão pelo público interno e externo e demonstrar a correlação existente entre os diversos objetivos buscados no longo prazo.

Cadeia de Valor

A Cadeia de Valor visa a demonstrar os processos e as atividades executadas internamente, cujos produtos são responsáveis por entregar bens e serviços para a sociedade em consonância com a estratégia da Anatel. Está organizada em quatro ambientes de processos, a saber:

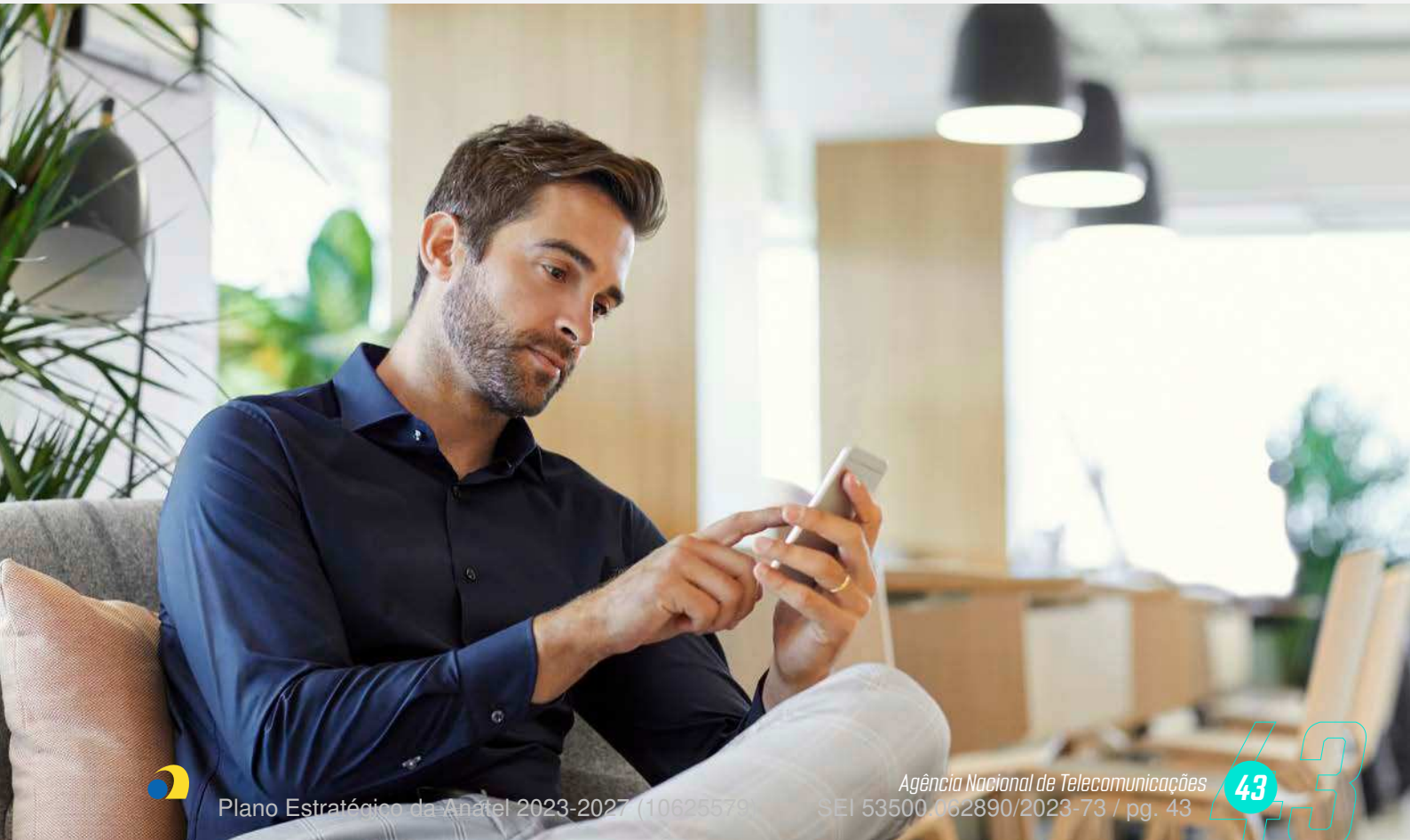
a. **Governança**: agrupa macroprocessos transversais de direcionamento ou controle dos demais processos institucionais;

b. **Relacionamento e Comunicação**: agrupa macroprocessos por meio dos quais a Agência se relaciona com outras instituições e com a sociedade;

c. **Regulação**: agrupa os macroprocessos finalísticos; e

d. **Gestão e Sustentação**: agrupa os macroprocessos transversais e multitemáticos voltados à execução dos outros processos da Agência.

Figura 14: Cadeia de Valor da ANATEL



5. OBJETIVOS ESTRATÉGICOS E METAS

Os Objetivos Estratégicos de Resultado servem para apoiar a Anatel no seu planejamento de atuação, delimitando os desafios futuros a serem superados. Os objetivos estão organizados em duas perspectivas – Resultados e Processos.

Os Objetivos de Resultado contemplam os objetivos finais da Agência, entendidos como aqueles que visam à entrega de um valor público à sociedade e estão alinhados com as exigências legais e com as políticas públicas vigentes.

Os Objetivos Estratégicos de Processos desdobram e detalham os objetivos estratégicos de resultado para um melhor direcionamento da atuação da Agência.

As metas visam a traduzir o valor público que será gerado e entregue pela Anatel à sociedade a partir do cumprimento de seus objetivos estratégicos a serem mensurados por indicadores que refletirão os principais resultados da regulação setorial e de sua gestão.

Objetivo de Resultado 1: Promover a conectividade e a prestação de serviços de comunicação com qualidade para todos

O ritmo acelerado de digitalização da economia, bem como a crescente dependência dos meios digitais para a realização de tarefas, intensifica ainda mais a vital importância dos serviços de comunicação para a efetiva participação de cada brasileiro na sociedade.

A transformação digital do País só será atingida de forma satisfatória se for universal. Por isso, a Agência deve fazer tudo que estiver ao seu alcance para garantir a universalidade e a qualidade dos serviços de comunicação.

A Agência atuará de forma responsiva e observará, em suas políticas regulatórias, as assimetrias regulatórias necessárias à garantia da inclusão digital.

Este objetivo visa, primordialmente, a direcionar as ações regulatórias futuras para um cenário em que todo e qualquer brasileiro, independentemente de classe ou localização geográfica, possa estar efetivamente integrado a essa nova sociedade da informação, aproveitando-se, de forma isonômica, de todos os benefícios inerentes ao acesso à conectividade.

5.0.1 Perspectiva de Processos: Infraestrutura e qualidade

5.0.1.1 1A) Viabilizar o acesso físico e a qualidade do serviço a todos

É preciso promover acesso a todos, conforme as particularidades do serviço e da região atendida, com conexão e capacidade adequadas para atender seus usos. Os padrões de excelência exigidos pelos novos usos da tecnologia serão significativamente superiores e precisarão de garantias contínuas para manter os usuários satisfeitos.

5.0.1.2 1B) Viabilizar a expansão e implantação da infraestrutura da rede de base

Os novos usos da conectividade exigirão cada vez mais a expansão da infraestrutura da rede de base, assim como a quantidade de acessos e de espaço em banda demandará um aumento da capacidade e da velocidade das redes de telecomunicações (*backbone* e *backhaul*).

5.0.1.3 1C) Garantir o cumprimento de obrigações regulatórias

O monitoramento adequado dos compromissos de investimento visará garantir a qualidade dos serviços prestados e, em razão do elevado crescimento de mercado, serão necessários novos mecanismos para regular o setor.

5.0.1.4 1D) Proteger as infraestruturas críticas da conectividade

As infraestruturas críticas são essenciais para o funcionamento da sociedade e da economia. A sua interrupção pode provocar sérios prejuízos, inclusive para a segurança nacional. Será necessário assegurar a proteção destas infraestruturas e definir boas práticas, padrões técnicos e regulatórios para garantir a segurança cibernética.

5.0.2 Metas

// **1.** Ampliar a cobertura da telefonia móvel 5G-SA de 0% em 2021 para 57,67% da população brasileira até 2027.

// **2.** Expandir a conectividade de backhaul de fibra óptica de 83,97% para 100% dos municípios brasileiros até 2027.

// **3.** Expandir a conectividade de backhaul de fibra óptica de 13,63% para 50% das localidades com mais de 600 habitantes até 2027.

// **4.** Aumentar a velocidade média contratada na banda larga fixa de 186,3 Mpbs para 1 Gbps até 2027.

// **5.** Impulsionar o cumprimento de excelência da velocidade contratada de 78,28% para 87% até 2027.

// **6.** Elevar o nível de satisfação geral dos consumidores da Banda Larga Fixa de 6,9 para 7,5 até 2027.

// **7.** Elevar o nível de satisfação geral dos consumidores da Telefonia Móvel de 7,6 para 8,1 até 2027.

Objetivo de Resultado 2: Estimular mercados dinâmicos e sustentáveis de serviços de comunicação e de conectividade

A ampliação do acesso aos serviços de comunicações e de conectividade, nos níveis de qualidade exigidos, movimenta diferentes atores do setor e depende de amplos investimentos nos diversos âmbitos da prestação, desde o desenvolvimento de novas tecnologias e a construção de redes, até a capacitação de pessoal e a melhoria de processos operacionais.

Para atrair os vultuosos investimentos necessários para a transformação digital do Brasil, será preciso zelar pela sustentabilidade econômica em todos os elos da cadeia de valor do setor produtivo para viabilizar seu desenvolvimento a longo prazo.

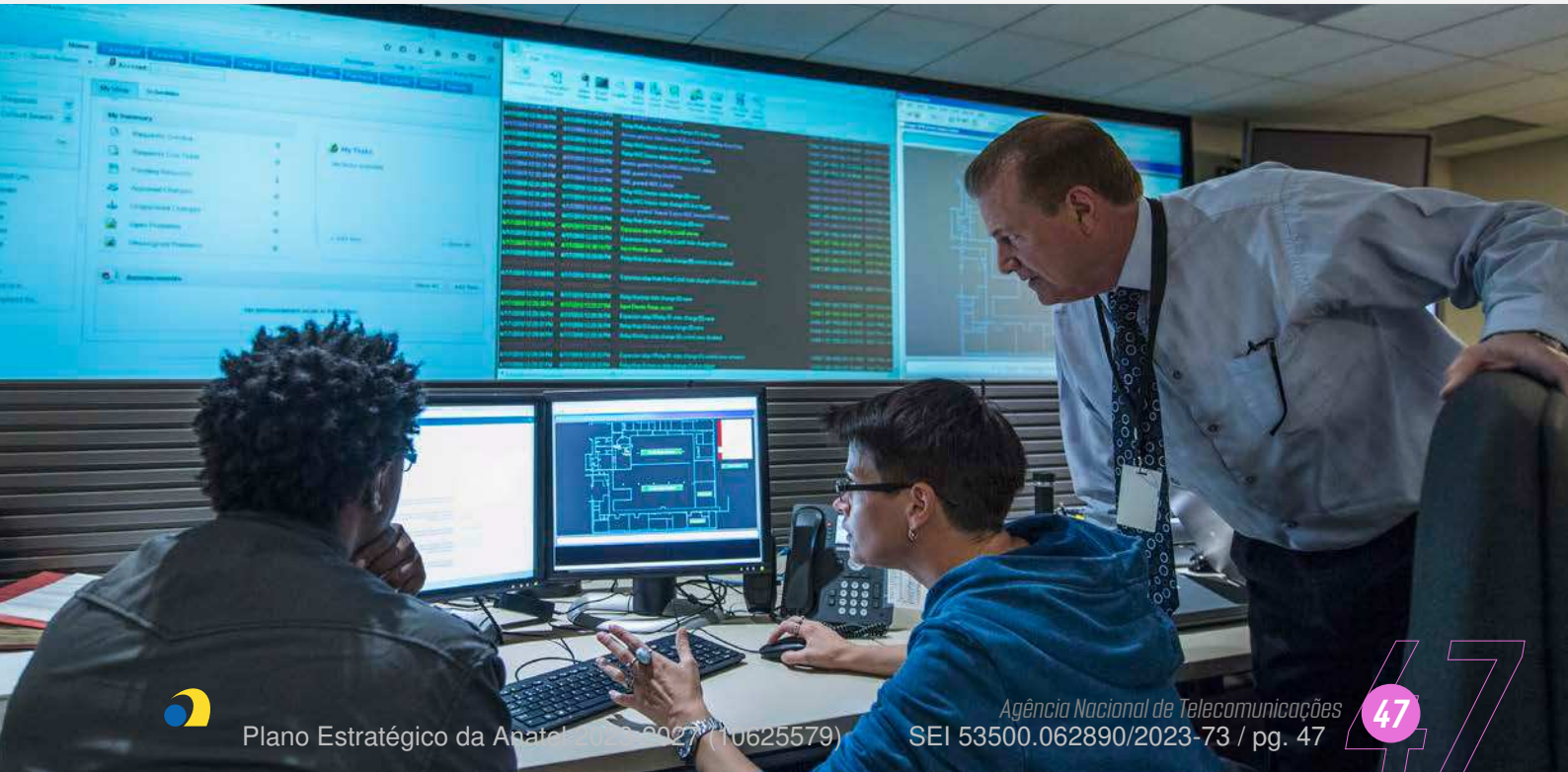
5.0.3 Perspectiva de Processos: Dinamismo de mercado

5.0.3.1 2A) Garantir a adequabilidade da definição do mercado

Com a digitalização e ampliação de serviços e agentes, as definições de mercado precisam ser atualizadas para que os serviços sejam devidamente regulados. Será necessário acompanhar a adoção das novas tecnologias e plataformas digitais, sua relação com os usuários e seus impactos no mercado.

5.0.3.2 2B) Garantir equidade no acesso e nas regras aplicáveis aos agentes

É fundamental que o mercado seja transparente, reduzindo a assimetria de informação por meio da disseminação de dados. É preciso assegurar que as barreiras de entrada sejam proporcionalmente idênticas a todos e que as condições de operação do mercado permitam a concorrencialidade, com regulação assimétrica quando necessário.



5.0.3.3 2C) Promover o uso eficiente dos recursos escassos

O foco deve ser a busca contínua pelo uso mais eficiente possível dos recursos escassos, como espectro, numeração, entre outros.

5.0.3.4 2D) Promover a atratividade e a sustentabilidade do setor pela modernidade da regulação

A regulação deve ser baseada em evidências e seguir o processo de aprimoramento e simplificação a fim de reduzir anacronismos. Para atrair e manter investidores é preciso oferecer previsibilidade, estabilidade e segurança regulatória.

5.0.3.5 2E) Promover o acesso econômico dos usuários

Em mercados concorrenciais, nem todos os usuários terão o acesso econômico aos serviços essenciais da conectividade, o que requer o desenvolvimento de iniciativas e políticas públicas para a promoção do acesso aos serviços de conectividade.

5.0.4 Metas

// **8.** Manter a competição de mercado de oferta de Banda Larga Fixa em cenário agressivo até 2027.

// **9.** Manter a competição de mercado de oferta de Telefonia Móvel em cenário conservador até 2027.

Objetivo de Resultado 3: Fomentar a transformação digital junto à sociedade em condições de equilíbrio de mercado

Com as mudanças na conectividade, nas quais plataformas e ecossistemas digitais ganham cada vez mais relevância, a Anatel atuará com foco específico na contribuição com a digitalização da sociedade e a condução do Brasil rumo ao estado da arte da tecnologia, zelando pelo equilíbrio tanto da oferta da conectividade (e dos serviços de telecomunicações que a apoiam) como também da demanda da conectividade, refletida na confiança dos usuários e os usos que eles enxergam nas redes.

5.0.5 Perspectiva de Processos: Modernidade, transformação digital, inovação e sociedade

5.0.5.1 3A) Promover a conscientização e a segurança digital dos usuários e demais agentes

Os usuários necessitam se manter capacitados para o bom uso da tecnologia e o entendimento de seus benefícios, estando conscientes de que suas interações digitais podem expor dados sensíveis na rede e que devem assumir a responsabilidade por suas ações.

Com o desenvolvimento de estudos e pesquisas, incluindo também a academia e o mercado em um trabalho colaborativo, a Anatel promoverá ações de prevenção contra fraudes no ecossistema digital e para a alfabetização digital dos usuários.

5.0.5.2 3B) Fomentar aplicações e modelos de negócio inovadores

O fomento de aplicações na digitalização da economia exigirá a eliminação das barreiras existentes, sejam elas regulatórias, de conhecimento, de capacitação ou de investimento, promovendo-se os benefícios, identificando-se gargalos e propondo-se soluções para os novos usos da conectividade. Portanto a Anatel buscará a proatividade no desenvolvimento do setor estando preparada para a construção de um ambiente convergente.

5.0.5.3 3C) Promover a modernização da tecnologia de forma isonômica e transparente

A Agência precisará antecipar-se às tendências e aferir os impactos de novas tecnologias, provendo informações à sociedade para ampliar o entendimento dos benefícios e impactos dessas mudanças.

5.0.6 Metas:

// **10.** Contribuir para ampliar o percentual de usuários de internet no Brasil de forma a mantê-lo compatível com os 20 países melhor avaliados pela União Internacional de Telecomunicações (UIT) até 2027.

// **11.** Contribuir para expandir o percentual de usuários de internet no Brasil com habilidades moderadas em tecnologias da informação e comunicação (TIC) de forma a mantê-lo compatível com os 20 países melhor avaliados pela União Internacional de Telecomunicações (UIT) até 2027.

Objetivo de Resultado 4: Garantir atuação de excelência com foco nos resultados para a sociedade

Será necessário garantir uma atuação de excelência, com foco nos resultados para a sociedade, de forma que os objetivos estratégicos sejam executados em sua plenitude.

A excelência deverá permear todas as atividades da Agência, englobando os processos de gestão e os finalísticos, sendo necessário buscar continuamente a manutenção da força de trabalho motivada e com alto nível de desempenho.

5.0.7 Perspectiva de Processos: Gestão interna

5.0.7.1 4A) Promover a oxigenação e a capacitação dos servidores

O equilíbrio da força de trabalho e sua capacitação são essenciais para garantir a excelência das entregas. O desempenho de excelência deve orientar a atuação, incluindo as alternativas de estratégias regulatórias e a avaliação dos servidores, que precisam estar alinhados com os instrumentos de incentivo utilizados pela Agência para promover a produtividade e um ambiente de trabalho saudável, capaz de motivar, desenvolver e reter talentos.

5.0.7.2 4B) Garantir a transparência e a gestão interna adequada

O planejamento é essencial para melhor alocar recursos e mitigar possíveis riscos, além de contribuir para a governança institucional. A Agência deve reforçar, de forma transparente e informativa, sua identidade institucional e seu papel desempenhado na regulação da conectividade. O uso de dados no processo de inteligência institucional permitirá a automação de processos e potencializará a qualidade e a velocidade das entregas.

5.0.7.3 4C) Garantir a adequabilidade da infraestrutura interna e das TICs

A Agência deve assegurar que todos os colaboradores possuam as ferramentas e as infraestruturas adequadas para trabalharem, buscando aproveitar oportunidades que porventura existam ou que venham a surgir para a automatização e digitalização de atividades.

5.0.8 Metas:

// **12.** Aprimorar o nível de governança e gestão da Anatel para estar compatível com os 20 órgãos e entidades melhor avaliados na Administração Pública Federal até 2027.

// **13.** Aumentar a disponibilidade de dados e informações da Anatel em formato aberto de 21,9% para 85% até 2027.

6. INICIATIVAS ESTRATÉGICAS

As iniciativas estratégicas são o conjunto de medidas a serem tomadas para impulsionar o atingimento dos objetivos estratégicos de processos com a finalidade de preencher as lacunas existentes entre o desempenho atual da Agência e o desejado para o futuro. Destinam-se, assim, a orientar o desenvolvimento de projetos ou planos de ação institucionais no bojo dos planejamentos táticos, com vistas ao alcance das metas da Anatel.

As iniciativas estratégicas serão detalhadas, priorizadas e executadas nos planos institucionais da Agência a partir das orientações constantes nos Planos de Gestão Táticos e dos resultados esperados abaixo:

Iniciativa 1: *Promover a cobertura nacional de redes e o aumento de capacidade disponibilizada no acesso*

Objetivo estratégico de processo:

1A) Viabilizar o acesso físico e a qualidade do serviço a todos

Resultados Esperados:

// Aumento na qualidade do serviço prestado; e

// Aumento da cobertura das redes.

Iniciativa 2: *Promover qualidade e transparência na oferta do serviço de Banda Larga Fixa*

Objetivo estratégico de processo:

1A) Viabilizar o acesso físico e a qualidade do serviço a todos

- Aumento na qualidade do serviço prestado;
- Aumento da competitividade do mercado; e
- Aumento da transparência na relação de consumo.

Iniciativa 3: *Aprimorar a capacidade, os mecanismos de compartilhamento e a qualidade da infraestrutura e de seu funcionamento*

Objetivo estratégico de processo:

1B) Viabilizar a expansão e implantação da infraestrutura da rede de base

Resultados Esperados:

- Realizar o diagnóstico de inteligência sobre a capacidade das redes;
- Subsidiar decisões quanto à cadeia de insumos de telecomunicações; e
- Elementos de rede e o compartilhamento de infraestrutura acessados de forma não discriminatória e a preços e condições justos e razoáveis.

Iniciativa 4: *Articular com o poder público pela padronização e simplificação de normas para instalação de antenas e demais infraestruturas*

Objetivo estratégico de processo:

1B) Viabilizar a expansão e implantação da infraestrutura da rede de base

Resultados Esperados:

- Articular nos âmbitos municipal e estadual para atualização das legislações de instalação de infraestrutura; e
- Estabelecer ferramenta de transparência e visibilidade acerca da simplificação e atualização de normas para instalação de infraestrutura.

Iniciativa 5: *Modernizar os mecanismos de inspeção*

Objetivo estratégico de processo:

1C) Garantir o cumprimento de obrigações regulatórias

Resultados Esperados:

- Redução no prazo de execução das ações de fiscalização; e
- Melhoria do relacionamento com o setor regulado.

Iniciativa 6: *Implementar o Regulamento de Fiscalização Regulatória e consolidar sua mudança cultural*

Objetivo estratégico de processo:

1C) Garantir o cumprimento de obrigações regulatórias

Resultados Esperados:

- Aumento do *compliance* na atuação regulatória pelos regulados;
- Aumento dos recursos regulatórios voltados à ampliação da infraestrutura;
- Aumento da cultura responsiva;
- Atuação mais responsiva e eficaz; e
- Redução dos passivos, desonerando os servidores para as atividades mais essenciais.

Iniciativa 7: *Promover o gerenciamento de risco holístico e a proteção das infraestruturas críticas*

Objetivo estratégico de processo:

1D) Proteger as infraestruturas críticas da conectividade

Resultados Esperados:

- Maior proteção das infraestruturas críticas; e
- Aumento da proteção contra ameaças cibernéticas.

Iniciativa 8: *Acompanhar a adoção das novas tecnologias e plataformas digitais*

Objetivo estratégico de processo:

2A) Garantir a adequabilidade das definições dos mercados

Resultados Esperados:

// Aumento do escopo de atuação da Agência; e

// Ampliação da clareza das definições de mercado.

Iniciativa 9: *Promover regulações adequadas ao contexto competitivo por meio do PGMC*

Objetivo estratégico de processo:

2B) Garantir equidade no acesso e nas regras aplicáveis aos agentes

Resultados Esperados:

// Maior assertividade da regulação;

// Aumento da competição do mercado;

// Maior eficiência alocativa e produtiva; e

// Maior transparência de informações disponibilizadas.

Iniciativa 10: *Otimizar as autorizações de uso de espectro e definir técnicas para implementação do mercado secundário*

Objetivo estratégico de processo:

2C) Promover o uso eficiente dos recursos escassos

Resultados Esperados:

// Aumentar a eficiência no uso do espectro; e

// Desenvolver técnicas para implementação do mercado secundário (transferência de direito de uso de radiofrequência).

Iniciativa 11: *Assegurar o equilíbrio e o planejamento dos usos futuros*

Objetivo estratégico de processo:

2C) Promover o uso eficiente dos recursos escassos

Resultados Esperados:

// Aumento da relevância do Brasil no cenário internacional; e

// Redução no prazo de início da utilização de novas tecnologias.

Iniciativa 12: *Buscar uma atuação baseada em evidências e a simplificação regulatória*

Objetivo estratégico de processo:

2D) Promover a atratividade e a sustentabilidade do setor pela modernidade da regulação

Resultados Esperados:

// Atuação mais principiológica; e

// Aumento da atratividade do setor.

Iniciativa 13: *Impulsionar a competição no ecossistema digital*

Objetivo estratégico de processo:

2D) Promover a atratividade e a sustentabilidade do setor pela modernidade da regulação

Resultados Esperados:

// Desenvolvimento do mercado de atacado; e

// Melhora do ambiente concorrencial.

Iniciativa 14: *Atingir o estado da arte da regulação para as novas tecnologias e modelos de negócio inovadores, inclusive através do sandbox regulatório*

Objetivo estratégico de processo:

2D) Promover a atratividade e a sustentabilidade do setor pela modernidade da regulação

Resultados Esperados:

- Aumento da velocidade de implementação e dos efeitos positivos do Open RAN e novas tecnologias; e
- Maior agilidade e capacidade na adaptação da regulação para as transformações futuras.

Iniciativa 15: *Estruturar o processo de monitoramento das ofertas varejistas*

Objetivo estratégico de processo:

2E) Promover o acesso econômico dos usuários.

Resultados Esperados:

- Disponibilizar para o consumidor informações precisas e atualizadas sobre os principais atributos das ofertas setoriais; e
- Subsidiar objetivamente políticas públicas voltadas ao fomento da demanda.

Iniciativa 16: *Promover instrumentos que permitam a viabilidade econômica aos serviços mesmo em situações de pouca atratividade*

Objetivo estratégico de processo:

2E) Promover o acesso econômico dos usuários

Resultados Esperados:

// Aumento da inclusão digital da população; e

// Melhora dos serviços prestados aos usuários.

Iniciativa 17: *Zelar pela prevenção contra fraudes no ecossistema digital*

Objetivo estratégico de processo:

3A) Promover a conscientização e a segurança digital dos usuários e demais agentes

Resultados Esperados:

// Redução de golpes/estelionatos digitais; e

// Aumento da confiança dos usuários na tecnologia.

Iniciativa 18: *Promover a alfabetização digital dos usuários*

Objetivo estratégico de processo:

3A) Promover a conscientização e a segurança digital dos usuários e demais agentes.

Resultados Esperados:

- Aumento da assimilação das informações sobre uso consciente de serviços digitais; e
- Aumento da participação e interesse interno da Agência na temática.

Iniciativa 19: *Promover a articulação e a cooperação para o desenvolvimento de novas tecnologias*

Objetivo estratégico de processo relacionado:

3B) Fomentar aplicações e modelos de negócio inovadores

Resultados Esperados:

- Maior agilidade no desenvolvimento da tecnologia;
- Ampliação das possibilidades de atuação;
- Aumento do reconhecimento da Agência como fomentadora de Inteligência e pesquisa;
- Promoção da articulação e da cooperação com o ecossistema de startups e empresas de TI; e
- Protagonismo nas discussões regulatórias por meio de uma atuação principiológica e convergente.

Iniciativa 20: *Promover estudos e acompanhar projetos sobre plataformas digitais e avaliar seus impactos no setor de telecomunicações*

Objetivo estratégico de processo:

3C) Promover a modernização da tecnologia de forma isonômica e transparente

Resultados Esperados:

- Fomentar o entendimento sobre as plataformas digitais, buscando maior equilíbrio entre os agentes do mercado.

Iniciativa 21: *Assegurar o desempenho, a capacitação e a motivação do quadro de servidores*

Objetivo estratégico de processo:

4A) Promover a oxigenação e capacitação dos servidores

Resultados Esperados:

- Aumento do desempenho dos servidores;
- Redução das lacunas de habilidades;
- Aumento da satisfação com o ambiente de trabalho;
- Desenvolvimento da capacidade de análise econômica e de negócios tecnológicos inovadores que impactem o ambiente de mercado regulado pela Anatel; e
- Uniformização do entendimento técnico e regulatório em face das Gerências Regionais.

Iniciativa 22: *Aprimorar a transparência, governança e a comunicação com os públicos externos*

Objetivo estratégico de processo:

4B) Garantir a transparência e a gestão interna adequada

Resultados Esperados:

- Melhoria da percepção pública sobre a Agência; e
- Aprimoramento de boas práticas de governança e gestão públicas adotadas pela Agência.

Iniciativa 23: *Promover a automação de processos manuais e a disponibilidade das ferramentas de trabalho necessárias*

Objetivo estratégico de processo relacionado:

4C) Garantir a adequabilidade da infraestrutura interna e das TIC

Resultados Esperados:

- Aumento da produtividade; e
- Aumento da transparência.

7. FATORES EXTERNOS E GESTÃO DE RISCOS

O ambiente externo de atuação da Anatel é desafiador por suas incertezas, ambiguidades e complexidade, caracterizado pela existência de diversas variáveis e agentes sobre os quais a Agência não tem controle, com potenciais impactos sobre os objetivos estratégicos institucionais.

O controle inflacionário, o câmbio, a taxa de juros, os índices de desemprego e de confiança, o poder de compra das pessoas e o controle fiscal podem exercer importante influência sobre as decisões empresariais e de consumo com efeitos sobre a conectividade e o setor regulado pela Anatel. O ambiente de mercado ainda tem sido impactado pelas consequências da pandemia do covid-19, com possíveis reflexos no curto e médio prazos.

As preocupações com um eventual desequilíbrio entre investimentos em telecomunicações e serviços OTT, cibersegurança, questões tributárias e até de segurança pública são outros aspectos relevantes para as decisões que afetam os investimentos setoriais e a demanda pelos serviços de telecomunicações.

Ademais, fatores externos ligados aos cenários político, legal, ambiental, social e tecnológico também contribuem para amplificar o desafio de executar a estratégia que oriente a Anatel na consecução de seus objetivos.

A fim de lidar com os diversos fatores externos e decorrentes incertezas e impactos sobre a estratégia institucional, um extensivo diagnóstico de ambiente foi realizado. Suas conclusões subsidiaram a construção de possíveis cenários futuros para conectividade e para o setor de telecomunicações, bem como a identificação de potenciais riscos a serem considerados pela Anatel para concretizar seus objetivos e construir o futuro desejado para setor.

A definição dos objetivos estratégicos associados implica lidar com um conjunto de riscos que, se não endereçados apropriadamente, podem dificultar ou mesmo impedir a consecução deste plano estratégico.

Nesse sentido, foram identificados riscos estratégicos, os quais, após minuciosa análise de probabilidades de sua ocorrência e impactos de sua concretização, tiveram seus planos de tratamento propostos a serem efetivados durante a execução deste plano.

8. GOVERNANÇA E AVALIAÇÃO DE RESULTADOS

A governança deste Plano Estratégico será exercida pelo Conselho Diretor e o acompanhamento e o monitoramento de sua execução será realizado pelo Comitê Interno de Governança, que auxilia a Alta Administração nas atividades de direcionamento, monitoramento, supervisão e avaliação da atuação da gestão estratégica da Anatel.

Execução e Monitoramento

A execução da estratégia definida nas iniciativas estratégicas deste Plano será desdobrada nos planos institucionais da Agência a partir das orientações constantes nos Planos de Gestão Táticos, que contemplarão as ações, os resultados e as metas relacionadas aos processos finalísticos e de gestão voltados ao alcance dos objetivos estratégicos no médio prazo.

O monitoramento da execução será realizado por meio do acompanhamento dos seguintes indicadores de desempenho e de governança:

1. **Porcentagem de cumprimento dos objetivos estratégicos de resultado:** calcula o nível de cumprimento de cada objetivo estratégico de resultado a partir dos indicadores e das metas de resultado definidos para traduzir o valor público que a Anatel entrega à sociedade.
2. **Porcentagem de cumprimento dos indicadores associados aos objetivos de processo:** corresponde ao cálculo do progresso dos indicadores dos objetivos estratégicos de processo, os quais serão definidos oportunamente nos Planos de Gestão Táticos.
3. **Porcentagem de execução dos projetos estratégicos derivados das iniciativas estratégicas:** corresponde à porcentagem de execução das iniciativas que efetivamente se tornaram projetos, contemplando o percentual de iniciativas concluídas e o percentual de execução de cada iniciativa estratégica.

Os resultados parciais dos indicadores de desempenho serão acompanhados por meio de painéis interativos (*dashboards*) e serão reportados trimestralmente ao Comitê Interno de Governança nas Reuniões de Avaliação da Estratégia (RAE).

Os principais resultados gerados pela atuação da Anatel e os seus impactos serão reportados periodicamente à sociedade e também aos responsáveis internos por meio dos canais de relacionamento disponíveis, como o Portal na internet e as mídias digitais.

Avaliação e Revisão

A avaliação dos resultados e do nível de alcance das metas estabelecidas para os objetivos estratégicos constarão no Relatório Anual de Gestão da Anatel, referente ao respectivo exercício de competência, bem como serão divulgados à sociedade por meio dos canais de relacionamento disponíveis.

O presente Plano poderá ser atualizado e revisto a qualquer tempo para promover o ajuste ao contexto de atuação regulatória e o alinhamento contínuo entre os instrumentos de planejamento governamental e de políticas públicas, com vistas ao fortalecimento da governança pública.

A atualização deverá considerar os resultados obtidos no ano anterior, em particular a evolução dos indicadores estratégicos e sua relação com as metas previamente definidas, bem como a situação dos projetos estratégicos.

ANEXO INDICADORES

O monitoramento da estratégia será realizado a partir do acompanhamento dos indicadores e das metas dos objetivos estratégicos de resultado a serem alcançadas ao final de 2027, conforme os atributos expostos a seguir.

Indicador 1:
Percentual da população com cobertura 5G ou superior

Finalidade: Fechar a lacuna digital, garantindo cobertura plena em tecnologia 5G, proxy de padrão de qualidade exigido

Linha de Base: 0% (dez/2021)

Meta 2027: 57,67%

Área responsável: PRUV / SPR

Periodicidade de aferição: anual

Fórmula de cálculo:

$$\%\ Cobertura\ 5G = \frac{\sum_{i=1}^{n}(\%\ cobertura_i\ * P_i)}{População\ do\ Brasil}$$

Onde:
i: é cada setor censitário do país definido pelo IBGE

Indicador 2.1:
Total de municípios com backhaul de fibra

Finalidade: Política de "ninguém fica para trás": todos os municípios devem ter a possibilidade de conexão por fibra

Linha de Base: 4.677 municípios - 83,97% (2021)

Meta 2027: 5.570 municípios - 100%

Área responsável: PRUV / SPR

Periodicidade de aferição: anual

Fórmula de cálculo:

Número absoluto de municípios que possuem cobertura de backhaul/ backbone de fibra óptica

Indicador 2.2:
Total de localidades com mais de 600 habitantes com backhaul de fibra

Finalidade: Política de "ninguém fica para trás": todos os municípios devem ter a possibilidade de conexão por fibra

Linha de Base: 598 localidades - 13,63% das localidades com mais de 600 habitantes (2021)

Meta 2027: 2.194 localidades - 50% das localidades com mais de 600 habitantes

Área responsável: PRUV / SPR

Periodicidade de aferição: anual

Fórmula de cálculo:

Número absoluto de localidades com mais de 600 habitantes que possuem cobertura de backhaul/backbone de fibra óptica

Indicador 3:
Velocidade média contratada na banda larga fixa

Finalidade: Fechar a lacuna digital, caminhando para a direção das *Full Gigabit Networks*

Linha de Base: 186,3 Mbps (dez/2021)

Meta 2027: 1 Gbps

Área responsável: PRUV / SPR

Periodicidade de aferição: mensal

Fórmula de cálculo:

$$vel.média = \frac{\sum_{i=1}^{n}(V_i * N_i)}{Quantidade\ de\ acessos}$$

Onde:
V_i: i-ésima velocidade em Mbps.
N_i: quantidade de acessos fixos da i-ésima velocidade

Indicador 4:
Capacidade das redes em relação ao cumprimento das referências de volume de dados transmitidos por segundo

Finalidade: Expressa a capacidade das redes no país em relação ao cumprimento do valor de referência de volume de dados transmitidos por segundo

Linha de Base: 78,28% (2021)
Meta 2027: > 87%

Área responsável: COQL / SCO

Periodicidade de aferição: anual

Fórmula de cálculo:

$$Ind = \frac{\sum_{i}^{n} IND4\_scm25_i\ x\ Acessos_i}{\sum_{i}^{n} Acessos_i}$$

Indicador 5.1:
Índice de satisfação geral dos consumidores da Banda Larga Fixa

Finalidade: Assegurar a satisfação dos usuários com o serviço de Banda Larga Fixa prestado pelas operadoras

Linha de Base: 6,9 (ISG Banda Larga Fixa 2021)

Meta 2027: 7,5

Área responsável: RCIC / SRC

Periodicidade de aferição: anual

Fórmula de cálculo:

$$ISG = \frac{\sum_{i=1}^{5}(\propto_i \ * J_i)}{\sum_{i=1}^{5}(\propto_i)}$$

Onde:
J: representa os itens que compõem a dimensão
Alfa (α): representa a carga fatorial de cada um dos itens

Indicador 5.2:
Índice de satisfação geral dos consumidores da Telefonia Móvel

Finalidade: *Assegurar e promover a satisfação dos usuários com o serviço de Telefonia Móvel prestado pelas operadoras*

Linha de Base: 7,6 (ISG Telefonia Móvel 2021)

Meta 2027: 8,1

Área responsável: RCIC / SRC

Periodicidade de aferição: anual

Fórmula de cálculo:

$$ISG = \frac{\sum_{i=1}^{5}(\propto_i \ * J_i)}{\sum_{i=1}^{5}(\propto_i)}$$

Onde:
J: representa os itens que compõem a dimensão
Alfa (α): representa a carga fatorial de cada um dos itens

Indicador 6.1:
Índice de Herfindahl-Hirschman (HHI – Banda Larga Fixa)

Finalidade: Mensurar de forma ponderada as concentrações do mercado de oferta de telefonia móvel

Linha de Base: 0,0964 (dez/2021)

Meta 2027: Abaixo de 0,1500

Área responsável: CPAE / SCP

Periodicidade de aferição: trimestral

Fórmula de cálculo:

$$HHI = \sum_{i=1}^{n} participação\ de\ mercado_i^2$$

Onde:
i: refere-se a cada empresa do mercado avaliado
n: refere-se ao total de empresas atuando no mercado avaliado.

Indicador 6.2:
Índice de Herfindahl-Hirschman (HHI - Telefonia Móvel)

Finalidade: Mensurar de forma ponderada as concentrações do mercado de oferta de telefonia móvel

Linha de Base: 0,2573 (dez/2021)

Meta 2027: Abaixo de 0,3594

Área responsável: CPAE / SCP

Periodicidade de aferição: trimestral

Fórmula de cálculo:

$$HHI = \sum_{i=1}^{n} participação\ de\ mercado_i^2$$

Onde:
i: refere-se a cada empresa do mercado avaliado
n: refere-se ao total de empresas atuando no mercado avaliado.

Indicador 7:
Percentual de indivíduos usuários de Internet

Finalidade: Estar com uma proporção de usuários de Internet compatível com os top 20 países avaliados pela União Internacional de Telecomunicações (UIT)

Linha de Base: 81,34% (ITU / TIC Domicílios 2020)

Meta 2027: 95% de usuários de internet no país

Área responsável: PRPE / SUE

Periodicidade de aferição: anual

Fórmula de cálculo:

$$\%\ Usuários\ de\ Internet = \frac{Indivíduos\ usuários\ de\ Internet}{Total\ de\ indivíduos}\ x\ 100$$

Nota: Indivíduos com 10 anos ou mais

Indicador 8:
Percentual de indivíduos com habilidades em TIC

Finalidade: Estar com uma proporção de usuários com habilidades TIC compatíveis com os top 20 países avaliados pela União Internacional de Telecomunicações (UIT)

Linha de Base: Habilidades baixas: 23% / Habilidades moderadas: 13% / Habilidades avançadas: 3% (2020)

Meta 2027: 30% de jovens e adultos com habilidades moderadas em Tecnologia da Informação e Comunicação (TIC)

Área responsável: PRPE / SUE

Periodicidade de aferição: anual

Fórmula de cálculo:

$$\%\ Indivíduos\ com\ habilidades\ TIC = \frac{Indivíduos\ com\ habilidade\ em\ TIC}{Total\ de\ indivíduos}\ x\ 100$$

Nota: Indivíduos com 10 anos ou mais

Indicador 9:
Índice integrado de governança e gestão públicas (IGG) - TCU

Finalidade: Estar com um IGG compatível com os top 20 entes avaliados da Administração Pública Federal

Linha de Base: 70,5% (2021)

Meta 2027: > 90%

Área responsável: PRPE / SUE

Periodicidade de aferição: Conforme orientação do TCU

Fórmula de cálculo:

$$N/A\ (calculado\ pelo\ TCU)$$

Indicador 10:
Percentual de dados e informações setoriais abertas

Finalidade: Aumentar a quantidade de informações disponíveis, reduzindo assimetrias

Linha de Base: 21,9% (2021)

Meta 2027: 85,0%

Área responsável: SUE

Periodicidade de aferição: trimestral

Fórmula de cálculo:

$$I = \frac{Ind_{dados} + Ind_{informações}}{2}$$

Onde:

$$Ind_{dados} = \%\ de\ bases\ de\ dados\ abertas$$

e

$$e\ Ind_{informações} = 100\ x\ \frac{Extratos\ e\ Reltórios\ de\ Planos\ Institucionais\ Publicados}{Total\ de\ Planos\ e\ Relatórios\ Institucionais}$$

plano estratégico 2023-27

ANATEL

Produto V | Iniciativa nº 17 do Planejamento Estratégico da ANATEL

Zelar pela prevenção contra fraudes no ecossistema digital

28 de abril de 2023

RELATÓRIO PARA A ITU E ANATEL

Contrato:
S-BDT-2023-006

Sumário

Apresentação do produto

Ementa: PLANO TÁTICO E DE AÇÃO – TELECOMUNICAÇÕES – FRAUDES ECOSSISTEMA DIGITAL – *BENCHMARKING* INTERNACIONAL – ANÁLISE DE IMPACTO E ESFORÇO – MAPEAMENTO DE ATORES E FÓRUNS – CONSCIENTIZAÇÃO DA POPULAÇÃO – COMBATE, PREVENÇÃO E MITIGAÇÃO A FRAUDES

O Projeto

O projeto de Apoio à Implementação do Plano Tático da Agência Nacional de Telecomunicações (ANATEL) para o período de 2023-24, através do contrato n° CTR-S-BDT-2023-006, de fevereiro de 2023, conduzido via União Internacional de Telecomunicações (UIT), tem como objetivo o apoio à implementação do novo planejamento tático da Agência, Trata-se de cooperação técnica internacional entre a UIT e a ANATEL. A consultoria contratada foi a ADVISIA OC&C Strategy Consultants, sediada em São Paulo – SP.

Pautado nos resultados esperados das iniciativas estratégicas, ele contempla o desenvolvimento e a entrega de produtos que irão apoiar a execução do portfólio de iniciativas táticas previstas para o biênio 2023-2024, com visão de futuro pautada no Plano Estratégico da Agência para o período de 2023-2027, garantindo o desdobramento e o alinhamento da execução da estratégia. Desse modo, seis iniciativas estratégicas foram selecionadas pela Agência para a formação do presente trabalho:

1. **Iniciativa Estratégica nº 02 – Produto II:** Promover qualidade e transparência na oferta do serviço de banda larga fixa;
2. **Iniciativa Estratégica nº 03 – Produto III:** Aprimorar a capacidade e a qualidade da infraestrutura e de seu funcionamento;
3. **Iniciativa Estratégica nº 05 – Produto IV:** Modernizar os mecanismos de fiscalização;
4. **Iniciativa Estratégica nº 17 – Produto V:** Zelar pela prevenção contra fraudes no ecossistema digital;

5. **Iniciativa Estratégica nº 18 – Produto VI:** Promover a alfabetização digital dos usuários;

6. **Iniciativa Estratégica nº 19 – Produto VII:** Promover a articulação e a cooperação para desenvolvimento de novas tecnologias.

Como forma de garantir que o resultado deste representasse a realidade do país, foi realizado um esforço no intuito de coletar percepções dos diferentes *stakeholders* relativas às iniciativas citadas anteriormente e aos seus respectivos impactos sobre o setor (Figura 1).

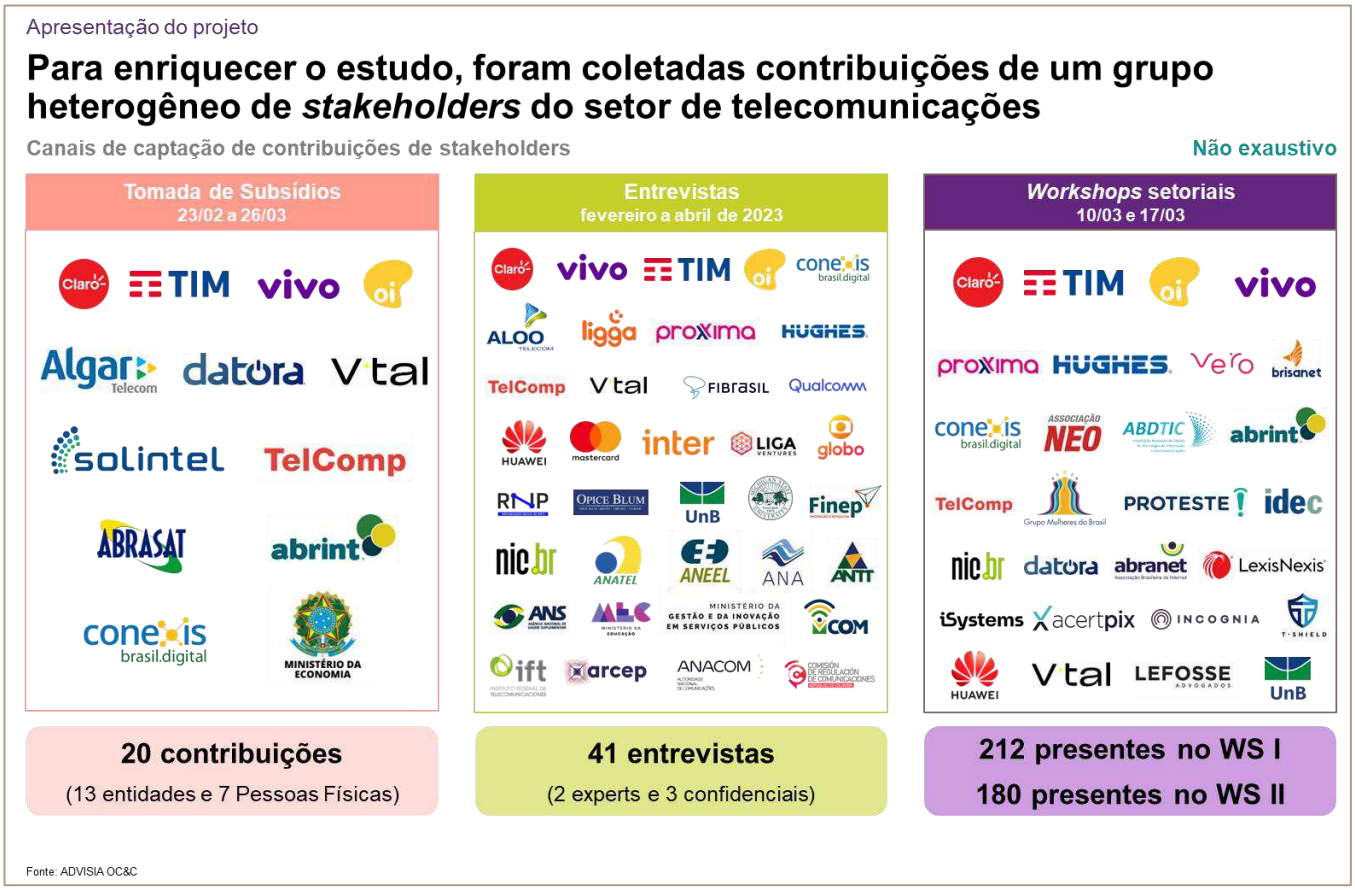


Figura 1

Neste esforço, foram reunidas especialistas, prestadoras de serviços de telecomunicações, associações, empresas de tecnologia, representantes do governo e da sociedade civil, de modo a identificar as diferentes nuances sobre as temáticas, por meio dos seguintes instrumentos:

1. **Tomada de Subsídios**

   - A Tomada de Subsídios nº 04/2023 ficou aberta à sociedade para contribuições pelo período de 23/02 a 26/03, e abarcou 30 perguntas sobre as diferentes temáticas das iniciativas estratégicas da Agência. Um total de 20 contribuições foram recebidas, sendo 7 provenientes de pessoas físicas e 13 de entidades públicas e privadas. A segunda seção deste documento trará em detalhes os principais *insights* coletados.

2. **Entrevistas**

   - Foram realizadas 41 entrevistas com especialistas, prestadoras de serviços de telecomunicações, associações, empresas de tecnologia, representantes do governo e sociedade civil de todo o país, totalizando mais de 60 horas de contato com os principais agentes do mercado, coletando suas percepções e sugestões para o setor. Além das entrevistas cujos agentes solicitaram anonimato, foram entrevistados representantes das instituições ilustradas na Figura 1.

3. **Workshops Setoriais**

   - Para permitir um canal adicional de contato com a sociedade e promover o diálogo entre diferentes agentes, foram conduzidos dois workshops, via plataforma Zoom. Eles tiveram uma divulgação massiva através de plataformas de notícias do governo federal, envio de e-mails e ofícios, bem como divulgação através da mídia setorial. Assim, contaram com representantes de prestadoras de serviços de telecomunicações, de associações, de empresas de tecnologia (inclusive fabricantes de equipamentos e prestadoras de serviços de cyber segurança), de universidades, de outras agências reguladoras, de entidades de certificação e de defesa do consumidor, da mídia setorial e de experts de mercado, além de outros agentes do governo, ANATEL e UIT. Instigados por algumas

perguntadas conduzidas pela ADVISIA, houve uma participação ativa dos participantes.

i. O Workshop I foi conduzido no dia 10/03 e contemplou as Iniciativas Estratégicas nº 17, 18 e 19. Este workshop teve uma duração de aproximadamente 3 horas e 30 minutos e contou com a presença de 212 participantes; (serão apresentados os principais *insights* coletados no próximo capítulo)

ii. O Workshop II foi conduzido no dia 17/03 e contemplou as Iniciativas Estratégicas nº 2, 3 e 5. Este workshop teve uma duração de aproximadamente 3 horas e contou com a presença de 180 participantes.

Durante estes *workshops*, todos os participantes tiveram a oportunidade de se manifestar, o que resultou em um rico debate técnico sobre as temáticas levantadas, obtendo-se diversas percepções dos participantes.

Além desses diversos diálogos com entidades brasileiras e da busca por informações no âmbito nacional, foi conduzido um esforço de ***benchmarking* internacional**, a fim de identificar boas práticas que pudessem ser adequadas para a realidade brasileira.

Para a seleção inicial de países que pudessem servir de referência para o Brasil em todas as 6 iniciativas estratégicas citadas previamente, foram analisados os seguintes critérios:

- Semelhança econômica e demográfica com o Brasil;
- Nível de penetração do serviço de banda larga;
- Estágio de desenvolvimento do setor de telecomunicações, segundo critérios da UIT[1];
- Disponibilidade e acessibilidade de informações;
- Facilidade de acesso à agência reguladora do país.

Para cada um desses critérios, os países foram avaliados em notas de 1 a 5. Para o critério de “Semelhança econômica e demográfica”, os países com maiores semelhanças em relação ao Brasil (IDH, PIB, população) receberam nota 5; os países menos semelhantes receberam nota 1. Para “Penetração de Serviço de internet”, foi avaliado o percentual da população com acesso à internet, segundo a UIT – países com penetração acima de 90% receberam a nota máxima.

No que tange ao “Estágio de Desenvolvimento em Telecom”, foi considerado o *ICT Development Index*, que é um índice publicado pela União Internacional de Telecomunicações das Nações Unidas com base em indicadores de tecnologias da informação e comunicações (IDI). Ele é um número importante para o entendimento do nível de informação da sociedade. Para o critério de seleção dos países de referência, atribuiu-se a nota máxima àqueles cujo IDI fosse maior do que 8.

Para avaliar o critério de “Acessibilidade de informações”, foi concedida a maior nota àqueles países com informações oficiais mais facilmente disponíveis para pesquisa. Por fim, para o critério de “Facilidade de acesso às agências reguladoras do país”, considerou-se notas superiores àquelas agências que, dada a facilidade de contato e as temáticas em questão, estariam mais dispostas a apoiar o projeto, através de entrevistas específicas.

Assim, foi possível selecionar cinco países para servir como *benchmark* em todas as seis iniciativas estratégias, devido às suas maiores notas finais, conforme ilustrado na Figura 2[2]:

Figura 2

Além desses cinco países que apoiaram as análises de todas as seis iniciativas estratégicas, foram também coletadas informações de outros países que apresentaram boas-práticas em relação aos diferentes temas. Por exemplo, Portugal, por ser referência na temática de alfabetização digital, também foi adicionado como *benchmark* nas análises relativas à Iniciativa Estratégica nº 18.

Adicionalmente, contatou-se, via e-mail, autoridades de 17 países que pudessem colaborar com o *benchmarking* internacional. Foram contatados representantes dos seguintes países: Argentina, Austrália, Canadá, Chile, Colômbia, Coreia do Sul, Espanha, Estados Unidos,

[2] ICT Development Index, 2022. Disponível em: https://www.itu.int/en/council/Documents/basic-texts-2023/RES-131-E.pdf

Estônia, França, Índia, Itália, México, Nova Zelândia, Portugal, Reino Unido e Singapura. Dentre estes, representantes de seis agências se prontificaram a apoiar o projeto através de entrevistas:

- Autoridade Nacional de Comunicações (ANACOM) – Portugal;
- Autorité de Régulation des Communications (ARCEP) – França;
- Canadian Radio-television and Telecommunications Commission (CRTC) – Canadá;
- Comisión de Regulación de Comunicaciones (CRC) – Colômbia;
- Instituto Federal de Telecomunicaciones (IFT) – México;
- Office of Communication (Ofcom) – Reino Unido;

Desta forma, os insumos provenientes dos contatos com a sociedade brasileira – via Tomada de Subsídios, entrevistas e *workshops* – somados às informações coletadas via *benchmarking* internacional foram essenciais para a robustez e a qualidade do trabalho desenvolvido. As principais informações coletadas serão apresentadas ao longo deste documento.

Para fins de organização do conhecimento adquirido, o conteúdo relativo a cada uma das seis iniciativas estratégicas da ANATEL está detalhado em um relatório específico, permitindo um maior detalhamento das premissas e análises que resultaram nas subiniciativas de direcionamento para a Agência. **Este documento aborda a Iniciativa Estratégica nº 17 – Produto V:** Zelar pela prevenção contra fraudes no ecossistema digital**.**

Produto V – Sumário Executivo

Iniciativa Estratégica nº 17: Zelar pela prevenção contra fraudes no ecossistema digital

O objetivo do Produto V é o desenvolvimento de análises e direcionamentos para auxiliar a implementação do Plano Tático da ANATEL de 2023-2024 referente à Iniciativa Estratégica n° 17, conforme consta na seção de **Terms of Reference (TOR) da Request for Proposal (RFP)** (RFP-S-BDT-2022-047, página 35).

Este relatório visa apoiar a Agência na estruturação de um plano de ação para combater, prevenir e mitigar os impactos das fraudes no ecossistema digital, contemplando o mapeamento de atores que atuam na proteção dos usuários nas esferas de consumo, segurança pública e academia; além do mapeamento de fóruns internacionais de debate sobre combate à fraude no ecossistema digital, mapeamento das estruturas de combate à fraude no ecossistema digital, realização de benchmarking para países pré-selecionados, estudo do cenário atual global e brasileiro, entendimento das perspectivas e anseios do mercado brasileiro e análises de tendência e dados .

Desta forma, este estudo irá apoiar a implementação do planejamento tático da ANATEL para a realização de três etapas críticas, a saber: combater, prevenir e mitigar os impactos das fraudes no ecossistema digital; promover estruturas de referência no combate e prevenção da fraude no ecossistema digital; e promover a relevância do tema para as principais partes interessadas. Neste sentido, este relatório contém subsídios com foco no alcance dos seguintes resultados: redução de golpes digitais; e aumento da confiança dos usuários na tecnologia.

O relatório está dividido em grandes seções: i. *Overview* sobre o mercado; ii. Percepções de mercado; iii. Plano de ação.

- O bloco referente ao ***Overview* sobre o mercado** é subdividido em 7 blocos, sendo eles:
    - Conceitos: são conceituados os principais termos necessários para o entendimento do projeto. Sendo os principais: i. **Golpe**: termo mais amplo

que descreve uma série de ações, táticas ou esquemas enganosos utilizados para obter vantagem indevida ou prejudicar outra pessoa ou organização. Pode incluir fraudes, estelionato e outras práticas desonestas; ii. **Fraude**: ato de enganar ou manipular deliberadamente para obter ganhos financeiros ou pessoais. Pode ser cometida por indivíduos, empresas ou até mesmo governos; iii: **Estelionato e fraudes tipificadas como crimes**: crimes tipificados no Código Penal brasileiro. O estelionato é um crime onde o objetivo principal é de se obter uma vantagem ilícita geralmente de cunho financeiro sobre a vítima, induzindo mediante artifício, ardil ou qualquer outro meio fraudulento. Além do estelionato, existem outras fraudes que são tipificadas como crime (Capítulo VI Artigos 171 a 179 do Código Penal) e utilizam a terminologia "fraude", são elas: fraude na entrega de coisa, fraude para recebimento de indenização ou valor de seguro, fraude no pagamento por meio de cheque e fraude eletrônica;

- Contextualização: 58% dos consumidores digitais globais conhecem alguém ou foram eles próprios vítimas de algum tipo de fraude online (no Brasil esse número foi de 64%), isso explica o porquê de a segurança ser é o fator chave na vivência online para 83% dos desses consumidores (no Brasil esse número foi de 87%);
- Mercado de *cybersecurity*: o mercado de segurança cibernética tem um tamanho estimado de 169 bilhões de dólares e uma de suas diversas soluções /serviços são as soluções antifraudes (equivale a cerca de 13% do mercado). O setor de telecomunicações junto com tecnologia possui um *market size* aproximado de 31 bilhões de dólares anuais;
- Mercado de soluções antifraude: o mercado de soluções antifraude é dividido em 5 grandes grupos de soluções, são eles: i. Fraud Analytics: soluções que detectam a fraude identificando padrões através de análise de dados; ii Autenticação: soluções de autenticações que visam identificar e proteger o usuário / empresa. Ex: senhas e PINs; iii. Report: soluções de relatórios e monitoramento de fraudes. Geralmente são integradas a plataformas de

detecção e prevenção de fraudes; iv. Visualização: ferramentas interativas de visualizações de dados que permitem uma fácil detecção de fraudes; v. GRC (Soluções de Governança, Risco e Compliance): ferramenta que engloba atividades de governança corporativa, gerenciamento de risco e conformidades corporativas relacionado a leis/regulamentos aplicáveis à empresa / serviço prestado;

- Fóruns e associações: os fóruns são ferramentas importantes no combate e prevenção às fraudes, havendo um compartilhamento de conhecimento entre os seus participantes. O principal fórum relacionado com o tema de fraudes no setor de telecomunicações é o **CFCA (Communications Fraud Control Association)**, uma associação global sem fins lucrativos que tem como objetivo combater a fraude em telecomunicações e serviços financeiros. O CFCA realiza eventos anuais e fornece recursos para seus membros sobre as melhores práticas e estratégias de combate à fraude;
- Métodos de fraude: referem-se às técnicas e estratégias específicas empregadas pelos criminosos para executar as fraudes. Os métodos de fraude descrevem o "como" das atividades fraudulentas, ou seja, as ações e os processos que os criminosos utilizam para atingir seus objetivos. Os principais métodos de fraudes que causaram prejuízo financeiro para a indústria de telecomunicações em 2021 foram: i. Spoofing; ii. Wangiri; iii. SMS Phishing/Pharming; iv. Subscrição; v. IP PBX Hacking; vi. Abuso de Rede; vii Roubo de conta; viii. SIM Swapping / Jacking; ix. Phising / Pharming; Robocalling;
- *Benchmarking* internacional: foi realizado um benchmarking com a Federal Communications Commission (FCC), Office of Communications (Ofcom), Australian Communications and Media Authority (ACMA), Instituto Federal de Telecomunicaciones (IFT) e Comisión de Regulación de Comunicaciones (CRC). Os principais destaques foram:
  - A FCC se destaca pelo poder de atuação contra fraudes, contando com uma divisão específica para segurança das infraestruturas e

comunicações críticas e se destaca também pelo trabalho em conjunto com outras agências governamentais;

- A Ofcom se destaca na produção de materiais para conscientização da população do Reino Unido e na sinergia entre agências com destaque para parcerias com a *Action Fraud;*
- A ACMA se destaca pela regulação criada no setor, sendo destaque a regulação de cadastro de chips pré-pagos que visa a mitigação de fraudes;
- O IFT trabalha em conjunto com agências governamentais e organizações para combater as fraudes e garantir a integridade no setor;
- A agência colombiana (CRC) utiliza estratégias semelhantes à IFT no combate às fraudes;

- A segunda parte do relatório fala sobre o **Percepções de mercado**, apresentando os seguintes blocos:
  - Atores no combate à fraude: o Brasil possui diversos atores que auxiliam no combate à fraude, com destaques para os de segurança pública e mercado financeiro, segue principais atores mapeados: Ministério da Justiça, Polícia Federal, Polícia Civil, Instituto Nacional de Tecnologia da Informação (ITI), Conselho de Controle de Atividades Financeiras (COAF), Federação Brasileira de Bancos (FEBRABAN), Banco Central do Brasil (Bacen), Procons, CERT.br e entre outros;
  - *Workshop*: foi realizado no 10/03 um *workshop* sobre as iniciativas estratégicas nº 17, 18 e 19 que contou com a presença de 212 participantes e com duração aproximada de 3 horas e 30 minutos. Os principais temas discutidos foram: i. Tipos de fraudes existentes no Brasil; ii; Principais soluções e ferramentas para o combate e prevenção às fraudes; iii. O que a sociedade como um todo espera da ANATEL; As respostas obtidas estavam em linha com os principais métodos globais de fraudes e as principais

soluções mapeadas no capítulo anterior. Alguns pontos de destaque foram relacionados com o que se esperar da ANATEL, tivemos as seguintes contribuições: a. Ampliação da divulgação das campanhas de conscientização utilizando a plataforma #FiqueEsperto e a possibilidade da impulsão do projeto já existente “Cadastro Pré”;

- Tomada de subsídios: a tomada de subsídios é um processo importante para as agências governamentais e o governo como um todo, pois permite coletar informações e opiniões relevantes para a formulação de políticas públicas e tomadas de decisões. Foram disponibilizadas 5 perguntas para sociedade no período de 23/02 a 26/03 referentes ao tema fraude no ecossistema digital. Uma média de 8 pessoas / instituições responderam cada pergunta (houve diferentes números de respondentes por pergunta) e os principais insumos foram: i. A necessidade de simplificar e divulgar os canais de reclamações da ANATEL; ii. Preocupações referentes a fraudes oriundas em brokers; iii. Desejo do mercado que a agência incentive as prestadoras de serviço para que elas ofereçam um bureau de dados categorizados pela confiabilidade das informações coletadas pelos clientes;
- Entrevistas com *stakeholders*: Para entender os anseios e expectativas dos principais *stakeholders* envolvidos no tema de fraude, foram conduzidas diversas entrevistas que trouxeram variadas visões sobre o que o mercado espera da agência, as principais foram: i. aumento na fiscalização de prestadoras de serviço para mitigar fraudes de 0800; ii. Criar medidas para dificultar o sequestro de terminais; iii. Realizar campanhas de conscientização sobre fraudes envolvendo engenharia social; iv. Estuar a possibilidade de restrição no número de linhas ativas por CPF e entre outros assuntos detalhados ao longo do documento;
- Base de dados: A análise da base de dados de reclamações da ANATEL não trouxe nenhum insumo relevante referente aos principais métodos de fraudes no Brasil, mas por outro lado serviu de inspiração para subiniciativas do plano de ação;

- A última parte do relatório traz o **Plano de Ação**, que foi construído baseado nos estudos feitos (seções Mercado Global e Mercado Brasileiro) e das percepções de mercado (*Workshop*, Tomada de subsídios e entrevistas). O plano está divido em:
    - Análise de impacto e esforço: o impacto das subiniciativas foi avaliado de acordo com o potencial de mudança que a iniciativa pode promover e o esforço está relacionado à dificuldade para realização da subiniciativa;
    - Subiniciativas levantadas: o estudo de mercado, benchmarking, workshop, tomada de subsídios e percepções coletadas do mercado pelas entrevistas serviram de inspiração para a criação das subiniciativas do plano de ação. Foram consolidadas 17 atividades, sendo 16 exclusivas da frente estratégica de fraudes e 1 transversal junto com o tema de alfabetização digital;
    - Priorização das subiniciativas: a priorização ocorreu por meio da originação de um gráfico de impacto versus esforço, seguindo a regra de Pareto. Sendo a iniciativa que apresenta um valor maior para impacto com esforço baixo considerada prioritária dentre as outras. Vale ressaltar que a análise de impacto e esforço foi realizada juntamente com a equipe da ANATEL para que todas as subiniciativas propostas estivessem aderentes à realidade da agência;
    - Descrição da ficha de plano de ação: Foi elaborada uma ficha detalhando cada uma das subiniciativas. As dimensões apresentadas nessa ficha são: objetivo, atividades, impacto vs. Esforço, *Key Performance Indicator* (KPI), envolvidos, referência, resultado, prazo e riscos;
    - Detalhamento das subiniciativas prioritárias: todas as subiniciativas foram detalhadas utilização a ficha de plano de ação descrita acima e foram priorizadas, seguindo-se a a seguinte ordem:
        - Subiniciativas Prioritárias: 17.1 Promover conscientização para usuários sobre pronto acionamento da prestadora para casos de interrupção dos serviços, 17.2 Conscientizar usuários sobre fraudes

de engenharia social, reconhecendo diferenças entre os diversos grupos sociais, 17.3 Promover conscientização de usuários não alfabetizados digitalmente e idosos contra phishing, 17.4 Realizar campanhas focadas em idosos, adolescentes e usuários não alfabetizados digitalmente para conscientização contra spoofing, 17.5 Realizar acompanhamento para diminuir fraudes de 0800;

- Subiniciativas Aconselháveis: 17.6 Fomentar a participação da ANATEL em fóruns e seminários, 17.7 Incentivar o uso de modems residenciais cuja avaliação de conformidade tenha contemplado os requisitos de segurança, 17.8 Criar procedimentos específicos contra fraudes oriundas em brokers, 17.9 Avaliar a criação de procedimento de compartilhamento de informações para identificar comportamentos fraudulentos entre diferentes setores da economia, 17.10 Aprimorar mecanismos para dificultar o sequestro de terminal; 17.11 Elaborar relatórios periódicos relacionados a fraudes reportadas para a ANATEL; 17.12 Divulgar plataforma "Cadastro Pré" para públicos específicos;
- Subiniciativas de avaliação da viabilidade: 17.13 Reavaliar imposição de limite de linhas ativas pré-pagas por CPF, 17.14 Simplificar e melhorar a experiência do cliente nos canais de reclamação da ANATEL; 17.15 Impulsionar Projeto Cadastro Pré-Pago, 17.16 Aprimorar mecanismos para dificultar a operação de "chipeiras" utilizadas em fraudes;

1. *Overview* sobre o mercado

O mercado global foi avaliado a partir de uma contextualização sobre a importância do tema de fraudes no ecossistema digital, seguida por um *overview* sobre os mercados de soluções antifraude, junto aos principais fóruns existentes. Por fim, foi estruturada uma visão sobre os principais métodos de fraude existentes no setor de telecomunicações e foi conduzido um *benchmarking* internacional comparando-se a atuação de 5 agências reguladoras. A Figura 3 consolida os principais pontos relativos ao mercado global.

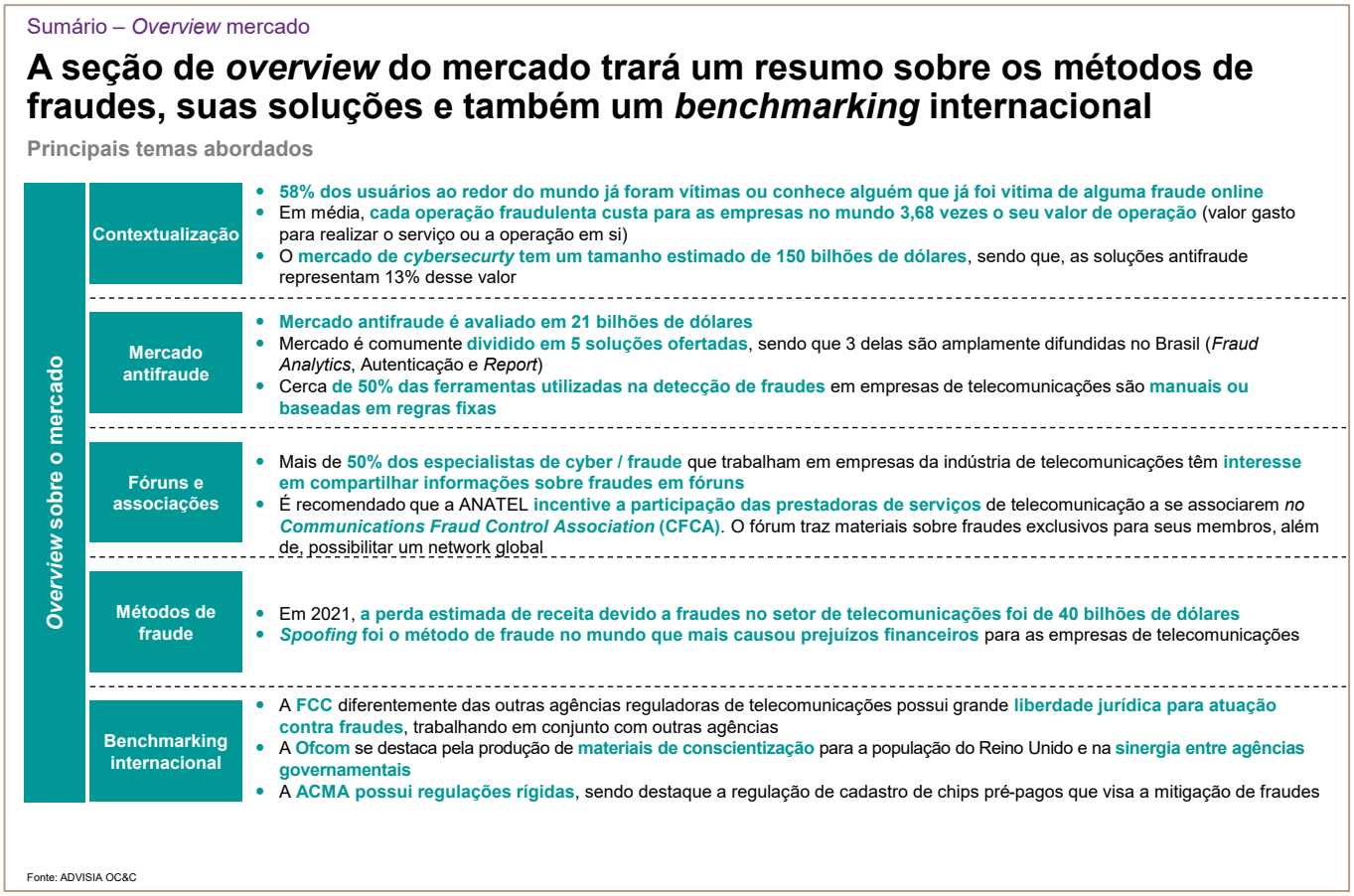


Figura 3

1.1. Conceitos

A era digital trouxe consigo inúmeras oportunidades e facilidades para a comunicação, o comércio e o acesso à informação. No entanto, também deu origem a novos desafios e ameaças, como as fraudes digitais. O estudo sobre o combate, prevenção e mitigação às fraudes digitais torna-se cada vez mais relevante e crucial, dado o impacto significativo que tais atividades podem ter na economia global, na segurança e na privacidade dos indivíduos e das organizações.

À medida em que a tecnologia avança e se torna mais sofisticada, os fraudadores também aprimoram suas táticas e estratégias para explorar vulnerabilidades e extrair informações confidenciais, gerando perdas financeiras e danos à reputação de empresas e entidades governamentais. A conscientização e a educação sobre as diversas formas de fraudes digitais, como *phishing*, roubo de identidade e ataques de *ransomware*, são fundamentais para prevenir e mitigar tais riscos.

Mas antes de adentrar no estudo em si é importante ter clareza sobre alguns conceitos que possuem significados parecidos e que muitas das vezes são utilizados de maneira equivocada. Os termos "golpe", "fraude" e “estelionato” são geralmente confundidos por terem significados análogos, se referindo a situações de engano ou trapaça e se diferenciado apenas pela forma como o engano é praticado. A figura abaixo ilustra de maneira resumida a diferença entre esses termos:

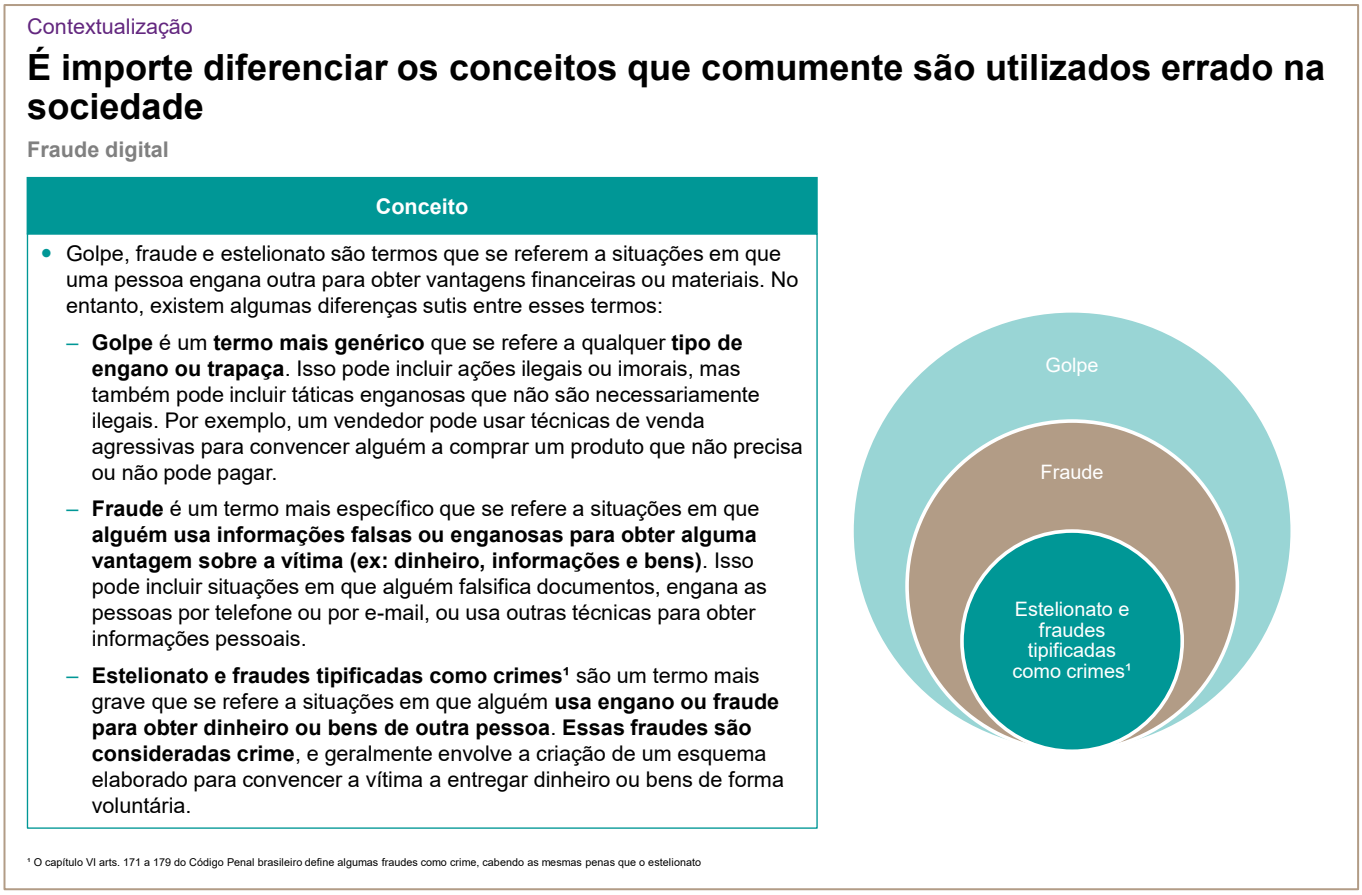


Figura 4

Golpe[3] é um termo mais amplo que descreve uma série de ações, táticas ou esquemas enganosos utilizados para obter vantagem indevida ou prejudicar outra pessoa ou organização. Pode incluir fraudes, estelionato e outras práticas desonestas. O termo "golpe" é frequentemente usado coloquialmente, e sua definição pode variar dependendo do contexto.

Já a fraude[4] é um ato de enganar ou manipular deliberadamente para obter ganhos financeiros ou pessoais. Pode ser cometida por indivíduos, empresas ou até mesmo governos. A fraude pode assumir várias formas, como falsificação de documentos, informações incorretas ou omissão de informações relevantes.

[3] Cambridge Dictionary. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/scam

[4] Black's Law Dictionary. 10ª edição, 2014. Disponível em: https://thelawdictionary.org/fraud/

O estelionato[5] por fim, é um crime específico, definido no Código Penal brasileiro. Trata-se de um crime onde o objetivo principal é de se obter uma vantagem ilícita geralmente de cunho financeiro sobre a vítima, induzindo mediante artifício, ardil ou qualquer outro meio fraudulento. No Brasil, o estelionato está previsto no Capítulo VI Artigos 171 a 179 do Código Penal.

Além do estelionato, existem outras fraudes que são tipificadas como crime (Capítulo VI Artigos 171 a 179 do Código Penal) e utilizam a terminologia “fraude”, são elas:

- Fraude na entrega de coisa: defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
- Fraude para recebimento de indenização ou valor de seguro: destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as consequências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;
- Fraude no pagamento por meio de cheque: emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento;
- Fraude eletrônica: fraude cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. As penalidades para essa fraude são:
  - § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021);
  - § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o

[5]BRASIL. Código Penal Brasileiro (Decreto-Lei nº 2.848/1940). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm

crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021);

- § 3º - A pena aumenta-se de um terço, se o crime for cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

Em resumo, fraude, golpe e estelionato são termos que compartilham características similares, pois todos envolvem atos desonestos e enganosos, geralmente com o objetivo de obter vantagens financeiras ou pessoais. No entanto, há diferenças importantes entre eles. A fraude refere-se à manipulação ou falsificação intencional de informações para enganar alguém, enquanto o golpe é um termo mais amplo que engloba uma variedade de ações e esquemas desonestos, abrangendo fraudes, estelionatos e outras práticas ilícitas. O estelionato, por sua vez, é um crime específico definido no contexto legal brasileiro e refere-se a obter vantagem ilícita induzindo ou engando alguém por meios fraudulentos. É importante ressaltar novamente a existência de fraudes tipificadas como crime pelo Código Penal brasileiro que são citadas no capítulo VI, artigos 171 a 179 que trata de crimes com a mesma penalidade do estelionato.

1.2. Contextualização

A era digital está revolucionando a maneira como as pessoas interagem umas com as outras. Hoje o mundo digital oferece diversas soluções que visam auxiliar os seus usuários no dia a dia. A confiança é um elemento fundamental para o sucesso de qualquer relacionamento online, seja entre consumidores e empresas, ou entre indivíduos em redes sociais e comunidades virtuais, no entanto, o aumento das fraudes digitais tem levantado preocupações significativas sobre a confiança e as experiências vividas pelos usuários na internet

As fraudes digitais podem prejudicar a confiança dos usuários na segurança e na privacidade de suas informações pessoais e financeiras. Consequentemente, as experiências negativas decorrentes dessas fraudes podem levar a um aumento no medo e na ansiedade dos usuários, fazendo com que evitem o uso de serviços digitais e adotem comportamentos cautelosos.

Cerca de 83% dos usuários que utilizam internet afirmam que a segurança é o fator mais importante na experiência e vivência online e aproximadamente 53% deles já foram vítimas ou conhecem alguém que já foi vítima de algum tipo de fraude digital. As Figuras 5 e 6 trazem um resumo das experiencias e percepções relatadas por esses usuários:

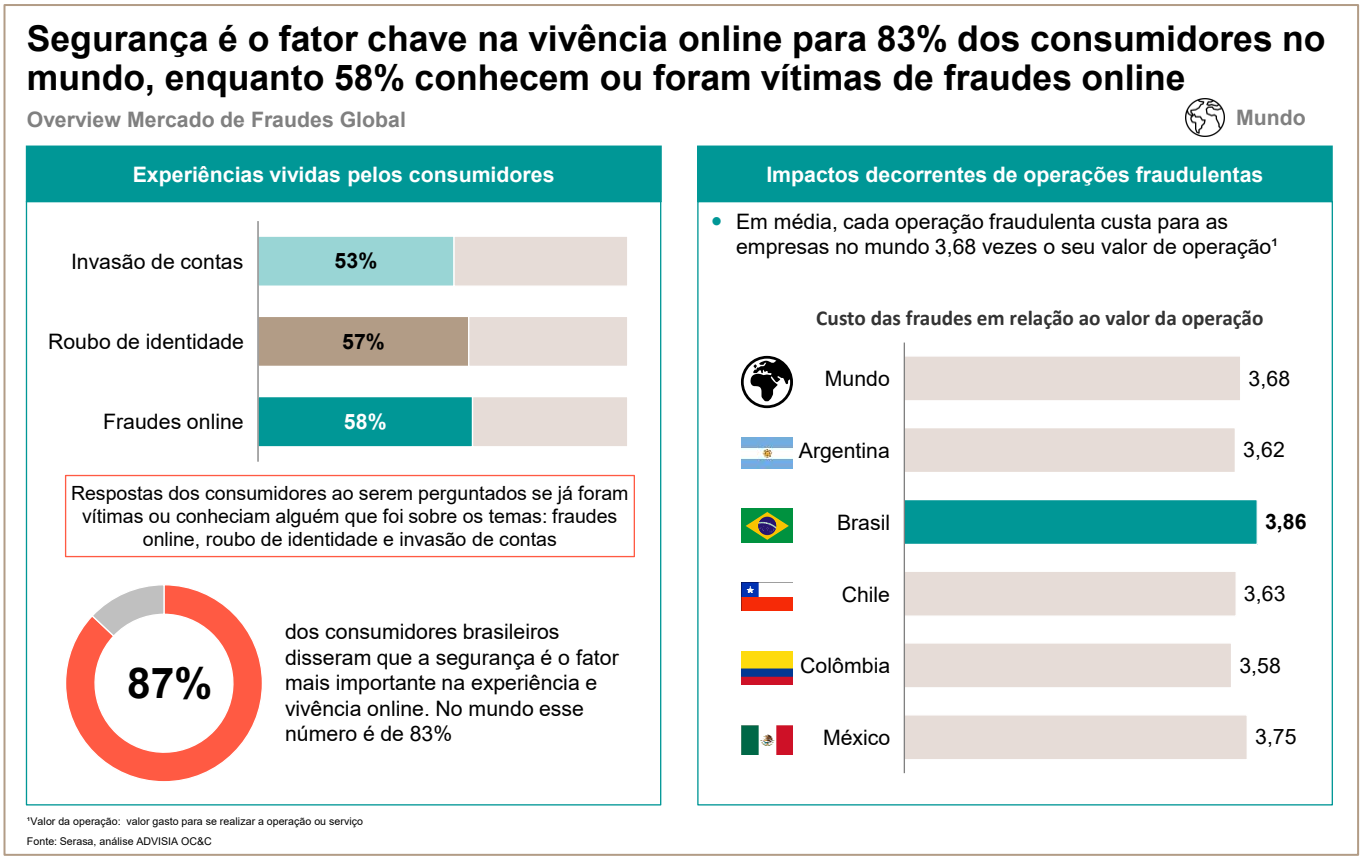


Figura 5

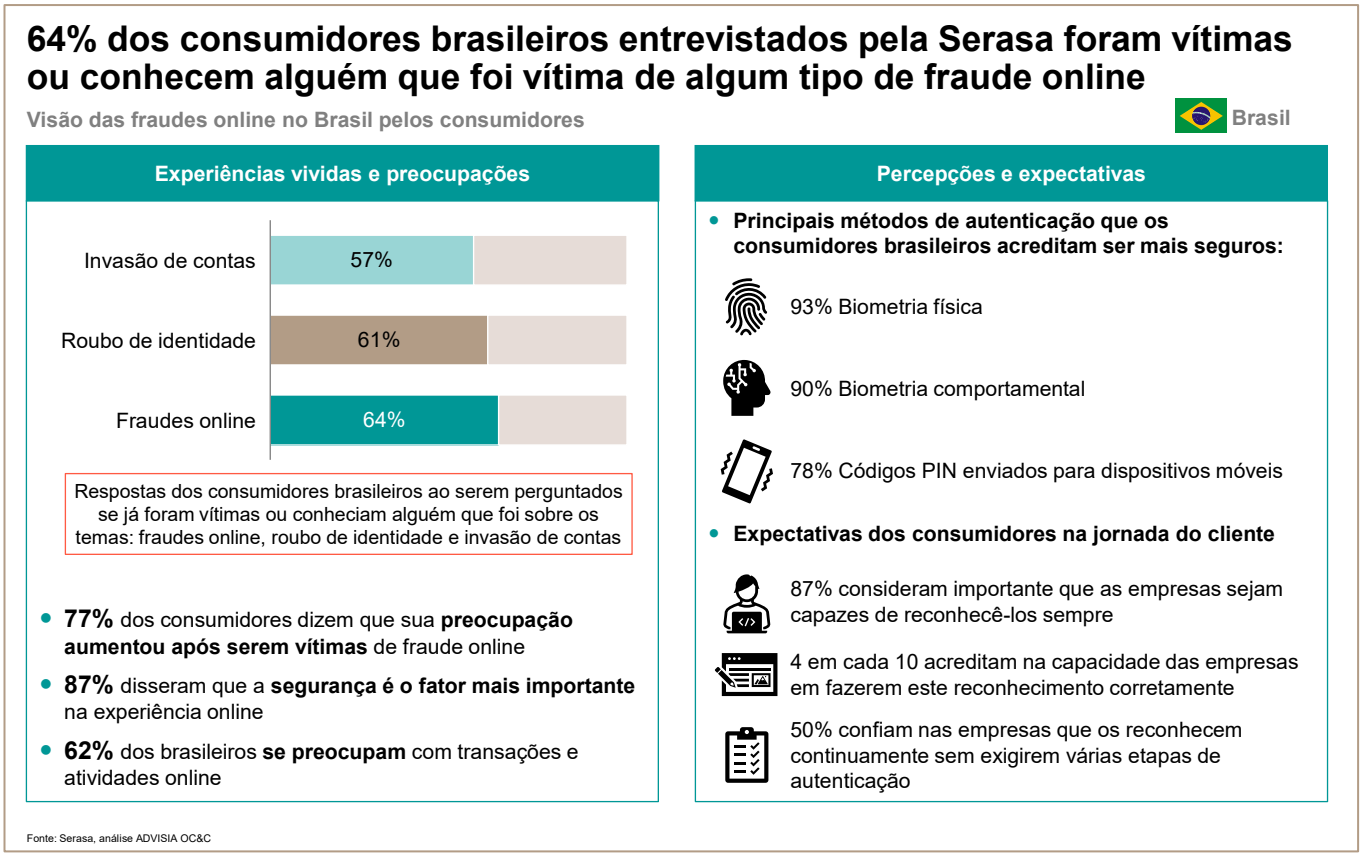


Figura 6

Como mostrado nas Figuras 5 e 6 o problema envolvendo fraudes digitais é grande em todo o mundo, cerca de 64% das pessoas entrevistadas no Brasil conhecem alguém ou já sofreram algum tipo de fraude online, sendo assim a segurança foi considerada o fator mais importante na experiência online dessas pessoas.

Os brasileiros preferem autenticações físicas, biometria comportamental e códigos PIN, em vez de senhas tradicionais de acordo com o Relatório Global de Identidade e Fraude 2022[6] da Experian. Outro ponto muito relevante citado no documento é a expectativa das pessoas em ter uma experiência online (jornada do cliente) fluida, em que as empresas tenham capacidade de reconhecê-las sempre. Isso é um grande desafio, pois existe uma necessidade de se colocar várias camadas de proteção antifraude criando a obrigação de algum tipo de ação por parte do cliente, por exemplo, autenticações em diferentes partes de sua jornada online.

[6] Experian. Relatório Global de Identidade e Fraude, 2022

Outra fonte utilizada foi o relatório “O Real Custo das Fraudes América Latina[7]” da empresa LexisNexis que traz insumos importantes relacionados ao custo / prejuízo que operações fraudulentas causam nas empresas da América Latina.

[7] LexisNexis. Relatório O Real Custo das Fraudes América Latina, 2021

1.3. Mercado de *cybersecurity*

O mercado de *cybersecurity*, também conhecido como mercado de segurança cibernética, abrange um conjunto de práticas, processos, serviços e tecnologias empregadas para proteger sistemas, redes, dispositivos e dados de ataques cibernéticos, danos e acessos não autorizados.

A segurança cibernética pode ser definida como ações voltadas para a segurança de operações, visando 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[8]. A crescente dependência da tecnologia e a expansão das atividades online tornam a segurança cibernética cada vez mais importante para indivíduos, empresas e governos.

A fraude digital é um desafio para a segurança cibernética pois ela pode resultar em perdas financeiras significativas e comprometer a privacidade e a segurança dos dados dos usuários. Para combater e prevenir as fraudes digitais são necessárias medidas eficazes de segurança cibernética, como por exemplo, o uso de criptografia de dados e a autenticação em dois fatores.

O mercado de *cybersecurity* [9]atualmente oferta soluções para diversas indústrias e tipos de empresa. As soluções mais comuns são:

- Serviços de nuvens;
- Soluções antifraude e de gerenciamento de identidade;
- Proteção de infraestrutura;
- Proteção de dados;
- Gestão de riscos;
- Equipamentos de segurança de rede;

[8] BRASIL. Gabinete de Segurança Institucional. Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/glossario-de-seguranca-da-informacao-1

[9] Mordor Intelligence. Report Global Cybersecurity Market (2022-2027)

- Segurança de aplicativos.

Vale lembrar que todo o processo envolvendo o uso de dados no ambiente digital deve ser permeado com soluções de segurança cibernética, o que torna esse mercado tão grande e heterogêneo. A Figura 7 traz o tamanho do mercado global estimado para segurança cibernética[10] - em torno de 150 bilhões de dólares, em 2021 - e as previsões de crescimento:

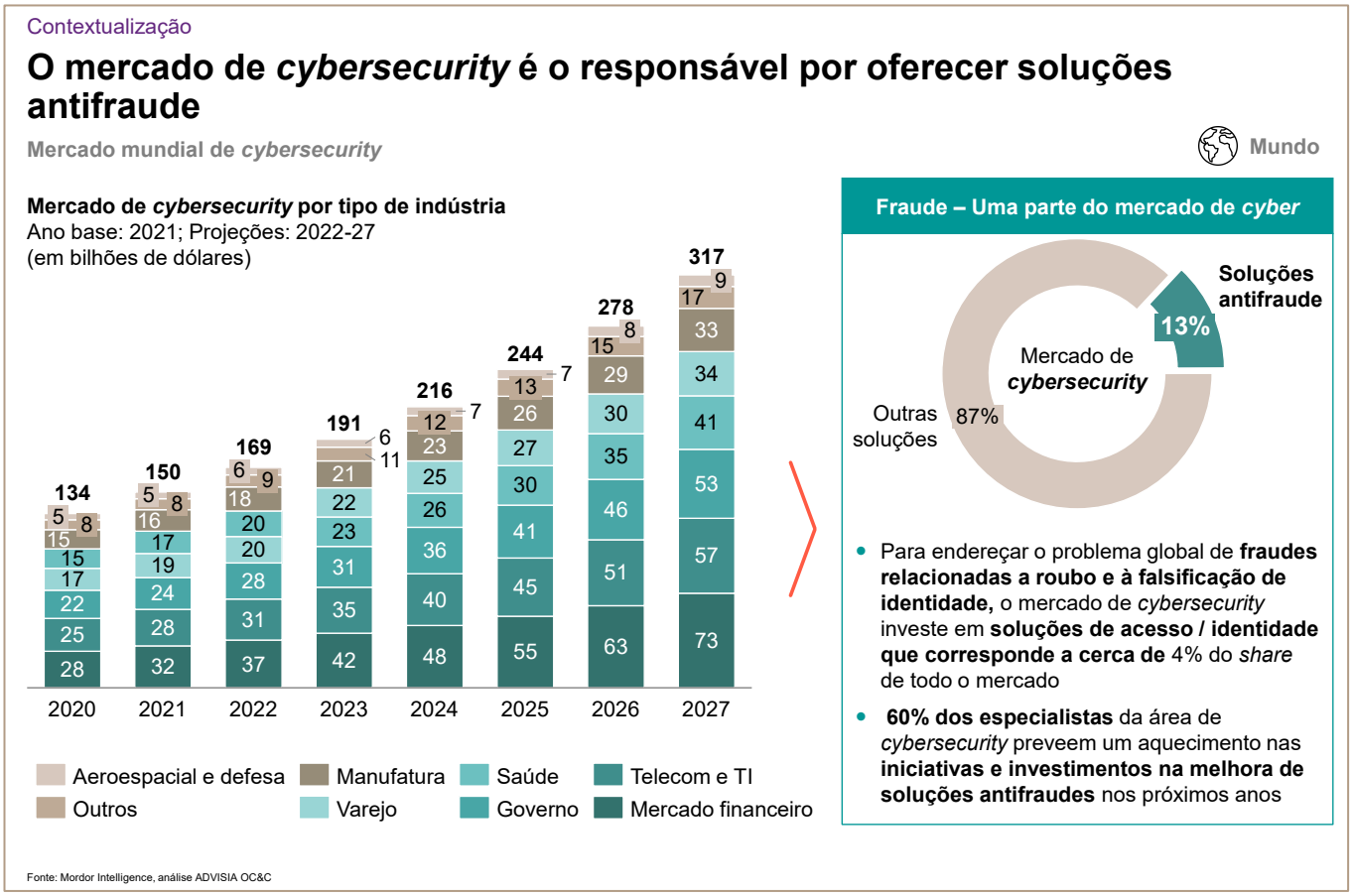


Figura 7

[10] Mordor Intelligence. Report Global Cybersecurity Market (2022-2027)

1.4. Mercado de soluções antifraude

O mercado global de soluções antifraude tem experimentado um crescimento substancial nos últimos anos, impulsionado pela crescente digitalização dos serviços, o aumento do comércio eletrônico e a necessidade constante de proteger informações e transações financeiras. Com a sofisticação das ameaças cibernéticas e a evolução das táticas de fraude, as soluções de detecção e prevenção de fraudes são cada vez mais cruciais para assegurar a confiança dos consumidores e a integridade dos sistemas financeiros e de dados.

Esse mercado abrange uma ampla gama de soluções[11], que são exemplificados na figura abaixo.

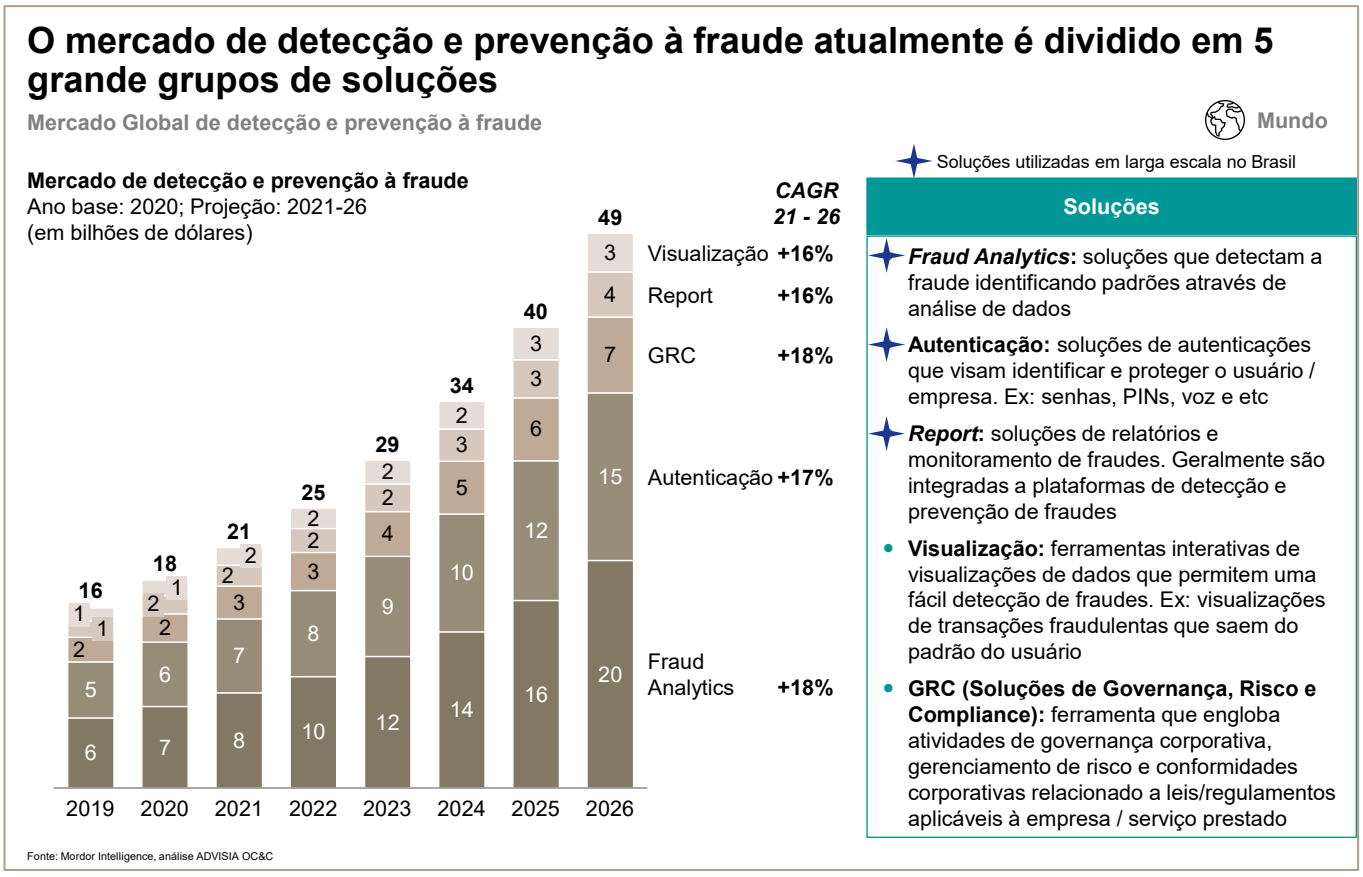


Figura 8

[11] Mordor Intelligence. Report Global Fraud Detection and Prevention Market

A solução de "*fraud analytics*" surgiu devido à necessidade de detecção de fraudes, em que métodos tradicionais e métodos baseados em regras acabam sendo limitados devido à falta de adaptabilidade. À medida em que mais dados foram surgindo em todo o mundo devido à adoção crescente da internet, as empresas passaram a integrar análises de dados aos seus métodos tradicionais para trazer uma aprimoração na detecção de fraudes e dar uma nova dimensão às técnicas. Hoje um sistema avançado de *fraud analytics* conta com uma gama de solução de análise de fraudes, utilizando várias técnicas, incluindo análise avançada com inteligência artificial (IA) embutida e *machine learning* destinados a revelar atividades suspeitas. Alertas são pontuados e priorizados com base na gravidade e, em seguida, encaminhados para analistas ou investigadores para uma revisão mais aprofundada.

As soluções de autenticação protegem principalmente clientes de bancos e instituições financeiras das últimas ameaças em fraudes online. Os ciber criminosos estão constantemente tentando penetrar nas redes empresariais e adquirir informações do cliente, o que leva a múltiplos casos de roubo de identidade. A autenticação de um único fator e a autenticação de múltiplos fatores são os dois subsegmentos da solução de autenticação no mercado de detecção e prevenção de fraudes.

Ferramentas de *reports* de fraudes (relatórios e monitoramento) podem relatar riscos e fraudes independentemente. Elas também podem ser integradas a uma plataforma completa de detecção e prevenção de fraudes. Empresas estão desenvolvendo soluções de relatórios de fraudes, nas quais é possível se ter uma visão unificada das atividades fraudulentas em vários portfólios, gerando relatórios de maneira ágil e precisa sobre as fraudes. Existem casos em que se há procedimentos internos para enviar relatos de fraudes de maneira automática para as agências de investigação.

A solução de visualização contempla um conjunto de ferramentas interativas de dados que permitem que o investigador mude a representação dos dados e texto para gráficos de maneira fácil e intuitiva. Este método pode ser vital para detectar transações fraudulentas de forma mais eficiente e eficaz. A visualização de dados pode ajudar a detectar fraudes, especialmente em relação a transações com cartões de crédito e débito em que geralmente se vê o desvio de padrão gerado por compras fraudulentas.

Soluções de governança, risco e compliance (GRC) abrangem atividades como governança corporativa, gerenciamento de riscos empresariais e conformidade corporativa com

leis e regulamentos aplicáveis. Uma estrutura eficaz permite que as organizações integrem e coordenem iniciativas de risco e conformidade com os processos de negócios, fornecendo uma visão holística das posturas de risco e conformidade da organização, permitindo que a administração tome decisões informadas sobre como alocar recursos e mitigar riscos.

No Brasil as soluções de *Fraud Analytics*, Autenticação e *Report* são amplamente utilizadas, principalmente no mercado financeiro.

O mercado financeiro possui 36% do *share* do mercado global de soluções antifraude, enquanto TI e Telecom representam 17%.A figura abaixo ilustra as participações das diversas indústrias no mercado de soluções antifraude.

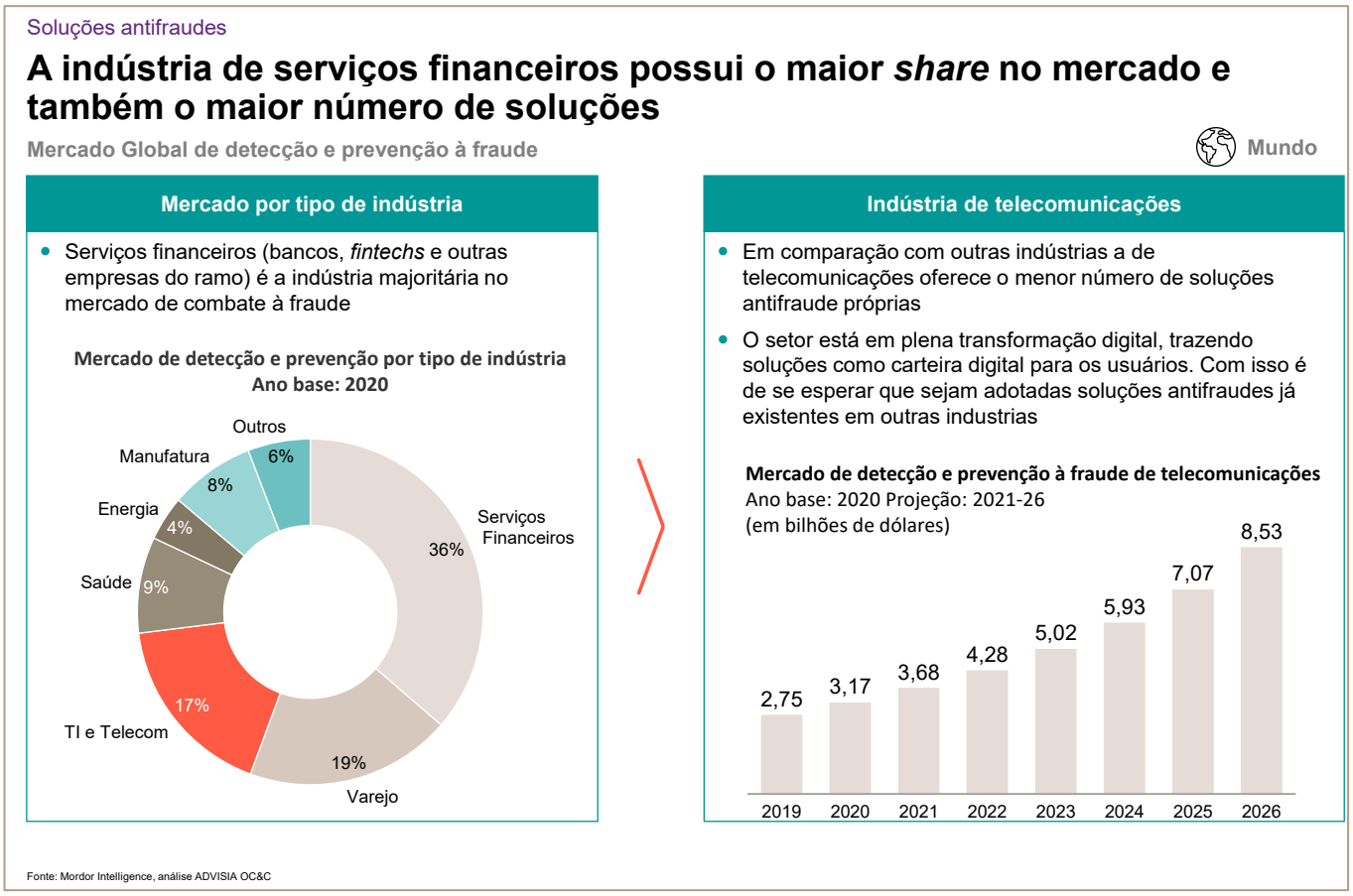


Figura 9

Ao contrário de outras indústrias, as telecomunicações possuem menos soluções específicas de proteção ao consumidor[12], podendo impactar na detecção de algumas fraudes.

Um exemplo da necessidade de o setor focar neste tipo de solução é o fato de as principais prestadoras de serviços de telecomunicações estarem começando a oferecer pagamento por seus serviços por meio de suas carteiras digitais, buscando incentivar o cliente a aderir a essa nova tecnologia, muitas vezes, é oferecido um desconto em algum serviço. Desta forma, espera-se que haja um aumento na adoção de carteiras móveis como solução de pagamento preferencial no setor, criando, assim, oportunidades para a adoção de soluções antifraudes mais sofisticadas.

A *Communications Fraud Control Association* (CFCA), disponibilizou um relatório chamado *Fraud Loss Survey* [13] (2021) onde ela destacou as principais ferramentas utilizadas para o combate à fraude no setor que está destacado na figura abaixo.

[12] Mordor Intelligence. Report Global Fraud Detection and Prevention Market

[13] Communications Fraud Control Association. Fraud Loss Survey Report, 2021

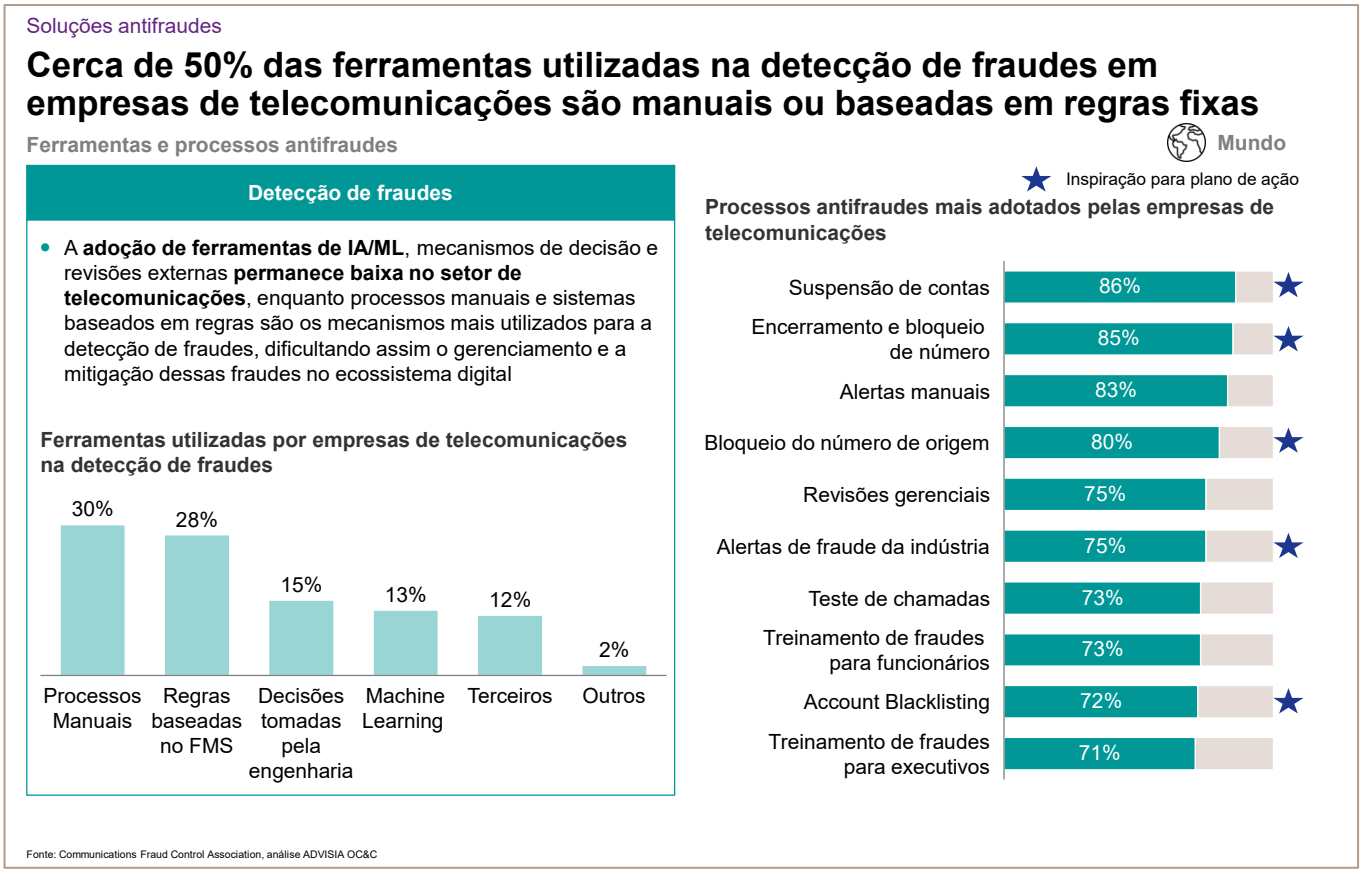


Figura 10

Dentre os 10 processos antifraudes mais adotados pelas empresas de telecomunicações, metade deles serviram de inspiração para o plano de ação que será detalhado no último capítulo desse documento. A outra metade não está relacionada com o plano, pois se trata de testes, treinamentos e revisões gerenciais.

Faz-se importante notar que as prestadoras de serviços de telecomunicações ainda estão se adaptando quanto ao uso de novas tecnologias, tais como IoT e 5G, com isso, ainda há bastante incerteza ao se tentar relacionar esses temas a fraudes. O CFCA trouxe alguns dados relevantes em sua pesquisa[10]. Os principais pontos estão representados na figura abaixo.

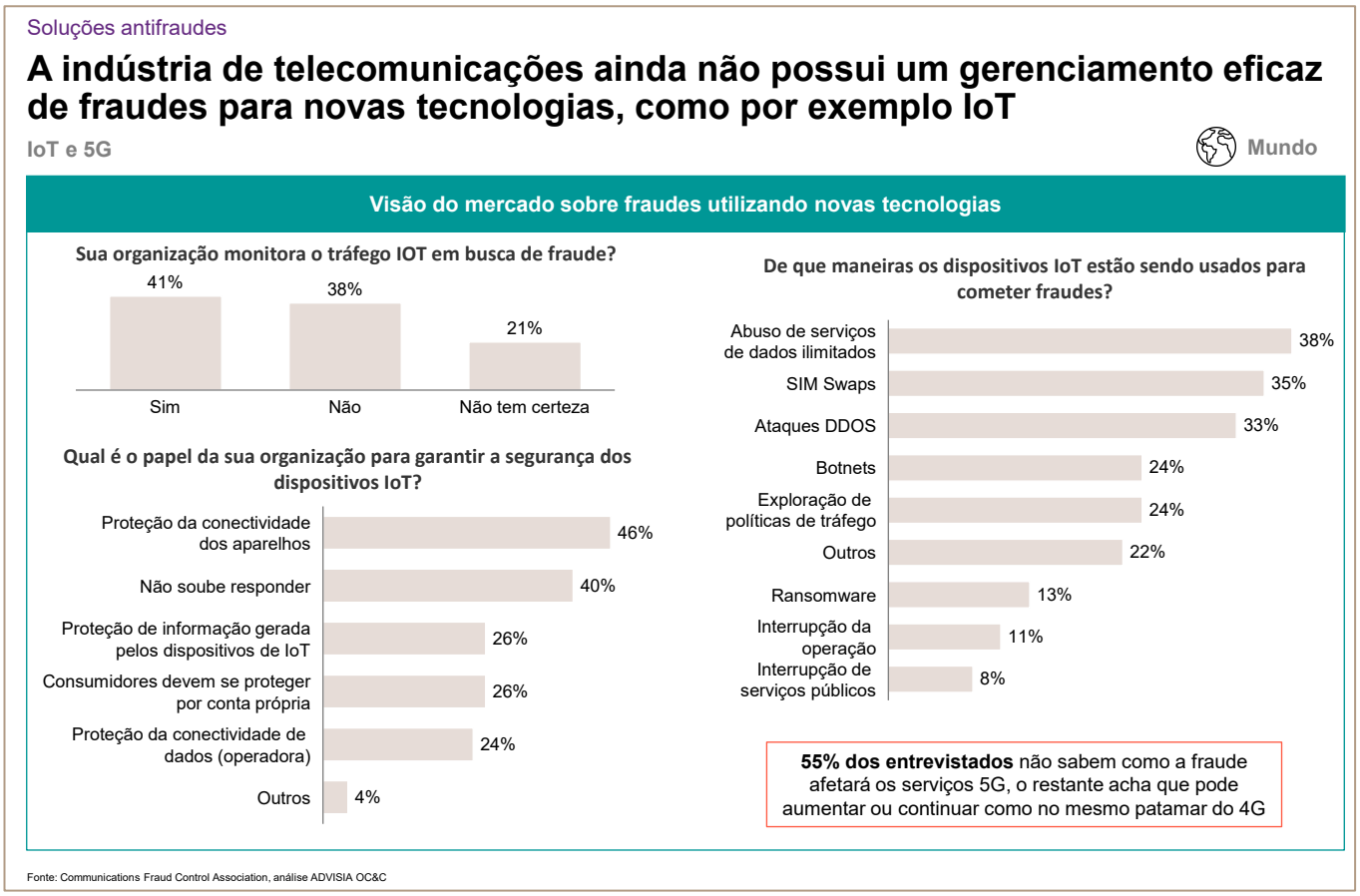


Figura 11

Certa de 70% dos funcionários que trabalham ao redor do mundo e que responderam à pesquisa do CFCA não monitoram o tráfego de IoT em busca de fraudes ou não tem certeza se a empresa o faz. Esse fato evidencia que as prestadoras de serviço ainda estão se adaptando para gerenciar as fraudes relacionadas às novas tecnologias.

Os cerca de 40% que afirmaram que monitoram as fraudes relataram que os dispositivos IoT estão sendo utilizados para cometer fraudes de:

- Abuso de rede[14]: atividade criminosa na qual um indivíduo ou grupo de indivíduos exploram de forma ilegal recursos de rede de telecomunicações para benefício

[14] CFCA. Fraud Loss Survey, 2021

próprio, sem a devida autorização ou compensação ao legítimo proprietário da rede;

- SIM Swap: também conhecido como SIM Swapping, é um tipo de golpe que envolve a transferência não autorizada do número de telefone de uma pessoa para um novo cartão SIM (essa fraude será detalhada no próximo capítulo);
- Ataques DDoS[15], que são ataques de rede distribuídos, muitas vezes chamados de ataques de negação de serviço distribuído (DDoS), esse tipo de ataque aproveita os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa. O ataque DDoS envia múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto;
- Botnet [16], que é uma rede de computadores infectados por *malware*, que são controlados remotamente por um ou mais indivíduos, sem o conhecimento dos usuários dos computadores infectados. Esses indivíduos, conhecidos como "botmasters", usam as *botnets* para realizar atividades maliciosas, como envio de *spam*, ataques de negação de serviço (DDoS), roubo de informações pessoais e financeiras, entre outras.;
- v. Exploração de políticas de tráfego[17]: tática utilizada por fraudadores para explorar vulnerabilidades nas políticas de tráfego de uma operadora de telecomunicações, com o objetivo de realizar atividades fraudulentas, como apropriação de identidade, roubo de serviços, tráfego de chamadas de voz ou mensagens de texto não autorizadas, entre outras.;

[15] Kaspersk. O que são ataques de DDoS. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ddos-attacks

[16] McQuade, S. C. (2017). Understanding and Managing Cybercrime

[17] CFCA. Fraud Loss Survey, 2021

- *Ransomware*, que é um tipo de *malware* que bloqueia o acesso a arquivos ou sistemas de um usuário, exigindo o pagamento de um resgate (*ransom*) para que o acesso seja restaurado. O *ransomware* [18]pode ser distribuído por meio de anexos de e-mail, links maliciosos ou através de downloads de software infectado.;
- vii. Interrupção da operação[19]:visa interromper ou prejudicar a operação de serviços de telecomunicações de uma empresa, causando danos financeiros e de reputação. Essa fraude pode ser realizada por meio de ataques cibernéticos, sabotagem física ou outras formas de interferência nos sistemas e infraestrutura de telecomunicações;
- viii. Interrupção de serviços públicos: objetivo interromper ou afetar negativamente a operação de serviços de telecomunicações que são considerados essenciais para o público em geral; A utilização de ferramentas e soluções de empresas terceiras no combate às fraudes é bem comum. As Figuras 12 e 13 trazem exemplos dessas empresas que atuam no Brasil e que oferecem essas soluções e ferramentas para o combate, prevenção e mitigação das principais fraudes existentes no setor de telecomunicações.

[18] Kaspersky. Ransomware: definição, prevenção e remoção. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware

[19] CFCA. Fraud Loss Survey, 2021

Soluções antifraudes

Exemplo de empresas que oferecem soluções ao combate às principais fraudes no setor de telecomunicações (1/2)

Empresas que oferecem soluções antifraude - Telecom

Fraudes	Exemplo de empresas e soluções
Spoofing (IP/CLI/ANI)	• **Cisco:** oferece o produto "Cisco Identity Services Engine", solução de segurança de rede projetada para proteger contra spoofing e outras ameaças de segurança de rede • **Symantec:** possui a solução "Symantec Email Security", voltado para a segurança cibernética que inclui proteção contra ameaças de spoofing em e-mails • **Fortinet:** oferece o produto "FortiGate", que é uma solução de segurança de rede que inclui proteção contra ataques de spoofing em vários protocolos de rede. • **Proofpoint:** possui o produto "Proofpoint Email Protection", que é uma solução de segurança de e-mail que inclui proteção contra ameaças de spoofing
SMS Phishing/Pharming	• **Adaptive Mobile Securty:** a solução “messaging protection” protege as operadoras de telecomunicações contrar SMS de Phishing/Pharming • **Lookout:** oferece a solução “Mobile Endpoint Security” contra Phishing/Pharming • **Symantec:** tem o produto “Mobile Security” que protege o usuário contra ameaças móveis incluindo Phishing • McAfee: oferece o produto “McAfee Mobile Security” que atua contra Phishing/Pharming
Phishing / Pharming	• **Cisco Systems:** Cisco Email Security solução contra phishing, spam e outras ameaças • **Microsoft:** Microsoft defender é a ferramenta que ajuda na proteção dos usuários contra phishing • **Proofpoint:** Proofpoint Email Protection, solução que bloqueia e-mails de phishing • **Symantec:** Symantec Email Security solução que protege contra malware e phishing
Abuso de Rede	• Existem várias soluções no mercado relacionadas com vulnerabilidade de redes que vão desde firewalls atpe sistema de prevenção de intrusões. Os principais players que oferecem esse tipo de solução são: **Cisco, Symantec, McAfee, IBM e entre outros**
Roubo de conta	• **Auth0**: é uma plataforma de identidade e autenticação que oferece uma variedade de recursos para proteger as contas dos usuários. Sua solução 2FA permite que as empresas adicionem uma camada extra de segurança às contas dos usuários • **IBM Security:** oferece soluções para combater a fraude de ATO. Sua solução de autenticação multifatorial ajuda a proteger as contas dos usuários
SIM Swapping / SIM Jacking	• **TeleSign:** fornece autenticação multifatorial por meio de SMS, voz e autenticação de dispositivo para evitar *SIM Swapping.* • **Google e Microsoft Authenticator:** aplicativos das empresas Google e Microsoft para autenticação de dois fatores, há a necessidade de acesso via dispositivo físico para pegar o código gerado

Fonte: ADVISIA OC&C

Figura 12

Soluções antifraudes

Exemplo de empresas que oferecem soluções ao combate às principais fraudes no setor de telecomunicações (2/2)

Empresas que oferecem soluções antifraude - Telecom

Fraudes	Exemplo de empresas e soluções
Robocalling	• **Nomorobo:** oferece um serviço de filtragem de chamadas que usa inteligência artificial para identificar e bloquear chamadas automatizadas, incluindo robocalls, antes que elas cheguem ao seu telefone • **YouMail:** fornece um sistema de correio de voz inteligente que identifica e bloqueia automaticamente chamadas fraudulentas, incluindo robocalls • **Hiya:** oferece um aplicativo móvel que bloqueia chamadas indesejadas, incluindo robocalls, e também fornece informações sobre a identidade do chamador • **RoboKiller:** usa tecnologia de inteligência artificial para identificar e bloquear chamadas automatizadas e também tem recursos para enganar e distrair os operadores de robocalls • **Truecaller:** identifica e bloqueia chamadas fraudulentas, incluindo robocalls, além de fornecer informações sobre o identificador de chamadas
Subscrição	• **ClearSale:** a solução de prevenção de fraudes ClearSale Subscription usa inteligência artificial identifica padrões suspeitos de atividade e bloqueia tentativas de fraude. A solução oferece suporte a diversos setores, incluindo varejo, telecomunicações, financeiro e outros • **Konduto:** Konduto Subscription é uma solução de detecção de fraudes que usa inteligência artificial e análise de dados para identificar padrões suspeitos de atividade, ela identifica e alerta possíveis fraudes de subscrição e envia notificação para a empresa • **Tempest:** Tempest Subscription Protect é uma solução completa contra a fraude de subscrição. O produto é utilizado em diversas industrias incluindo telecomunicações

Fonte: ADVISIA OC&C

OC&C Template (2017)

Figura 13

1.5. Fóruns e associações

A participação da ANATEL em fóruns relacionados ao tema de fraudes e ataques cibernéticos é fundamental para que se haja a promoção de conhecimento sobre os assuntos no setor de telecomunicações. Esses fóruns, sejam eles conferências, painéis de discussão ou eventos especializados, oferecem trocas de conhecimentos, experiências e práticas recomendadas entre diferentes partes interessadas, incluindo reguladores, empresas, acadêmicos, profissionais do setor e o público em geral.

A presença da Agência nesses fóruns permite que ela se mantenha atualizada sobre as últimas tendências, inovações, desafios enfrentados pelos diversos atores do setor podendo trazer uma imagem de confiança e transparência para o mercado. Isso, por sua vez, permite que a ANATEL tome decisões mais atualizadas e eficazes na formulação de normas e na implementação de regulamentações. A Figura 14 ilustra os principais fóruns existentes no mundo que debatem sobre o tema de fraude digital.

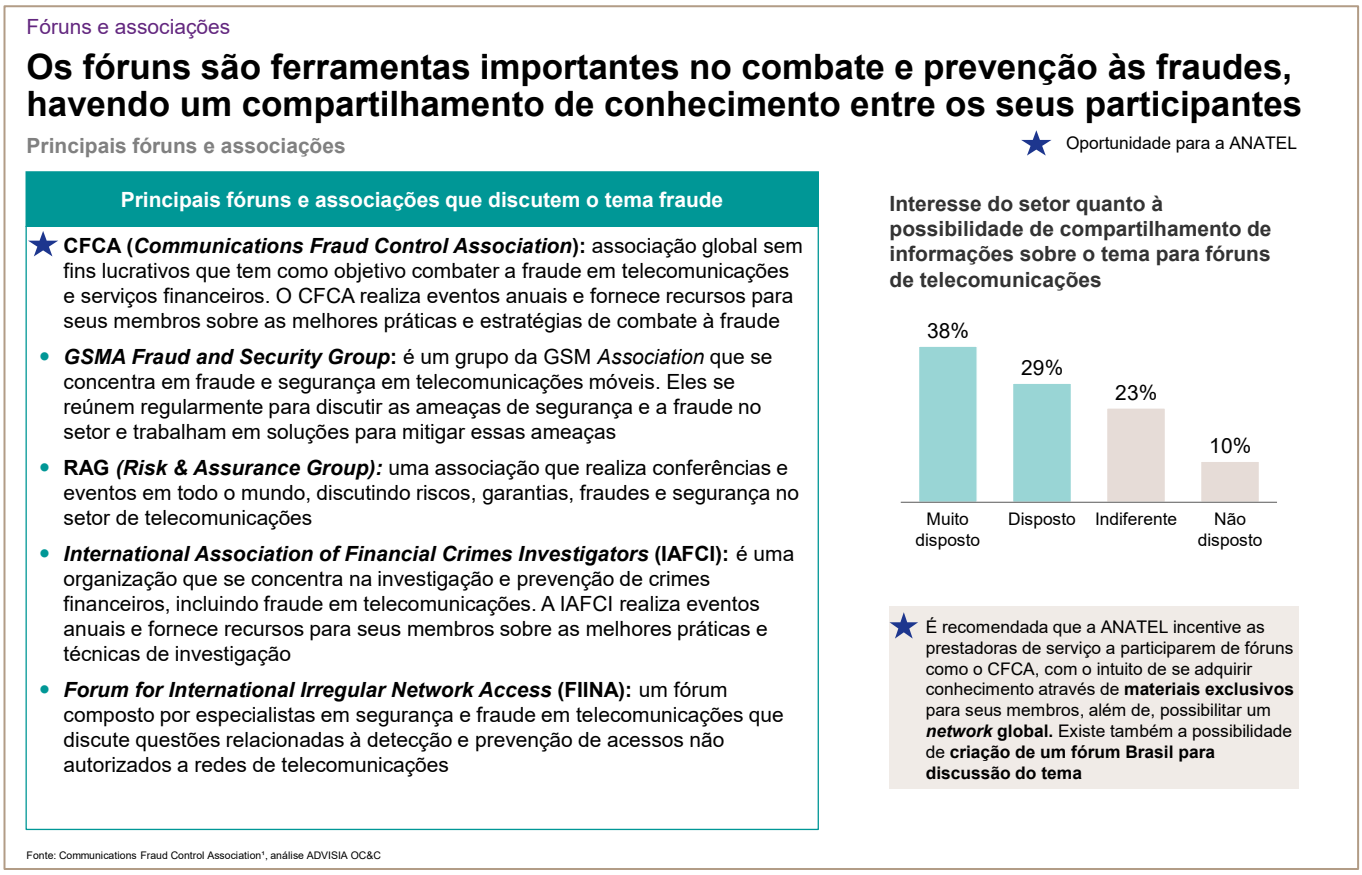


Figura 14

O CFCA descrito na figura acima possui grande relevância no cenário de fraude na indústria de telecomunicações. Diversas empresas se associam ao CFCA com o intuito de acessar materiais exclusivos, participar de *workshops* e fazer *networking*, no Brasil, temos como membro a prestadora de serviço Telefônica e outras empresas que atuam em diferentes mercados, por exemplo, a LexisNexis, Microsoft e Oracle.

Vale destacar que no Brasil, há diversos fóruns, eventos e conferências que discutem e abordam o tema de fraudes, especialmente no contexto de segurança cibernética e financeira. Esses eventos reúnem profissionais do setor, especialistas em segurança, representantes de agências reguladoras, empresas e acadêmicos para debater questões relacionadas à prevenção, detecção e combate às fraudes. Dentre as conferências, eventos, congressos e fóruns mais relevantes no Brasil, pode-se destacar:

- Fórum Brasileiro de Segurança Pública (FBSP): O FBSP tem como objetivo promover a discussão e a proposição de políticas de segurança pública no Brasil. Fundado em 2006, o FBSP atua como um espaço de diálogo e cooperação entre os diferentes setores da sociedade, incluindo acadêmicos, especialistas, gestores públicos e representantes da sociedade civil.
- Fórum Brasileiro de Combate à Pirataria e à Ilegalidade (FNCP): o FNCP é uma organização sem fins lucrativos que tem como objetivo combater a pirataria e outras formas de ilegalidade na internet. Ele atua em parceria com órgãos governamentais e empresas para promover a proteção da propriedade intelectual.
- Fórum de Combate à Corrupção e à Lavagem de Dinheiro (FOCCOSP): O fórum tem o objetivo de promover a cooperação e a troca de informações entre diferentes órgãos e entidades envolvidas no combate à corrupção e à lavagem de dinheiro no estado de São Paulo, Brasil. O FOCCOSP busca fortalecer e aprimorar a atuação de suas instituições participantes no enfrentamento desses crimes, promovendo ações coordenadas e integradas.
- Fórum E-Commerce Brasil: Este evento é voltado para o setor de comércio eletrônico e aborda temas como segurança de dados, prevenção de fraudes e melhores práticas em pagamentos online.
- FEBRABAN CIAB / TECH: Organizado pela Federação Brasileira de Bancos (FEBRABAN), o CIAB é um dos principais eventos de tecnologia bancária da América Latina e aborda temas relacionados à inovação, segurança cibernética e prevenção de fraudes no setor financeiro.
- Cyber Security Summit Brasil: é considerado o maior evento de cibersegurança do país e, de acordo com a Forbes, um dos mais importantes do mundo. O objetivo é disseminar conhecimento e possibilitar a troca de experiências sobre segurança da informação, trazendo palestrantes de peso que atuam em empresas multinacionais, governos, agências de segurança e outras grandes instituições.

- Futurecom: Considerado um dos maiores eventos de tecnologia e telecomunicações da América Latina, o Futurecom aborda temas como transformação digital, segurança cibernética e prevenção de fraudes no setor de telecomunicações.
- Congresso Internacional de Gestão de Riscos: Congresso realizado pela Febraban que reúne profissionais do setor financeiro, acadêmicos e órgãos reguladores para discutir tendências e inovações sobre práticas relacionadas com gestão de risco e compliance.
- Congresso Brasileiro de Auditoria Interna (CONBRAI): Evento anual que reúne especialistas sobre auditoria para compartilhar conhecimentos, tendências e melhores práticas sobre o setor

1.6. Métodos de fraude

O foco dessa seção será o estudo dos principais métodos de fraudes existentes no setor de telecomunicações, mas antes disso é importante salientar a diferença conceitual entre os termos "tipos de fraude" e "métodos de fraude", que, de acordo com a *Fraud Control Association* (CFCA), podem ser entendidos como:

- Tipos de fraude: Os tipos de fraude são classificados de acordo com o objetivo final do criminoso, a área afetada ou o tipo de benefício obtido. Eles descrevem a natureza e as características das atividades fraudulentas, como fraude de aumento de tráfego, fraude de serviços *premium* e fraude de interconexão.
- Métodos de fraude: Os métodos de fraude, por outro lado, referem-se às técnicas e estratégias específicas empregadas pelos criminosos para executar esses tipos de fraude. Os métodos de fraude descrevem o "como" das atividades fraudulentas, ou seja, as ações e os processos que os criminosos utilizam para atingir seus objetivos. Alguns exemplos de métodos de fraude incluem *phishing e spoofing* que serão detalhados abaixo.

Em resumo, os tipos de fraude estão relacionados às categorias de atividades fraudulentas, enquanto os métodos de fraude referem-se às técnicas utilizadas pelos criminosos para realizar essas atividades. Vários métodos de fraude podem estar relacionados com um tipo de fraude, ou seja, um fraudador pode utilizar várias técnicas / estratégias (método de fraude) para se chegar a um objetivo ou benefício (tipo de fraude).

O *Fraud Loss Survey Report*[10], publicado anualmente pela Communications Fraud Control Association (CFCA), traz informações detalhadas sobre os principais tipos e métodos de fraude que as empresas de telecomunicações sofrem. Para abordar adequadamente essas atividades criminosas, é essencial conhecer esses tipos de fraude que estão em constante evolução.

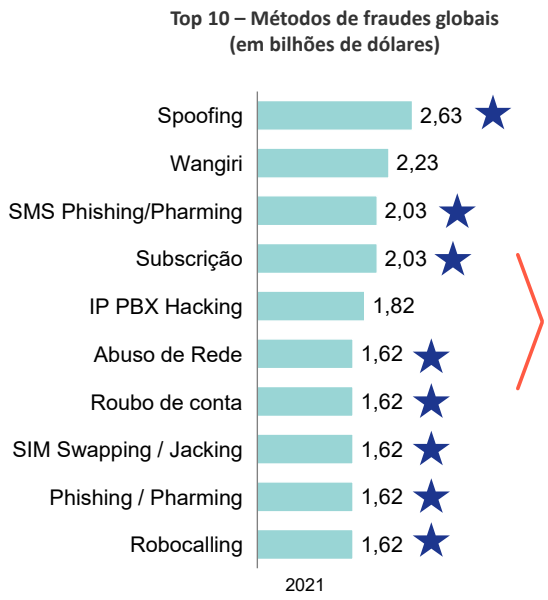
As principais fraudes serão apresentadas a seguir tendo como base este relatório da CFC. A figura abaixo ilustra os principais métodos de fraudes que a indústria de telecomunicações reportou em 2021:

Fraudes Telecom

Em 2021, a perda estimada de receita devido a fraudes no setor de telecomunicações foi de 40 bilhões de dólares

Visão macro – Fraudes no setor de telecomunicações

★ Fraude endereçada no plano de ação



Métodos	Breve descrição
Spoofing	Manipulação do endereço IP/CLI/ANI para ocultar a verdadeira origem ou identidade de alguém
Wangiri	Esquemas de fraude de retorno de chamada
SMS Phishing/Pharming	Roubo de informações pessoais ou credenciais via *hacking* de SMS, *phishing*, *vishing*, etc.
Subscrição	Utilização de uma identidade real ou sintética com ou sem o conhecimento do proprietário para obter bens e serviços (sem intenção de pagamento)
IP PBX Hacking	PBX IP comprometido usado para fazer chamadas fraudulentas
Abuso de Rede	Exploração de uma fraqueza de configuração para obter acesso a uma rede ou dispositivo; inclui equipamentos VoIP, como um modem ou roteador
Roubo de conta	Manipulação e utilização da conta do cliente / usuário existente para obter acesso a um dispositivo ou serviço
SIM Swapping / Jacking	Substituir / clonar / roubar o cartão SIM para obter acesso ao dispositivo ou serviço
Phishing / Pharming	Roubo de informações pessoais ou credenciais via hacking, phishing, vishing, etc ...
Robocalling	Uso de discadores automáticos computadorizados para entregar mensagens pré-gravadas para perpetuar fraudes

Fonte: Communications Fraud Control Association, análise ADVISIA OC&C

Figura 15

Dentre os 10 principais métodos de fraudes que mais causaram prejuízos financeiros para o setor de telecomunicação em 2021, 8 deles serão endereçados diretamente ou indiretamente no plano de ação proposto neste documento, os outros 2 não foram priorizados, pois são fraudes com pouca relevância no cenário brasileiro.

A compreensão desses métodos de fraude é fundamental para a construção de um plano bem estruturado para o combate, prevenção e mitigação a fraudes. Sendo assim eles serão detalhados a seguir. Os três métodos de fraudes que causaram um maior prejuízo financeiro para o mercado global de telecomunicações estão ilustrados nas figuras abaixo.

- ***Spoofing***[20]

Spoofing é quando um chamador falsifica deliberadamente as informações transmitidas para o identificador de chamadas para disfarçar sua identidade. Os golpistas geralmente usam a falsificação utilizando números locais para parecer que uma chamada recebida está vindo da mesma área. Eles também podem falsificar um número de uma empresa ou agência governamental. Quando a possível vítima responde geralmente já existe um script feito onde o golpista tenta obter alguma vantagem, a maioria das vezes é financeira ou informações pessoais que podem ser utilizadas posteriormente em atividades fraudulentas. A figura abaixo ilustra os tipos de *spoofing* mais comuns:

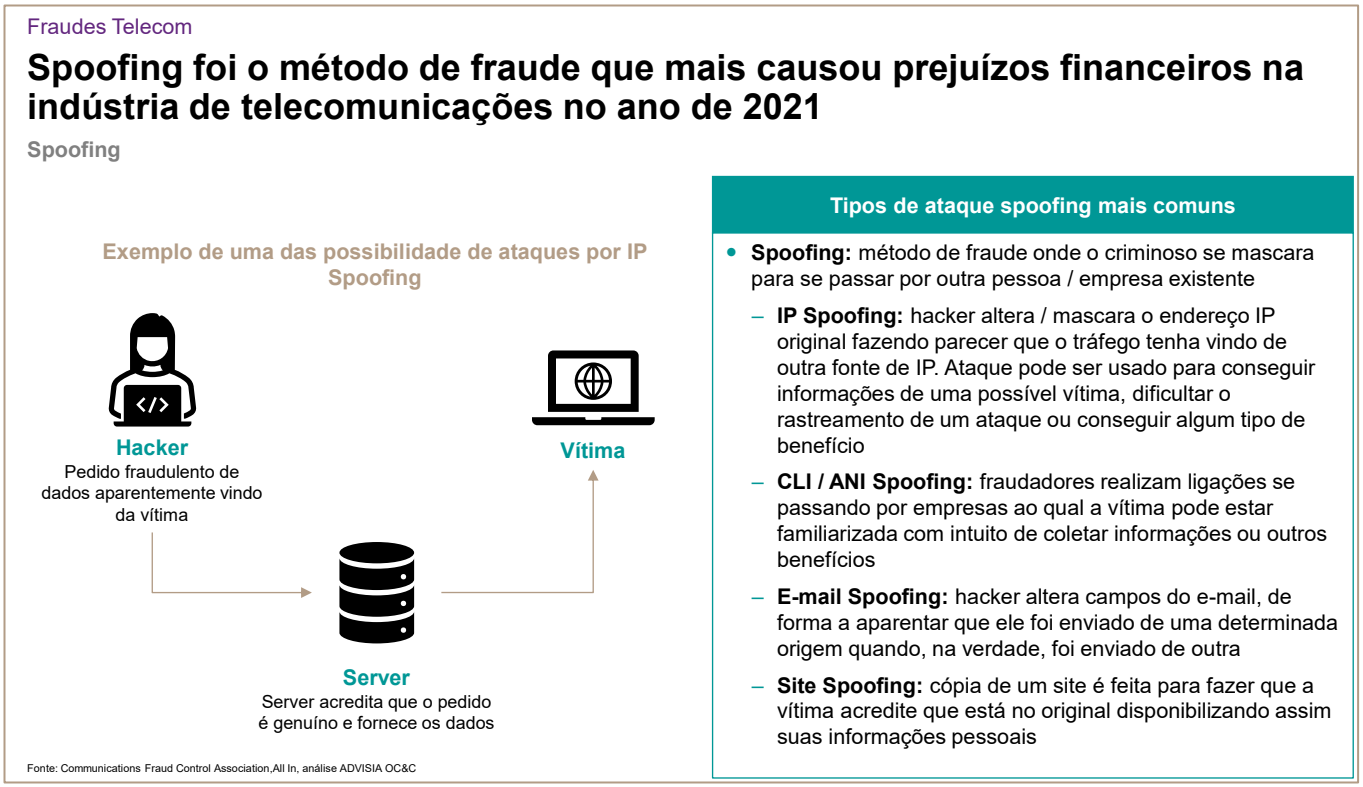


Figura 16

[20] EUA. Federal Communications Commission. Caller ID Spoofing. Disponível em: https://www.fcc.gov/spoofing

- **Wangiri**

'Wangiri' [21]é uma palavra japonesa que significa “um toque / ligação e corta”. É um golpe telefônico em que os criminosos o induzem a ligar para números de tarifa premium. O intuito da fraude é induzir a vítima a ligar para o número, quando ela liga acontece um redirecionamento para um número de tarifa premium no exterior e posteriormente essa chamada telefônica é cobrada. Os fraudadores obtêm lucro aumentando o tráfego artificialmente para esses números internacionais de tarifas premium. Esse golpe é mais comum na América do Norte e Europa. A Europol (agência da União Europeia para cooperação policial) aconselha que as vítimas desse tipo de golpe façam a denúncia para a sua respectiva polícia nacional para que elas bloqueiem esses números de tarifa *premium*.

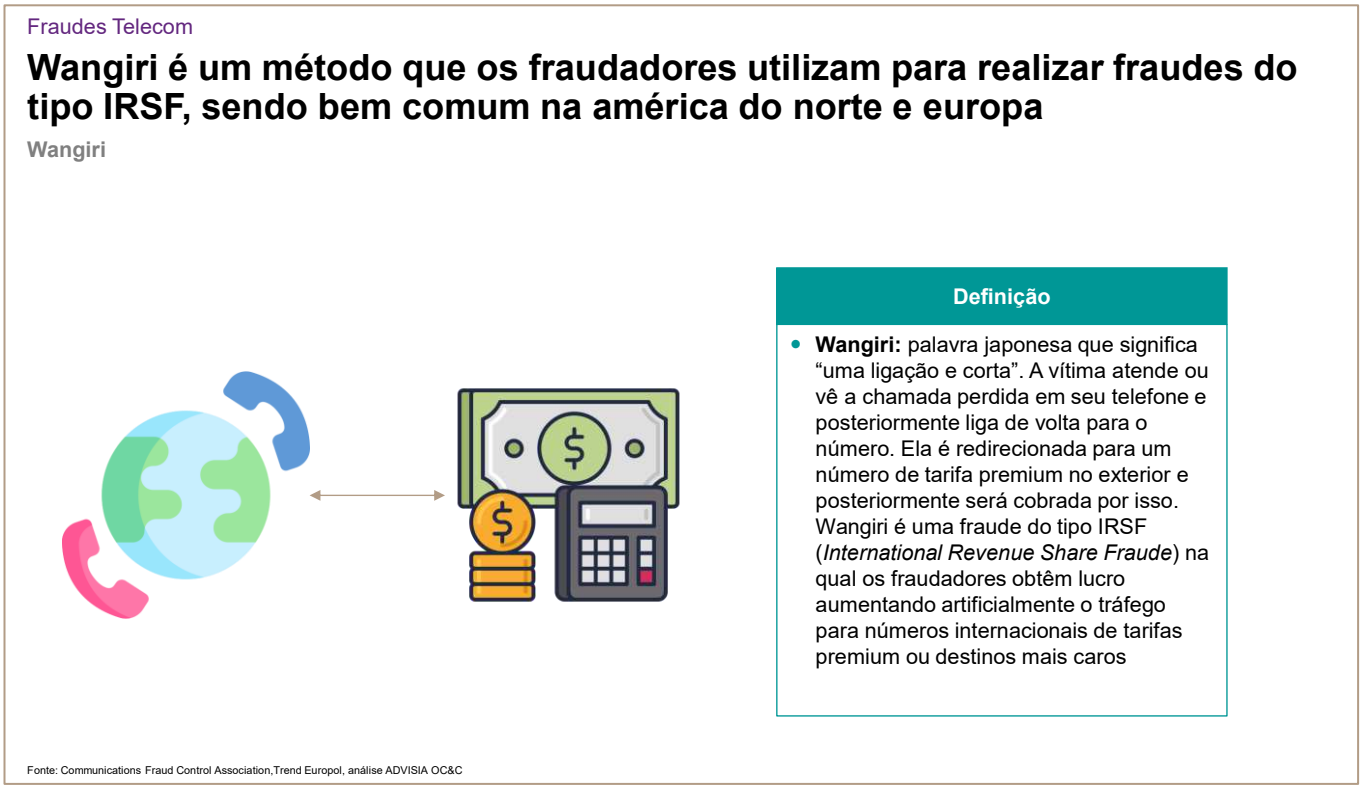


Figura 17

[21] União Europeia. Europol. Wangiri. Disponível em: https://www.europol.europa.eu/sites/default/files/documents/wangiri_final_2.pdf

- **Phishing / Pharming[22]**

Phishing e *pharming* são fraudes similares que utilizam engenharia social para roubar informações confidenciais, mas que funcionam de maneiras distintas.

Mais conhecido, o *phishing* normalmente ocorre via e-mail, enquanto o *pharming* usa técnicas mais sofisticadas. Ambos, no entanto, são ameaças digitais comuns devido a facilidade de utilização da fraude.

Geralmente os fraudadores utilizam e-mail, mensagens de texto ou SMS para tentar roubar senhas, números de contas ou números de CPF. Quando eles obtêm sucesso no roubo desses dados, eles geralmente acessam o e-mail, banco ou outras contas da vítima. Há relatos de venda de informações pessoas para outros golpistas. A figura abaixo ilustra esse tipo de fraude.

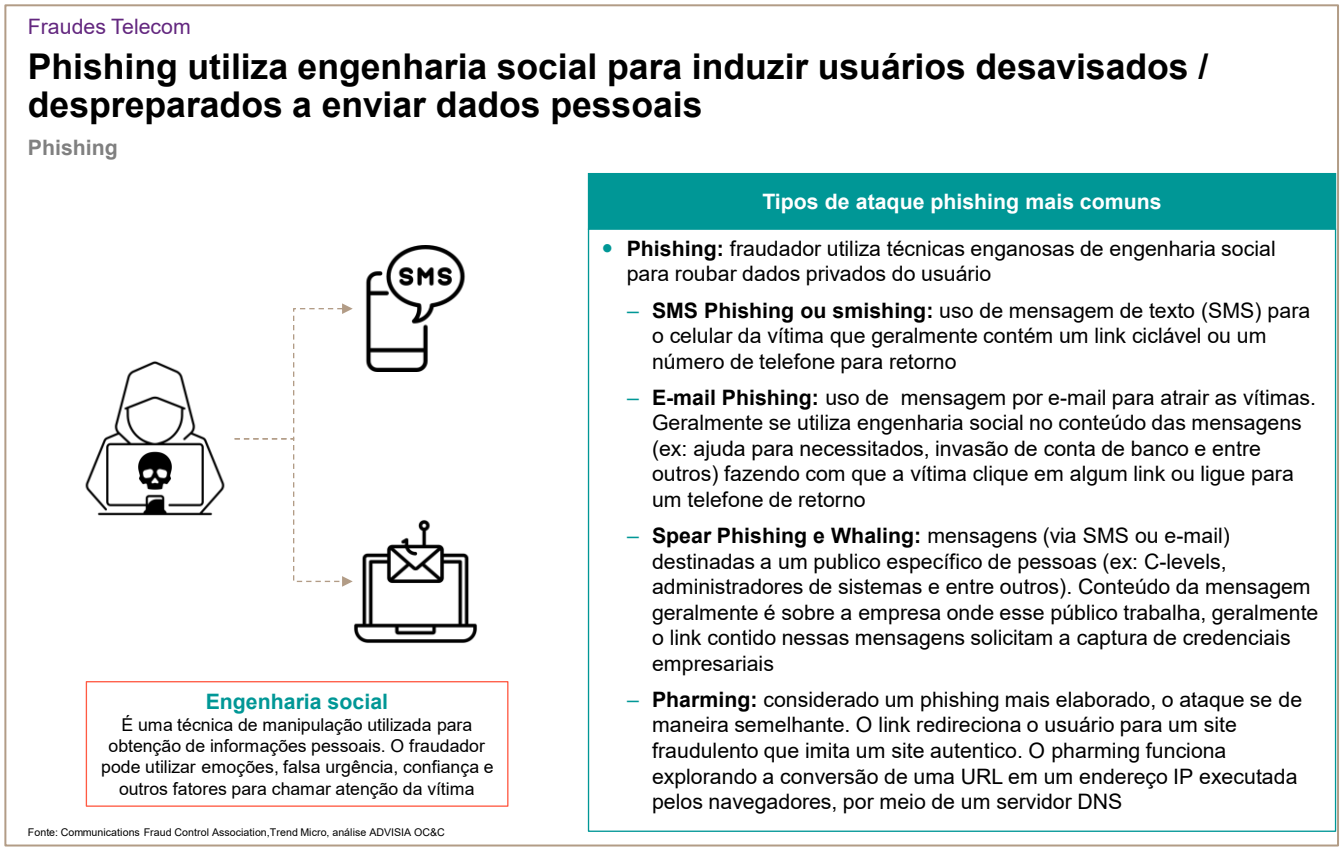


Figura 18

[22] EUA. Federak Trade Commission. How to Recognize and Avoid Phishing Scams. Disponível em: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

- **Subscrição**[10]: também conhecida como fraude de assinatura ou fraude de assinante, é um tipo de atividade criminosa que envolve a utilização de uma identidade real ou falsa para obter serviços ou produtos, geralmente sem a intenção de pagar por eles. No setor de telecomunicações, a fraude de subscrição ocorre quando um indivíduo ou grupo usa informações de identificação pessoal (PII) autênticas ou falsificadas para abrir uma conta e obter serviços de telecomunicações, como telefonia fixa, celular, internet ou serviços de TV por assinatura. Esse tipo de fraude traz implicações significativas tanto para as empresas quanto para os consumidores. As empresas enfrentam perdas financeiras, uma vez que os criminosos geralmente não pagam pelos serviços utilizados, e os clientes afetados podem sofrer danos ao crédito e ter sua privacidade comprometida.
- **IP PBX Hacking**[10]: também conhecida como fraude de PBX IP comprometido, é um tipo de fraude em telecomunicações que envolve a exploração de vulnerabilidades em sistemas de telefonia IP privados (Private Branch Exchange, ou PBX) para realizar chamadas fraudulentas. O PBX IP é um sistema telefônico baseado em tecnologia VoIP (Voice over IP) que permite a comunicação interna e externa em empresas e outras organizações. Os criminosos comprometem o PBX IP para obter acesso não autorizado e utilizar os recursos de telecomunicações da empresa para fazer chamadas de longa distância, internacionais ou para números de tarifação adicional.
- **Abuso de rede**[10]: também conhecida como exploração de rede, ocorre quando criminosos exploram fraquezas ou vulnerabilidades de configuração em redes ou dispositivos para obter acesso não autorizado e realizar atividades fraudulentas ou maliciosas. Essas atividades podem incluir roubo de dados, espionagem, negação de serviço (DoS), uso indevido de recursos de rede e outros ataques cibernéticos.

- **SIM Swap**[23]: também conhecido como SIM Swapping, é um tipo de golpe que envolve a transferência não autorizada do número de telefone de uma pessoa para um novo cartão SIM. O Sim Swap também pode ocorrer por meio de fraude interna, quando os fraudadores realizam a cooptação de colaboradores das prestadoras para realizar as configurações de troca do Simcard. Isso permite que os criminosos assumam o controle do número de telefone da vítima, o que pode levar ao roubo de identidade, acesso não autorizado a contas bancárias e serviços online, bem como a divulgação de informações pessoais confidenciais. De acordo com a Europol, a fraude SIM Swap geralmente segue os passos a seguir:
    - Coleta de informações: Os criminosos obtêm informações pessoais da vítima, como nome completo, data de nascimento e número de telefone. Isso pode ser feito por meio de *phishing*, engenharia social ou roubo de dados.
    - Contato com a operadora: Os criminosos se passam pela vítima e entram em contato com a operadora de telefonia móvel, solicitando a transferência do número de telefone da vítima para um novo cartão SIM que está sob seu controle.
    - Verificação de identidade: A operadora geralmente solicita informações pessoais para verificar a identidade do solicitante. Nesse caso, os criminosos fornecem as informações coletadas anteriormente para convencer a operadora de que são a pessoa legítima.
    - Transferência do número: Uma vez que a operadora esteja convencida da identidade do solicitante, o número de telefone da vítima é transferido para o novo cartão SIM controlado pelos criminosos.
    - Acesso não autorizado: Com o controle do número de telefone da vítima, os criminosos podem solicitar a redefinição de senhas, obter códigos de

[23] EUROPOL. Disponível em: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/sim-swapping-%E2%80%93-mobile-phone-scam

verificação por SMS para acessar contas bancárias, e-mails e outros serviços online da vítima e eles também podem aplicar golpes e fraudes aos contatos da vítima, ampliando as vítimas e os prejuízos financeiros.

- ***Unlawful Robocalling*** [24]é um tipo de golpe em que os criminosos usam sistemas de discagem automática e tecnologias de voz computadorizada para realizar chamadas em massa e enganar as vítimas, induzindo-as a fornecer informações pessoais, financeiras ou confidenciais. De acordo com a *Federal Communications Commission* (FCC) dos Estados Unidos, um dos aspectos-chave das chamadas de *robocalling* fraudulentas é o uso de *spoofing* de identificador de chamadas, que permite aos criminosos falsificar o número de telefone que aparece no identificador de chamadas das vítimas. Os criminosos podem usar *robocalls* fraudulentas para realizar uma variedade de golpes, incluindo:
    - Falsas cobranças de dívidas ou ofertas de empréstimos: Os criminosos podem alegar que a vítima deve dinheiro ou é elegível para um empréstimo, solicitando informações financeiras ou pessoais para "resolver" a situação.
    - Golpes de suporte técnico: Os criminosos se passam por representantes de suporte técnico de empresas conhecidas e afirmam que o dispositivo da vítima está infectado por *malware*, solicitando acesso remoto ou pagamento para "consertar" o problema.
    - Golpes de impostos ou benefícios governamentais: Os criminosos afirmam ser representantes de agências governamentais, como a Receita Federal ou a Segurança Social, solicitando informações pessoais ou pagamento para resolver questões fiscais ou processar benefícios.

Além dos métodos de fraudes citados na Figura 15 existem outros métodos relevantes no cenário brasileiro que serão exemplificados abaixo:

[24] EUA. Federal Communications Commission. Disponível em: https://www.fcc.gov/spoofed-robocalls

- Fraude de ligação de falso sequestro[25] é um tipo de golpe onde o fraudador se passa por uma criança da família simulando uma voz de choro chamando pela mãe ou pelo pai dizendo que foi sequestrada. A intenção do fraudador é extrair alguma quantia financeira da vítima.
- Fraudes de identidade ou falsa identidade[26] é considerado um crime pelo Código Penal Brasileiro (Art 307 e 308) com pena que pode vaiar a detenção de três meses a dois anos. A falta identidade é conceituada da seguinte maneira: “Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem” (Art 307) ou “Usar, como próprio, passaporte, título de eleitor, caderneta de reservista ou qualquer documento de identidade alheia ou ceder a outrem, para que dele se utilize, documento dessa natureza, próprio ou de terceiros” (Art 308).
- Fraudes de 0800 ou 0300[27]: golpistas enviam mensagens maliciosas via SMS, enviadas por um número curto *(shorts-codes)* para possíveis vítimas solicitando contato para um 0800 ou 0300. Caso a vítima entre em contato usando o 0800 da mensagem falsa, os criminosos solicitam a confirmação da conta e agência (para roubá-la), e questionam se o correntista tem alguma autenticação temporária ativada. Há alguns casos relatados onde os fraudadores também utilizam o 0800 para influenciar a vítima a baixar um *malware* em seu dispositivo móvel (golpe da mão fantasma).
- Golpe da mão fantasma[28]: também conhecido como “golpe do acesso remoto”. A fraude acontece quando o criminoso entra em contato com a vítima se passando

[25] PicPay. Disponível em: https://blog.picpay.com/golpe-do-falso-sequestro/

[26] BRASIL. Código Penal (Art 307 e 308). Disponível em: https://www.jusbrasil.com.br/busca?q=art.+307+e+308+do+c%C3%B3digo+penal

[27] Telesintese. Disponível em: https://www.telesintese.com.br/empresa-identifica-uso-fraudulento-de-numeros-0800/

[28] Serasa. Disponível em: https://www.serasa.com.br/premium/blog/golpe-da-mao-fantasma-dicas-para-se-proteger/?gclid=CjwKCAjwov6hBhBsEiwAvrvN6AMjDgc25VQjSAsU-bg9yViJ2ekzDpXxfZcIleL0pGy6sLS75fG_IBoCLPwQAvD_BwE

geralmente por um falso funcionário do banco (pode ser utilizado 0800 fraudulentos para o contato) em que a pessoa é correntista solicitando que a vítima instale um *malware* que dá ao fraudador acesso irrestrito ao aparelho celular do cliente. Geralmente o golpista acessa os aplicativos dos bancos com o intuito de fraudar a vítima.

- Fraude de boletos falsos[29] são um tipo de golpe financeiro utilizando boletos bancários que são uma forma popular de pagamento de contas entre a população brasileira. Os fraudadores emitem boletos falsos com informações manipuladas, levando as vítimas a realizarem pagamentos para contas controladas, em vez de pagarem às empresas ou instituições legítimas. Esses golpes podem ocorrer em várias situações, como pagamentos de compras online, mensalidades de escolas e universidades, ou até mesmo contas de serviços públicos.
- Golpes de Whatsapp e redes sociais[30] estão sendo utilizados por criminosos que se passam pela vítima e tentam obter vantagens (principalmente financeiras) com os contatos salvos do usuário. Existem alguns recursos de segurança que podem auxiliar no combate a esse tipo de fraude, como por exemplo códigos PIN.

[29] Serasa. Disponível em: https://www.serasa.com.br/premium/blog/boleto-falso-4-sinais-para-identificar/

[30] Serasa. Disponível em: https://www.serasa.com.br/premium/blog/whatsapp-clonado/

1.7. *Benchmarking* internacional

Como descrito na introdução deste documento, foram selecionados 5 países para construção do *benchmarking*. O *benchmarking* visa capturar as melhores práticas existentes no mercado para identificação de lacunas e oportunidades existentes. O processo de análise de "*gaps*" servirá de insumo e inspiração para a implementação do plano tático dos anos de 2023 e 2024.

A Figura 19 ilustra as agências analisadas no *benchmarking:*

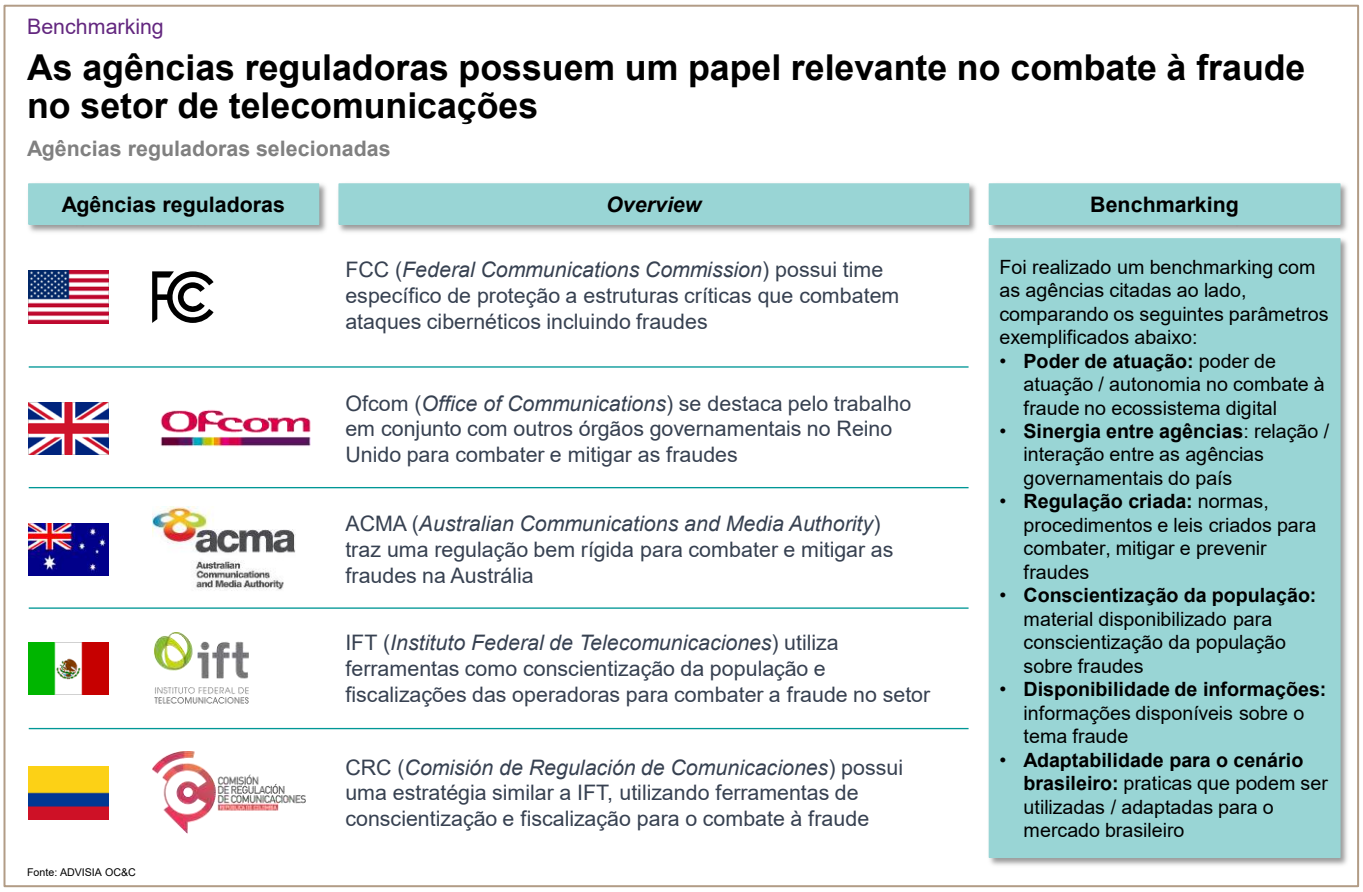


Figura 19

Como citado na Figura 19, foram utilizados 6 parâmetros qualitativos de comparação entre as agências que seguiram as seguintes regras avaliativas:

- Poder de atuação: a nota varia pelo escopo de atuação de cada agência, a nota é dada considerando-se a liberdade de atuação e o histórico do escopo das

agências no combate e prevenção à fraude. O maior histórico público ficou com a agência reguladora dos EUA, as demais notas foram uma comparação direta com esse histórico;

- Sinergia entre agências: foi considerado o histórico das agências na realização de trabalhos com outras entidades do governo envolvendo o tema fraude. As agências com maiores registros públicos de coparticipação com outras entidades governamentais foram as agências dos EUA e do Reino Unido, as demais notas foram baseadas comparando com os históricos dessas duas agências;
- Regulação criada: levou em consideração as normas, regulamentos e leis criadas que possuem alguma correlação com o tema de fraude. A nota máxima foi dada para a agência da Austrália devido à grande quantidade de normas envolvendo os cadastros dos serviços de telecomunicações, por exemplo, normas relacionadas com cadastro de chips pré-pago (vale ressaltar que o cadastro de chip pré-pagos acontece em poucos países ao redor do mundo, devido à grande complexidade envolvida e a própria natura do serviço pré);
- Conscientização da população: foram analisadas a qualidade e a quantidade de materiais divulgados para a população sobre conscientização a respeito do tema de fraude. A nota máxima foi dada para a agência do Reino Unido devido à qualidade apresentada nas campanhas de conscientização, com destaque para o material áudio visual criado;
- Disponibilidade de informações: foi avaliada a quantidade de informação disponível sobre o tema fraude nos sites oficiais das agências (cartilhas, operações, regulação, notícias e entre outros). A agência que obteve a maior nota foi a dos EUA devido à grande quantidade de materiais disponibilizados, com destaque para as operações realizadas em parceria com outras agências governamentais.
- Adaptabilidade para o cenário brasileiro: foram considerados os 6 parâmetros anteriores levando-se em conta a possibilidade de se utilizar / adaptar essas melhores práticas estudadas para o cenário brasileiro

Após feita essa análise foi criada uma tabela comparativa ilustrada abaixo:

Benchmarking

Algumas das práticas para o combate e a prevenção a fraudes utilizadas pela Ofcom e pela ACMA podem servir de inspiração para a ANATEL

Comparação

	Aspectos relacionados com combate, prevenção e mitigação a fraudes digitais					
Agências reguladoras	**Poder de atuação**	**Sinergia entre agências**	**Regulação criada**	**Conscientização da população**	**Disponibilidade de informações**	**Adaptabilidade para o cenário brasileiro**
FCC	●	●	◕	◕	◕	◑
Ofcom	◑	●	◑	●	◕	◕
ACMA	◕	◕	●	◕	◕	◕
IFT	◑	◑	◑	◑	◑	◑
CRC	◑	◑	◑	◑	◑	◑

Fonte: ADVISIA OC&C

Figura 20

A FCC (Federal Communications Commission) - Estados Unidos

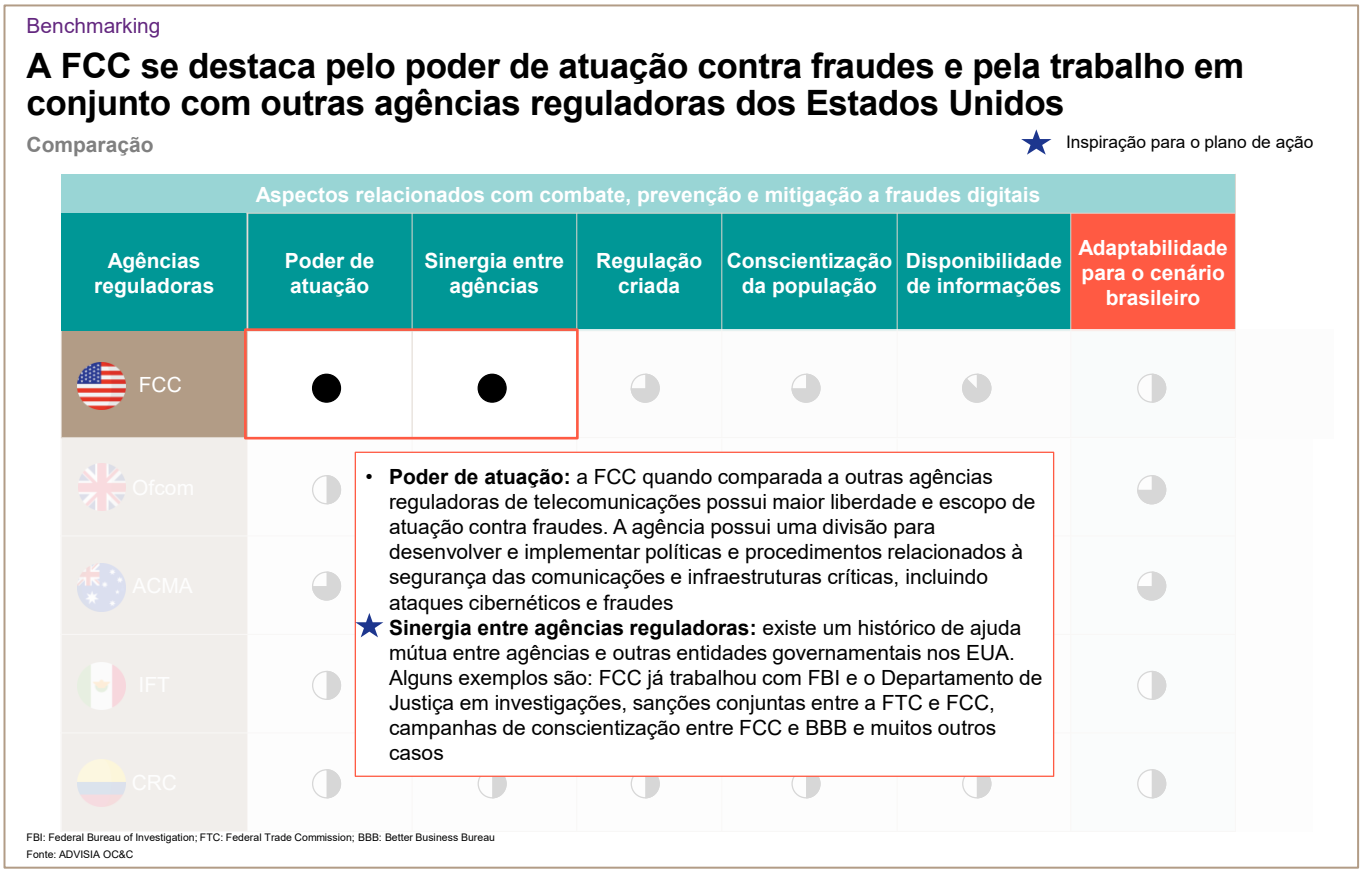


Figura 21

A FCC desempenha um papel fundamental na proteção dos consumidores, na garantia da segurança das redes de telecomunicações e na promoção do acesso a serviços de telecomunicações de qualidade, ela é a autoridade reguladora que cria e aplica as regras e regulamentações relacionadas às comunicações nos EUA. A agência dos EUA criou uma equipe de resposta [31]contra fraudes envolvendo *Robocalls* e *Spoofing* reunindo especialistas com o intuito de combater essas chamadas ilegais de cunho malicioso, criando procedimentos para identificação desses tipos de ligações.

[31] EUA. Federal Communications Commission. Robocall Response Team. Disponível em: https://www.fcc.gov/spoofed-robocalls

A agência possui uma subdivisão interna especifica de cibersegurança e confiabilidade chamada Cybersecurity and Communications Reliability Division (CCR)[32] responsável por garantir que as redes de comunicação nos EUA estejam seguras para o público. A CCR é dividida em 4 grandes áreas de atuação, são elas:

- Confiabilidade da Rede: monitoramento e análise das interrupções da rede de comunicações para identificar tendências e avaliar as ações que a FCC pode tomar para ajudar a prevenir e mitigar interrupções;
- Preparação e resposta a desastres: durante emergências, a CCR coleta informações sobre o status operacional da infraestrutura de comunicações para apoiar os esforços governamentais de assistência a desastres e monitorar a restauração e recuperação;
- Riscos e vulnerabilidades: a divisão trabalha para identificar e reduzir os riscos à confiabilidade da rede de comunicações do país;
- Supply Chain: a CCR realiza análises direcionadas a empresas que podem representar uma ameaça potencial à segurança nacional à integridade das redes de comunicações dos EUA ou à cadeia de fornecimento de comunicações.

Também vale ressaltar a existência de uma área específica para a fraudes na FCC, a Fraud Division [33]. O escopo dessa área não possui correlação com o tema deste estudo, pois as fraudes avaliadas estão relacionadas a fraudes direcionadas a programas críticos financiados e administrados pela FCC, como apoio do Fundo de Serviço Universal (USF), Benefícios Emergenciais de Banda Larga (EBB), Programa de Conectividade Acessível (ACP), com ênfase particular no tratamento de atividades fraudulentas.

O *Electronic Code of Federal Regulations* (eCFR) é um repositório online de regulamentos federais que são atualizados regularmente para refletir as mudanças nas regras e

[32] EUA. Federal Communications Commission. CCR. Disponível em: https://www.fcc.gov/cybersecurity-and-communications-reliability-division-public-safety-and-homeland-security-bureau

[33] EUA. FCC. Fraud Division. Disponível em: https://www.fcc.gov/enforcement/divisions-offices/fd

regulamentações. O *Title* 47 [34]do eCFR de responsabilidade da FCC é dedicado às regras e regulamentações relacionadas às comunicações, incluindo telecomunicações, radiodifusão, rádio e televisão por satélite, e serviços móveis e sem fio. Seguem alguns exemplos das regras criadas pela FCC que possuem alguma correlação com o tema fraude:

- Parte 0 - Comissão (Federal Communications Commission): Esta parte inclui disposições sobre a organização e delegação de funções da FCC, que é a agência responsável pela supervisão e regulamentação do setor de telecomunicações, incluindo o combate às fraudes e proteção dos consumidores.
- Parte 1 - Prática e Procedimento: A seção 1.80 inclui disposições sobre penalidades civis e aplicações monetárias por violação das regras da FCC, incluindo aquelas relacionadas a fraudes e abusos.
- Parte 20 - Serviços de Telecomunicações Móveis Comerciais: A seção 20.22 aborda a responsabilidade dos portadores de serviços móveis em relação à proteção e uso das informações de localização do cliente, ajudando a prevenir fraudes e abusos relacionados à privacidade.
- Parte 42 - Preservação de Registros de Comunicações: Esta parte contém regras sobre a preservação de registros de comunicações por prestadoras de serviços de telecomunicações, o que pode ser relevante para investigações de fraude e outros processos legais.
- Parte 64 - Disposições de Telecomunicações Miscelâneas: A seção 64.2001 a 64.2011 aborda as regras de Privacidade do CPNI (Informações de Rede Proprietária do Cliente), que são relevantes para a proteção dos dados pessoais dos consumidores e a prevenção de fraudes.
- Além dessas regulações presentes no eCFR a FCC tem implementado regras e normas relacionadas à prevenção de fraudes que incluem:

[34] EUA. Code of Federal Regulations. Title 47. Disponível em: https://www.ecfr.gov/current/title-47

- Regra de Autenticação de Identificador de Chamadas (STIR/SHAKEN35): A FCC adotou a regra de autenticação do identificador de chamadas, exigindo que as prestadoras de serviços de telecomunicações implementem a tecnologia STIR/SHAKEN em suas redes. Essa tecnologia ajuda a combater o spoofing de chamadas e o aumento das chamadas fraudulentas e indesejadas. A regra foi adotada como parte do combate às chamadas ilegais sob a Lei TRACED Act. Essa regra de verificação também é utilizada para chamadas internacionais exigindo que as prestadoras de serviços de telecomunicações verifiquem a autenticidade antes de conectá-las aos consumidores nos Estados Unidos. Isso ajuda a proteger os consumidores contra fraudes telefônicas internacionais e chamadas indesejadas.
- Regras de Privacidade do CPNI 36(Informações de Rede Proprietária do Cliente): A FCC estabeleceu regras para proteger as informações pessoais dos consumidores relacionadas ao uso de serviços de telecomunicações, conhecidas como CPNI. As regras do CPNI exigem que as prestadoras de serviços de telecomunicações obtenham o consentimento dos consumidores antes de usar ou compartilhar suas informações para fins de marketing e tomem medidas para proteger a segurança dessas informações.
- Regras de Faturamento e Cobrança Justas (Truth-in-Billing37): A FCC implementou regras de faturamento e cobrança justas para ajudar os consumidores a entenderem suas contas de telecomunicações e evitar fraudes de cobrança. Essas regras exigem que as prestadoras de serviços de

[35] EUA. Federal Communications Commission. STIR/SHAKEN. Disponível em: https://www.fcc.gov/call-authentication

[36] EUA. Federal Communications Commission. FCC Rules. Disponível em: https://www.fcc.gov/protecting-your-personal-data#:~:text=FCC%20rules%20protect%20customer%20proprietary,consumer%2C%20such%20as%20call%20waiting.

[37] EUA. Federal Communications Commission. *Truth-in-Billing.* Disponível em: https://www.fcc.gov/general/truth-billing-policy

telecomunicações forneçam contas claras, não enganosas e de fácil compreensão, e que obtenham o consentimento dos consumidores antes de cobrar por serviços adicionais.

- Regras de Registro de Revendedores e Intermediários (Intermediate Provider Registry38): A FCC exige que revendedores e intermediários de serviços de telecomunicações se registrem junto à agência e cumpram certos requisitos de transparência e responsabilidade. Essas regras ajudam a combater fraudes e abusos no setor de telecomunicações ao garantir a responsabilidade dos participantes do mercado.

Outro aspecto destacável da FCC é a sinergia com outras agências governamentais dos EUA. Por exemplo a operação *Call It Quits*[39], em que a FTC ou Federal Trade Commission [40](agência governamental dos Estados Unidos responsável por proteger os consumidores de práticas comerciais desleais e enganosas) liderou, em parceria com a FCC, procuradores-gerais estaduais e autoridades locais para combater chamadas ilegais de telemarketing e *robocalls*. A operação resultou em várias ações de aplicação da lei, incluindo multas e processos contra infratores.

Existe também um histórico de ajuda mútua entre FCC e outras agências, por exemplo:

- Parceria de trabalho em conjunto com o Departamento de Segurança Interna (DHS) e Cybersecurity and Infrastructure Security Agency (CISA) para proteger a infraestrutura crítica de comunicações dos EUA contra ameaças cibernéticas, fraudes e outros riscos. Essas agências colaboram na avaliação de vulnerabilidades, compartilhamento de informações sobre ameaças e coordenação de resposta a incidentes de segurança.

---

[38] EUA. Federal Communications Commission. *Intermediate Provider Registry.* Disponível em: https://opendata.fcc.gov/dataset/Intermediate-Provider-Registry

[39] EUA. Federal Trade Commission. Call It Quits. Disponível em: https://www.ftc.gov/business-guidance/blog/2019/06/operation-call-it-quits-theres-no-quit-our-fight-against-illegal-robocalls

[40] EUA. Federal Trade Commission. About the FTC. Disponível em: https://www.ftc.gov/

- Parceria com o Federal Bureau of Investigation (FBI) em investigações envolvendo crimes cibernéticos, fraudes e golpes que afetam o setor de comunicações, compartilhando informações e recursos para identificar e processar infratores.

A Ofcom (Office of Communications) – Reino Unido

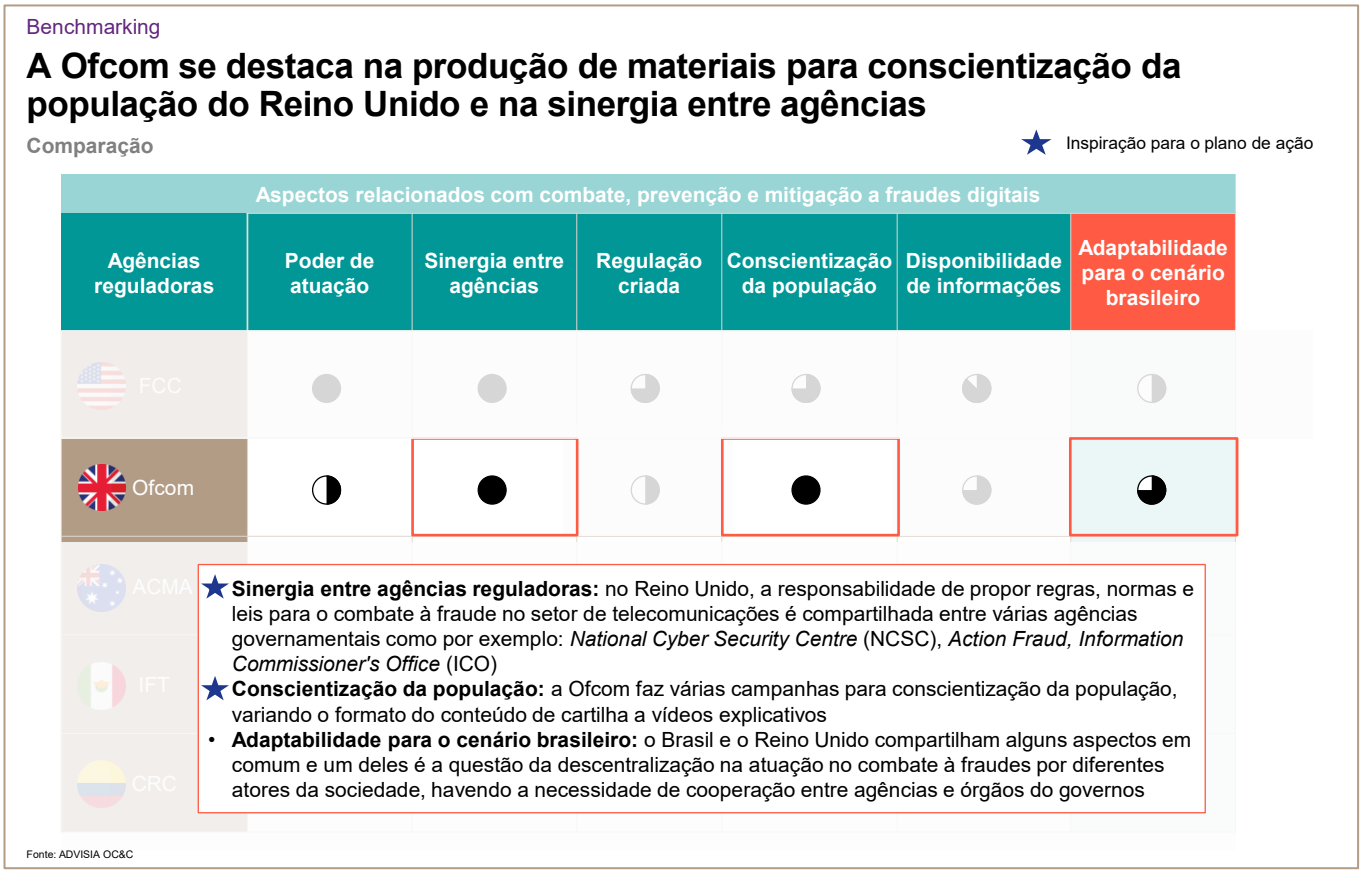


Figura 22

A Ofcom, o órgão regulador de comunicações do Reino Unido, tem trabalhado em colaboração com várias outras agências governamentais, organizações e entidades para combater fraudes e golpes no setor de telecomunicações. Alguns exemplos de atuação conjunta incluem:

- Parceria com a *Action Fraud*[41]: A Ofcom trabalha em conjunto com a *Action Fraud*[42](uma agência nacional de crimes cibernéticos e fraudes no Reino Unido, criada em 2009), o centro nacional de denúncias de fraudes e crimes cibernéticos

[41] REINO UNIDO. Ofcom. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0018/232074/statement-tackling-scam-calls-and-texts.pdf

[42] REINO UNIDO. Action Fraud. Disponível em: https://www.actionfraud.police.uk/what-is-action-fraud

do Reino Unido, para compartilhar informações e orientar os consumidores afetados por fraudes e golpes relacionados às telecomunicações.

- Parceria com a *Information Commissioner's Office* [43](ICO[44]): A Ofcom colabora com a ICO (autoridade criada para defender os direitos da informação no Reino Unido, responsável por garantir que as empresas e organizações que lidam com dados pessoais cumpram as leis de proteção de dados do país) no combate a chamadas não solicitadas e outras formas de comunicação eletrônica indesejada, como *spam* por e-mail e mensagens de texto. Juntas, as agências compartilham informações e recursos para investigar e processar infratores, além de coordenar campanhas de conscientização pública.
- Parceria com a *National Cyber Security Centre* [45](NCSC[46]): A Ofcom trabalha em estreita colaboração com a NCSC (agência responsável pela proteção da infraestrutura crítica do Reino Unido, respondendo a incidente de segurança cibernética), para proteger as redes de telecomunicações contra ameaças cibernéticas e garantir a segurança e resiliência da infraestrutura de comunicações.
- Cooperação com *a Phone-paid Services Authority* [47](PSA[48]): A Ofcom coopera com a PSA (é a entidade reguladora do Reino Unido responsável por supervisionar e regulamentar os serviços pagos por telefone, também conhecidos como serviços de pagamento móvel ou serviços pagos por operadora. A PSA é

[43] REINO UNIDO. Ofcom and ICO. Disponível em: https://www.ofcom.org.uk/news-centre/2021/tackling-nuisance-calls

[44] REINO UNIDO. ICO. Disponível em: https://ico.org.uk/about-the-ico/who-we-are/

[45] REINO UNIDO. Fraud Taskforce. Disponível em: https://www.gov.uk/government/publications/joint-fraud-taskforce-partner-organisations/joint-fraud-taskforce-partner-organisations

[46] REINO UNIDO. NCSC. Disponível em: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

[47] REINO UNIDO. Phone-paid Services. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/833921/PSA_Annual_Report_and_Accounts_2018_2019.pdf

[48] REINO UNIDO. PSA. Disponível em: https://psauthority.org.uk/About-Us

responsável por garantir que esses serviços sejam justos, seguros e transparentes para os consumidores), o órgão regulador dos serviços pagos por telefone no Reino Unido, para garantir a proteção dos consumidores contra fraudes e abusos nesse setor.

A Ofcom também possui um papel importante na conscientização do público sobre fraudes e golpes no setor de telecomunicações do Reino Unido. Algumas das principais ações e iniciativas que a Ofcom realiza para informar e proteger os consumidores incluem:

- Publicação de guias e recursos informativos: A Ofcom disponibiliza em seu site uma série de guias e recursos educativos sobre diversos tipos de fraudes e golpes, incluindo chamadas indesejadas, chamadas falsificadas (*spoofing*) e golpes por SMS. Esses materiais ajudam os consumidores a identificar e evitar fraudes e golpes comuns.
- Campanhas de conscientização: A Ofcom realiza campanhas de conscientização em conjunto com outras agências e organizações, como a ICO *(Information Commissioner´s Office)* e a TPS (*Telephone Preference Service*), para educar o público sobre como evitar chamadas indesejadas e denunciar casos de abuso. Um exemplo é a campanha "Go Cold Call Free", que foi uma parceria com a ICO e outros parceiros do setor, como a TPS e a FCA (*Financial Conduct Authority*). A campanha tem como objetivo aumentar a conscientização dos consumidores sobre como evitar chamadas indesejadas e denunciar casos de abuso.
- Divulgação de informações e alertas: A Ofcom divulga regularmente informações e alertas sobre as últimas tendências de fraudes e golpes no setor de telecomunicações, ajudando os consumidores a se manterem informados e protegidos contra novos tipos de ameaças.
- Redes sociais e mídia: A Ofcom utiliza suas plataformas de redes sociais e outros canais de mídia para compartilhar informações e dicas sobre como os consumidores podem se proteger contra fraudes e golpes no setor de telecomunicações.

Um ponto destacável para o projeto é a possibilidade da ANATEL em absorver as melhores práticas da Ofcom no âmbito de parcerias público / privada feitas entre a agência e as empresas no Reino Unido. Diferentemente da FCC, o poder da Ofcom contra o combate às fraudes se assemelha muito ao da ANATEL, isso gera a necessidade de as agências criarem parcerias estratégicas para o combate mais efetivo à fraude no setor de telecomunicações.

A ACMA (Australian Communications and Media Authority) – Austrália

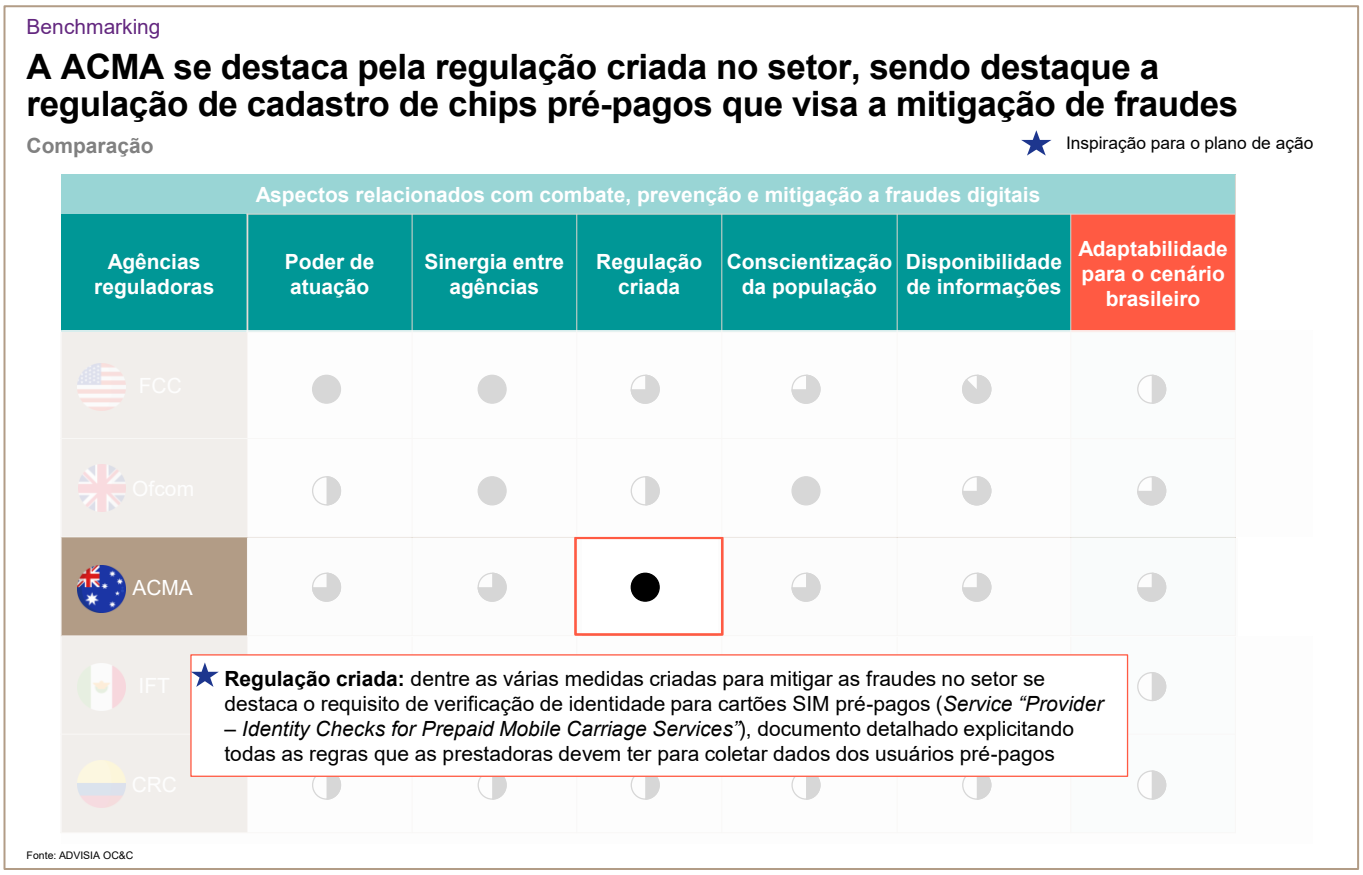


Figura 23

A *Australian Communications and Media Authority* (ACMA) implementou várias regulações e iniciativas para combater fraudes e golpes no setor. Algumas das principais regulações incluem:

- Verificação de identidade para serviços móveis pré-pagos ("Telecommunications Service Provider — Identity Checks for Prepaid Mobile Carriage Services[49] Determination 2017") que exige que os provedores de serviços de telefonia móvel realizem verificações de identidade antes de ativar os serviços pré-pagos. Essa medida ajuda a prevenir o uso de serviços móveis pré-pagos para atividades

[49] AUSTRALIA. ACMA. Identity Checks for Prepaid Mobile Carriage Services, 2017. Disponível em: https://www.legislation.gov.au/Details/F2017L00399

fraudulentas e criminosas. As informações necessárias para adquirir um chip pré-pago na Austrália incluem:

- Nome completo do cliente;
- Endereço residencial do cliente;
- Data de nascimento do cliente;

Além disso, é necessário fornecer um dos seguintes documentos de identificação:

- Opção 1: Documento primário
  - Passaporte australiano válido ou que tenha expirado há menos de dois anos;
  - Carteira de motorista ou permissão de aprendiz australiana;
  - Cartão de identificação emitido por um estado ou território australiano
- Opção 2: Documento primário estrangeiro
  - Passaporte estrangeiro válido;
  - Carteira de motorista estrangeira válida (deve incluir uma fotografia e ser emitida por um país reconhecido pela Austrália).
- Opção 3: Documento secundário mais um documento complementar
  - Documento secundário: Cartão de identificação de estudante, cartão de crédito ou débito, cartão de saúde do Medicare, cartão de seguro de saúde privado etc.
  - Documento complementar: Conta de serviços públicos, conta bancária, documento de propriedade ou aluguel, declaração de imposto de renda etc.

Vale lembrar que é de responsabilidade das prestadoras de telecomunicações de verificar / validar os documentos solicitados e manter todos os dados

armazenados por no mínimo 2 anos de forma acessível apenas para as autoridades e pessoas autorizadas

- Regulação do telemarketing e chamadas indesejadas: A ACMA administra o Registro de Não Perturbe (Do Not Call Register[50]) na Austrália, que permite aos consumidores optar por não receberem chamadas de telemarketing e outros tipos de comunicações não solicitadas. A ACMA também é responsável por supervisionar e aplicar as disposições da Lei de Telecomunicações de 1997 (Telecommunications Act 1997) e do Código de Práticas do Setor de 2017 (Industry Standard 2017) relacionadas a chamadas indesejadas.
- Combate ao spam: A ACMA supervisiona a aplicação da Lei de Spam [51]de 2003 (Spam Act 2003), que estabelece regras e restrições para o envio de mensagens eletrônicas comerciais não solicitadas, como e-mails e mensagens de texto.
- Proteção ao consumidor e combate a fraudes em serviços de tarifação premium: A ACMA administra o Código de Práticas dos Serviços Móveis Premium [52](Mobile Premium Services Code), que estabelece regras e requisitos para a prestação de serviços móveis *premium*, como números de telefone de tarifação adicional e serviços de mensagens de texto *premium*. Essas regras incluem a exigência de informações claras e transparentes sobre preços e termos de serviço, além de mecanismos de cancelamento fáceis de usar para proteger os consumidores contra fraudes e cobranças indevidas.

[50] AUSTRALIA. ACMA. Do Not Call Register. Disponível em: https://www.acma.gov.au/say-no-to-telemarketers

[51] AUSTRALIA. ACMA. Do Not Call Register. Disponível em: https://www.acma.gov.au/avoid-sending-spam

[52] AUSTRALIA. ACMA. Do Not Call Register. Disponível em: https://www.acma.gov.au/rules-mobile-premium-services

O IFT (Instituto Federal de Telecomunicaciones) - México

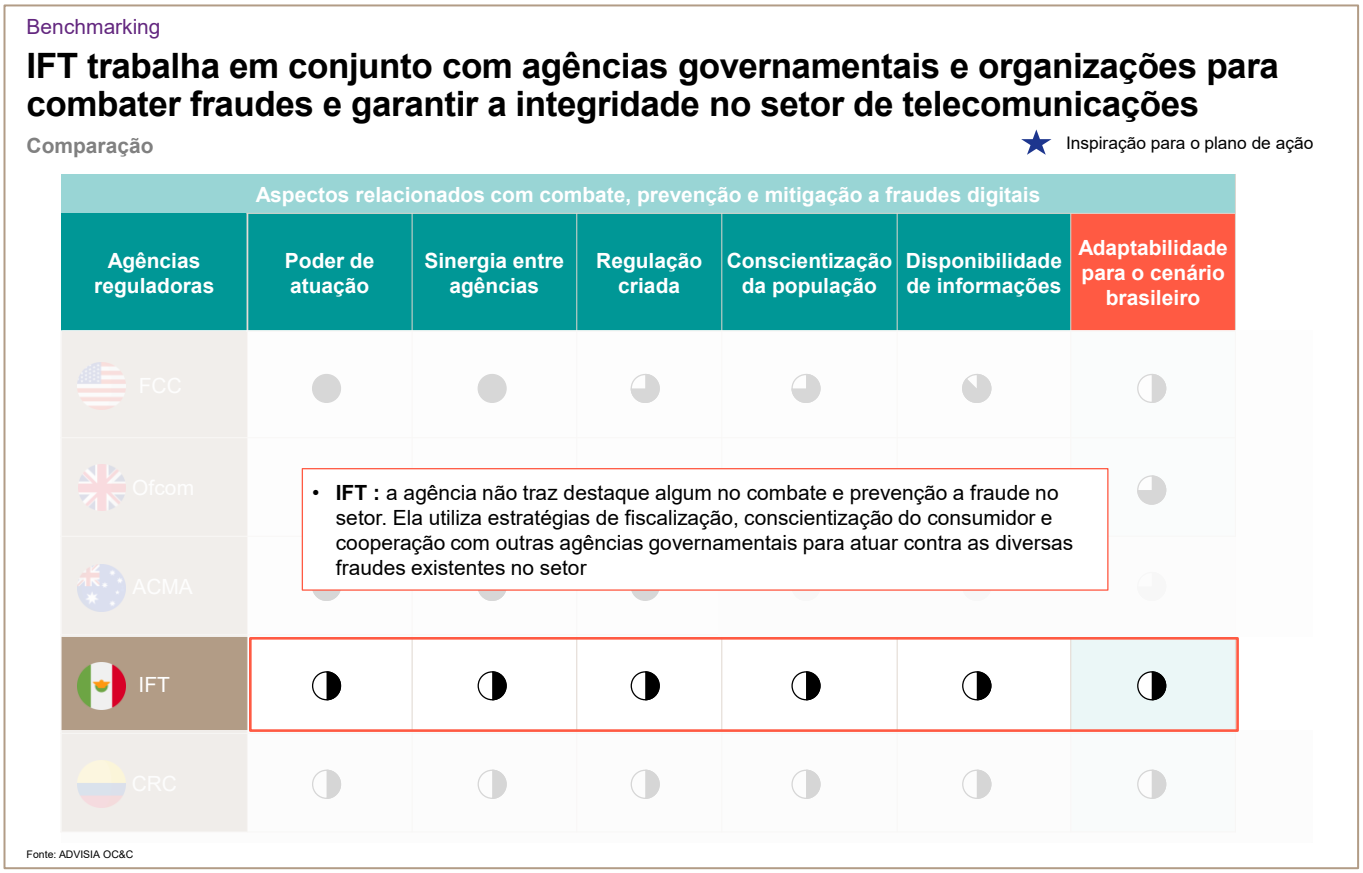


Figura 24

O Instituto Federal de Telecomunicaciones (IFT) no que diz respeito ao combate, prevenção e mitigação de fraudes na indústria de telecomunicações adota medidas, como:

- Regulamentação e fiscalização[53]: O IFT estabelece regulamentações e diretrizes que os provedores de serviços de telecomunicações devem seguir para garantir a prestação de serviços de qualidade e proteger os usuários. A agência também é responsável por fiscalizar e garantir a conformidade com essas regulamentações. Mesmo não havendo nenhuma regulação específica de fraude existem regulações correlatas que focam na proteção dos usuários.

[53] MÉXICO. IFT. Disponível em: https://www.ift.org.mx/industria/homologacion-evaluacion-conformidad

- Combate ao uso de equipamentos não homologados[27]: O IFT trabalha para combater o uso de equipamentos de telecomunicações não homologados, que podem facilitar atividades fraudulentas ou prejudicar a qualidade dos serviços. Isso inclui a supervisão do processo de homologação de equipamentos e ações de fiscalização para coibir o uso de dispositivos não autorizados.
- Proteção ao consumidor e educação: O IFT tem como objetivo garantir que os consumidores estejam informados sobre seus direitos e responsabilidades no setor de telecomunicações. A agência promove campanhas de conscientização e educação para ajudar os consumidores a se protegerem de fraudes e golpes. Além disso, o IFT oferece um canal para que os consumidores denunciem problemas e apresentem reclamações.

A CRC (Comisión de Regulación de Comunicaciones) - Colômbia

Benchmarking

A agência colombiana utiliza estratégias semelhantes à IFT no combate à fraude, como por exemplo a fiscalização e conscientização da população

Comparação

★ Inspiração para o plano de ação

Agências reguladoras	Aspectos relacionados com combate, prevenção e mitigação a fraudes digitais: Poder de atuação	Sinergia entre agências	Regulação criada	Conscientização da população	Disponibilidade de informações	Adaptabilidade para o cenário brasileiro
FCC	●	●	◕	◕	◕	◑
Ofcom	◑	●	◑	●	◕	◕
ACMA	◑	◑	◑	◑	◑	◑
IFT	◑	◑	◑	◑	◑	◑
CRC	◑	◑	◑	◑	◑	◑

- **CRC:** com o mesmo escopo de atuação que a IFT, a agência da Colômbia utiliza estratégias de combate e prevenção a fraudes semelhantes (fiscalização, conscientização e cooperação com agências governamentais)

Fonte: ADVISIA OC&C

Figura 25

A CRC (*Comisión de Regulación de Comunicaciones*) trabalha em conjunto com outras agências governamentais, como a *Autoridad Nacional de Televisión* (ANTV) e *o Ministerio de Tecnologías de la Información y las Comunicaciones* (MinTIC), para garantir a qualidade dos serviços e proteger os consumidores de fraudes e golpes no setor. Algumas das principais iniciativas e abordagens adotadas pela CRC para combater, prevenir e mitigar fraudes na indústria de telecomunicações incluem:

- Regulamentação e fiscalização: A CRC estabelece regulamentações e diretrizes para provedores de serviços de telecomunicações na Colômbia, abordando questões como qualidade do serviço, tarifas, direitos do consumidor e segurança. A agência monitora o cumprimento dessas regulamentações e pode impor sanções aos provedores que não as cumpram.

- Proteção ao consumidor e educação[54]: A CRC trabalha para garantir que os consumidores estejam informados sobre seus direitos e responsabilidades no setor de telecomunicações. A agência promove campanhas de conscientização e educação para ajudar os consumidores a se protegerem de fraudes e golpes. Além disso, a CRC oferece canais para que os consumidores denunciem problemas e apresentem reclamações.
- Combate ao uso de equipamentos não homologados: A CRC, em conjunto com outras agências governamentais, trabalha para combater o uso de equipamentos de telecomunicações não homologados, que podem facilitar atividades fraudulentas ou prejudicar a qualidade dos serviços. Isso inclui a supervisão do processo de homologação de equipamentos e ações de fiscalização para coibir o uso de dispositivos não autorizados.
- Resolução de disputas e aplicação de sanções: A CRC intervém em disputas entre consumidores e provedores de serviços de telecomunicações. A agência também pode impor sanções aos provedores que não cumpram as regulamentações ou se envolvam em atividades fraudulentas.

[54] COLÔMBIA. CRC. Presentations. Disponível em: https://www.slideshare.net/ComisindeRegulacinde/presentations

2. Percepções de mercado

No contexto nacional, é importante destacar quem são os principais atores brasileiros responsáveis por ações de combate, prevenção e mitigação a fraudes, mostrando um *overview* do *workshop* e da tomada de subsídios realizados durante a execução deste projeto, como descrito na introdução deste documento. Por fim, é importante avaliar as percepções do mercado, bem como o papel da ANATEL em relação ao tema. A figura abaixo resume os principais pontos que foram analisados neste capítulo:

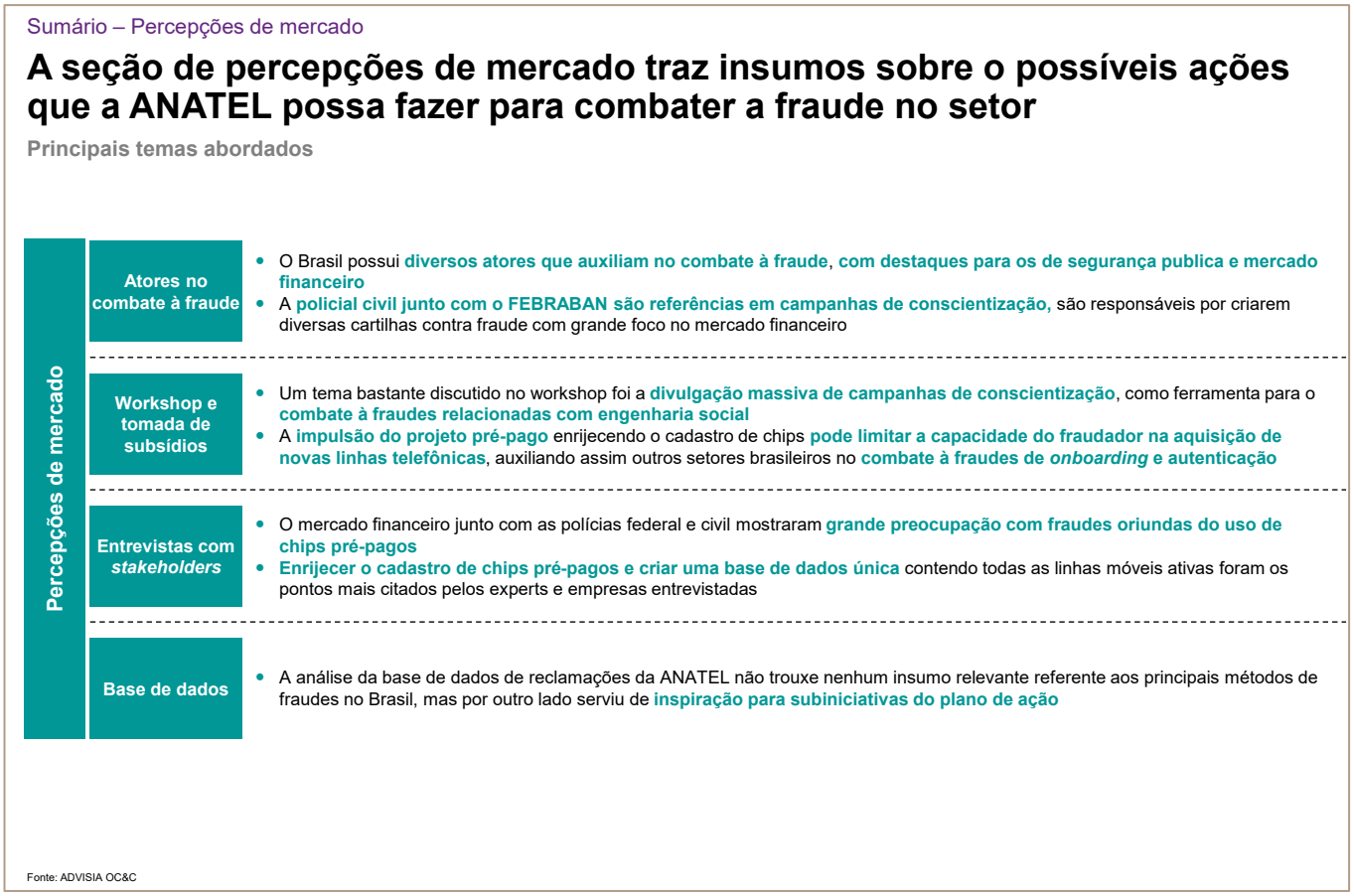


Figura 26

A ANATEL conta com grupos técnicos que auxiliam no combate às fraudes no setor de telecomunicações, são eles: Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) e o subgrupo técnico SGT Fraudes.

O Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) é um grupo de trabalho criado pela ANATEL em 2021 com o objetivo fazer o acompanhamento da Política de Segurança Cibernética e Gestão de Infraestrutura Crítica; à configuração de equipamentos, requisitos técnicos e fornecedores; ao compartilhamento de informações e boas práticas, bem como à conscientização, capacitação, estudos e interação com as Comissões Brasileiras de Comunicações (CBCs). Além disso, o grupo é responsável por fomentar a cooperação entre as empresas de telecomunicações e as agências reguladoras.

Já o SGT Fraudes é um subgrupo técnico do Grupo Técnico de Suporte à Segurança Pública (GT-Seg), que tem como coordenar ações de combate e prevenção a fraudes relacionadas à prestação de serviços de telecomunicações. O subgrupo é coordenado pela ANATEL, com a participação das prestadoras, autoridades policiais e outros atores afetos ao combate à fraude.

Uma das iniciativas de prevenção à fraude e de conscientização dos usuários sobre riscos e dicas de segurança digital foi a criação do Movimento #FiqueEsperto, que nasce a partir de uma demanda da Agência às prestadoras de serviço de telecomunicações no âmbito de uma Fiscalização Regulatória e ultrapassa o setor de telecomunicações agregando outros parceiros que assinam coletivamente a iniciativa. O #FiqueEsperto promove a segurança e conscientização dos consumidores, funcionando como um canal de informação e alerta sobre golpes, fraudes, e outras práticas maliciosas que podem afetar os consumidores.

Através da plataforma #FiqueEsperto os usuários podem encontrar informações sobre como se proteger de ameaças cibernéticas, além de ter acesso a dicas de segurança e sugestões para o uso responsável dos serviços de telecomunicações.

A figura abaixo ilustra as principais áreas / grupos da ANATEL que possuem alguma correlação com o tema de fraudes:

Contextualização

A ANATEL conta com grupos técnicos voltados para segurança cibernética e pública, tendo objetivos em comum em torno do combate às fraudes

Anatel

Time técnico ANATEL	Escopo de atuação
GEAFT	• Grupo Executivo Antifraude de Telecomunicações (GEAFT), do qual participam, além da Agência, representantes das prestadoras de serviços de telecomunicações. Cabe ao Grupo propor ações a serem tomadas em conjunto no sentido de prevenir, diminuir ou extinguir a prática de fraudes contra a prestação dos serviços de telecomunicações.
GT-Ciber	• Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) que atua na área de segurança cibernética no setor de telecomunicações. O grupo é composto por especialistas em segurança cibernética da própria Anatel e de outras entidades governamentais e privadas. Atualmente possui 4 subgrupos de estudos - SGT PSC e Gestão de Riscos de IEC: subgrupo técnico de política de segurança cibernética e gestão de riscos de infraestruturas críticas - SGT Temas internacionais: subgrupo técnico de temas internacionais - SGT Equipamentos: subgrupo técnico de equipamentos, fornecedores e requisitos - SGT Compartilhamento: subgrupo técnico de compartilhamento de informações e boas práticas
SGT Fraudes	• O SGT Fraudes ou é um subgrupo técnico do Grupo Técnico de Suporte à Segurança Pública (GT-Seg) . Esse subgrupo é responsável por coordenar ações de combate e prevenção a fraudes relacionadas à prestação de serviços de telecomunicações.

Figura 27

2.1. Atores no combate à fraude

O combate, prevenção e mitigação de fraudes no Brasil são tarefas complexas e desafiadoras, devido à diversidade e à dimensão do país, bem como às constantes evoluções tecnológicas e aos diferentes tipos de fraudes existentes. Para enfrentar esse cenário, diversos atores brasileiros desempenham papéis fundamentais na luta contra a fraude, trabalhando de forma colaborativa e eficiente. Dentre os principais atores envolvidos nessa batalha, destacam-se:

Figura 28

A segurança pública é um elemento fundamental no combate às fraudes, uma vez que atua na proteção dos cidadãos e na manutenção da ordem pública. O Ministério da Justiça e Segurança Pública, a Polícia Federal e a Polícia Civil (com destaque para a Polícia Civil do estado de São Paulo) desempenham papéis essenciais nesse contexto, trabalhando em

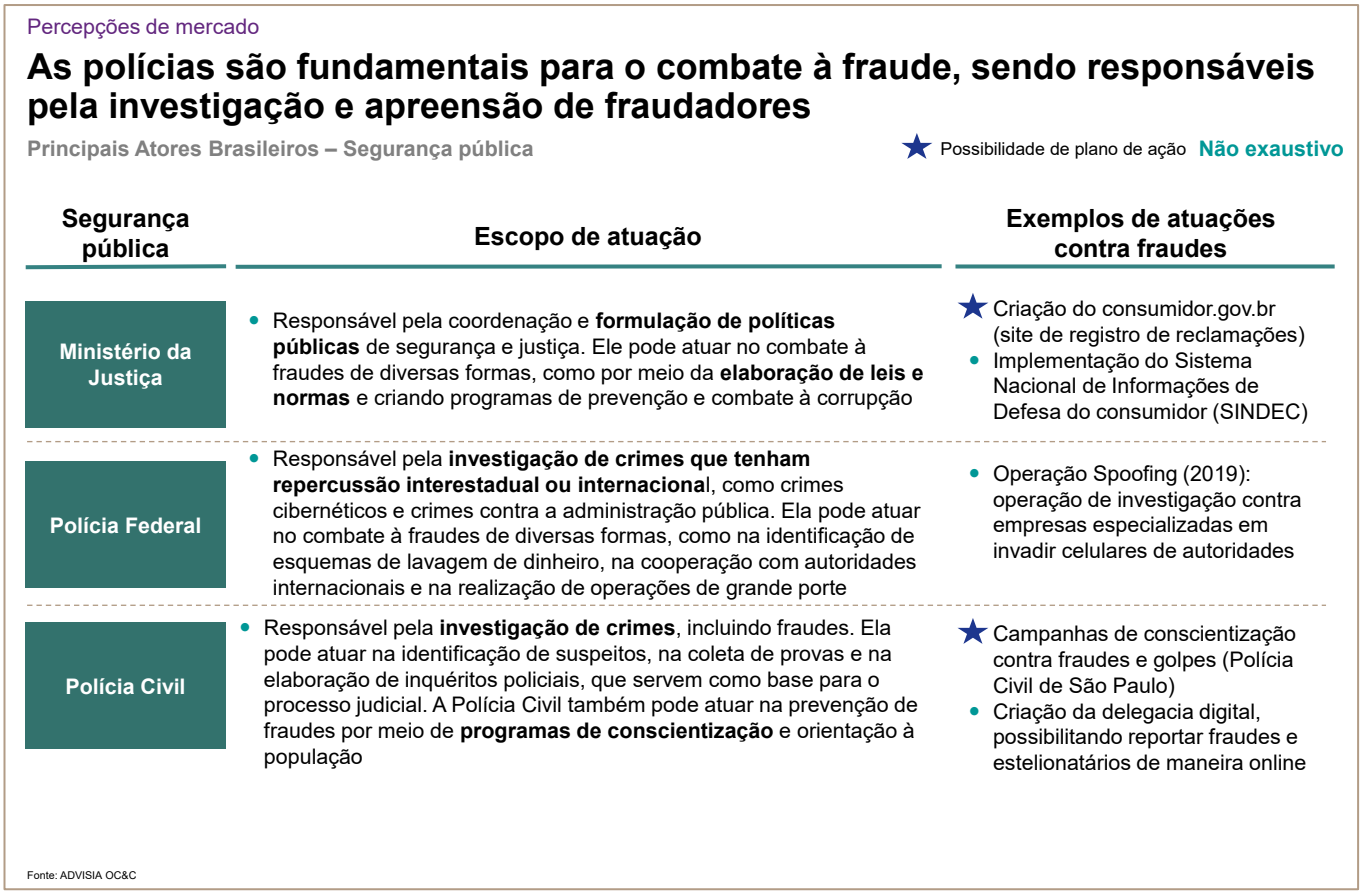
conjunto e em parceria com outras instituições para prevenir, investigar e punir os responsáveis por atividades fraudulentas.

A exemplo, a Polícia Civil de São Paulo, através de sua Divisão de Crimes Cibernéticos (DCCIBER), [55]tem trabalhado incessantemente para combater e prevenir as fraudes digitais no estado. Esse órgão é responsável por investigar casos que envolvam fraudes contra instituições financeiras e no comércio eletrônico. Ela também possui um centro de inteligência cibernética e um laboratório técnico. A Polícia Civil de São Paulo se destaca por suas campanhas de conscientização e por sua delegacia eletrônica.[56]

A imagem abaixo ilustra, de forma resumida, o escopo de ação dos atores de segurança pública.

[55] BRASIL. Polícia Civil SP. Delegacia de crimes cibernéticos. Disponível em: https://www.policiacivil.sp.gov.br/portal/faces/pages_home/institucional/departamentosOrgaos/departamentosOrgaosDetalhes?titulo=DEIC&collectionId=980175918762000603&_afrLoop=1096736352513178&_afrWindowMode=0&_afrWindowId=null#!%40%40%3F_afrWindowId%3Dnull%26collectionId%3D980175918762000603%26_afrLoop%3D1096736352513178%26titulo%3DDEIC%26_afrWindowMode%3D0%26_adf.ctrl-state%3Dnad7gddah_4

[56] BRASIL. Polícia Civil SP. Delegacia Virtual. Disponível em: https://www.ssp.sp.gov.br/acoes/leAcoes.aspx?id=33364.



57

Figura 29

O Conselho de Controle de Atividades Financeiras (COAF) e o Instituto Nacional de Tecnologia da Informação (ITI) são órgãos governamentais brasileiros que desempenham

---

[57] BRASIL. Ministério da Justiça e Segurança Pública. Portais referentes a defesa do consumidor. Disponível em: consumidor.gov.br; sindecnacional.mj.gov.br/

[57]BRASIL. Polícia Federal. Unidade de combate a crimes cibernéticos. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos

[57]BRASIL. Polícia Civil. Campanhas de conscientização. Disponível em: https://www.policiacivil.sp.gov.br/portal/imagens/CRIMES%20CIBERN%C3%89TICOS%20-%20PERGUNTAS%20E%20RESPOSTAS%20V2.pdf

papéis importantes na promoção da segurança no país. Apesar de terem objetivos e responsabilidades distintos, ambos trabalham no sentido de prevenir e combater atividades ilícitas, contribuindo para um ambiente mais seguro e confiável no Brasil.

O COAF [58]é responsável pela prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e a outras atividades financeiras ilícitas. Para isso, o órgão realiza o monitoramento e a análise de operações financeiras suspeitas, regula e fiscaliza setores obrigados, promove a cooperação nacional e internacional, capacitando e educando os envolvidos na identificação e no reporte de operações suspeitas, bem como aplicando sanções administrativas quando necessário (Ministério da Economia, 2021).

Por outro lado, o ITI [59] tem como principal objetivo a implementação e a promoção do uso da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), um sistema que garante a autenticidade, integridade e confidencialidade das informações eletrônicas. O ITI atua na certificação digital, assegurando a segurança das transações e dos serviços eletrônicos, o que pode incluir a prevenção e detecção de fraudes eletrônicas e cibernéticas (Instituto Nacional de Tecnologia da Informação, 2021).

[58] COAF. Conselho de Controle de Atividades Financeiras. Disponível em: https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-atividade-de-supervisao

[59] Instituto Nacional de Tecnologia da Informação. Sobre o ITI, 2021 Disponível em: https://www.iti.gov.br/institucional/sobre-o-iti

Percepções de mercado

Tanto o ITI como o COAF atuam de forma indireta no combate e prevenção a fraude no Brasil

Principais Atores Brasileiros – Outros administração pública

Não exaustivo

Outros adm. pública	Escopo de atuação	Exemplos de atuações contra fraudes
Instituto Nacional de Tecnologia da Informação (ITI)	• O ITI é responsável por desenvolver e implementar **políticas e padrões de segurança para o uso da tecnologia da informação no país**, incluindo medidas para prevenção e detecção de fraudes digitais	• Emissão de certificados digitais no Brasil, garantindo a autenticidade e integridade das informações
Conselho de Controle de Atividades Financeiras (COAF)	• COAF monitora e **analisa as transações financeiras suspeitas**, relatando às autoridades competentes para investigação. É o órgão brasileiro responsável pela prevenção e combate à lavagem de dinheiro, financiamento do terrorismo e outras atividades ilícitas relacionadas.	• O COAF analisa relatórios de operações suspeitas enviados por instituições financeiras e outros setores obrigados a reportar transações atípicas. Isso permite identificar atividades fraudulentas e iniciar investigações apropriadas.

Fonte: ADVISIA OC&C

Figura 30

No setor financeiro, a prevenção e o combate à fraude desempenham um papel crucial na proteção dos interesses dos consumidores, na manutenção da integridade das instituições financeiras e na estabilidade do sistema financeiro como um todo. No Brasil, dois atores-chave na luta contra a fraude são o Banco Central do Brasil (BACEN) e a Federação Brasileira de Bancos (FEBRABAN). Essas entidades trabalham em conjunto com o objetivo de estabelecer diretrizes, normas e políticas para garantir a segurança das transações financeiras e prevenir atividades ilícitas.

O BACEN, como órgão regulador e supervisor do sistema financeiro nacional, é responsável por estabelecer as regras e os padrões de conduta a serem seguidos pelas instituições financeiras. Além disso, o BACEN monitora constantemente o mercado, assegurando que os bancos estejam cumprindo a legislação vigente e adotando práticas adequadas de gerenciamento de riscos.

A FEBRABAN, por sua vez, é uma entidade representativa dos bancos brasileiros e tem como missão promover o desenvolvimento sustentável do setor bancário. Entre suas atribuições, a FEBRABAN atua na elaboração de diretrizes e na disseminação de melhores práticas para prevenir e combater fraudes financeiras[60], além de possuir um laboratório de segurança cibernética [61]criado em 2020.

Juntos, o BACEN e a FEBRABAN são fundamentais para garantir um ambiente financeiro seguro, transparente e eficiente, contribuindo para a confiança dos consumidores, a competitividade do setor e o crescimento econômico sustentável no Brasil. A figura abaixo ilustra um pouco mais o escopo de atuação dessas duas entidades.

[60] FEBRABAN. Campanhas de conscientização contra fraudes. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/bancos-promovem-campanha-de-conscientizacao-digital-contra-fraudes

[61] FEBRABAN. Laboratório de Segurança Cibernética. Disponível em: https://portal.febraban.org.br/pagina/3322/1108/pt-br/lab-seguranca-cibernetica

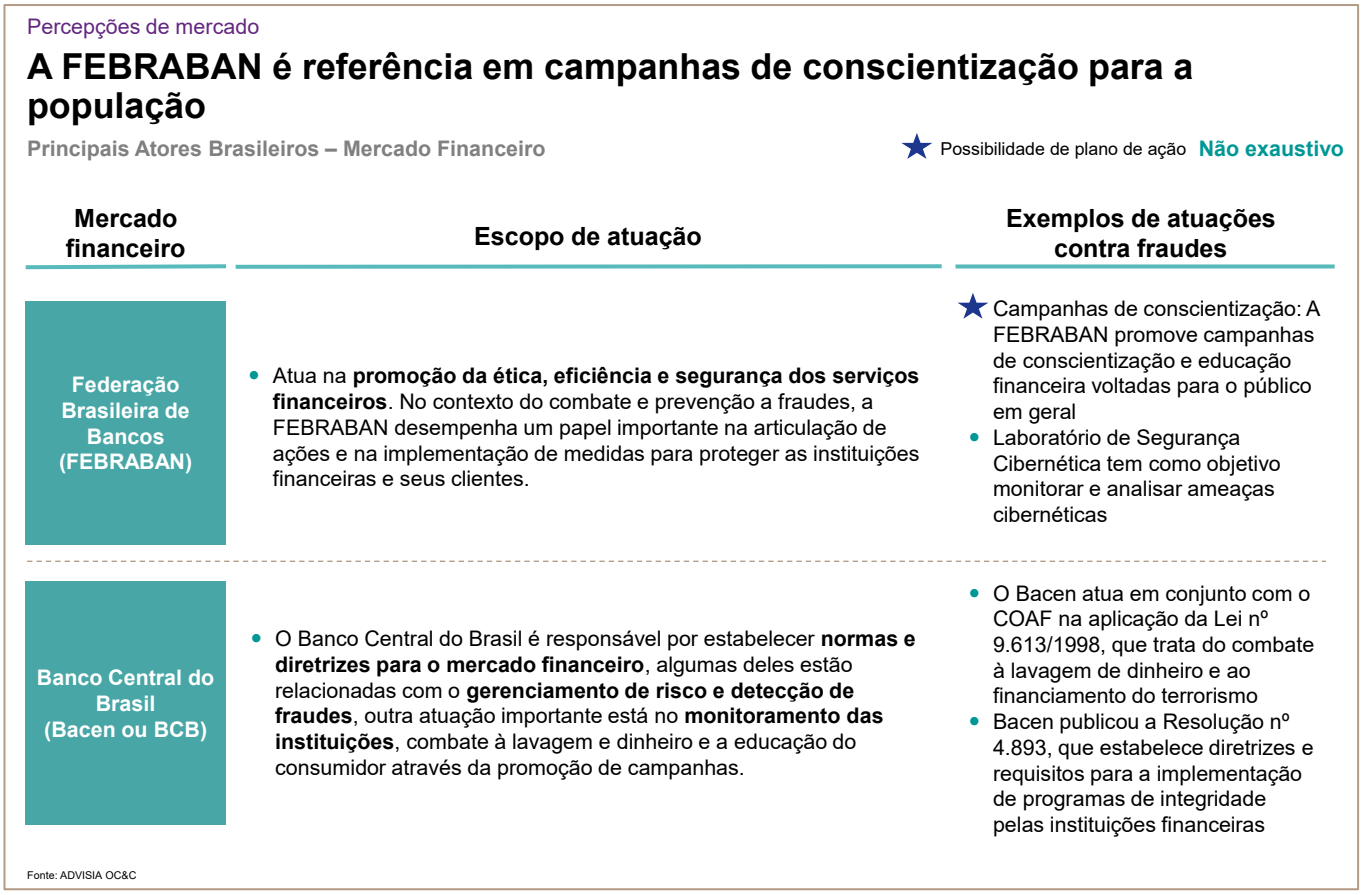


Figura 31

O Programa de Proteção e Defesa do Consumidor (PROCON) e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) são instituições de "suporte" que desempenham um papel fundamental na promoção da segurança digital, na conscientização dos consumidores e na resposta a incidentes de fraude no país.

O PROCON, como órgão de proteção aos direitos do consumidor, tem como objetivo principal garantir que os consumidores sejam tratados de forma justa e transparente pelas empresas. A instituição atua na prevenção e combate às fraudes ao fiscalizar as práticas comerciais e ao receber e analisar denúncias de violações aos direitos do consumidor. Além disso, o PROCON promove a educação e conscientização dos consumidores por meio de

campanhas [62]e programas informativos, ajudando-os a identificar e evitar potenciais golpes e fraudes.

O CERT.br é responsável por coordenar a resposta a incidentes [63] de segurança na internet brasileira (domínios ".br"). Este centro atua na prevenção e combate à fraude ao monitorar, analisar e divulgar informações sobre ameaças e vulnerabilidades, bem como ao propor medidas e soluções para mitigar os riscos. O CERT.br também colabora com outras organizações nacionais e internacionais, compartilhando conhecimento e experiências para aprimorar a resposta a incidentes e promover a segurança cibernética.

A atuação do PROCON e do CERT.br são fundamentais para criar um ambiente seguro para os consumidores e empresas brasileiras, contribuindo para a confiança nas transações online e para a redução dos prejuízos causados pelas fraudes. A figura abaixo exemplifica algumas de suas atuações:

[62] PROCON. Campanhas de conscientização. Disponível em: https://www.almg.gov.br/comunicacao/noticias/arquivos/Procon-lanca-a-campanha-desligueotelefone/

[63] CERT.br. Atuação. Disponível em: https://cert.br/sobre/

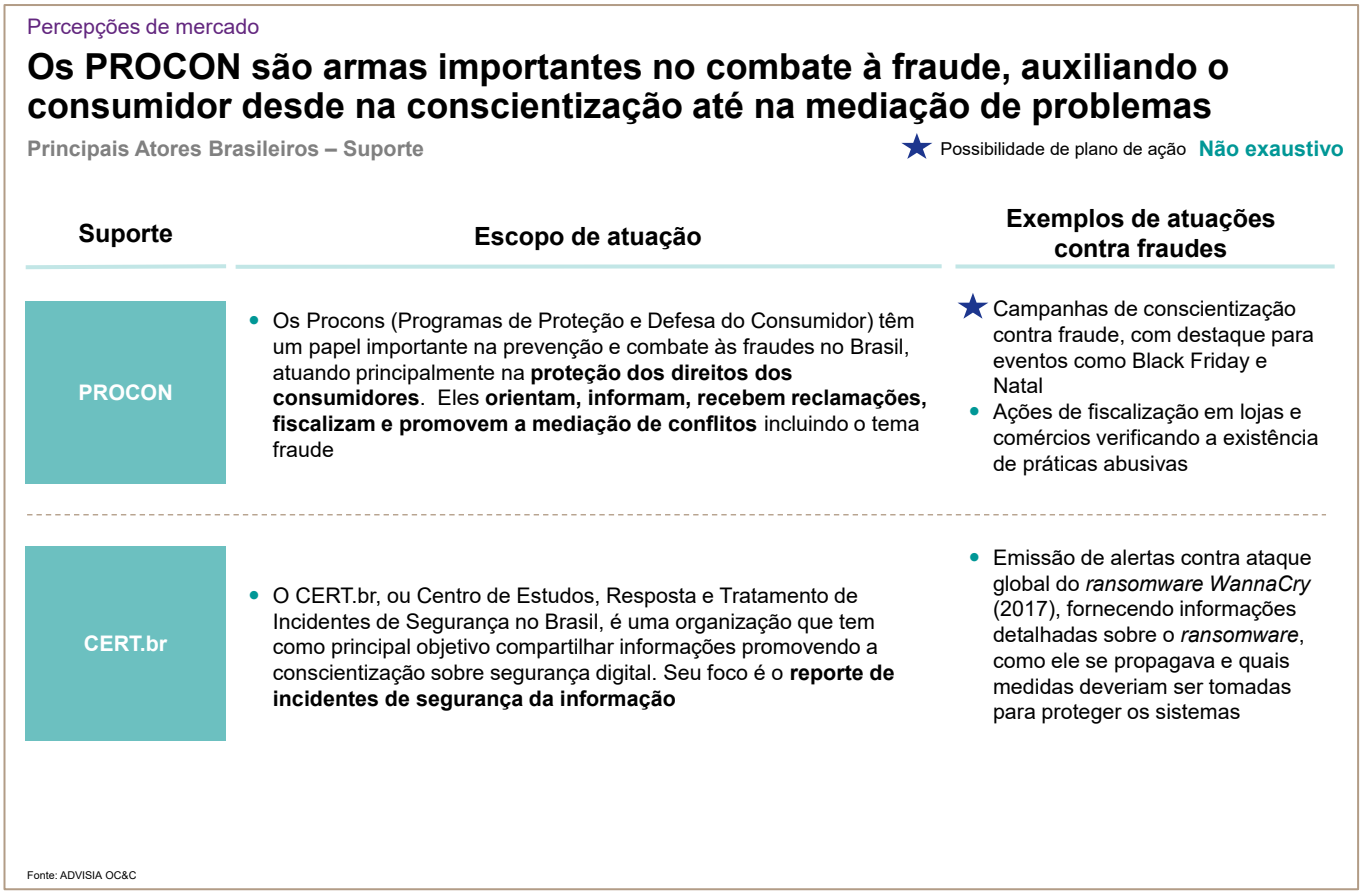


Figura 32

A importância do meio acadêmico no estudo sobre combate e prevenção à fraude no Brasil é inegável. Universidades, centros de pesquisa e instituições de ensino superior desempenham um papel fundamental na produção e disseminação do conhecimento sobre fraudes, contribuindo para o desenvolvimento de estratégias eficazes e inovadoras para enfrentar esse desafio. Ao promover a pesquisa e a formação de profissionais qualificados, o meio acadêmico auxilia na construção de um ambiente mais seguro e resiliente contra ações fraudulentas no país.

O estudo acadêmico da temática de fraude abrange diversas áreas do conhecimento, como ciências sociais, direito, economia, administração, tecnologia da informação e ciência de dados. Pesquisadores e acadêmicos investigam as causas, características, consequências e tendências das fraudes, identificando padrões de comportamento e desenvolvendo modelos preditivos que ajudam na prevenção e detecção de atividades ilícitas.

Além disso, o meio acadêmico promove a formação de profissionais com habilidades e competências necessárias para atuar no combate e prevenção à fraude. Por meio de cursos de graduação, pós-graduação e programas de capacitação, as instituições de ensino preparam os estudantes para enfrentar os desafios do mercado de trabalho e contribuir para a criação de soluções inovadoras na área.

A cooperação entre o meio acadêmico e outros setores, como o público, o privado e organizações não governamentais, é crucial para o sucesso na luta contra a fraude. Através dessa colaboração, é possível compartilhar informações, recursos e conhecimentos, bem como criar sinergias para enfrentar os desafios impostos pela evolução das práticas fraudulentas.

Em suma, o meio acadêmico desempenha um papel crucial na luta contra a fraude no Brasil, contribuindo para o avanço do conhecimento, o desenvolvimento de soluções inovadoras e a formação de profissionais capacitados para lidar com esse fenômeno complexo e em constante transformação.

A figura abaixo ilustra algumas faculdades do Brasil com laboratórios e centros de pesquisa que possuem alguma relação com fraudes digitais.

Percepções de mercado

As universidades brasileiras possuem laboratórios e especializações voltadas para o estudo de segurança cibernética e de informação

Principais Atores Brasileiros – Meio acadêmico

Não exaustivo

Meio acadêmico	Escopo de atuação
Universidade de São Paulo (USP)	• A USP possui o LARC (Laboratório de Arquitetura e Redes de Computadores), responsável por realiza **pesquisas em diversas áreas da Ciência da Computação, incluindo segurança de redes, privacidade e proteção de dados**.
Universidade Estadual de Campinas (UNICAMP)	• A UNICAMP possui o O Laboratório de Segurança e Criptografia (LASCA). O LASCA faz parte do Instituto de Computação (IC) da Unicamp e é dedicado ao estudo e **desenvolvimento de tecnologias de segurança da informação e criptografia**.
Universidade Federal de Minas Gerais (UFMG)	• A UFMG possui o Centro de Pesquisa e Desenvolvimento em Engenharia Elétrica (CPDEE) que abriga grupos de pesquisa que trabalham em áreas relacionadas à **segurança cibernética, como segurança de redes, sistemas distribuídos e computação em nuvem.**

Fonte: ADVISIA OC&C

64

Figura 33

A crescente complexidade e sofisticação das fraudes no Brasil têm exigido uma abordagem colaborativa e inovadora para prevenir e combater esse fenômeno. Nesse contexto, empresas e entidades da sociedade civil desempenham um papel fundamental na luta contra a fraude, desenvolvendo tecnologias, soluções e serviços que auxiliam na detecção e prevenção de atividades ilícitas. Exemplos notáveis de organizações atuantes neste campo incluem IRIS, Movimento código Brasil e muitas outras.

A IRIS (Instituto de Referência em Internet e Sociedade) é uma organização sem fins lucrativos que busca promover o debate sobre questões relacionadas à internet e à sociedade,

[64] USP. LARC. Disponível em: https://cursos.larc.usp.br/sobre-o-larc/
UNICAMP. LASCA. Disponível em: https://ic.unicamp.br/pesquisa/projetos-e-laboratorios-de-pesquisa/
UFMG. CPDEE. Disponível em: https://delt.eng.ufmg.br/historia/

incluindo a segurança digital e o combate à fraude. Através de pesquisas[65], publicações[66] e eventos, a IRIS contribui para a construção de políticas públicas e estratégias de prevenção à fraude no ambiente digital.

Movimento Código Brasil: O Movimento Código Brasil é uma iniciativa que busca fomentar o desenvolvimento de competências digitais e estimular a criação de soluções tecnológicas voltadas para a segurança digital, a inclusão e a cidadania. Ao apoiar o desenvolvimento de projetos e a formação de profissionais na área de tecnologia da informação, o Movimento Código Brasil contribui para a criação de novas ferramentas e estratégias no combate e prevenção à fraude.

A atuação dessas organizações e empresas no combate e prevenção à fraude no Brasil é essencial, pois elas complementam os esforços das autoridades e dos órgãos reguladores, trazendo inovação e novas perspectivas para enfrentar esse desafio. A cooperação entre os diversos setores da sociedade é fundamental para criar um ambiente mais seguro e resiliente contra ações fraudulentas, promovendo a confiança nas transações e o desenvolvimento econômico sustentável no país. As figuras abaixo resumem o escopo de atuação dessas empresas:

---

[65] IRIS. Projeto de rastreabilidade de mensagens privadas. Disponível em: https://irisbh.com.br/projetos/comunicacoes-privadas-investigacoes-e-direitos/

[66] IRIS. Publicações relacionadas com o tema fraude. Disponível em: https://irisbh.com.br/?s=fraude

IRIS. Publicações diversas. Disponível em: https://irisbh.com.br/publicacoes/

IRIS. Contribuições sobre incidentes de segurança. Disponível em: https://irisbh.com.br/publicacoes/tomada-de-subsidios-2-2021-da-autoridade-nacional-de-protecao-de-dados-contribuicoes-do-iris-sobre-incidentes-de-seguranca/

Percepções de mercado

Existem vários institutos, centros de pesquisas e organizações sem fins lucrativos que visam a promoção da segurança digital no Brasil

Principais Atores Brasileiros – Entidades sociedade civil — **Não exaustivo**

Entidades sociedade civil	Escopo de atuação
Movimento Código Brasil	• É uma iniciativa que tem como **objetivo promover o ensino de programação e tecnologia** para crianças e jovens, visando formar uma geração mais consciente e crítica em relação aos riscos e ameaças na internet
Instituto de Referência em Internet e Sociedade (IRIS)	• Organização sem fins lucrativos que tem como objetivo estudar e **promover políticas públicas relacionadas à internet e à sociedade em geral**. Entre os principais temas de pesquisa da IRIS estão a privacidade na internet, a liberdade de expressão, a proteção de dados, a regulação da internet e a governança da mesma. A organização realiza pesquisa em parceria com outras instituições e organizações da sociedade civil, além de produzir publicações e relatórios sobre esses temas

Fonte: ADVISIA OC&C

67

Figura 34

[67] Movimento Código Brasil. Disponível em: https://brasilemcodigo.com.br/

IRIS. Disponível em: https://irisbh.com.br/

2.2. Workshop

A realização de workshops setoriais é uma prática importante para a obtenção de insumos relevantes sobre determinado tema. Esses eventos são focados na discussão e troca de experiências entre profissionais, especialistas e interessados em uma área específica, possibilitando a identificação de novas tendências, problemas e soluções.

Nesta seção, serão abordados os insumos coletados no Workshop I, realizado no 10/03 sobre as iniciativas estratégicas nº 17, 18 e 19 que contou com a presença de 212 participantes e com duração aproximada de 3 horas e 30 minutos

Figura 35

Para passar por todos os temas propostos, a ADVISIA iniciou o *Workshop* com 2 salas simultâneas onde os participantes puderam escolher qual tema eles queriam contribuir / participar (prevenção de fraudes no ecossistema digital ou alfabetização digital) e

posteriormente todos foram levados para uma sala única onde foi abordado o tema "Desenvolvimento de novas tecnologias". O foco desse estudo será apenas nas principais percepções coletadas sobre o tema de fraudes digitais. A figura abaixo traz um resumo desse tópico:

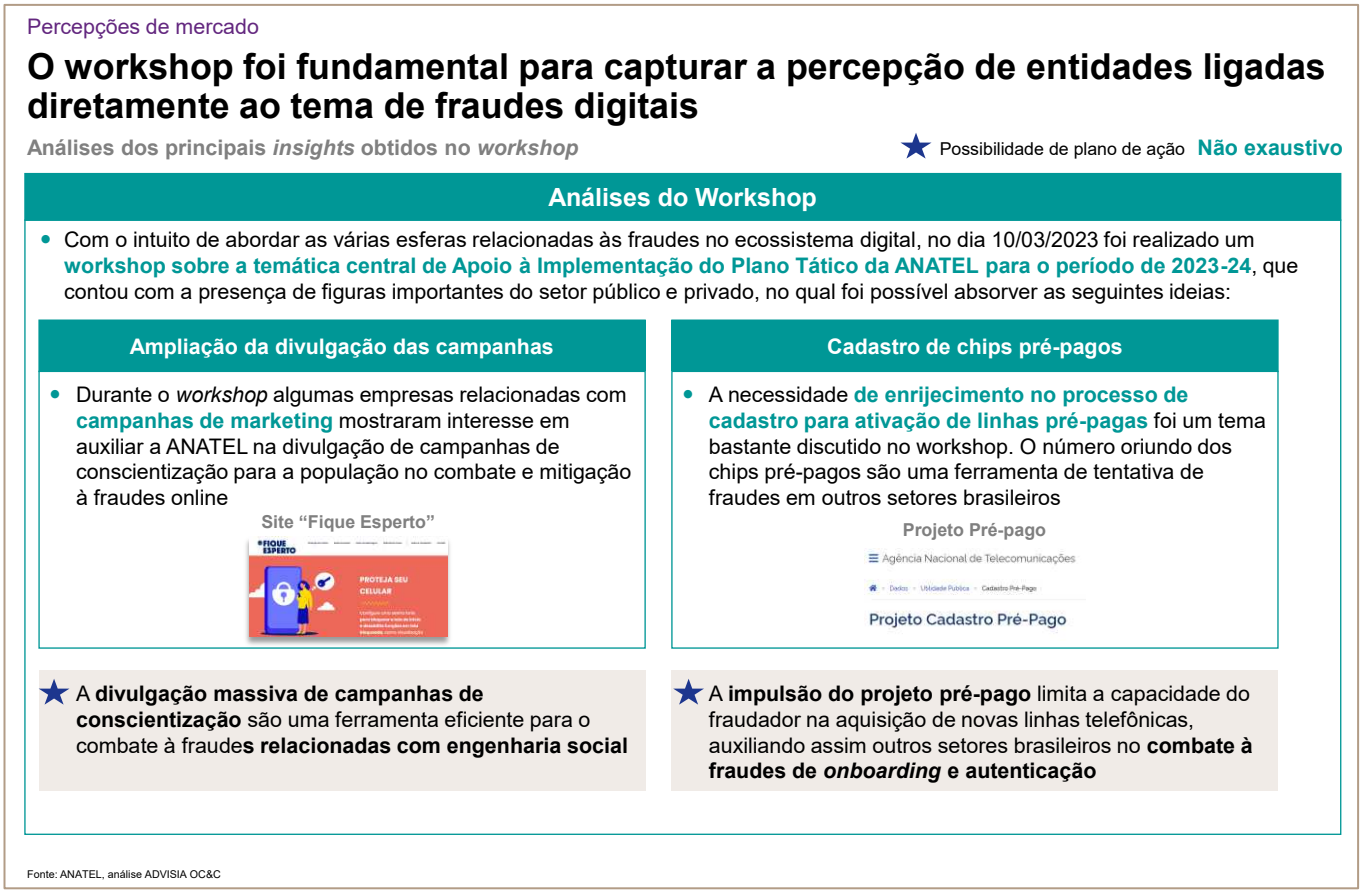


Figura 36

É importante destacar a diferença entre a percepção do que o mercado espera da ANATEL e as reais responsabilidades e deveres da Agência. Um ponto muito citado no workshop que também estará presente nas seções "Tomada de Subsídios" e "Percepções de mercado" é o tema de enrijecimento do cadastro pré-pago para a mitigação de fraudes envolvendo cadastros em outros setores da economia brasileira.

Para alguns atores, a ANATEL poderia promover o enrijecimento desse cadastro. No entanto, no entanto existem vários debates questionando se isso seria de interesse da sociedade. O aumento no número de dados coletados no ato do cadastro do chip pré-pago não é a única forma de se mitigar fraudes como as de cadastro e *onboarding* nos outros setores

brasileiros, existem outras soluções que podem ser exploradas pela Agência nos próximos anos para se buscar o resultado esperado sem causar grandes consequências para a sociedade brasileira (o enrijecimento do cadastro do pré-pago pode excluir o acesso de uma parcela da sociedade aos serviços de telecomunicações devido a inexistência de documentos de identificação e residência por exemplo. Vale ressaltar também que no *benchmarking* internacional realizado, apenas a agência da Austrália conseguiu criar meios bem sucedidos para a coleta de dados de cadastro para clientes do produto pré-pago.

2.3. Tomada de subsídios

A tomada de subsídios é um processo importante para as agências governamentais e o governo como um todo, pois permite coletar informações e opiniões relevantes para a formulação de políticas públicas e tomadas de decisões. Essa prática traz algumas implicações positivas como por exemplo:

- Transparência e participação cidadã: A tomada de subsídios incentiva a participação da sociedade civil no processo decisório, permitindo que as pessoas compartilhem suas opiniões e preocupações com os formuladores de políticas.
- Identificação de necessidades e prioridades: Ao coletar informações de várias fontes, o governo pode identificar com mais precisão as necessidades e prioridades da sociedade.
- Prevenção de conflitos e construção de consenso: A tomada de subsídios pode ajudar a prevenir conflitos e construir consenso entre os interessados, garantindo que as preocupações de todos sejam levadas em consideração e que as decisões tomadas sejam mais bem aceitas.

Em relação a fraudes, foram disponibilizadas 5 perguntas para sociedade no período de 23/02 a 26/03, a saber:

1. Cite as tecnologias e/ou ferramentas que conhece e/ou utiliza para o combate e prevenção à fraude digital. (Exemplo: 2 fatores de autenticidade, senha para faturas, identificação por impressão digital, sistemas de gerenciamento de fraudes, entre outros).
2. Na sua percepção, quais são os tipos mais frequentes de fraudes no âmbito digital? (Exemplo: envio de e-mail fraudulento para clientes com intuito de coleta de dados).
3. Sabendo que a utilização de terceirizados é uma prática comum das empresas brasileiras, muitas vezes os fraudadores tentam fraudar essas empresas devido a uma maior fragilidade sistêmica. Qual é a participação relativa das tentativas de fraudes oriundas de terceiros em relação ao todo? Quais ações de prevenção e mitigação conhece para esse tipo de fraude? Favor exemplificar.

4. Cite os principais mecanismos de controle que conhece e/ou utiliza para mitigar as fraudes no ecossistema digital. Conhece planos de ação/mitigação caso seja identificada uma tentativa fraudulenta? (Exemplo: plano de ação caso seja constatado o uso de dados de terceiros para compra de produtos e serviços).
5. Na sua percepção, quais são os principais temas relacionados à fraude no ecossistema digital que a ANATEL pode utilizar como auxílio no combate por meio de determinações, especificações de procedimentos e normas? Favor exemplificar.

Uma média de 8 pessoas / instituições responderam cada pergunta acima (houve diferentes números de respondentes por pergunta). A figura abaixo traz um resumo sobre os principais *insights* obtidos na tomada de subsídio.

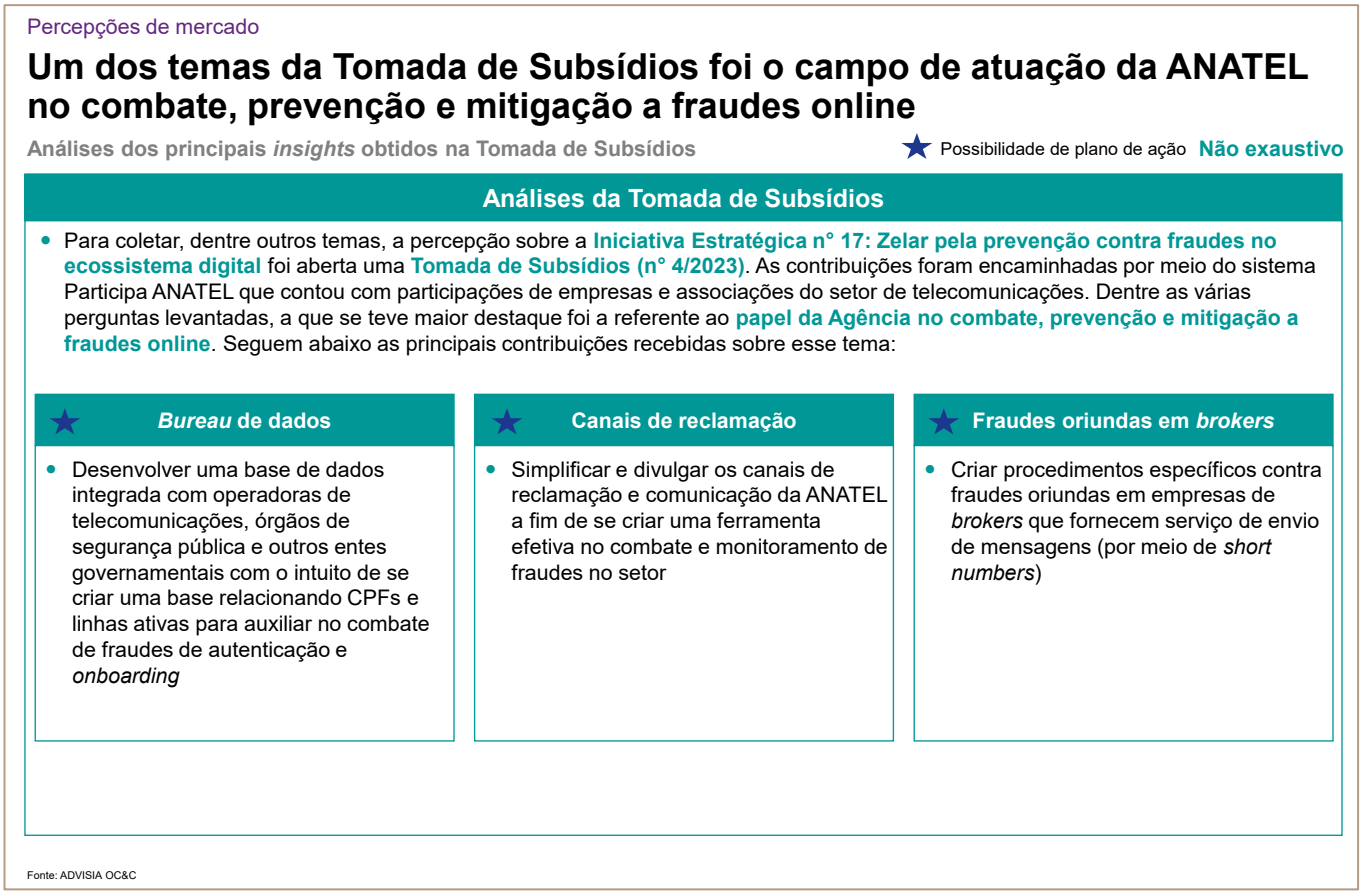


Figura 37

A seguir serão apresentadas em detalhes as respostas de cada uma das 5 perguntas feitas. Vale ressaltar que algumas respostas não serviram de insumo para o plano tático de

combate, prevenção e mitigação a fraudes no ecossistema digital, pois foram consideradas fora do escopo de trabalho da ANATEL, mas serão documentadas abaixo.

A primeira pergunta foi relacionada com as principais tecnologias e/ou ferramentas que as empresas mais utilizam para o combate e prevenção à fraude digital. Foram citadas diversas soluções que são exemplificadas na figura abaixo:

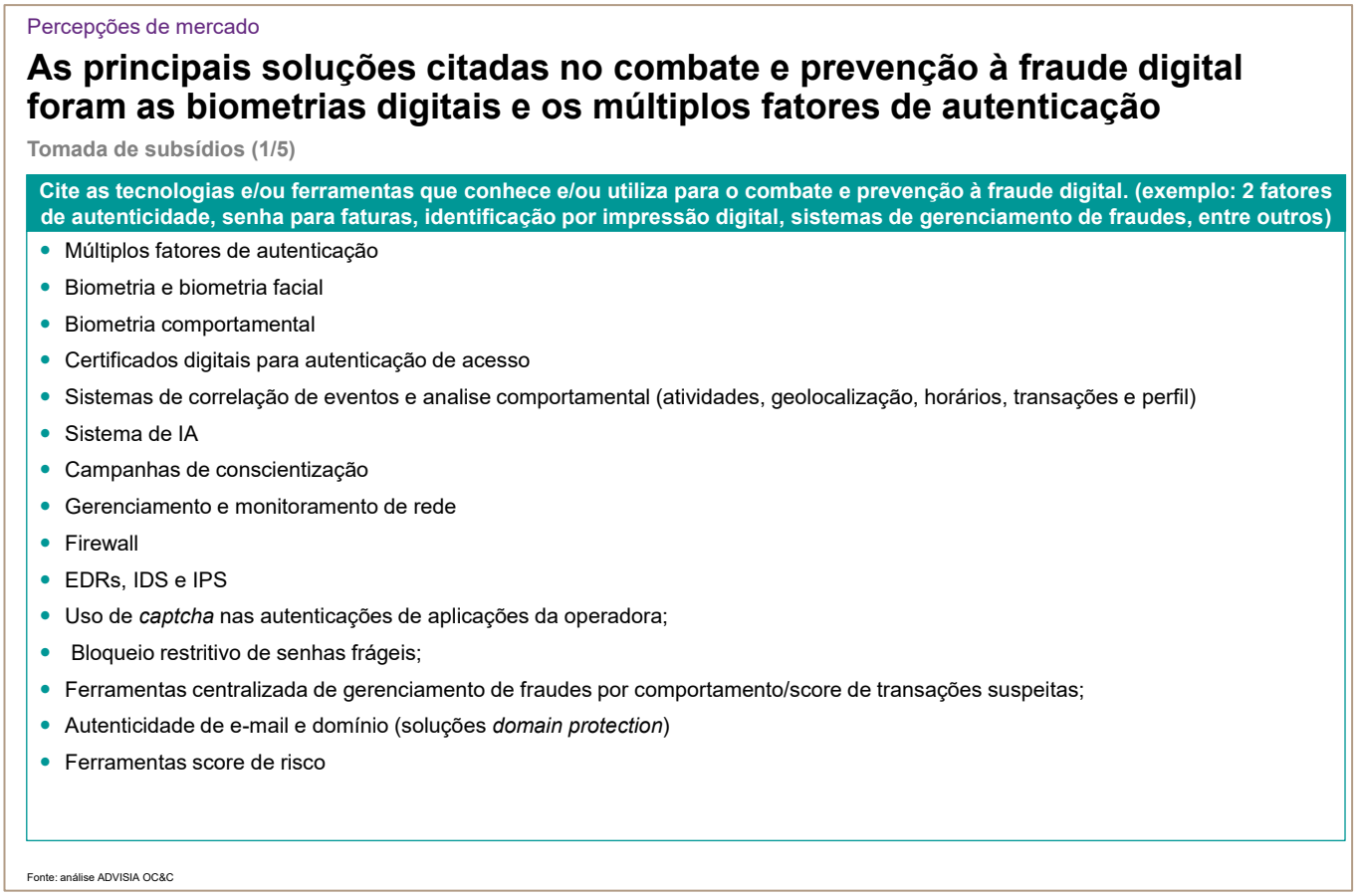


Figura 38

Soluções de múltiplos fatores de autenticação e biometrias sejam elas facial ou comportamental são comumente encontradas em processos / atividades financeiras, sendo assim amplamente difundidas e utilizadas por diversos setores.

Também foram citadas algumas ferramentas utilizadas para detectar e prevenir atividades maliciosas em sistemas de tecnologia da informação como, por exemplo, EDR *(Endpoint Detection and Response)*, IDS *(Intrusion Detection System)* e IPS *(Intrusion Prevention System)*.

De maneira geral as ferramentas citadas na tomada de subsídios corresponderam com a expectativa da agência e estavam em linha com as soluções discutidas no *workshop*.

A segunda pergunta foi referente aos tipos mais frequente de fraudes existentes no âmbito digital, a figura abaixo mostra as respostas para essa pergunta:

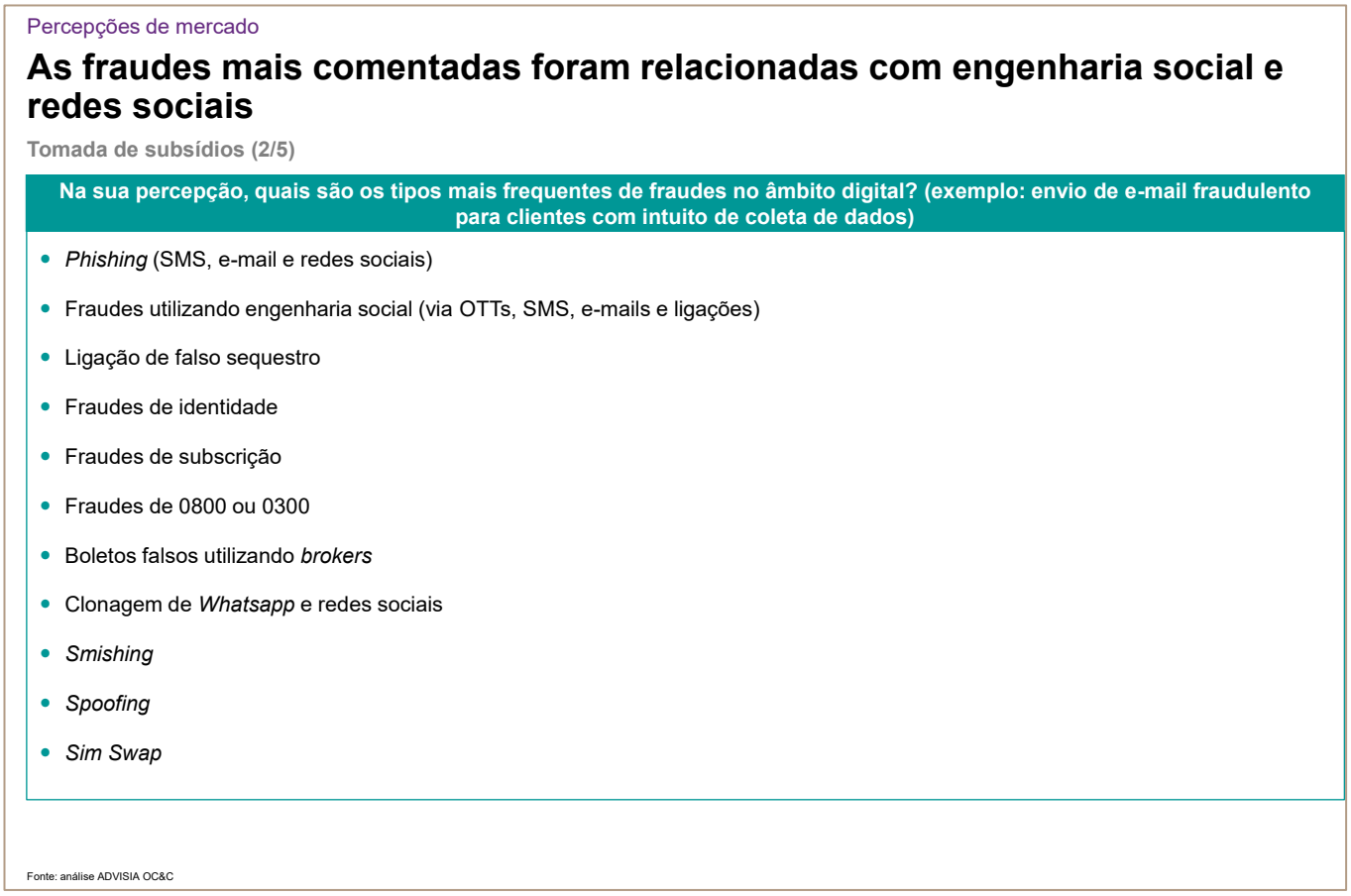


Figura 39

Todas as fraudes citadas na Figura 39 estão detalhadas na secção anterior (1.6 Métodos de fraude).

A terceira pergunta da tomada de subsídios foi composta por uma introdução e duas subi perguntas. É importante ressaltar que não houve resposta referente à primeira parte da pergunta anterior (participação relativa das tentativas de fraudes oriundas de terceiros em relação ao todo).

Percepções de mercado

A limitação de acesso para terceirizados tanto fisicamente e digitalmente foram as ações mais comentadas pelos participantes da pesquisa

Tomada de subsídios (3/5)

Sabendo que a utilização de terceirizados é uma prática comum das empresas brasileiras, muitas vezes os fraudadores tentam fraudar essas empresas devido a uma maior fragilidade sistêmica. Qual é a participação relativa das tentativas de fraudes oriundas de terceiros em relação ao todo? Quais ações de prevenção e mitigação conhece para esse tipo de fraude?

- Restringir o acesso a ambientes críticos, tanto físicos como digitais, como servidores e banco de dados
- Criar credenciais de acessos com baixa permissão de extração, manipulação de dados sensíveis e instalações de aplicativos
- Aplicar políticas de segurança exclusivas para terceiros, como navegação por *proxys*
- Restringir dispositivos de armazenamento, como artefatos USB.
- Restringir acesso a plataformas em nuvens, como: *whatsapp*, e-mail externo, Dropbox, *onedrive* etc.
- Criar clausulas contratuais estabelecendo obrigatoriedade de alinhamento com a politica de segurança da informação da empresa contratante
- Criar processo de gestão de acesso rigoroso, concessão de acesso com o mínimo de privilégio necessário; acessos rastreáveis
- Segregar redes (*firewall* e *vpn*)
- Aplicar políticas de senha, incluindo expiração e remoção de acesso quando da demissão/deslocação dos prestadores de serviço
- Usar ferramenta de monitoração de segurança (SIEM), de auditoria (registrando todos acessos de leitura e escrita a ativos de informação) e de processo de gestão de incidentes

Fonte: análise ADVISIA OC&C

Figura 40

A maioria das respostas listadas acima estão relacionadas com a limitação de acesso as pessoas terceirizadas, seja ela por sistemas, dispositivos, plataformas, redes sociais, credenciais, acesso físico e entre outros.

A quarta pergunta também foi subdividida em duas partes, no entanto não foram citados nenhum tipo de plano de ação ou mitigação para os casos em que se foi comprovada uma fraude ou tentativa de fraude. Segue as respostas para os principais mecanismos de controle para mitigar as fraudes digitais:

Percepções de mercado

Várias ferramentas são utilizadas no combate à fraude, com destaque para programas que utilizam análises de dados e padrões

Tomada de subsídios (4/5)

Cite os principais mecanismos de controle que conhece e/ou utiliza para mitigar as fraudes no ecossistema digital. Conhece planos de ação/mitigação caso seja identificada uma tentativa fraudulenta? (exemplo: plano de ação caso seja constatado o uso de dados de terceiros para compra de produtos e serviços)

- Políticas e práticas de segurança da informação
- Programas de *complieance* em proteção e privacidade de dados
- Ferramentas de identificação de anormalidades e desvio de processos
- Ferramentas de múltiplo fator de autenticação
- Testes externos de vulnerabilidades
- Modelos baseados em *Machine Learning*
- Ferramentas para controle de tráfego de dados sensíveis
- Regras analíticas para detecção e tratativa de riscos de fraudes
- Adoção das melhores praticas regulatórias

Fonte: análise ADVISIA OC&C

Figura 41

A maioria das ferramentas citadas tem relação com as soluções faladas na primeira pergunta.

A última pergunta foi direcionada para a agência. Foi perguntado quais os principais temas relacionados à fraude no ecossistema digital que a ANATEL possa utilizar como auxílio no combate por meio de determinações, especificações de procedimentos e normas? As respostas estão contidas na figura abaixo.

Percepções de mercado

O mercado espera que a ANATEL crie diversos procedimentos para o combate a fraude

Tomada de subsídios (5/5)

Na sua percepção, quais são os principais temas relacionados à fraude no ecossistema digital que a ANATEL possa utilizar como auxílio no combate por meio de determinações, especificações de procedimentos e normas? Favor exemplificar.

- Criar mecanismo de identificação de acesso móveis usados como acessórios em tentativas de fraude (SMS de *phishing*, por exemplo), que permita o rápido bloqueio e identificação dos responsáveis.
- Criar sistema integrado com operadoras de telecomunicação, grandes plataformas, órgãos de segurança pública, outros entes governamentais e a própria sociedade de forma a se criar ambiente adequado à investigação, mitigação e responsabilização de fraudes nos meios digitais. Tal sistema permitiria a rápida comunicação de incidentes, riscos e ameaças, incluindo cooperação técnica
- Identificar rotas e provedores de SMS piratas, nacionais e internacionais.
- Criar procedimentos ágeis para que linhas utilizadas em crimes como “falso sequestro”, “golpe do *Whatsapp*” sejam facilmente rastreadas pelas forças de segurança, para que a origem possa ser identificada e neutralizada.
- Criar canais de comunicação e ferramentas para diagnóstico de ataques de negação de serviço e coleta de subsídios para identificação do atacante e redução do número de casos no país
- Utilizar ferramentas para o combate a fraude no momento de aquisição de linhas móveis, de forma a garantir uma melhor acuracidade sobre a propriedade da linha
- Elaborar regras e diretrizes para identificar e bloquear chamadas e mensagens automáticas (*robocall*) não desejadas, assim como exigir que as operadoras de telefonia implementassem soluções de TI para coibir estas práticas
- Criar canais de comunicação hábeis para monitoramento e identificação de fraudes e ataques
- Criar procedimentos contra fraudes para empresas de brokers que fornecem serviço de envio de mensagens (por meio de *short numbers*)

Fonte: análise ADVISIA OC&C

Figura 42

Importante ressaltar que o mercado em geral espera que a ANATEL crie algum procedimento ou mecanismo que vise ao combate a algum tipo de fraude existente, mas em alguns casos a Agência ou a sociedade já dispõe de tais procedimentos (exemplo: identificação de chamadas e mensagens automáticas) e em outros não existe uma base técnica que viabilize essa criação (exemplo: a utilização de ferramentas para o combate à fraude no momento de aquisição de linhas móveis).

2.4. Entrevista com *stakeholders*

A coleta de percepções de mercado desempenha um papel crucial na elaboração do plano tático da ANATEL, uma vez que permite a identificação das necessidades e expectativas dos diversos agentes envolvidos no combate, prevenção e mitigação às fraudes no ecossistema digital. Ao analisar e compreender essas percepções, a Agência pode desenvolver estratégias focadas nos pontos mais latentes relatados pela sociedade.

Além disso, a coleta de percepções de mercado auxilia a ANATEL a antecipar tendências e desafios futuros, possibilitando a implementação de medidas preventivas e ações corretivas que assegurem a resiliência e a adaptabilidade do setor às mudanças. Dessa forma, a análise das percepções de mercado é um elemento-chave para a elaboração de um plano tático eficiente e bem-sucedido.

Para entender os anseios e expectativas dos principais *stakeholders* envolvidos no tema de fraude, foram conduzidas diversas entrevistas que trouxeram variadas visões sobre o que o mercado espera da Agência. A figura abaixo traz alguns exemplos do público entrevistado.

Figura 43

Como mostrado na figura acima, foram entrevistados diversos *players* e setores da economia brasileira, com destaque para o mercado financeiro que contribuiu trazendo diversos pontos de vista sobre o assunto de fraude. A maior preocupação relatada por essa indústria está relacionada a fraudes utilizando chips pré-pagos. Houve diversos relatos onde as empresas afirmaram que há um volume considerável de tentavas de fraudes de cadastro, *onboarding* e autenticação em que o fraudador se passa por um usuário do banco ou *fintech* e tenta coletar dados ou adquirir algum ganho financeiro através do uso de números oriundos de chips pré-pagos. Vale ressaltar que essas fraudes citadas anteriormente não se restringem ao uso discriminado do chip pré-pago, que é apenas uma de muitas ferramentas existentes que os fraudadores utilizam.

A figura abaixo traz as principais fraudes relatadas nas entrevistas que envolvem o setor de telecomunicações.

Figura 44

A fraude de retenção da linha descrita na Figura 44 recebeu tratamento no processo 53500.045145-2019. A formalização do processo ainda não foi concluída, mas já houve relatos do mercado financeiro afirmando a migração desta modalidade.

Outro ponto bastante discutido nas entrevistas foi o que se espera da ANATEL no combate, prevenção e mitigação às fraudes no setor de telecomunicações. A figura abaixo traz as percepções coletadas (importante ressaltar que a figura mostra apenas o ponto de vista das empresas e *experts* entrevistados):

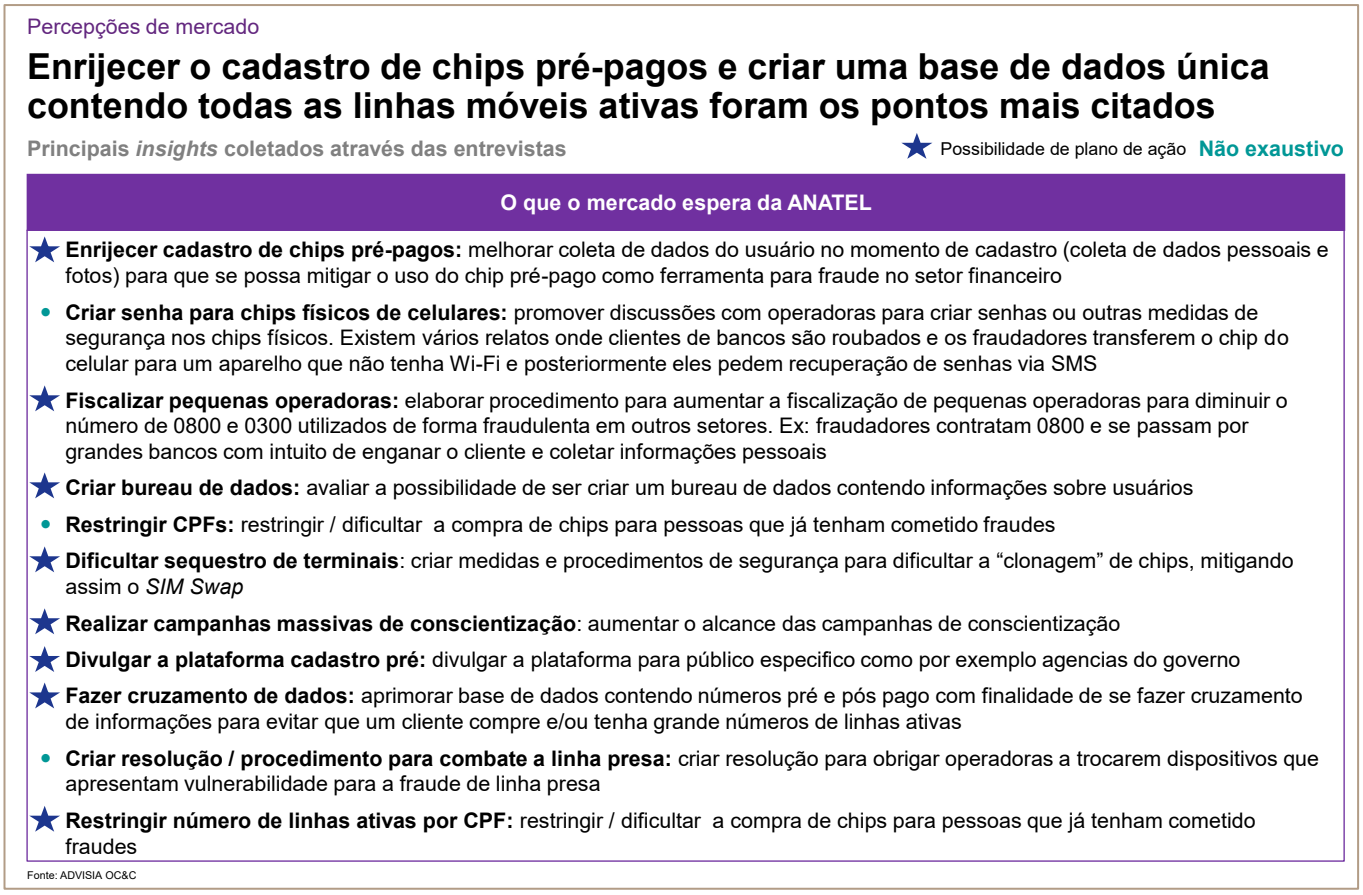


Figura 45

Esses pontos relatados na Figura 45 serviram de inspiração para algumas atividades do plano de ação. Foi considerado no plano apenas os problemas relacionados com o escopo da ANATEL levando em conta a origem e não a solução proposta pelas empresas. Segue abaixo um exemplo:

- Fraudes envolvendo autenticação e cadastro relatadas pelo mercado financeiro podem ser mitigadas de várias maneiras, por exemplo, através do aprimoramento das bases já existentes de pré e pós-pago correlacionando CPFs e linhas ativas ou garantindo que o projeto "Cadastro Pré", já existente, esteja sendo cumprido pelas prestadoras de serviço, cabe à ANATEL avaliar qual solução será mais viável.

2.5. Base de dados

A ANATEL, através da Superintendência de Relações com Consumidores, possibilita ao consumidor o registro de reclamações contra as prestadoras de serviços de telecomunicações (como telefonia móvel, telefonia fixa, internet e TV por assinatura). Esse serviço ofertado pela Agência registra as reclamações, denúncias, pedidos de informação e sugestões. É possível realizar as reclamações via aplicativo móvel, internet, telefone ou de forma presencial (em cada capital brasileira a Agência disponibiliza uma “sala do cidadão” para que o consumidor possar registrar solicitações).

Esse canal de reclamação gera uma base de dados que pode ser utilizada como insumo para diversas áreas da empresa. Essa base foi disponibilizada para a ADVISIA, após anonimizadas todas as informações pessoais dos clientes / usuários, com a intenção de se extrair o máximo de informações possíveis referentes a reclamações relacionadas com o tema de fraude digital.

Atualmente, a base conta com os seguintes campos relacionados ao chamado do cliente: i. Assunto: categorização do chamado; ii. Problema: subcategorização do chamado, ou seja, uma categorização dentro de cada campo “assunto”; iii. Descrição: campo aberto onde o cliente ou atendente relata a reclamação.

Não existe categorização referente a fraudes, golpes ou ataques cibernéticos na base de reclamações. Para se conduzir uma extração inicial da base, foi necessário utilizar palavras chaves no campo “descrição” relacionadas ao tema de fraude, como ilustradas na figura abaixo.

Palavras-chave utilizadas para extração da base de dados

Palavras-chave		
• Golpe	• Farsa	• Spoofing
• Fraude	• Falsificação	• Pharming
• Fraudulento	• Falsificado	• SIM Swapping
• Fraudar	• Adulterado	• SIM Jacking
• Fraudador	• Adulteração	• Clonagem
• Falcatrua	• Roubo	• Clonou
• Trama	• Roubado	• Clonado
• Tramou	• Roubaram	
• Tramoia	• Imitação	
• Trapaça	• Imitar	
• Enganado	• Imitou	
• Enganou	• Plágio	

Fonte: ADVISIA OC&C

Figura 46

Foram extraídas todas as reclamações feitas pelos clientes que tiveram essas palavras no campo “descrição” no ano de 2022. Com isso, a base analisada contou com mais de 37 mil reclamações, sendo 38 diferentes assuntos e 150 problemas. A figura abaixo traz um *overview* da base de dados analisada.

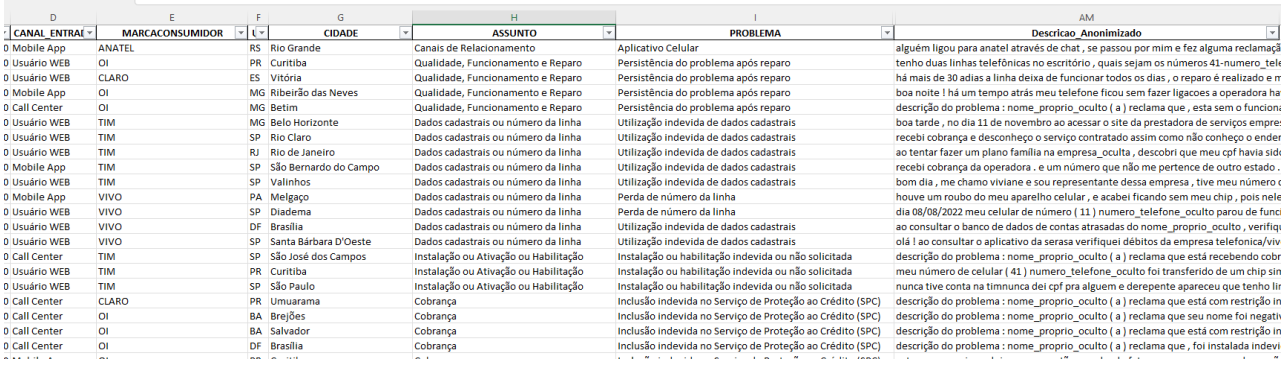
Base de dados

Apesar da base de dados ter 150 possíveis problemas nenhuma deles trouxe alguma correlação direta com o tema de fraudes digitais

Overview Base

Base de dados

- **4 canais onde consumidor pode realizar a sugestão ou reclamação** (SEI, aplicativo de celular, ligação e internet)
- **38 diferentes assuntos e 150 possíveis problemas onde as sugestões ou reclamações são categorizadas**
- **37.701 reclamações, sugestões, denuncias ou pedidos de informação** relatados no ano de 2022 que continham no campo "descrição" palavras com significado semelhante à **"Fraude"**



	D	E	F	G	H	I	AM
	CANAL_ENTRAD	MARCACONSUMIDOR	UF	CIDADE	ASSUNTO	PROBLEMA	Descricao_Anonimizado
0	Mobile App	ANATEL	RS	Rio Grande	Canais de Relacionamento	Aplicativo Celular	alguém ligou para anatel através de chat , se passou por mim e fez alguma reclamaçã
0	Usuário WEB	OI	PR	Curitiba	Qualidade, Funcionamento e Reparo	Persistência do problema após reparo	tenho duas linhas telefônicas no escritório , quais sejam os números 41-numero_tele
0	Usuário WEB	CLARO	ES	Vitória	Qualidade, Funcionamento e Reparo	Persistência do problema após reparo	há mais de 30 adias a linha deixa de funcionar todos os dias , o reparo é realizado e n
0	Mobile App	OI	MG	Ribeirão das Neves	Qualidade, Funcionamento e Reparo	Persistência do problema após reparo	boa noite ! há um tempo atrás meu telefone ficou sem fazer ligacoes a operadora ha
0	Call Center	OI	MG	Betim	Qualidade, Funcionamento e Reparo	Persistência do problema após reparo	descrição do problema : nome_proprio_oculto (a) reclama que , esta sem o funciona
0	Usuário WEB	TIM	MG	Belo Horizonte	Dados cadastrais ou número da linha	Utilização indevida de dados cadastrais	boa tarde , no dia 11 de novembro ao acessar o site da prestadora de serviços empres
0	Usuário WEB	TIM	SP	Rio Claro	Dados cadastrais ou número da linha	Utilização indevida de dados cadastrais	recebi cobrança e desconheço o serviço contratado assim como não conheço o ender
0	Usuário WEB	TIM	RJ	Rio de Janeiro	Dados cadastrais ou número da linha	Utilização indevida de dados cadastrais	ao tentar fazer um plano família na empresa_oculta , descobri que meu cpf havia sid
0	Mobile App	TIM	SP	São Bernardo do Campo	Dados cadastrais ou número da linha	Utilização indevida de dados cadastrais	recebi cobrança da operadora . e um número que não me pertence de outro estado .
0	Usuário WEB	TIM	SP	Valinhos	Dados cadastrais ou número da linha	Utilização indevida de dados cadastrais	bom dia , me chamo viviane e sou representante dessa empresa , tive meu número
0	Mobile App	VIVO	PA	Melgaço	Dados cadastrais ou número da linha	Perda de número da linha	houve um roubo do meu aparelho celular , e acabei ficando sem meu chip , pois nele
0	Usuário WEB	VIVO	SP	Diadema	Dados cadastrais ou número da linha	Perda de número da linha	dia 08/08/2022 meu celular de número (11) numero_telefone_oculto parou de funci
0	Usuário WEB	VIVO	DF	Brasília	Dados cadastrais ou número da linha	Utilização indevida de dados cadastrais	ao consultar o banco de dados de contas atrasadas do nome_proprio_oculto , verifiq
0	Usuário WEB	VIVO	SP	Santa Bárbara D'Oeste	Dados cadastrais ou número da linha	Utilização indevida de dados cadastrais	olá ! ao consultar o aplicativo da serasa verifiquei débitos da empresa telefonica/viv
0	Call Center	TIM	SP	São José dos Campos	Instalação ou Ativação ou Habilitação	Instalação ou habilitação indevida ou não solicitada	descrição do problema : nome_proprio_oculto (a) reclama que está recebendo cobr
0	Usuário WEB	TIM	PR	Curitiba	Instalação ou Ativação ou Habilitação	Instalação ou habilitação indevida ou não solicitada	meu número de celular (41) numero_telefone_oculto foi transferido de um chip sin
0	Usuário WEB	TIM	SP	São Paulo	Instalação ou Ativação ou Habilitação	Instalação ou habilitação indevida ou não solicitada	nunca tive conta na timnunca dei cpf pra alguem e derepente apareceu que tenho lir
0	Call Center	CLARO	PR	Umuarama	Cobrança	Inclusão indevida no Serviço de Proteção ao Crédito (SPC)	descrição do problema : nome_proprio_oculto (a) reclama que está com restrição in
0	Call Center	OI	BA	Brejões	Cobrança	Inclusão indevida no Serviço de Proteção ao Crédito (SPC)	descrição do problema : nome_proprio_oculto (a) reclama que seu nome foi negati
0	Call Center	OI	BA	Salvador	Cobrança	Inclusão indevida no Serviço de Proteção ao Crédito (SPC)	descrição do problema : nome_proprio_oculto (a) reclama que está com restrição in
0	Call Center	OI	DF	Brasília	Cobrança	Inclusão indevida no Serviço de Proteção ao Crédito (SPC)	descrição do problema : nome_proprio_oculto (a) reclama que , foi instalada indevi

Fonte: ADVISIA OC&C

Figura 47

A falta de categorizações relacionadas ao tema fraude gerou uma alta complexidade de análise. Foi escolhido utilizar para a análise o processamento de linguagem natural conhecida como NLP (área da ciência da computação que se concentra em ajudar as máquinas a entender e processar a linguagem humana). Uma das bibliotecas de código aberto mais populares para NLP em Python é o Natural Language Toolkit (NLTK). O NLTK fornece uma ampla variedade de ferramentas para lidar com textos em vários idiomas e tarefas relacionadas ao NLP, como tokenização, análise de sintaxe, extração de informações, análise de sentimentos, dentre outras. A figura abaixo traz um resumo da análise realizada.

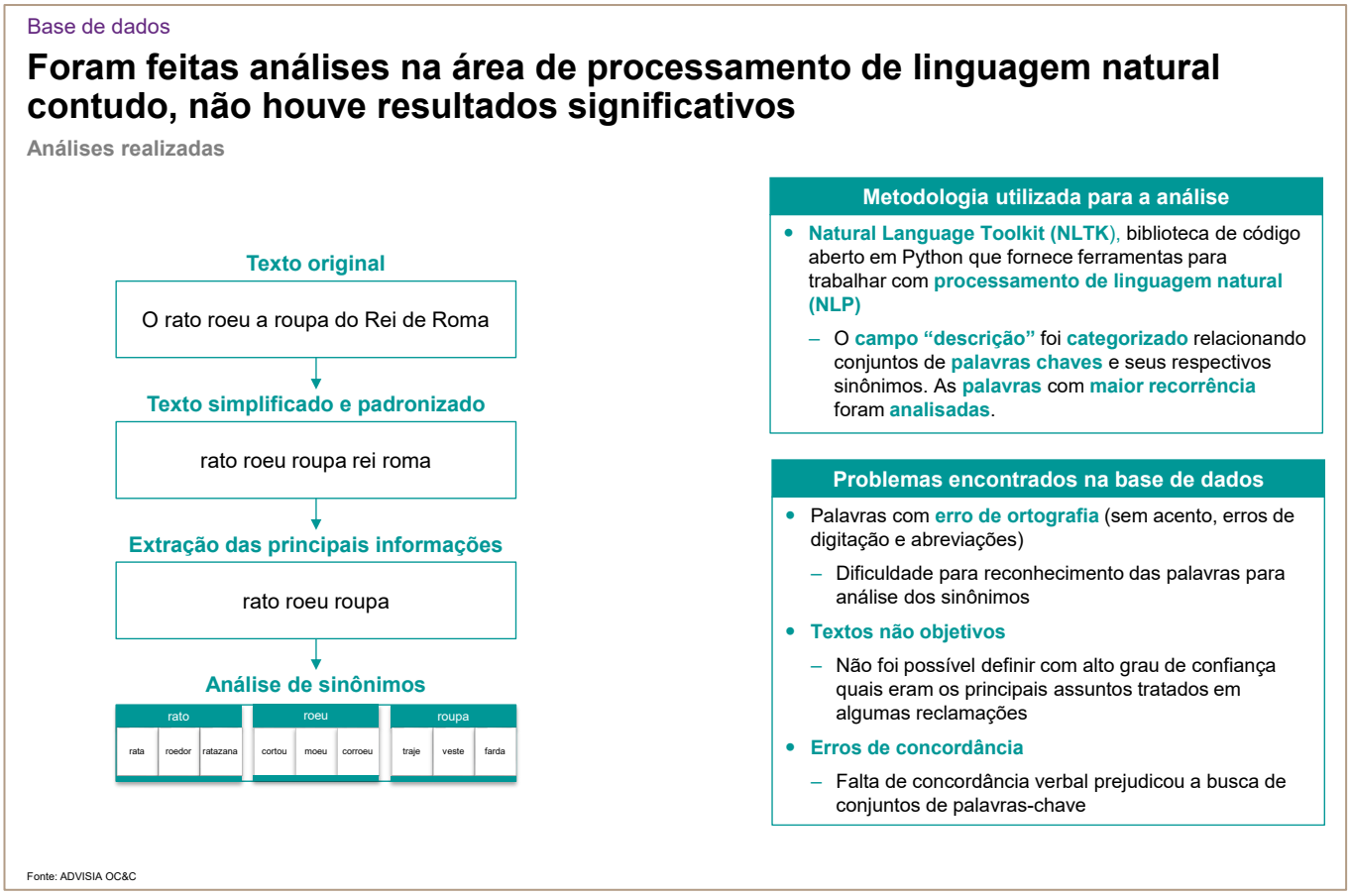


Figura 48

Vários problemas da base foram identificados no decorrer da análise, todos relacionados ao campo "descrição". Problemas ortográficos, textos não objetivos e erros de concordância verbal inviabilizaram um resultado preciso.

No decorrer das análises, foram vislumbradas algumas oportunidades futuras que serviram de inspiração para as subiniciativas 17.11 e 17.14, listadas no próximo capítulo. A figura abaixo exemplifica algumas dessas oportunidades.

Base de dados

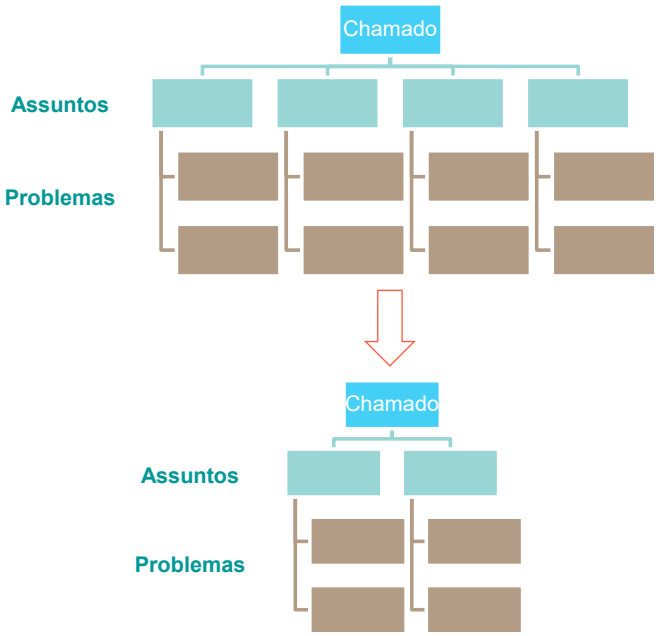
Existem oportunidades para melhorar a categorização dos chamados e a experiência dos usuários principalmente no site

Oportunidades Futuras

Oportunidades detectadas

- **Simplificação das categorizações e criação de novas categorias para fraudes e ataques cibernéticos**, com o intuito de melhorar a experiência dos usuários e futuras análises dos dados
- Criação de novos **scripts** de atendimento com o intuito de **padronizar a categorização dos chamados**
- **Redesenho da árvore do site e aplicativo** para facilitar e incentivar a reclamação ou feedback dos usuários

Simplificação das categorizações existentes



Fonte: ADVISIA OC&C

Figura 49

3. Plano de ação

Este diagnóstico apresentado previamente serviu de insumo para a elaboração de subiniciativas para compor o plano de ação da Agência. Após a estruturação e a alinhamentos internos junto ao time da ANATEL, as subiniciativas foram definidas e priorizadas de forma a atenderem ao Planejamento Estratégico 2023-2027.

A metodologia para categorização e priorização das subiniciativas foi desenvolvida por meio de uma análise de impacto *versus* esforço (Figura 45):

3.1. Análise de impacto e esforço

1. Análise de impacto

- O impacto das subiniciativas foi avaliado de acordo com o potencial de mudança que a iniciativa pode promover. Dessa maneira, esta dimensão foi medida por meio de dois índices, mensurados de 1 até 3 (baixo, médio e alto)
  - Abrangência: mede o grau de penetração da iniciativa, sendo o valor 3 aquele que consegue ser melhor disseminada, englobando mais setores, por exemplo;
  - Eficácia: mede o quanto a iniciativa consegue resolver o problema abordado, sendo o valor 3 aquele que resolve de maneira satisfatória o problema;

2. Análise de esforço

- O esforço está relacionado à dificuldade para realização da subiniciativa. Dessa maneira, esta dimensão é medida por meio de dois índices mensurados de 1 até 3 (baixo, médio e alto)
  - Complexidade: mede o grau de obstáculos para a realização da iniciativa, sendo o valor 3 o mais complicado para a sua finalização;
  - Prazo: mede o tempo necessário para o início e o fim da iniciativa, sendo o valor 3 considerado como Longo e com período de execução acima de 1 ano.

O impacto e o esforço de cada subiniciativa foram discutidos junto ao time da ANATEL e neste documento é apresentado o resultado destas discussões.

3. Plotagem do gráfico:

- Após a classificação de cada subiniciativa, a priorização ocorreu por meio da originação de um gráfico de impacto *versus* esforço, seguindo a regra de pareto[68]. Sendo a subiniciativa que apresenta um valor maior para impacto com esforço baixo considerada prioritária dentre as outras.

A figura abaixo ilustra a metodologia de priorização descrita anteriormente:

Figura 50

[68] Calculou-se o percentil 20 e o percentil 80 para os eixos de impacto e esforço, assim foram traçadas retas para priorização das subiniciativas.

3.2. Subiniciativas levantadas

O estudo de mercado, *benchmarking*, *workshop*, tomada de subsídios e percepções coletadas do mercado pelas entrevistas serviram de inspiração para a criação das subiniciativas do plano de ação. Foram consolidadas 17 atividades, sendo 16 exclusivas da frente estratégica de fraudes e 1 transversal junto com o tema de alfabetização digital. As 16 subiniciativas exclusivas dessa frente foram categorizadas em 5 grupos, apresentados abaixo.

Plano de ação

A partir das diferentes referências, foram consolidadas 17[1] subiniciativas para o Plano Tático 2023-2024 da ANATEL

Lista das 16[1] subiniciativas exclusivas Produto V

Tipo	Nome
Conscientização da população	Promover campanhas massivas de conscientização para usuários a respeito da importância de pronto acionamento da prestadora, para casos de interrupção dos serviços.
	Conscientizar usuários sobre fraudes de engenharia social, reconhecendo diferenças entre os diversos grupos sociais
	Promover conscientização de usuários não alfabetizados digitalmente e idosos contra *phishing*
	Realizar campanhas focadas em idosos, adolescentes e usuários não alfabetizados digitalmente para conscientização contra *spoofing*
	Realizar acompanhamento para diminuir fraudes de 0800
Procedimentos e mecanismos	Incentivar o uso de *modems* residenciais cuja avaliação de conformidade tenha contemplado os requisitos de segurança
	Criar procedimentos específicos contra fraudes oriundas em *brokers*
	Aprimorar mecanismos para dificultar o sequestro de terminal
	Aprimorar mecanismos para dificultar a operação de "chipeiras" utilizadas em fraudes
Chips pré-pagos	Impulsionar Projeto Cadastro Pré-Pago
	Divulgar plataforma "Cadastro Pré" para públicos específicos
	Reavaliar imposição de limite de linhas ativas pré-pagas por CPF
Base de dados	Avaliar a criação de procedimento de compartilhamento de informações para identificar comportamentos fraudulentos entre diferentes setores da economia
Outras Ações	Fomentar a participação da ANATEL em fóruns e seminários
	Simplificar e melhorar a experiência do cliente nos canais de reclamação da ANATEL
	Elaborar relatórios periódicos relacionados a fraudes reportadas para a ANATEL

[1] 17 atividades são exclusivas do produto fraude no ecossistema digital, 1 atividade é transversal com o produto alfabetização digital

Fonte: ADVISIA OC&C

Figura 51

3.3. Priorização das subiniciativas

Como explicado previamente, após a classificação de cada subiniciativa, a priorização ocorreu por meio da originação de um gráfico de impacto *versus* esforço, seguindo a regra de Pareto[69]. Sendo a iniciativa que apresenta um valor maior para impacto com esforço baixo considerada prioritária dentre as outras. Vale ressaltar que a análise de impacto e esforço foi realizada juntamente com a equipe da ANATEL para que todas as subiniciativas propostas estivessem aderentes à realidade da Agência (Figura 48).

Figura 52

[69] Calculou-se o percentil 20 e o percentil 80 para os eixos de impacto e esforço, assim foram traçadas retas para priorização das subiniciativas.

Também foi proposta uma visão das subiniciativas segmentadas de acordo com o tempo de implementação (Figura 49), visando contribuir para o planejamento da execução do plano de ação. As atividades estão listadas pela priorização descrita na Figura 48.

Plano de ação

Uma outra visão que pode contribuir para o planejamento da execução dos planos é a visão por prazo

Visão de prazo das subiniciativas

Curto Prazo (até 6 meses)

#	Subiniciativa
17.1	Promover conscientização para usuários sobre pronto acionamento da prestadora para casos de interrupção dos serviços
17.2	Conscientizar usuários sobre fraudes de engenharia social, reconhecendo diferenças entre os diversos grupos sociais
17.3	Promover conscientização de usuários não alfabetizados digitalmente e idosos contra *phishing*
17.4	Realizar campanhas focadas em idosos, adolescentes e usuários não alfabetizados digitalmente para conscientização contra *spoofing*
17.5	Realizar acompanhamento para diminuir fraudes de 0800
17.6	Fomentar a participação da ANATEL em fóruns e seminários
17.12	Divulgar plataforma "Cadastro Pré" para públicos específicos

Médio Prazo (de 6 meses a 1 ano)

#	Subiniciativa
17.9	Avaliar a criação de procedimento de compartilhamento de informações para identificar comportamentos fraudulentos
17.10	Avaliar aprimoramentos dos mecanismos para dificultar o sequestro de terminal
17.11	Elaborar relatórios periódicos relacionados a fraudes reportadas para a ANATEL

Longo Prazo (acima de 1 ano)

#	Subiniciativa
17.7	Incentivar o uso de modems residenciais cuja avaliação de conformidade tenha contemplado os requisitos de segurança
17.8	Criar procedimentos específicos contra fraudes oriundas em *brokers*
17.13	Reavaliar imposição de limite de linhas ativas pré-pagas por CPF
17.14	Simplificar e melhorar a experiência do cliente nos canais de reclamação da ANATEL
17.15	Impulsionar Projeto Cadastro Pré-Pago
17.16	Aprimorar mecanismos para dificultar a operação de "chipeiras" utilizadas em fraudes

Fonte: ADVISIA OC&C

Figura 53

3.4. Descrição da ficha de plano de ação

Foi elaborada uma ficha detalhando cada uma das subiniciativas. As dimensões apresentadas nessa ficha são:

- Objetivo: define a finalidade daquela subiniciativa, ou seja, qual será a principal entrega e seu objetivo;
- Atividades: descreve, em linhas gerais, quais etapas devem ser realizadas para conclusão da subiniciativa;
- Impacto *vs.* esforço: mensura o nível de impacto e de esforço de cada subiniciativa, sendo o valor 6, aquele com alto impacto e alto esforço;
- *KPI (Key Performance Indicator):* mensura o nível de desempenho e a taxa de sucesso da subiniciativa;
- Envolvidos: destaca as entidades que deverão participar do processo para desenvolvimento da subiniciativa, além do responsável geral pela gestão das atividades;
- Referência: destaca os programas, agências e regras que serviram de inspiração para a construção da subiniciativa, quando houver;
- Resultado: destaca o resultado esperado da iniciativa, sendo i. Cessar, reverter, mitigar e prevenir[70] (referente ao termo utilizado na RFP "combate, mitigação e prevenção a fraude"); ii. Aumentar confiança dos usuários iii. Reduzir golpes digitais;
- Prazo: demonstra a expectativa de duração da subiniciativa, sendo curto (até 6 meses), médio (6 meses até 1 ano) ou longo (acima de 1 ano);
- Riscos: destaca quais os principais pontos de atenção que podem surgir durante a implementação da subiniciativa.

[70] BRASIL, ANATEL, Resolução 73. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/1998/34-resolucao-73

Essas dimensões foram avaliadas para cada uma das subiniciativas propostas, e serão detalhadas na sequência. Vale mencionar que as subiniciativas estão apresentadas seguindo a análise de impacto *versus* esforço, e seu detalhamento foi realizado em grupos, começando pelas “priorizadas” e finalizando pelas “verificar a prioridade”.

3.5. Detalhamento das subiniciativas prioritárias

As subiniciativas analisadas nesta seção serão aquelas classificadas como prioritárias. A saber: nº 17.1 a 17.5.

Subiniciativa nº 17.1: Promover conscientização para usuários sobre pronto acionamento da prestadora para casos de interrupção dos serviços (Figura 54)

- Essa subiniciativa surgiu a partir das entrevistas com as polícias brasileiras e a partir de discussões durante o *workshop,* tendo como maior referência a plataforma "#FiqueEsperto" da ANATEL;
- O objetivo da subiniciativa é conscientizar usuários sobre o pronto acionamento da prestadora para casos de interrupção dos serviços de maneira não esperada ou solicitada (falta de sinal nos dispositivos móveis e impossibilidade de realizar ligações ou utilizar dados móveis) pode ser um indício de que a linha foi habilitada em outro *SIM Card*. A rápida ação dos usuários contatando as empresas de telefonia pode ajudar na reversão dos casos de *SIM Swap*. Importante ressaltar que a perda / interrupção momentânea de sinal nos dispositivos móveis pode acontecer devido ao local onde o usuário se encontra, como por exemplo, elevador, hospitais ou áreas remotas. Sendo assim é importante ter ciência da diferença entre uma interrupção causada devido ao *SIM Swap* e outra devido à falta de sinal oriunda da localização do cliente;
- As principais atividades propostas são:
    - Definir quais redes sociais serão selecionadas para atuação;
    - Definir temática e conteúdo de divulgação;
    - Definir público-alvo;
    - Elaborar cronograma de divulgações;
    - Produzir material e vídeos;
    - Divulgar;

- O impacto é considerado alto, pois a conscientização da vítima é uma das maneiras mais eficientes de se mitigar a fraude de SIM Swap;
- O esforço é considerado baixo, levando em consideração o material já existente no “#FiqueEsperto” e a disposição da Proteste e da Polícia Federal em ajudar a Agência no combate a esse tipo de fraude;
- O KPI a ser monitorado é a quantidade de visualizações por postagem;
- A Superintendência de Controle de Obrigações será a responsável pelo desenvolvimento dessa subiniciativa junto com a Superintendência de Relações com Consumidores, contando com o apoio da Proteste, das grandes prestadoras de serviço de telecomunicações, da plataforma “#FiqueEsperto” e da Polícia Federal;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;
- A sua realização é considerada de curto prazo (até 6 meses), mas podendo se estender caso seja necessário a prolongamento da campanha;
- Os principais riscos levantados são:
    - Baixa adesão e pouca efetividade da ação;
    - Falta de constância na publicação dos informativos;
    - Falta de uma curadoria;

Plano de ação

Subiniciativa nº17.1 : Promover conscientização para usuários sobre pronto acionamento da prestadora para casos de interrupção dos serviços

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL + Outros

Objetivo

Promover conscientização para usuários a respeito de *SIM Swap* com o intuito de mitigar a fraude com a rápida recuperação dos serviços de telefonia

Atividades

- 1. Definir quais redes sociais de atuação
- 2. Definir temática e conteúdo de divulgação
- 3. Definir público-alvo
- 4. Construir calendário de divulgações
- 5. Construir de material / vídeos
- 6. Divulgar

Impacto vs esforço

Impacto

Esforço

KPI

 # visualizações por postagem

Envolvidos

- **ANATEL** (responsável)
- **Proteste**
- **Grandes Operadoras**
- **# Fique Esperto**
- **Polícia Federal**

Referência

- # Fique Esperto
- *Action Fraud Police (UK)*

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	X
Reduzir golpes digitais	X

Prazo[1]

Curto (até 6 meses)

Riscos

- 1. Baixa adesão e pouca efetividade; 2. Falta de constância na publicação dos informativos; 3. Falta de uma curadoria

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)

Fonte: ADVISIA OC&C

Figura 54

Subiniciativa nº 17.2: Conscientizar usuários sobre fraudes de engenharia social, reconhecendo diferenças entre os diversos grupos sociais (Figura 55)

- Essa subiniciativa surgiu a partir das entrevistas e do workshop tendo como maior referência a plataforma "#FiqueEsperto" da ANATEL;
- O objetivo dessa iniciativa é realizar a conscientização de grupos específicos (crianças, idosos e pessoas não alfabetizadas digitalmente) sobre fraudes que envolvam engenharia social;
- As principais atividades propostas são:
    - Definir grupo de trabalho;
    - Definir redes sociais de atuação;
    - Definir temática e conteúdo de divulgação;
    - Definir público-alvo;
    - Elaborar cronograma de divulgações;
    - Produzir material e vídeos;
    - Divulgar nas redes sociais, por SMS e e-mail marketing;
    - Divulgar presencialmente (escolas e organizações não governamentais);
- O impacto é considerado alto, pois a conscientização é a maneira mais eficiente existente no combate a fraudes relacionadas com engenharia social;
- O esforço é considerado baixo, levando em consideração o material já existente no ""#FiqueEsperto";
- O KPI a ser monitorado é a quantidade de visualizações por postagem;
- A Superintendência de Controle de Obrigações e a Superintendência de Relações com Consumidores serão responsáveis pelo desenvolvimento dessa subiniciativa e deve contar com o apoio da plataforma "#FiqueEsperto" e do Ministério da Educação;

- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;
- A sua realização é considerada de curto prazo (até 6 meses)
- Os principais riscos levantados são:
    - Baixa adesão e pouca efetividade da ação;
    - Falta de constância na publicação dos informativos;
    - Falta de uma curadoria;

Plano de ação

Subiniciativa nº17.2 : Conscientizar usuários sobre fraudes de engenharia social, reconhecendo diferenças entre os diversos grupos sociais

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL + Outros

Objetivo

Diminuir o número de fraudes relacionadas com engenharia social promovendo campanhas de conscientização para usuários a respeito de fraudes envolvendo engenharia social

Atividades

- 1. Definir grupo de trabalho
- 2. Definir redes sociais de atuação
- 3. Definir temática e conteúdo de divulgação
- 4. Definir público-alvo
- 5. Construir calendário de divulgações
- 6. Construir de material / vídeos
- 7. Divulgar nas redes sociais
- 8. Divulgar presencialmente (escolas e organizações não governamentais)

Impacto vs esforço

Impacto

Esforço

KPI

 # visualizações por postagem

Envolvidos

- **ANATEL SCO e SRC** (responsáveis)
- **# Fique Esperto**
- **Ministério da educação**

Referência

- # Fique Esperto

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	X
Reduzir golpes digitais	X

Prazo[1]

Curto (até 6 meses)

Riscos

- 1. Baixa adesão e pouca efetividade; 2. Falta de constância na publicação dos informativos; 3. Falta de uma curadoria

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)

Fonte: ADVISIA OC&C

Figura 55

Subiniciativa nº 17.3: Promover conscientização de usuários não alfabetizados digitalmente e idosos contra *phishing* (Figura 56)

- Essa subiniciativa surgiu a partir do estudo de mercado, das entrevistas e do workshop, tendo como maior referência a plataforma "#FiqueEsperto" da ANATEL;
- O objetivo dessa iniciativa é realizar a conscientização de grupos específicos (idosos e pessoas não alfabetizadas digitalmente) sobre *phishing* e promover a conscientização indireta desses grupos através de mensagens para a população em geral mostrando a importância de ajudar idosos e não alfabetizados digitalmente;
- As principais atividades propostas são:
    - Definir quais redes sociais de atuação serão utilizadas para promover campanhas para grupo específico e para a população em geral;
    - Definir temática e conteúdo de divulgação;
    - Definir público-alvo;
    - Elaborar cronograma de divulgações;
    - Produzir material e vídeos;
    - Divulgar;
- O impacto é considerado alto, pois a conscientização é a maneira mais eficiente para evitar que as vítimas passem dados pessoas para terceiros através de links duvidosos, e-mails e outras meios que os fraudadores utilizam;
- O esforço é considerado baixo, levando em consideração o material já existente no "#FiqueEsperto" e a disposição da Proteste e da Polícia Federal em ajudar a Agência no combate a esse tipo de fraude;

- O KPI a ser monitorado é a quantidade de visualizações por postagem para a população em geral e a quantidade de materiais áudio visual criado para a conscientização do grupo específico;
- A Superintendência de Controle de Obrigações e a Superintendência de Relações com Consumidores serão os responsáveis pelo desenvolvimento dessa subiniciativa e deve contar com o apoio da Proteste, das grandes prestadoras de serviço de telecomunicações, da plataforma "#FiqueEsperto" e da Polícia Federal;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;
- A sua realização é considerada de curto prazo (até 6 meses)
- Os principais riscos levantados são:
    - Baixa adesão e pouca efetividade da ação;
    - Falta de constância na publicação dos informativos;
    - Falta de uma curadoria;

Plano de ação

Subiniciativa nº17.3 : Promover conscientização de usuários não alfabetizados digitalmente e idosos contra *phising*

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL + Outros

Objetivo

Criar cartilhas e vídeos curtos de no máximo 2 minutos sobre o que é e como combater ataques fraudulentos de *phising*

Atividades

- 1. Definir quais redes sociais de atuação
- 2. Definir temática e conteúdo de divulgação
- 3. Definir público-alvo
- 4. Construir calendário de divulgações
- 5. Construir de material / vídeos
- 6. Divulgar

Impacto vs esforço

Impacto

Esforço

KPI

 # de conteúdos criados e divulgados

Envolvidos

- **ANATEL SCO e SRC** (responsáveis)
- **Proteste**
- **Grandes Operadoras**
- **# Fique Esperto**
- **Polícia Federal**

Referência

- # Fique Esperto
- Cartilhas polícia civil SP
- Ofcom

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	X
Reduzir golpes digitais	X

Prazo[1]

Curto (até 6 meses)

Riscos

- 1. Baixa adesão e pouca efetividade; 2. Falta de constância na publicação dos informativos; 3. Falta de uma curadoria

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 56

Subiniciativa nº 17.4: Realizar campanhas focadas em idosos, adolescentes e usuários não alfabetizados digitalmente para combate ao *spoofing* (Figura 57)

- Essa subiniciativa surgiu a partir do estudo de mercado, das entrevistas e do workshop, tendo como maior referência a plataforma "#FiqueEsperto" da ANATEL;
- O objetivo dessa iniciativa é realizar a conscientização de grupos específicos (idosos e pessoas não alfabetizadas digitalmente) sobre *spoofing*;
- As principais atividades propostas são:
    - Definir quais redes sociais de atuação;
    - Definir temática e conteúdo de divulgação;
    - Definir público-alvo;
    - Elaborar cronograma de divulgações;
    - Produzir material e vídeos;
    - Divulgar;
- O impacto é considerado alto, pois a conscientização é fundamental para que a vítima saiba que o fraudador está se passando por uma empresa ou instituição, evitando assim possíveis fraudes;
- O esforço é considerado baixo, levando em consideração o material já existente no "#FiqueEsperto" e a disposição da Proteste e da Polícia Federal em ajudar a Agência no combate a esse tipo de fraude;
- O KPI a ser monitorado é a quantidade de visualizações por postagem;
- A Superintendência de Controle de Obrigações e a Superintendência de Relações com Consumidores serão os responsáveis pelo desenvolvimento dessa subiniciativa e deve contar com o apoio da Proteste, das grandes prestadoras de serviço de telecomunicações, da plataforma "#FiqueEsperto" e da Polícia Federal;

- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;
- A sua realização é considerada de curto prazo (até 6 meses)
- Os principais riscos levantados são:
    - Baixa adesão e pouca efetividade da ação;
    - Falta de constância na publicação dos informativos;
    - Falta de uma curadoria;

Plano de ação

Subiniciativa nº17.4 : Realizar campanhas focadas em idosos, adolescentes e usuários não alfabetizados digitalmente para combate ao *spoofing*

Propostas de Plano de Ação

Legenda: ● Alto ◔ Baixo

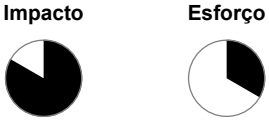
ANATEL + Outros

Objetivo	Promover campanhas massivas de conscientização para usuários a respeito de *Spoofing,* aumentando a confiança e o conhecimento dos usuários

Atividades

- 1. Definir quais redes sociais de atuação
- 2. Definir temática e conteúdo de divulgação
- 3. Definir público-alvo
- 4. Construir calendário de divulgações
- 5. Construir de material / vídeos
- 6. Divulgar

Impacto vs esforço



KPI

 # de conteúdos criados e divulgados

Envolvidos

- **ANATEL SCO e SRC** (responsáveis)
- **Proteste**
- **Grandes Operadoras**
- **# Fique Esperto**
- **Polícia Federal**

Referência

- # Fique Esperto
- *Action Fraud Police (UK)*
- Ofcom

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	X
Reduzir golpes digitais	X

Prazo[1]

Curto (até 6 meses)

Riscos

- 1. Baixa adesão e pouca efetividade; 2. Falta de constância na publicação dos informativos; 3. Falta de uma curadoria

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 57

Subiniciativa nº 17.5: Realizar acompanhamento para diminuir fraudes de 0800 (Figura 58)

- Essa subiniciativa surgiu a partir das entrevistas e do workshop, em que foi relatada a alta eficiência dos fraudadores em capturar dados dos clientes pela credibilidade passada em se usar número 0800 e 0300;
- O objetivo desta subiniciativa é combater as centrais de atendimentos fraudulentas que utilizam números 0800 e 0300. Uma possibilidade para combater esse tipo de é o desenvolvimento de mecanismos para promover a segurança associada à utilização dos números;
- As principais atividades propostas são:
    - Promover conversa com operadoras;
    - Criar procedimentos para enrijecer o cadastro de clientes;
    - Aumentar a fiscalização;
- O impacto é considerado alto, pois o combate às centrais de atendimentos fraudulentas é uma das maneiras mais eficientes para mitigar esse tipo de fraude;
- O esforço é considerado baixo, pois a complexidade para se desenvolver mecanismos para a promoção da segurança associada à utilização dos números é relativamente baixa;
- O KPI a ser monitorado é o número de reclamações feitas para a ANATEL sobre centrais de atendimento falsas;
- A Superintendência de Controle de Obrigações será a responsável pelo desenvolvimento dessa subiniciativa;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;
- A sua realização é considerada de curto prazo (até 6 meses)
- O principal risco levantado é o baixo engajamento das prestadoras de serviço de telecomunicações;

Plano de ação

Subiniciativa nº17.5 : Realizar acompanhamento para diminuir fraudes de 0800

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL

Objetivo	Combater fraudes de central de atendimento falsa criando procedimentos para mitigar a contratação do serviço por pessoas ou empresas mal intencionadas

Atividades

- 1. Promover conversa com operadoras
- 2. Criar procedimentos para enrijecer o cadastro de clientes
- 3. Aumentar a fiscalização

Impacto vs esforço

Impacto	Esforço
	

KPI

 # de reclamações sobre centrais falsas

Envolvidos

- **ANATEL SCO** (responsável)

Referência

- n/a

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	X
Reduzir golpes digitais	X

Prazo[1]

Curto (até 6 meses)

Riscos

- 1. Baixo engajamento das operadoras

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 58

3.6. Detalhamento das subiniciativas aconselháveis

As subiniciativas analisadas nesta seção são aquelas classificadas na matriz de impacto *versus* esforço como “aconselháveis”, ou seja, a serem implementadas na sequência daquelas classificadas como “prioritárias”, a saber: nº 17.6 a 17.12.

Subiniciativa nº 17.6: Fomentar a participação da ANATEL em fóruns e seminários (Figura 59)

- Essa subiniciativa surgiu a partir de interesses internos da Agência e do estudo realizado;
- O objetivo desta subiniciativa é inserir a ANATEL em fóruns e seminários relacionados ao tema de fraude digital e cibersegurança. Foram mapeados fóruns nacionais e internacionais. Existe a possibilidade de a própria Agência criar um fórum e/ou seminários periódicos para o debate do tema;
- As principais atividades propostas são:
    - Mapear fóruns e seminários existentes sobre o tema fraude;
    - Fazer inscrições nos fóruns e seminários selecionados;
    - Participar dos eventos e discussões sobre o tema;
- O *impacto* é considerado médio, pois a ação não combate às fraudes de maneira direta, gerando apenas insumo sobre o tema;
- O *esforço* é considerado baixo, pois a complexidade das atividades é baixa;
- O KPI a ser monitorado é a quantidade de fóruns e seminários associados sobre o tema fraude digital que a ANATEL se engajar;
- A Superintendência de Controle de Obrigações será a responsável pelo desenvolvimento dessa subiniciativa;

- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes (mesmo que seja obtido de forma indireta, através do networking e informações compartilhadas);
- A sua realização é considerada de curto prazo (até 6 meses)
- O principal risco levantado é o baixo engajamento interno ou falta de participação ativa nos fóruns e seminários selecionados;

Plano de ação

Subiniciativa nº17.6 : Fomentar a participação da ANATEL em fóruns e seminários

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL

Objetivo	Inserir a ANATEL nas discussões relacionadas com o tema fraude digital, fomentando troca de conhecimentos e engajamento interno na agencia

Atividades

- 1. Mapear fóruns e seminários existentes sobre o tema fraude
- 2. Fazer inscrição
- 3. Participar dos eventos e discussões sobre o tema

Impacto vs esforço

Impacto | Esforço

KPI

 # fóruns associados
 # seminários inscritos

Envolvidos

- **ANATEL SCO** (responsável)

Referência

- CFCA

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	
Reduzir golpes digitais	

Prazo[1]

Curto (até 6 meses)

Riscos

- 1. Baixo engajamento interno ou falta de constância na participação

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 59

Subiniciativa nº 17.7: Incentivar o uso de modems residenciais cuja avaliação de conformidade tenha contemplado os requisitos de segurança (Figura 60)

- Essa subiniciativa surgiu a partir das entrevistas com *experts* do setor e através do estudo realizado;
- O objetivo desta subiniciativa é combater fraudes relacionadas à exploração de vulnerabilidade de CPE (CPEs são dispositivos como modems, roteadores e *gateways* usados por assinantes de serviços de telecomunicações e internet para se conectar às redes dos provedores). A ANATEL deve acompanhar a implementação do Ato 2436 a fim de garantir que sejam homologados pela Agência somente equipamentos CPEs que atendam os requisitos mínimos de segurança estabelecidos no Ato;
- As principais atividades propostas são:
    - Promover conversas com fabricantes de CPEs e com as prestadoras de serviço de telecomunicações;
    - Propor calendário para atualização da certificação de aparelhos defasados já homologados;
    - Realizar o monitoramento sobre a substituição dos equipamentos defasados na forma estabelecida no Despacho Decisório 48/2021/COQL/SCO (SEI 7363344);
    - Revisar e atualizar norma de segurança periodicamente;
- O impacto é considerado alto, pois a substituição de aparelhos defasados para aparelhos que possuem proteção mínima de segurança da informação cria uma barreira contra fraudes e ataques cibernéticos;
- O esforço é considerado alto, devido ao grande número de dispositivos defasados presentes no mercado e a diversidade de fornecedores;
- Os KPIs a serem monitorados são:

- A quantidade de equipamentos cujo processo de conformidade atenda o Ato n.º 2436/23;
- A quantidade de equipamentos homologados antes de 10/03/2024 que atualizaram sua certificação para atendimento ao Ato n.º 2436/23;
- A quantidade de equipamentos defasados instalados nas redes das prestadoras

- A Superintendência de Controle de Obrigações junto com a Superintendência de Outorga e Recursos à Prestação serão os responsáveis pelo desenvolvimento dessa subiniciativa;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;
- A sua realização é considerada de alto prazo (acima de 1 ano)
- Os principais riscos levantados são:
  - Baixo engajamento dos fabricantes de equipamentos;
  - Dificuldade técnica para identificar os equipamentos;

Plano de ação

Subiniciativa nº17.7 : Incentivar o uso de modems residenciais cuja avaliação de conformidade tenha contemplado os requisitos de segurança

Propostas de Plano de Ação

Legenda: ● Alto ◔ Baixo

ANATEL

Objetivo	Combater fraudes relacionadas a exploração de vulnerabilidade de CPE

Atividades

- 1. Promover conversas com fabricantes de CPEs e com as prestadoras de serviço de telecomunicações;
- 2. Propor calendário para atualização da certificação de aparelhos defasados já homologados;
- 3. Realizar o monitoramento sobre a substituição dos equipamentos defasados na forma estabelecida no Despacho Decisório 48/2021/COQL/SCO (SEI 7363344);
- 4. Revisar e atualizar norma de segurança periodicamente

Impacto vs esforço

Impacto	Esforço
●	●

KPI

 # equipamentos que atenda o Ato nº 2436/23
 # equipamentos homologados antes de 10/03 atendendo o Ato nº 2436/23
 # equipamentos defasados instalados nas redes das prestadoras

Envolvidos

- **ANATEL SCO** (responsável)

Referência

- Ato n.º 2436/23

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	X
Reduzir golpes digitais	X

Prazo[1]

Alto (acima de 1 ano)

Riscos

- 1. Baixo engajamento dos fabricantes de equipamento

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 60

Subiniciativa nº 17.8: Criar procedimentos específicos contra fraudes oriundas em *brokers* (Figura 61)

- Essa subiniciativa surgiu a partir das entrevistas com o mercado e através do workshop;
- O objetivo desta subiniciativa é combater fraudes oriundas em *brokers*[71] (os brokers de telecomunicações são empresas que facilitam a negociação de serviços de telecomunicações entre operadoras de telecomunicações, provedores de serviços e clientes finais), como por exemplo, através do envio massivo de SMS fraudulentos, quando o fraudador tenta induzir a vítima a clicar em algum *link* malicioso ou a entrar em contato com alguma central de atendimento falsa;
- As principais atividades propostas são:
    - Promover conversas com as prestadoras de serviço e com os *brokers;*
    - Propor procedimentos que visam ao combate às fraudes envolvendo o envio de mensagens automáticas;
    - Realizar o monitoramento periódico;
- O impacto é considerado alto, pois a criação de procedimentos específicos para contra fraudes nas empresas de brokers é uma forma efetiva no combate e prevenção, pois ele atinge a raiz do problema;
- O esforço é considerado alto, devido à complexidade do problema e de como ele está relacionado o modelo de negócio, como por exemplo, envio de e-mails marketing;
- O KPI a ser monitorado é o número de procedimentos criados;

[71] INTERNATIONAL TELECOMMUNICATION UNION. Telecommunication Service Brokers: ITU-T E.391, 2013.

- A Superintendência de Controle de Obrigações junto com a Superintendência de Planejamento e Regulação (responsável pela liderança do Grupo Técnico de Suporte à Segurança Pública) serão as responsáveis pelo desenvolvimento dessa subiniciativa
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;
- A sua realização é considerada de alto prazo (acima de 1 ano)
- Os principais riscos levantados são:
    - Impacto dos procedimentos no modelo de negócio dos *brokers*;
    - Dificuldade técnica para se desenvolver soluções;

Plano de ação

Subiniciativa nº17.8 : Criar procedimentos específicos contra fraudes oriundas em *brokers*

Propostas de Plano de Ação

Legenda: ● Alto ◔ Baixo

ANATEL

Objetivo	Combater fraudes de phishing por SMS, mensagens de spam, assinatura de serviço e outros, criando procedimentos contra fraudes para *brokers*

Atividades

- 1. Promover conversas com fabricantes com empresas que utilizam *brokers*
- 2. Propor procedimentos que visam o combate à fraudes envolvendo o envio de mensagens automáticas
- 3. Realizar o monitoramento periódico

Impacto vs esforço

Impacto	Esforço
●	●

KPI

 # de procedimentos criados

Envolvidos

- **ANATEL SCO** (responsável)

Referência

- Ato n.º 2436/23

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	X
Reduzir golpes digitais	X

Prazo[1]

Alto (acima de 1 ano)

Riscos

- 1. Impacto dos procedimentos no modelo de negócio dos *brokers* 2. Dificuldade técnica para se desenvolver soluções

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)

Fonte: ADVISIA OC&C

Figura 61

Subiniciativa nº 17.9: Avaliar a criação de procedimento de compartilhamento de informações para identificar comportamentos fraudulentos entre diferentes setores da economia (Figura 62)

- Essa subiniciativa surgiu a partir das entrevistas com o mercado financeiro e com as polícias;
- O objetivo desta subiniciativa é avaliar a viabilidade e desenvolver um procedimento de compartilhamento de informações entre diferentes setores da economia, com o intuito de identificar comportamentos fraudulentos. O procedimento será criado com base em análises de dados e informações coletadas, para possibilitar a identificação de padrões e comportamentos suspeitos, que possam indicar a ocorrência de atividades fraudulentas em diferentes áreas da economia. Com essa avaliação, busca-se aumentar a eficácia na prevenção e combate a fraudes, bem como aprimorar a integração e colaboração entre setores, contribuindo para a proteção dos interesses e direitos de consumidores e empresas.
- As principais atividades propostas são:
    - Avaliar viabilidade jurídica da subiniciativa;
    - Identificar os setores da economia que poderão participar do procedimento e formalizar convênios e acordos de cooperação com as entidades representativas desses setores;
    - Estabelecer uma estrutura organizacional para gerenciar o procedimento de compartilhamento de informações, definindo as funções e responsabilidades dos agentes envolvidos;
    - Definir as informações relevantes que serão compartilhadas entre os setores, garantindo a proteção de dados pessoais e comerciais, e estabelecer os mecanismos e padrões de comunicação para o compartilhamento dessas informações;

- Elaborar um plano de capacitação para os agentes envolvidos, com o objetivo de garantir a compreensão e aderência aos procedimentos e padrões de comunicação definidos;
- Realizar testes e simulações para validar a efetividade do procedimento de compartilhamento de informações e realizar ajustes necessários antes da implementação final;

- O impacto é considerado alto, pois o compartilhamento de informações para identificar comportamentos fraudulentos pode ajudar a indústria em limitar a possibilidade de realização desses golpes;
- O esforço é considerado alto, devido à complexidade de manutenção e compartilhamento da base de dados;
- O KPI a ser monitorado é a quantidade de empresas compartilhando dados na base;

a. A Superintendência de Controle de Obrigações junto com a Superintendência de Planejamento e Regulamentação (responsável pela liderança do Grupo Técnico de Suporte à Segurança Pública) serão os responsáveis pelo desenvolvimento dessa subiniciativa, junto às grandes prestadoras de serviço de telecomunicações e as polícias;

- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes e reduzir os golpes digitais;
- A sua realização é considerada de médio prazo (6 meses até 1 ano)
- Os principais riscos levantados são:
  - Dificuldade para atualização da base de dados;
  - Baixo engajamento das prestadoras de telecomunicações;
  - Barreiras jurídicas

Plano de ação

Subiniciativa nº17.9 : Avaliar a criação de procedimento de compartilhamento de informações para identificar comportamentos fraudulentos

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL + Outros

Objetivo

Combater fraudes de autenticação, *onboarding* e cadastro em setores como o bancário e varejo

Atividades

- 1. Avaliar viabilidade jurídica da subiniciativa
- 2. Estabelecer estrutura de participantes e formalizar convênios e acordos
- 3. Estabelecer estrutura organizacional para gerenciamento de informações
- 4. Definir informações e padrões de comunicação
- 5. Elaborar plano de capacitação
- 6. Realizar testes e ajustes

Impacto vs esforço

Impacto

Esforço

KPI

 # empresas compartilhando base

Envolvidos

- **ANATEL SCO** (responsável)
- **Grandes Operadoras**
- **Polícia civil**
- **Polícia federal**
- **Mercado Financeiro**

Referência

- Projeto pré-pago
- Cadastro pré

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	
Reduzir golpes digitais	X

Prazo[1]

Médio (6 meses até 1 ano)

Riscos

- 1. Dificuldade para atualização da base de dados; 2. Baixo engajamento das operadoras; 3. Barreiras jurídicas

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 62

Subiniciativa nº 17.10: Avaliar aprimoramentos dos mecanismos para dificultar o sequestro de terminal (Figura 63)

- Essa subiniciativa surgiu a partir das entrevistas com o mercado, estudo realizado e procedimentos já existentes;
- O objetivo desta subiniciativa é aprimorar os mecanismos já existentes contra o sequestro de terminais, para combater a fraude de SIM Swap. Exemplo: limitar acesso de funcionários, criar planos de contingência quando for detectado o sequestro de terminal e assim por diante. Também é recomendado melhorias na relação empresa - colaborador;
- As principais atividades propostas são:
    - Definir grupo responsável pela coordenação do projeto (GT-SEG ou SGT-Fraudes);
    - Definir fórum de discussão (associações e operadoras);
    - Definir dinâmica do fórum (workshops, periodicidade e entre outros);
    - Construir material guia contento tendências envolvendo fraudes de SIM Swap;
    - Conduzir workshop;
    - Coletar principais percepções;
    - Criar plano de ação baseado nas percepções;
- O impacto é considerado médio, pois mesmo que esses mecanismos sejam eficientes parte das fraudes de SIM Swap são de origens internas (proveniente da má conduta de funcionários);
- O esforço é considerado médio, pois já existem mecanismos com a finalidade de dificultar o sequestro de terminais e eles precisarão ser redesenhados ou será preciso discutir novos processos;
- O KPI a ser monitorado é a quantidade de mecanismos já existentes foram reavaliados / atualizados;

- A Superintendência de Controle de Obrigações junto com a Superintendência de Planejamento e Regulação (responsável pela liderança do Grupo Técnico de Suporte à Segurança Pública) serão as responsáveis pelo desenvolvimento dessa subiniciativa, junto com as grandes prestadoras de serviço de telecomunicações, associações, FEBRABAN, bancos e o Bacen;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes e reduzir os golpes digitais;
- A sua realização é considerada de médio prazo (6 meses até 1 ano)
- Os principais riscos levantados são:
    - Baixa adesão das prestadoras de serviço de telecomunicações;
    - Dificuldade técnica para propor soluções de aprimoramentos dos mecanismos para dificultar o sequestro de terminal;

Plano de ação

Subiniciativa nº17.10 : Avaliar aprimoramentos dos mecanismos para dificultar o sequestro de terminal

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL + Outros

Objetivo

Diminuir o número de fraudes de *SIM Swap*, promovendo discussões com operadoras com o intuito de se avaliar aprimoramentos das medidas de segurança

Atividades

- 1. Definir grupo responsável pela coordenação do projeto (GT-Ciber ou GT-Seg)
- 2. Definir fórum de discussão (associações e operadoras)
- 3. Definir dinâmica do fórum (workshops, periodicidade e entre outros)
- 3. Construir material guia contento tendências envolvendo fraudes de *SIM Swap*
- 4. Conduzir workshop
- 5. Coletar principais percepções
- 6. Criar plano de ação baseado nas percepções

Impacto vs esforço

Impacto

Esforço

KPI

 # de mecanismos atualizados / revisados

Envolvidos

- **ANATEL SCO** (responsável)
- **Grandes Operadoras**
- **Associações**
- **Bacen**
- **FEBRABAN**
- **Bancos**

Referência

- Europol

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	
Reduzir golpes digitais	X

Prazo[1]

Médio (6 meses até 1 ano)

Riscos

- 1. Baixa adesão das operadoras

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 63

Subiniciativa nº 17.11: Elaborar relatórios periódicos relacionados a fraudes reportadas para a ANATEL (Figura 64)

- Essa subiniciativa surgiu a partir de entrevistas internas com o time ANATEL;
- O objetivo desta subiniciativa é estabelecer diretrizes e procedimentos para o monitoramento e análise das fraudes e ataques cibernéticos reportados para a Agência via canal de reclamação;
- As principais atividades propostas são:
    - Definir time de trabalho;
    - Criar processo para compartilhamento periódico das fraudes reportadas via registro de reclamações (essa atividade está relacionada com a subiniciativa 17.15, responsável pela adequação da árvore e canais de atendimento ao cliente, a fim de auxiliar na extração a análise dos dados provenientes das reclamações feitas à agência);
    - Elaborar relatório sobre fraudes;
    - Divulgar;
- O impacto é considerado médio, pois não é uma ação que tem impacto direto ao combate e prevenção às fraudes;
- O esforço é considerado médio, pois já existe uma base de dados para ser trabalhada, porém existe a necessidade de se fazer ajustes na atual árvore de atendimento;
- O KPI a ser monitorado é a quantidade de reclamações feitas e analisadas pela ANATEL sobre o tema fraude / golpe;
- A Superintendência de Controle de Obrigações em conjunto com a Superintendência de Fiscalização e a Superintendência de Relações com Consumidores serão responsáveis pelo desenvolvimento dessa subiniciativa;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes e reduzir os golpes digitais;

- A sua realização é considerada de médio prazo (6 meses até 1 ano)
- Os principais riscos levantados são:
    - Baixo alcance dos relatórios;
    - Baixo conhecimento da população sobre o canal de reclamações da ANATEL;

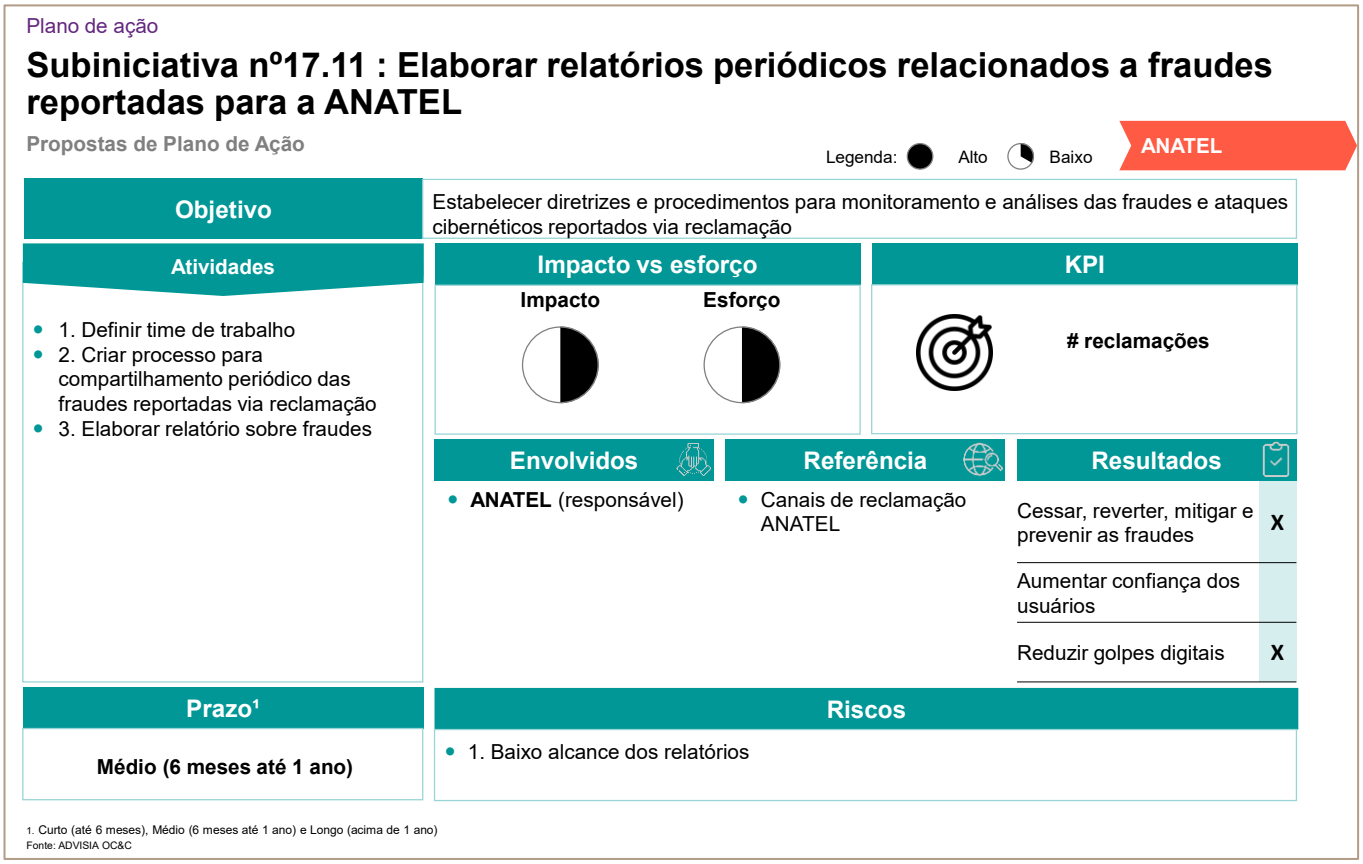


Figura 64

Subiniciativa nº 17.12: Divulgar plataforma "Cadastro Pré" para públicos específicos (Figura 65)

- Essa subiniciativa surgiu a partir de entrevistas com o mercado financeiro e as polícias;
- O objetivo desta subiniciativa é fazer a divulgação da plataforma "Cadastro Pré" para públicos específicos da sociedade, por exemplo, a polícia federal. Em um segundo momento, a Agência pode avaliar possíveis melhorias na plataforma caso haja necessidade e demanda de órgãos de segurança pública;
- As principais atividades propostas são:
    - Mapear público-alvo;
    - Elaborar cronograma de divulgações;
    - Produzir material e vídeos;
    - Divulgar;
- O impacto é considerado baixo, pois não é uma ação que tem impacto direto ao combate e prevenção às fraudes;
- O esforço é considerado baixo, devida a baixa complexidade de divulgação para públicos específicos;
- O KPI a ser monitorado é o número de consultas feitas na plataforma por mês;
- A Superintendência de Controle de Obrigações será a responsável pelo desenvolvimento dessa subiniciativa, junto com a Assessoria de Relações Institucionais da agência;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;
- A sua realização é considerada de curto prazo (até 6 meses)
- Os principais riscos levantados são:
    - Baixo alcance de divulgação;

- Falta de interesse do público-alvo;

Plano de ação

Subiniciativa nº17.12 : Divulgar plataforma "Cadastro Pré" para públicos específicos

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL

Objetivo	Divulgação da plataforma para cadastropre.com.br para entidades governamentais e mercado financeiro

Atividades

- 1. Mapear público alvo
- 2. Construir calendário de divulgações
- 3. Construir de material / vídeos
- 4. Divulgar

Impacto vs esforço

Impacto

Esforço

KPI

 # de consultas feitas por mês

Envolvidos

- **ANATEL SCO e SRC** (responsáveis)

Referência

- Cadastro pré

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	X
Reduzir golpes digitais	X

Prazo[1]

Curto (até 6 meses)

Riscos

- 1. Baixo alcance da divulgação

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)

Fonte: ADVISIA OC&C

Figura 65

3.1. Detalhamento das subiniciativas cuja viabilidade precisa ser avaliada

As subiniciativas analisadas nesse bloco são aquelas cuja viabilidade precisa ser avaliada, a saber: nº 17.13 a 17.16.

Subiniciativa nº 17.13: Reavaliar imposição de limite de linhas ativas pré-pagas por CPF (Figura 66)

- Essa subiniciativa surgiu a partir de entrevistas com o mercado e workshop;
- O objetivo desta subiniciativa é reavaliar uma possível imposição de limite para linhas ativas pré-pagas por CPF, criando assim uma barreira inicial para fraudadores que utilizam números pré-pagos para cometer fraudes;
- As principais atividades propostas são:
    - Reavaliar imposição sobre limite de linhas pré-pagas por CPF;
    - Divulgar decisão para operadoras;
    - Definir processo de fiscalização;
- O impacto é considerado médio, pois não é uma ação que tem impacto direto ao combate e prevenção às fraudes;
- O esforço é considerado alto, pois demanda várias ações em conjunto com as grandes prestadoras de serviço;
- O KPI a ser monitorado é o número de linhas ativas por CPF;
- A Superintendência de Controle de Obrigações junto com a Superintendência de Planejamento e Regulamentação serão responsáveis pelo desenvolvimento dessa subiniciativa;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes e reduzir os golpes digitais;

- A sua realização é considerada de alto prazo (acima de 1 ano)
- Os principais riscos levantados são:
    - Baixo engajamento das prestadoras de serviço;
    - Uso de “CPFs laranja”;

Plano de ação

Subiniciativa nº17.13 : Reavaliar imposição de limite de linhas ativas pré-pagas por CPF

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL

Objetivo	Criar processo para garantir que o limite do número de linhas ativas para chips pré-pagos esteja sendo cumprido

Atividades

- 1. Reavaliar imposição sobre limite de linhas pré-pagas por CPF
- 2. Divulgar decisão para operadoras
- 3. Definir processo de fiscalização

Impacto vs esforço

Impacto  Esforço 

KPI

de linhas ativas por CPF

Envolvidos

- **ANATEL SCO** (responsável)

Referência

- Cadastro pré
- Resoluções nº 619/2014 e 716/2019

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	
Reduzir golpes digitais	X

Prazo[1]

Alto (acima de 1 ano)

Riscos

- 1. Baixo engajamento das operadoras; 2. Uso de CPFs laranja

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 66

Subiniciativa nº 17.14: Simplificar e melhorar a experiência do cliente nos canais de reclamação da ANATEL (Figura 67)

- Essa subiniciativa surgiu a partir de conversas internas com a ANATEL, com a tomada de subsídios e com a análise da base de dados disponibilizada pela Superintendência de Relações com Investidores;
- Os objetivos desta subiniciativa são: simplificar e melhorar a experiência do cliente nos canais oficiais de reclamação da ANATEL com intuito de incentivar a reclamação dos usuários para que a agência tenha mais insumos para poder trabalhar e simplificar e recategorizar os campos responsáveis pela categorização dos chamados de atendimento, com o intuito de facilitar a análise de dados. É recomendada a criação de opções de reclamações relacionadas com o tema fraude, golpe e ou ataques cibernéticos, garantindo assim que as reclamações sejam classificadas da forma correta e contenham as informações necessárias para servirem de subsídio à agência, inclusive para alimentar a subiniciativa 17.11;
- As principais atividades propostas são:
    - Reavaliar URA e árvore de reclamação do site;
    - Definir opções de reclamações que estarão disponíveis para os usuários (trazer opções para que os usuários possam registrar reclamações relacionadas com golpes / fraudes e ataques cibernéticos);
    - Simplificar URA e árvore de reclamação;
- O impacto é considerado médio, pois não é uma ação que tem impacto direto ao combate e prevenção às fraudes;
- O esforço é considerado alto, devido à necessidade de envolvimento de diversas áreas internas da agência;
- O KPI a ser monitorado é o número de opções de reclamações disponíveis;

- A Superintendência de Relações com Consumidores será a responsável pelo desenvolvimento dessa subiniciativa;
- A sua realização é considerada de alto prazo (acima de 1 ano)
- O resultado esperado é o aumento na confiança dos usuários;
- O principal risco levantado é o aumento da complexidade e dificuldade de entendimento pelo usuário;

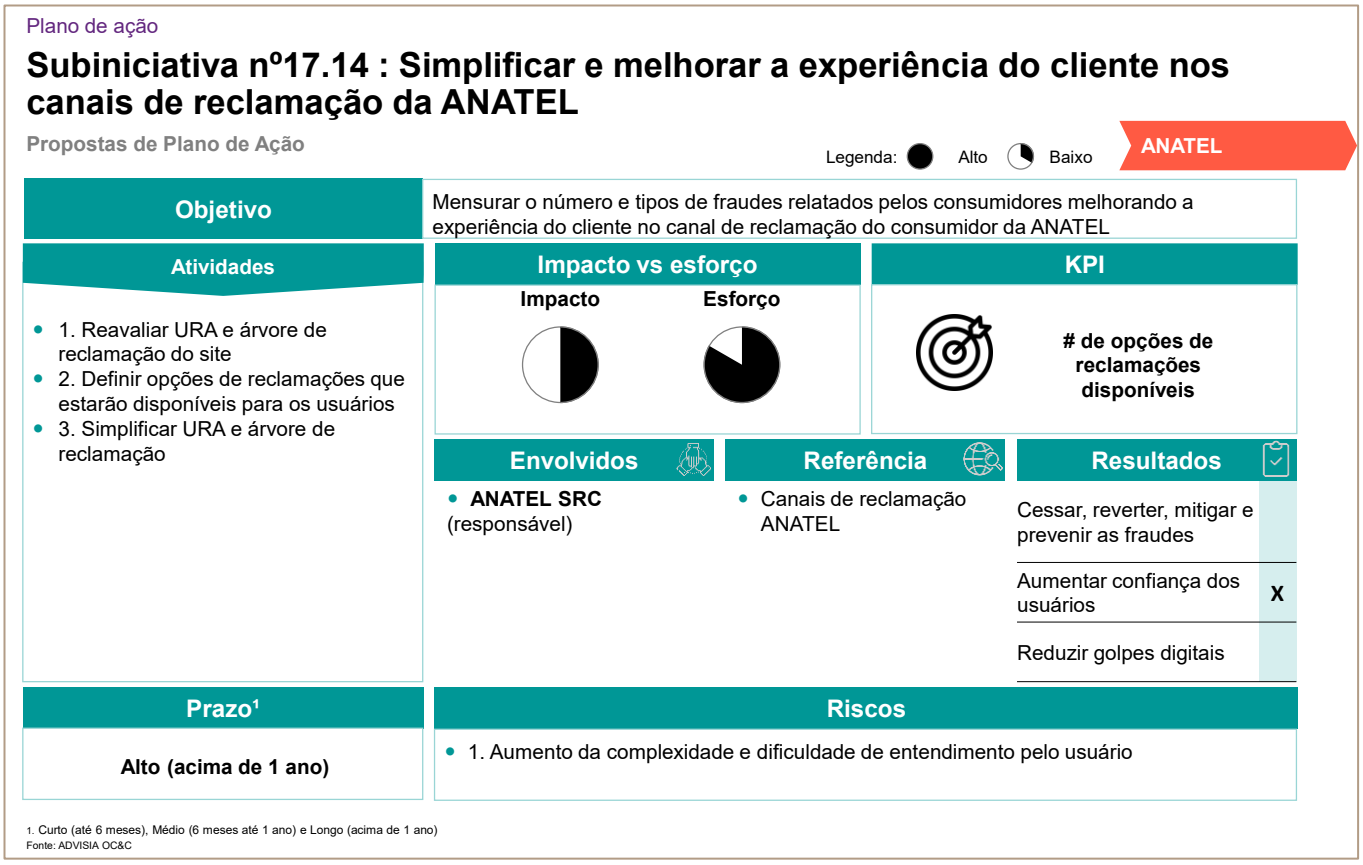


Figura 67

Subiniciativa nº 17.15: Impulsionar Projeto Cadastro Pré-pago (Figura 68)

- Essa subiniciativa surgiu a partir de entrevistas com o mercado e com o estudo realizado;
- O objetivo desta subiniciativa é impulsionar o projeto já existente chamado "Projeto Cadastro Pré-pago". A subiniciativa visa garantir que as prestadoras de serviço de telecomunicações estejam cumprindo a regulamentação aplicável e determinações da ANATEL;
- As principais atividades propostas são:
    - Reforçar fiscalizações para garantir que toda operadora esteja coletando os dados de clientes pré-pagos;
    - Garantir que o cruzamento de dados (CPF vs Nome) esteja sendo feito pelas operadoras no ato do cadastro;
    - Incentivar o uso do ID Digital pelas operadoras;
    - Garantir que banco de dados seja atualizado semestralmente;
- O impacto é considerado médio, devido a existência de vários métodos para se falsificar o cadastro;
- O esforço é considerado alto, devido à complexidade de operacionalização (coleta de dados, manutenção da base de dados, atualização da base e entre outros aspectos);
- O KPI a ser monitorado é o número de linhas pré-pagas ativas cadastradas na base;
- A Superintendência de Controle de Obrigações será a responsável pelo desenvolvimento dessa subiniciativa, junto com a Assessoria de Relações Institucionais da agência;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes, aumentar a confiança dos usuários e reduzir os golpes digitais;

- A sua realização é considerada de alto prazo (acima de 1 ano)
- Os principais riscos levantados são:
    - Baixo engajamento das prestadoras de serviço;
    - Uso de “CPFs laranjas” e falsificações no cadastro;

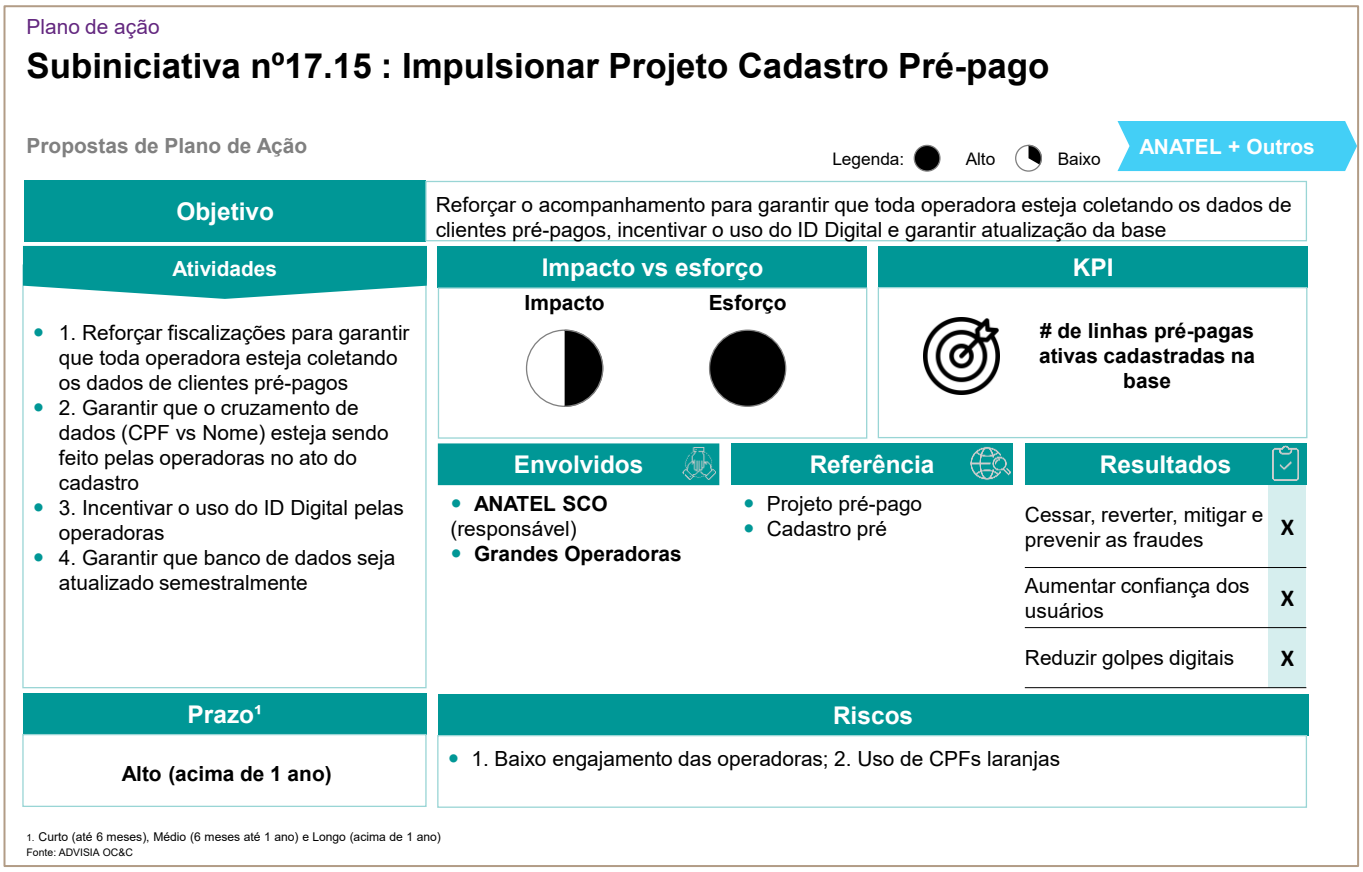


Figura 68

Subiniciativa nº 17.16: Aprimorar mecanismos para dificultar a operação de "chipeiras" utilizadas em fraudes (Figura 69)

- Essa subiniciativa surgiu a partir de conversas com *experts* e com o mercado;
- O objetivo desta subiniciativa é diminuir o número de fraudes de *robocall* e outras a partir da criação de normas e procedimentos que visam dificultar a operação de "chipeiras" (dispositivos eletrônicos que permitem a conexão simultânea de vários chips de celular em uma única máquina) utilizadas para fraudes;
- As principais atividades propostas são:
    - Definir grupo de trabalho;
    - Estabelecer regras / procedimentos claros para o uso de *gateways* de GMS e SMS ("chipeiras");
    - Criar procedimentos de fiscalização / monitoramento das empresas a fim de garantir o bom funcionamento das regras / procedimentos;
- O impacto é considerado baixo, devido à complexidade de operacionalização;
- O esforço é considerado alto, devido à complexidade envolvida em aprimorar os procedimentos já existentes envolvendo o uso ilegal das "chipeiras".
- O KPI a ser monitorado é a quantidade de regras / procedimentos criados / reajustados para o uso de gateways de GMS e SMS;
- A Superintendência de Controle de Obrigações será a responsável pelo desenvolvimento dessa subiniciativa;
- O resultado esperado é cessar, reverter, mitigar e prevenir às fraudes e reduzir os golpes digitais;
- A sua realização é considerada de alto prazo (acima de 1 ano)
- Os principais riscos levantados são:
    - Não cumprimento das regras e procedimentos estabelecidos;

- Dificuldade técnica de se criar soluções;

Plano de ação

Subiniciativa nº17.16 : Aprimorar mecanismos para dificultar a operação de "chipeiras" utilizadas em fraudes

Propostas de Plano de Ação

Legenda: Alto Baixo

ANATEL

Objetivo	Diminuir o número de fraudes de *robocall*, *phising* e entre outros criando normas e procedimentos que dificultam a criação das "chipeiras"

Atividades

- 1. Definir grupo de trabalho
- 2. Estabelecer regras / procedimentos claros para o uso de gateways de GMS e SMS ("chipeiras")
- 3. Criar procedimentos de fiscalização / monitoramento das empresas a fim de garantir o bom funcionamento das regras / procedimentos

Impacto vs esforço

Impacto

Esforço

KPI

 # regras ou procedimentos para gateways de GMS e SMS

Envolvidos

- **ANATEL SCO** (responsável)

Referência

- Federal Communication Commission

Resultados

Cessar, reverter, mitigar e prevenir as fraudes	X
Aumentar confiança dos usuários	
Reduzir golpes digitais	X

Prazo[1]

Alto (acima de 1 ano)

Riscos

- 1. Não cumprimento das regras e procedimentos estabelecidos

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)
Fonte: ADVISIA OC&C

Figura 69

Subiniciativa Transversal: Divulgar material de segurança digital por grupos prioritários (Figura 70)

- Essa subiniciativa é uma proposta transversal que surgiu a partir da elaboração do Produto VI deste projeto, a saber: “Iniciativa Estratégica nº 18 – Promover a alfabetização digital dos usuários”, que identificou uma quantidade significativa de materiais ligados à segurança digital, que necessitam de melhor divulgação;
- O objetivo é criar metodologia de divulgação de conteúdo sobre segurança digital para grupos prioritários;
- As principais atividades propostas são:
    - Alinhar com grupo “#FiqueEsperto”;
    - Realizar seleção de materiais publicados de acordo com a iniciativa de fraudes do planejamento tático da Agência;
    - Definir quais meios de comunicação serão utilizados;
    - Escolher grupo prioritário (exemplo, crianças) como piloto;
    - Criar calendário de publicações;
    - Definir responsáveis pela curadoria e gestão;
    - Definir metodologia para coleta de *feedbacks*;
    - Realizar a publicação do material;
- O impacto é considerado baixo, pois mesmo havendo uma melhor divulgação dos materiais, essa atividade não garante o entendimento das habilidades digitais;
- O esforço é considerado baixo, pois já existe material para ser divulgado e, portanto, deve ser mais bem estruturado para divulgação;
- O KPI a ser monitorado é a nota de feedback dos grupos prioritários em relação ao material;

- A Superintendência de Controle e Obrigações (SCO) será responsável pelo gerenciamento dos materiais e a Superintendência de Relacionamento com o Consumidor (SRC) dará o suporte;
- O resultado esperado é que mais pessoas tenham à disposição informações sobre segurança digital e assim minimizar que a população sofra com problemas ligados ao ambiente digital;
- A sua realização é considerada de curto prazo (até 6 meses);
- Os principais riscos levantados são:
    - Conteúdo do material não aderente para o grupo (não-atual, não efetivo, complexo etc.);
    - Divulgação ineficaz, não atingindo os grupos prioritários;

Plano de ação

Subiniciativa nº18.8: Divulgar material de segurança digital por grupos prioritários

Propostas de Plano de Ação

Legenda: ● Alto ◔ Baixo

ANATEL

Objetivo	Criar metodologia de divulgação massiva de segurança digital para grupos prioritários

Atividades

- 1. Alinhar com grupo "Fique Esperto"
- 2. Realizar seleção de materiais publicados de acordo com a iniciativa de fraudes do planejamento tático da Agência
- 3. Definir quais meios de comunicação serão utilizados
- 4. Escolher grupo prioritário (exemplo, crianças) como piloto
- 5. Criar calendário de publicações
- 6. Definir responsáveis pela curadoria e gestão
- 7. Definir metodologia para coleta de feedbacks
- 8. Realizar a publicação do material

Impacto vs esforço

Impacto  Esforço 

Revisada com a ANATEL

KPI

Nota de feedback dos grupos prioritários relação ao material

Envolvidos

- **ANATEL – Supte. SSCO** (responsável)
- **ANATEL – Supte. SRC**

Referências

- Sou digital (ONG)
- Fe.Seg (Nic.Br)
- EVG (ENAP)
- AVAMEC

Resultados

Aprendizado sobre o tema	X
Impacto intersetorial	X
Engajamento interno	X

Prazo[1]

Curto prazo (até 6 meses)

Riscos

- 1. Conteúdo do material não aderente para o grupo (não-atual, não efetivo, complexo, etc.); 2. Divulgação ineficaz não atingir os grupos prioritários

1. Curto (até 6 meses), Médio (6 meses até 1 ano) e Longo (acima de 1 ano)

Fonte: ADVISIA OC&C

Figura 70

4. Recomendações

Durante o desenvolvimento deste trabalho, foi possível entender a complexidade envolvida no tema fraude digital. As fraudes digitais representam um grande desafio para o setor de telecomunicações, visto que podem trazer prejuízos financeiros e de reputação para as empresas, além de afetar diretamente a confiança dos consumidores na utilização de serviços digitais. Portanto, é de extrema importância que sejam promovidas ações efetivas de combate, mitigação e prevenção a esses tipos de fraudes.

Dentre os principais desafios enfrentados pelas empresas de telecomunicações está a relação de se manter uma boa qualidade de serviço prestada para os usuários e soluções antifraudes que não impactem a experiência e os serviços. Processos de identificação precoce de fraudes, a adoção de medidas de segurança eficazes, o fortalecimento da educação e a conscientização dos usuários sobre práticas seguras na internet, bem como a colaboração com autoridades e órgãos reguladores para aprimorar a legislação e as políticas públicas voltadas para o combate às fraudes digitais são pontos fundamentais para que a indústria de telecomunicações diminua a quantidade de fraudes / golpes no Brasil.

Nesse contexto, com o intuito de aprimorar as ações que a ANATEL já vem fazendo para mitigar e combater às fraudes no setor, foram propostas 16 subiniciativas para serem incorporadas ao Plano Tático da Agência, seguindo-se a ordem de priorização a seguir:

1. Subiniciativas Prioritárias: 17.1 Promover conscientização para usuários sobre pronto acionamento da prestadora para casos de interrupção dos serviços, 17.2 Conscientizar usuários sobre fraudes de engenharia social, reconhecendo diferenças entre os diversos grupos sociais, 17.3 Promover conscientização de usuários não alfabetizados digitalmente e idosos contra *phishing*, 17.4 Realizar campanhas focadas em idosos, adolescentes e usuários não alfabetizados digitalmente para conscientização contra *spoofing*, 17.5 Realizar acompanhamento para diminuir fraudes de 0800;
2. Subiniciativas Aconselháveis: 17.6 Fomentar a participação da ANATEL em fóruns e seminários, 17.7 Incentivar o uso de modems residenciais cuja avaliação de conformidade tenha contemplado os requisitos de segurança, 17.8 Criar procedimentos específicos contra fraudes oriundas em brokers, 17.9 Avaliar a criação

de procedimento de compartilhamento de informações para identificar comportamentos fraudulentos entre diferentes setores da economia, 17.10 Aprimorar mecanismos para dificultar o sequestro de terminal; 17.11 Elaborar relatórios periódicos relacionados a fraudes reportadas para a ANATEL; 17.12 Divulgar plataforma "Cadastro Pré" para públicos específicos;

3. Subiniciativas de avaliação da viabilidade: 17.13 Reavaliar imposição de limite de linhas ativas pré-pagas por CPF, 17.14 Simplificar e melhorar a experiência do cliente nos canais de reclamação da ANATEL; 17.15 Impulsionar Projeto Cadastro Pré-Pago, 17.16 Aprimorar mecanismos para dificultar a operação de "chipeiras" utilizadas em fraudes;

De forma a garantir a eficácia da implementação das subiniciativas do Plano Tático, é aconselhável que se crie um grupo de trabalho multidisciplinar para organizar, gerir e executar todas as subiniciativas indicadas neste trabalho. Além disso, esse grupo de trabalho poderá complementar as subiniciativas apresentadas com outras a serem ainda criadas pela ANATEL, se aplicável, assim como reavaliar prioridades e ajustar direcionamentos. Para que esse grupo de trabalho seja instaurado é necessário:

I. Definir grupos para execução das subiniciativas;

II. Definir responsáveis pelos grupos;

III. Mapear os participantes necessários;

IV. Planejar a implementação do Plano Tático, incluindo as subiniciativas;

V. Estruturar a periodicidade das reuniões de acompanhamento das atividades;

VI. Acompanhar o progresso da implementação;

VII. Acompanhar os *KPIs* definidos em cada subiniciativa.

Dessa forma, o grupo de trabalho poderá promover o acompanhamento e a entrega das subiniciativas selecionadas para implementação, assim como revisar periodicamente o planejamento e mensurar os resultados e impactos gerados.

5. Referências

AUSTRALIA. ACMA. Do Not Call Register. Disponível em: https://www.acma.gov.au/say-no-to-telemarketers

AUSTRALIA. ACMA. Do Not Call Register. Disponível em: https://www.acma.gov.au/avoid-sending-spam

AUSTRALIA. ACMA. Do Not Call Register. Disponível em: https://www.acma.gov.au/rules-mobile-premium-services

AUSTRALIA. ACMA. Identity Checks for Prepaid Mobile Carriage Services, 2017. Disponível em: https://www.legislation.gov.au/Details/F2017L00399

Black's Law Dictionary. 10ª edição, 2014. Disponível em: https://thelawdictionary.org/fraud/

BRASIL. ANATEL. Resolução 73. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/1998/34-resolucao-73

BRASIL. Código Penal (Art 307 e 308). Disponível em: https://www.jusbrasil.com.br/busca?q=art.+307+e+308+do+c%C3%B3digo+penal

BRASIL. Gabinete de Segurança Institucional. Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/glossario-de-seguranca-da-informacao-1

BRASIL. Ministério da Justiça e Segurança Pública. Portais referentes a defesa do consumidor. Disponível em: consumidor.gov.br; sindecnacional.mj.gov.br/

BRASIL. Polícia Civil SP. Delegacia de crimes cibernéticos. Disponível em: https://www.policiacivil.sp.gov.br/portal/faces/pages_home/institucional/departamentosOrgaos/departamentosOrgaosDetalhes?titulo=DEIC&collectionId=980175918762000603&_afrLoop=10967363525131 78&_afrWindowMode=0&_afrWindowId=null#!%40%40%3F_afrWindowId%3Dnull%26collectionId%3D980175918762000603%26_afrLoop%3D1096736352513178%26titulo%3DDEIC%26_afrWindowMode%3D0%26_adf.ctrl-state%3Dnad7gddah_4

BRASIL. Polícia Civil SP. Delegacia Virtual. Disponível em: https://www.ssp.sp.gov.br/acoes/leAcoes.aspx?id=33364.

BRASIL. Polícia Civil. Campanhas de conscientização. Disponível em: https://www.policiacivil.sp.gov.br/portal/imagens/CRIMES%20CIBERN%C3%89TICOS%20-%20PERGUNTAS%20E%20RESPOSTAS%20V2.pdf

BRASIL. Polícia Federal. Unidade de combate a crimes cibernéticos. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos

BRASIL. Código Penal Brasileiro (Decreto-Lei nº 2.848/1940). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm

BRASIL. Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Brasília: Presidência da República, 2018

Cambridge Dictionary. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/scam

CERT.br. Atuação. Disponível em: https://cert.br/sobre/

COAF. Conselho de Controle de Atividades Financeiras. Disponível em: https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-atividade-de-supervisao

COLÔMBIA. CRC. Presentations. Disponível em: https://www.slideshare.net/ComisindeRegulacinde/presentations

Communications Fraud Control Association. Fraud Loss Survey Report, 2021

EUA. Federal Communications Commission. Disponível em: https://www.fcc.gov/spoofed-robocalls

EUA. Code of Federal Regulations. Title 47. Disponível em: https://www.ecfr.gov/current/title-47

EUA. Federal Communications Commission. FCC Rules. Disponível em: https://www.fcc.gov/protecting-your-personal-data#:~:text=FCC%20rules%20protect%20customer%20proprietary,consumer%2C%20such%20as%20call%20waiting.

EUA. Federal Communications Commission. Intermediate Provider Registry. Disponível em: https://opendata.fcc.gov/dataset/Intermediate-Provider-Registry

EUA. Federal Communications Commission. STIR/SHAKEN. Disponível em: https://www.fcc.gov/call-authentication

EUA. Federal Communications Commission. Truth-in-Billing. Disponível em: https://www.fcc.gov/general/truth-billing-policy

EUA. Federal Trade Commission. Call It Quits. Disponível em: https://www.ftc.gov/business-guidance/blog/2019/06/operation-call-it-quits-theres-no-quit-our-fight-against-illegal-robocalls

EUROPOL. Disponível em: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/sim-swapping-%E2%80%93-mobile-phone-scam

Experian. Relatório Global de Identidade e Fraude, 2022

FEBRABAN. Campanhas de conscientização contra fraudes. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/bancos-promovem-campanha-de-conscientizacao-digital-contra-fraudes

FEBRABAN. Laboratório de Segurança Cibernética. Disponível em: https://portal.febraban.org.br/pagina/3322/1108/pt-br/lab-seguranca-cibernetica

Instituto Nacional de Tecnologia da Informação. Sobre o ITI, 2021. Disponível em: https://www.iti.gov.br/institucional/sobre-o-iti

INTERNATIONAL TELECOMMUNICATION UNION. Telecommunication Service Brokers: ITU-T E.391, 2013.

IRIS. Contribuições sobre incidentes de segurança. Disponível em: https://irisbh.com.br/publicacoes/tomada-de-subsidios-2-2021-da-autoridade-nacional-de-protecao-de-dados-contribuicoes-do-iris-sobre-incidentes-de-seguranca/

IRIS. Projeto de rastreabilidade de mensagens privadas. Disponível em: https://irisbh.com.br/projetos/comunicacoes-privadas-investigacoes-e-direitos/

IRIS. Publicações diversas. Disponível em: https://irisbh.com.br/publicacoes/

IRIS. Publicações relacionadas com o tema fraude. Disponível em: https://irisbh.com.br/?s=fraude

LexisNexis. Relatório O Real Custo das Fraudes América Latina, 2021

MÉXICO. IFT. Disponível em: https://www.ift.org.mx/industria/homologacion-evaluacion-conformidad

Mordor Intelligence. Report Global Cybersecurity Market (2022-2027)

Mordor Intelligence. Report Global Cybersecurity Market (2022-2027)

Mordor Intelligence. Report Global Fraud Detection and Prevention Market

Movimento Código Brasil. Disponível em: https://brasilemcodigo.com.br/

PicPay. Disponível em: https://blog.picpay.com/golpe-do-falso-sequestro/

PROCON. Campanhas de conscientização. Disponível em: https://www.almg.gov.br/comunicacao/noticias/arquivos/Procon-lanca-a-campanha-desligueotelefone/

REINO UNIDO. Fraud Taskforce. Disponível em: https://www.gov.uk/government/publications/joint-fraud-taskforce-partner-organisations/joint-fraud-taskforce-partner-organisations

REINO UNIDO. Ofcom and ICO. Disponível em: https://www.ofcom.org.uk/news-centre/2021/tackling-nuisance-calls

REINO UNIDO. Phone-paid Services. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/833921/PSA_Annual_Report_and_Accounts_2018_2019.pdf

REINO UNIDO. Ofcom. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0018/232074/statement-tackling-scam-calls-and-texts.pdf

SaferNet Brasil. Campanhas de conscientização sobre golpes e fraudes. Disponível em: https://new.safernet.org.br/?field_subject_value=Seguran%C3%A7a%20Digital&field_seguran_a_digital_value[]=Dados%20Pessoais&field_seguran_a_digital_value[]=Compras%20Online&field_type_value=All

SaferNet. Disponível em: https://new.safernet.org.br/

Serasa. Disponível em: https://www.serasa.com.br/premium/blog/boleto-falso-4-sinais-para-identificar/

Serasa. Disponível em: https://www.serasa.com.br/premium/blog/golpe-da-mao-fantasma-dicas-para-se-proteger/?gclid=CjwKCAjwov6hBhBsEiwAvrvN6AMjDgc25VQjSAsU

Serasa. Disponível em: https://www.serasa.com.br/premium/blog/whatsapp-clonado/

Telesintese. Disponível em: https://www.telesintese.com.br/empresa-identifica-uso-fraudulento-de-numeros-0800/

UFMG. CPDEE. Disponível em: https://delt.eng.ufmg.br/historia/

UNICAMP. LASCA. Disponível em: https://ic.unicamp.br/pesquisa/projetos-e-laboratorios-de-pesquisa/

USP. LARC. Disponível em: https://cursos.larc.usp.br/sobre-o-lar

Conforme o contrato CTR-S-BDT-2023-006 firmado entre ADVISIA OC&C STRATEGY CONSULTANTS e UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES (UIT), para o projeto de apoio à implementação do Plano Tático da ANATEL para o período de 2023-24, formalizamos a entrega do produto:

Produto V – Zelar pela prevenção contra fraudes no ecossistema digital

Para a elaboração deste produto foram desenvolvidas as atividades acordadas entre a ADVISIA, UIT e ANATEL.

O presente produto é composto por:
- Relatório do Plano de Ação, em PDF;
- Apresentação de slides, em formato PDF;
- Perguntas disponibilizadas via Tomada de Subsídios nº 04/2023, em formato PDF;
- Contribuições recebidas via Tomada de Subsídios nº 04/2023, em formato de planilha de Excel;

Eu, abaixo-assinado, certifico que estou devidamente autorizado pela ADVISIA OC&C STRATEGY CONSULTANTS, CNPJ nº 03.625.874/0001-22, para assinar este documento.

Assinatura: DocuSigned by: Daniel Kitawara Wada 70F6B08C1B164CA...
Nome: Daniel Kitawara Wada
Título/Cargo: Sócio
Telefone: +55 11 3053-0434, +55 11 96843-1663
E-mail: daniel.wada@advisia.com

Razão social: ADVISIA CONSULTORIA DE GESTAO EMPRESARIAL S.S.
CNPJ: 03.625.874/0001-22
Endereço completo: AV JUSCELINO KUBITSCHEK, 1726, ANDAR 22 CONJ 221 E 223 - VILA OLIMPIA, SAO PAULO – SP CEP: 04543-000
Telefone: +55 11 3053 0434
E-mail: advisia@advisia.com

Data: 28/04/2023

ANATEL
Agência Nacional de Telecomunicações
SAUS, Quadra 6, Bloco H, 10º Andar, Ala Norte - Bairro Asa Sul, Brasília/DF, CEP 70070-940
Telefone: (61) 2312-2010 - https://www.gov.br/anatel

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 53500.062890/2023-73
Importante: O Acesso Externo do SEI (www.anatel.gov.br/seiusuarioexterno) possibilita o Peticionamento Eletrônico para abrir Processo Novo e Intercorrente, podendo utilizar a segunda opção para responder este Ofício. Página de Pesquisa Pública do SEI: www.anatel.gov.br/seipesquisa

Ofício nº 589/2023/GPR-ANATEL

À Senhora
SÔNIA FAUSTINO MENDES
Secretária-Executiva
Ministério das Comunicações
Esplanada dos Ministérios, Bloco R, Zona Cívico-Administrativa
CEP: 70044-900 – Brasília/DF

Assunto: **Requerimento de Informação nº 1820/2023, de autoria do Deputado Federal Marcos Pereira .**

Referência: Processo nº 53115.017628/2023-18.

Senhora Secretária,

1. Refiro-me ao Ofício nº 19600/2023/MCOM (SEI-10540672), de 10 de julho de 2023, por meio do qual essa Secretaria-Executiva encaminha para análise e manifestação desta Agência, o Requerimento de Informação nº 1820/2023 (SEI-10540665), de autoria do Deputado Federal Marcos Pereira (Republicanos/SP), que requer informações "sobre a ocorrência de fraudes nos processos que envolvem a portabilidade de celulares, prática conhecida no mercado como SIM SWAP" em uma série de questionamentos.

2. Relativamente ao assunto, encaminha-se, em anexo, o Informe nº 274/2023/COGE/SCO, elaborado pela Superintendência de Controle de Obrigações desta Agência, que presta os esclarecimentos pertinentes.

3. A Anatel permanece à disposição para outros esclarecimentos que porventura se façam necessários.

Anexos:
I - Requerimento de Informação nº 1820/2023 (SEI nº 10540665)
II - Ofício nº 19600/2023/MCOM (SEI nº 10540672)
III - Informe nº 274/2023/COGE/SCO (SEI nº 10631797)
IV - Informe nº 540/2023/COGE/SCO (SEI nº 10625577)
V - Manual Operacional da Portabilidade (SEI nº 10625576)
VI - Plano Estratégico da ANATEL 2023/2027 (SEI nº 10625579)
VII - Plano Tático da ANATEL 2023/2034 (SEI-10625581) (SEI nº 10625581)

Atenciosamente,

Documento assinado eletronicamente por **Carlos Manuel Baigorri**, **Presidente**, em 31/07/2023, às 17:44, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da Portaria nº 912/2017 da Anatel.

A autenticidade deste documento pode ser conferida em http://www.anatel.gov.br/autenticidade, informando o código verificador **10633900** e o código CRC **1644DEFE**.

MANUAL OPERACIONAL DA PORTABILIDADE

ÍNDICE

Sumário

HISTÓRICO

Versão	Data	Comentários	Responsável
V.01	**28/09/07**	- Revisão de conteúdo pelo GT-OP-Sub-grupo Aprovisionamento em 07/08 e após deliberações do GT-OP em sua reunião ordinária do dia 08/08	GT-OP
V.02	**11/10/07**	- Revisão de conteúdo pelo GTOP conforme ata de reunião de 10 e 11/10/07	GT-OP
V.03	**28/10/07**	- Revisão de layout e transferência de itens do documento GIP_GTOP_PROC_ATIV – V07 para este manual. - Inclusão do Glossário. - Inclusão de Referências.	Rodrigo Menon
V.04	**30/11/07**	- Reflete a atualização no fluxo de ativação que gerou o documento GIP_GTOP_PROC_ATIV – V.9.1 - Inclusão do item 2.6 Processo de Indicadores.	Rodrigo Menon
V.05	**12/02/08**	- Atualizado conforme reuniões GIP-GTOP de 13 e 14/12/07, 24 e 25/01/2008.	GTOP
V.06	**26/11/08**	- Atualizado conforme reuniões GIP-GTOP de 26 à 28/11/2008.	GTOP
V.07	**17/01/17**	- Inclusão do protocolo e responsabilidades de conexão ao Ambiente da Portabilidade GIP_GTOP_PROC_SIST_ACESSO	GTOP
V.08	**28/05/18**	- Inclusão de todos os anexos no documento principal. - Atualizações conforme cronograma apresentado na reunião presencial do GTOP em 04/04/18 e 14/08/18.	GTOP
V.08	**27/09/18**	- Aprovação das atualizações conforme aprovado na reunião presencial do GTOP.	GTOP
v.09	**30/08/22**	- Inclusão do processo de dupla autenticação de portabilidade numérica com envio de SMS ao usuário	GTOP

Notas da Revisão

Esse Manual é parte integrante do Regulamento Geral da Portabilidade no qual é referenciado como DOP - Documento Operacional da Portabilidade - e foi desenvolvido pelas Prestadoras do SMP e STFC, participantes do GTOP/GIP, sob a coordenação da Anatel.

A Versão 9.0 deste Manual engloba e extingue todos os demais documentos anteriores associados ao mesmo, a saber:

GIP_GTOP_PROC_ATIVAÇÃO: Processo de Ativação de Terminal Portado;
GIP_GTOP_PROC_ESTORNO: Processo de Estorno por Fraude ou Erro;
GIP_GTOP_PROC_CANCEL: Processo de Cancelamento de Pedido de Portabilidade;
GIP_GTOP_PROC_DESLIG: Processo de Desligamento de Número;
GIP_GTOP_PROC_INDICADORES: Processo de Indicadores.
GIP_GTOP_PROC_FALHAS: Processo de Falhas e Reparos;

Anexos:
GIP_GTOP_PROC_SIST_ACESSO: Procedimentos de sistemas e acesso à EA.

Créditos

Coordenação: Renan Martins de Souza – Anatel

Relatoria: Paulo César Valete e Alexandre José Oliveira de Araujo

Sub-relatorias: Rodrigo Augusto Menon, Roberto Rivelino de Andrade, Gustavo de Assis Ferreira Coelho, Vânia Cristina de Souza Correa, Paulo César Valete, Jose Messias Teixeira, Luis Carlos Rocha, Gladston Figueira, Matheus Pucci, Marcilio Assis Albuquerque, Antonio Roberto Gorgulho da Silva, Diogo Rios Neves, José Lecy Costa, Jefferson de Souza Calixto, Denner Ribeiro de Sousa, Laerte Delfino Magalhães, Anna Cristina Papa Vaz Sampaio e Érica Carneiro de Castro.

Agradecimentos

Agradecemos a todos os profissionais das Prestadoras que integraram o Grupo Técnico Operacional da Portabilidade - GTOP - e que através do elevado nível de maturidade profissional registrado em suas participações contribuíram decisivamente para a excelência do modelo brasileiro de portabilidade.

Agradecemos a Associação Brasileira de Recursos em Telecomunicações - ABRT - pelo engajamento e apoio nesse trabalho, sem os quais seria impossível concluí-lo com qualidade.

Glossário

1. **Acesso Múltiplo**: Tipo de linha do SMP ou STFC que pertence a um grupo fechado com possibilidade de Discagem Abreviada entre membros.

2. **Análise de Impacto**: Avalia a abrangência com relação aos elementos da estrutura do serviço e a possível interferência de uma mudança qualquer, na qualidade ou disponibilidade do serviço.

3. **Ativação de Portabilidade**: Processo que cria registro na BDO, contendo informações básicas que possibilitam a realização do correto encaminhamento das chamadas;

4. **Autorização tácita**: Quando determinada ação que demande autorização por parte das prestadoras, tenha seu prazo esgotado, a autorização será realizada de forma automática pelo sistema.

5. **Número Único:** Trata-se de um tipo de linha STFC, que possibilita a prestação de serviços de voz por meio de um mesmo número de acesso em todo território nacional ou localidades com pontos de presença/Interconexão pelas prestadoras, alterando apenas o CN e mantendo o prefixo/MCDU."

6. **Tabela de Pré-existente**: Funcionalidade disponibilizada no sistema GUI do NPAC, onde é possível consultar os CNG´s de 10 dígitos ativados sem BP Intrínseco e os coincidentes de 11 dígitos que não podem ser ativados.

7. **Black list**: Arquivo disponibilizado no Sistema de Gestão de Documentos (GED) da EA, no qual informa os SPID's e CNG's de 10 dígitos ativos e coincidentes de 11 dígitos.

8. **BDO**: Base de Dados Operacional - Base de dados pertencente às Prestadoras, atualizada a partir do espelhamento da BDR, que contém os dados dos acessos portados, somente ativos, bem como a identificação da operadora as quais estes pertencem e que é utilizada pelas Prestadoras para identificação do correto encaminhamento das chamadas para números portados.

9. **BDO Implementada**: BDO que foi desenvolvida de acordo com os padrões estabelecidos e que é utilizada pelas Prestadoras para identificar o correto encaminhamento das chamadas para números portados.

10. **BP**: Bilhete de Portabilidade: Solicitação de portabilidade contendo os dados do cliente, da linha a ser portada, da Prestadora atual e da nova Prestadora necessários para cumprimento da fase de habilitação e conclusão do processo de portabilidade e que possui uma identificação única e sequencial

11. **BP Agrupador**: Código que identifica univocamente um determinado grupo de BP's. Esse código é gerado pela EA por ocasião da abertura do BP.

12. **BP Intrínseco**: Bilhete de Portabilidade utilizado pelas Prestadoras para execução de correção de parâmetros na BDR para números já portados, Mudança de Endereço dentro da mesma Prestadora envolvendo a troca de CNL e ativação de novo CNG.

13. **BDR**: Base de Dados de Referência – Base de Dados nacional mantida pela EA e que contém os registros necessários para o correto encaminhamento de chamadas para números portados.

14. **CN**: Tecnicamente chamado de Código Nacional, ele corresponde a dois caracteres numéricos que identificam uma área geográfica específica.

15. **CNG:** Código Não Geográfico - Código cuja marcação da chamada é realizada em todo o Território Nacional sem a necessidade de acréscimo de código de DDD, CSP e CN.

16. **CNL**: Código Nacional de Localidade - Código a 5 (cinco) dígitos, atribuído pelo IBGE a toda localidade oficialmente reconhecida do território nacional.

17. **Códigos Especiais**: Códigos utilizados em chamadas abreviadas. Exemplo: Trí-Dígito.

18. **Comitê Executivo**: Representantes das associadas da EA com alçada formal para assumir riscos relatados, aprovar orçamentos e prazos para implementação das mudanças solicitadas.

19. **Comitê de Indústria**: Grupo de profissionais responsável por avaliar a mudança solicitada e alcançar um consenso sobre sua necessidade ao negócio das operadoras. Este grupo é formado pelos Representantes dos envolvidos, dentre eles os representantes da a EA e Prestadoras.

20. **Conflito**: Situação em que um BP pode encontrar-se devido à recusa da solicitação de portabilidade pela Doadora ou pelo não cumprimento pelo cliente da fase de Habilitação junto a Receptora.

21. **DDR**: Tipo de linha do STFC que está associada ao serviço de Discagem Direta ao Ramal.

22. **Doadora**: Prestadora do serviço do STFC ou SMP que participa do processo de portabilidade numérica como cedente da linha a ser portada.

23. **EA:** Entidade Administradora – Pessoa Jurídica independente e de neutralidade comprovada, contratada pelas Prestadoras para administrar o serviço de portabilidade.

24. **EOT Fiscal**: Código que representa a operadora de telecomunicações em cada área de atuação.

25. **GED**: Sistema de Gestão Eletrônica de Documento utilizado para registro de todos os documentos pertinentes aos processos da Portabilidade Numérica.

26. **GEX**: Grupo Executivo coordenado pela Anatel com participação de representantes das Prestadoras do STFC e SMP, responsável pela coordenação das ações dos demais grupos que compõe o GIP, a saber: GTOP, GTREDE, GTNEGÓCIOS, GTEA e GTSIS.

27. **GIP**: Grupo de Implantação da Portabilidade coordenado pela Anatel com participação de representantes das Prestadoras do SFTC e SMP, composto pelos subgrupos GTOP, GTREDE, GTNEGÓCIOS, GTEA e GTSIS.

28. **GTOP**: Grupo Técnico Operacional da Portabilidade, coordenado pela Anatel com participação de representantes das Prestadoras do STFC e SMP com a finalidade principal de escrever o MOP.

29. **Gerenciamento de Mudanças**: É o processo responsável por estabelecer as atividades, regras, indicadores de desempenho, papéis e responsabilidades inerentes ao gerenciamento, acompanhamento e coordenação das alterações necessárias ou solicitadas, visando à melhoria no ambiente de trabalho.

30. **Habilitação**: Fase na qual o cliente apresenta a documentação legal que comprova a titularidade da linha a ser portada junto a Prestadora Receptora.

31. **Janela de Migração**: Representa o Período de Transição de que trata o Art. 4º do Capítulo XIV do RGP. Tecnicamente são intervalos de duas horas pré-definidos – Ver Anexo I – em que se realiza a atualização das Bases de Dados (BDR/BDO), a ativação do cliente na Receptora e a desativação na Doadora.

32. **MOP**: Manual Operacional da Portabilidade – É parte integrante do RGP onde é referenciado como Documento Operacional da Portabilidade. Construído pelo GIP/GTOP detalha o fluxo padronizado de comunicação entre as Prestadoras, EA, Parceiro Tecnológico da EA e Anatel para a execução da Portabilidade Numérica e demais processos inerentes.

33. **Mudança**: Qualquer alteração realizada em hardware, software ou documento integrante da estrutura do serviço a qual deve ser registrada através de uma RdM.

34. **PTI**: Projeto Técnico de Interconexão – Mecanismo através do qual são definidos os requisitos técnicos para interligação das redes das Prestadoras dos serviços de telecomunicações.

35. **Receptora**: Prestadora do serviço do STFC ou SMP que inicia o processo de portabilidade numérica recebendo a linha a ser portada ao final do mesmo.

36. **Representantes dos Envolvidos**: Representantes das Prestadoras, EA e Parceiro Tecnológico da EA diretamente ligados ao serviço de portabilidade numérica.

37. **RdM**: Requisição de Mudanças-: Solicitação de Mudança registrada através de formulário específico conforme previsto no Processo de Gerenciamento de Mudanças.

38. **RGP**: Regulamento Geral da Portabilidade - Documento estabelecido pela Resolução n° 460, de 19 de Março de 2007 da ANATEL que tem por objetivo estabelecer as condições para a implantação da Portabilidade de Numérica.

39. **RN1**: Código numérico que identifica a Prestadora Receptora, utilizado para o correto encaminhamento de chamada para terminal portado.

40. **STFC**: Sistema de Telefonia Fixa Comutada – Sigla atribuída às Prestadoras do Serviço Fixo de telefonia.

41. **SAPN**: Sistema de Administração do Plano de Numeração, mantido pela Anatel.

42. **SLA**: Acordo de Nível de Serviço celebrado entre as partes envolvidas.

43. **SMS:** Short Message Service – Serviço de mensagem curta, conhecido como torpedo.

44. **SMP**: Sistema Móvel Pessoal – Sigla atribuída às Prestadoras do Serviço de Telefonia Celular Móvel.

45. **Suspenso**: Situação em que um BP pode encontrar-se devido à necessidade de paralisação temporária da portabilidade por necessidade do cliente.

1. Solicitação de Portabilidade entre Prestadoras

1.1. O usuário solicita à Prestadora Receptora a portabilidade de seu(s) código(s) de acesso.

1.2. A Prestadora Receptora, no ato da solicitação, deve informar as condições e prazos relativos à portabilidade. A Receptora pode ainda acordar com o cliente a data e o período em que este deseja a migração. Após o aceite do cliente, a Prestadora Receptora registra o pedido de Portabilidade, solicitando do usuário as seguintes informações:

1.2.1. Nome ou Razão Social;
1.2.2. CPF ou Documento de Identidade ou CNPJ;

NOTA I: No caso de pessoa física deverá ser informado preferencialmente o CPF. Somente no caso do cliente não possuir CPF deverá ser informado um documento de identificação válido onde o mesmo deverá ser registrado no campo “ID genérico”.

NOTA II: Quando a Pessoa Jurídica não possuir CNPJ, como é o caso das embaixadas e consulados, por exemplo, o documento legal existente deverá também ser registrado no campo “ID genérico”.

1.2.3. Código de acesso do usuário;
1.2.4. Nome da Prestadora Doadora atual;
1.2.5. Endereço completo;
1.2.6. Tipo de acesso: Básico, Múltiplo e CNG.

1.3. Tipos de agendamento de Janela de Migração.

1.3.1. A Receptora pode sinalizar para que o sistema da EA agende a portabilidade para a primeira Janela de Migração com cota disponível.

1.3.2. A Receptora poderá agendar a portabilidade informando o período para alocação da Janela de Migração, deixando que o sistema da EA agende a primeira Janela com cota disponível dentro do período informado.

1.3.3. A Receptora poderá agendar a portabilidade informando a Janela de Migração especifica.

1.4. Critérios de agendamento do BP e administração de Janelas de Migração.

1.4.1. Cabe à EA administrar a ocupação das Janelas de Migração e disponibilizar para consulta as Janelas com cotas disponíveis.

1.4.2. Não poderá haver agendamento antes do prazo de 2 (dois) dias úteis a partir do dia da solicitação do bilhete, exceto no caso dos BP's que possuam tratamento diferenciado, a saber: Portabilidade de Estorno e Portabilidade Intrínseca.

1.4.3. O agendamento, além do prazo regulamentar, somente será permitido quando for solicitado pelo cliente ou houver negociação entre as partes com anuência do cliente. Neste caso o prazo não poderá ser maior que 90 (noventa) dias corridos. O agendamento fora do prazo regulamentar deverá ser assinalado pela Prestadora Receptora no BP.

1.4.4. As Prestadoras são passíveis das sanções previstas no RGP nos casos de agendamento além do prazo regulamentar sem anuência do cliente.

1.4.5. Não será possível realizar o agendamento em Janelas de Migração reservadas para manutenção programada, conforme Processo de Tratamento de Incidentes descrito no ANEXO II desse documento.

1.4.6. A EA deverá garantir que o agendamento de todos os BP's que possuam o mesmo Identificador de Grupo ocorra em uma única Janela de Migração.

1.4.6.1. A Receptora poderá associar BP's a um Identificador de Grupo exclusivamente para o mesmo cliente.

1.4.6.2. A Receptora poderá criar BP's com Identificador de Grupo, das seguintes maneiras:

i. Por faixa: A Receptora informa a EA o número inicial e o número final de uma faixa continua de CN + Códigos de Acesso;
ii. Por lista: A Receptora informa à EA uma lista de CN + Código de Acesso;
iii. Por adição: A Receptora pode associar outros BP's a um Identificador de Grupo já existente.

1.4.7. Compete à EA administrar os valores de cotas de Portabilidade, garantindo que os mesmos sejam estabelecidos e atualizados segundo os critérios definidos no item 2 do Anexo I deste documento.

1.5. Finalizado o registro da solicitação do usuário, a Prestadora Receptora envia à EA, as seguintes informações:

i. Nome completo ou Razão Social;
ii. CPF ou Documento de Identidade ou CNPJ, conforme item 1.2.2;
iii. Código de acesso do usuário;
iv. Código de Identificação da Prestadora Receptora;
v. Código de Identificação da Prestadora Doadora;
vi. Número do CNL do endereço de destino (somente para Prestadoras do STFC);
vii. A data/janela em que ocorrerá a migração, conforme item 1.3;
viii. Código da EOT fiscal da Receptora;
ix. Código RN1 da Receptora;
x. Tipo de acesso: básico, múltiplo ou CNG.

Nota I: O tipo de acesso múltiplo deve ser empregado apenas para os casos de portabilidade que deverão ocorrer dentro de uma mesma Janela de Migração.

Nota II: o cliente de Acesso Múltiplo do tipo DDR poderá solicitar a portabilidade desde um único terminal até todos os terminais que compõem o DDR.

Nota III: Todos os ramais de um determinado DDR devem ser migrados em uma única Janela de Migração.

1.6. Recebidos os dados da Prestadora Receptora, a EA realiza a pré-validação dos dados da solicitação de portabilidade, verificando:

1.6.1. A consistência numérica do CPF/CNPJ - com base em algoritmo da Receita Federal – Módulo 11 para CPF e módulo 14 para CNPJ;

1.6.2. O formato do Código de Acesso informado;

1.6.3. Se o Código de Acesso pertence à Prestadora Doadora;

1.6.4. Se já existe alguma solicitação de portabilidade em andamento para o mesmo Código de Acesso;

1.6.5. Se a portabilidade é admissível conforme os critérios estabelecidos no RGP;

1.6.6. Se os códigos RN1 e EOT fiscal pertencem à Receptora.

1.7. A Receptora deverá assinalar no BP quando identificar que o Código de Acesso que será portado pertence ao seu plano de numeração original, exceto para códigos do tipo CNG.

1.8. Se for identificada alguma inconsistência, a EA deve retornar uma mensagem à Receptora informando o(s) motivo(s) da recusa de abertura do BP de acordo com o item 1.6.

1.9. Recebida a mensagem de notificação de inconsistência da EA, a Receptora realiza um dos procedimentos a seguir:

1.9.1. Corrige o(s) dado(s) na solicitação e a submete novamente à EA;

1.9.2. Informa ao cliente o motivo da impossibilidade de executar a portabilidade solicitada e, caso seja necessário, encerra o processo cancelando o BP;

1.9.3. Caso seja identificado que a recusa da Doadora é indevida, caberá a Receptora tratar a inconsistência através do Processo de Tratamento de Incidentes descrito no Anexo II desse documento.

1.10. Caso não seja identificada nenhuma inconsistência nos dados fornecidos pela Receptora, a EA gera o BP para a respectiva solicitação de portabilidade e envia as seguintes informações para as Prestadoras Receptora e Doadora:

i. Número do protocolo do BP;
ii. Nome completo ou Razão Social;
iii. CPF e/ou Documento de Identidade ou CNPJ, conforme item 1.2.2;
iv. Código de acesso do usuário;
v. Código de Identificação da Doadora;
vi. Data/janela agendada pela Receptora;
vii. Código de Identificação da Receptora.

Nota I: A Receptora deve informar ao cliente o protocolo do BP, fornecido pela EA, como comprovante da abertura da solicitação de portabilidade.

Nota II: Quando a solicitação for para vários Códigos de Acesso de um mesmo cliente, cada código de acesso terá seu próprio BP e tratamento individualizado, ainda que exista um único Identificador de Agrupamento associado aos mesmos.

1.11. A Doadora envia mensagem para a EA confirmando o recebimento da Solicitação de Portabilidade.

1.12. A Doadora terá no máximo 1 (um) dia útil para conferência e confirmação dos dados do usuário, desconsiderando-se o dia da criação do BP.

1.13. Recebidos os dados a serem validados descritos no item 1.10, a Doadora procede à conferência e validação dos mesmos, observando:

1.13.1. Se o BP refere-se a Código de Acesso inexistente, não-designado, temporário, de Uso Público ou associado a Código Especial de terminação de Serviço de Utilidade Pública. Estando o Código de Acesso enquadrado em qualquer um desses casos a Prestadora Doadora deverá recusar a solicitação de portabilidade;

1.13.2. Nome completo ou Razão Social;

1.13.3. CPF ou Documento de Identidade ou CNPJ;

NOTA I: No caso de pessoa física, para efeito de validação, a Doadora deve utilizar preferencialmente o CPF. Somente se este não existir é que será feita a validação do documento de identidade. Caso sejam fornecidos ambos os documentos, CPF e outro documento válido de identificação, a validação deverá ser obrigatoriamente pelo CPF.

NOTA II: A Doadora deverá consistir a raiz do CNPJ (oito primeiros dígitos) com qualquer CNPJ válido existente nos cadastros do cliente.

NOTA III: A inconsistência do campo descrito no item 1.13.2 não deve ser motivo para recusa da portabilidade, entretanto poderá haver por parte da Doadora a indicação no BP de suspeita de fraude.

1.13.4. Código de Acesso do usuário;

1.13.5. Código de Identificação da Doadora;

1.13.6. Caso a Doadora identifique a possibilidade de haver fraude no processo de portabilidade esta deverá informar no BP um dos seguintes códigos abaixo:

i. 01: “FRAUDE JÁ IDENTIFICADA”;
ii. 02: “ALERTA DA ÁREA DE RETENÇÃO PORTABILIDADE NÃO RECONHECIDA”.

1.13.7. As Doadoras do SMP, em caso de divergência cadastral do CPF/CNPJ para clientes do modelo Pré-Pago, deverão seguir os seguintes procedimentos, conforme Despacho 3.103 de 08 de maio de 2009:

i. Verifica em seu cadastro se o acesso possui bloqueio por perda, roubo ou extravio;
ii. Em caso de acesso bloqueado por um dos motivos acima, recusa a portabilidade por documento inconsistente;

iii. Em caso de acesso ativo, autoriza a portabilidade, indica a existência de fraude ou erro e envia a seguinte mensagem: “3 - CPF DIVERGENTE PRÉ-PAGO MÓVEL”.

1.14. A Prestadora Doadora deve enviar mensagem à EA com o resultado da autenticação, autorizando ou recusando o BP. Caso a Doadora não cumpra este requisito no prazo estabelecido no item 1.12, caberá a EA autenticar automaticamente o BP assinalando no mesmo que houve uma autorização tácita.

1.14.1. No processo de autenticação do BP de Códigos de Acessos do STFC, as Doadoras deverão incluir na mensagem de retorno à EA o CNL atual do Código de Acesso a ser portado.

1.14.2. Caso a Doadora do STFC não conclua o processo de Autenticação do BP no prazo previsto no item 1.12, caberá a EA consultar a informação do CNL de Origem do Código de Acesso em sua Base de Dados de referência e proceder a validação de Área Local antes de realizar a autenticação tácita.

1.15. No caso de recusa a Doadora deve enviar mensagem à EA explicitando o(s) motivo(s), quais sejam:

1.15.1. Dados enviados incorretos ou incompletos;

1.15.2. Código inexistente, não designado, temporário ou designado a terminais de uso público;

NOTA I: Usuário com acesso cancelado na Doadora não poderá solicitar a Portabilidade. Nesse caso, a Doadora deverá informar a recusa com o motivo “Código de Acesso inexistente”.

NOTA II: A Doadora não poderá recusar as solicitações de portabilidade para os Códigos de Acesso que estejam em processo de instalação e reservados para o cliente em contrato firmado.

1.16. A Doadora deve informar aos órgãos de Justiça sobre o processo de portabilidade e para qual Prestadora irá portar a linha que está sob processo de Quebra de Sigilo, considerando os aspectos individuais de cada ordem judicial.

1.17. Recebida a mensagem da Doadora, a EA deverá fazer as seguintes validações:

1.17.1. Validação de Área Local para BP do STFC através da compatibilidade entre o CNL de destino informado pela Receptora e o CNL de origem informado pela Doadora;

1.17.2. Validação de Área de Registro para BP do SMP através da compatibilidade entre o CN de destino informado pela Receptora e o CN de origem informado pela Doadora.

1.18. Havendo a recusa por parte da Doadora o BP assumirá o estado de CONFLITO, podendo a Receptora cancelá-lo ou submetê-lo novamente a EA. No segundo caso a Doadora terá novamente o prazo estabelecido no item 1.12 para autenticar o BP reenviado. Caso o BP permaneça no estado de CONFLITO por 30 (trinta) dias corridos, o BP será automaticamente cancelado pela EA.

1.19. Durante o processo de validação dos CNL's de origem e destino o BP assumirá o estado de CONFLITO caso a EA identifique que os CNL´s informados não pertencem a uma mesma Área Local, podendo a Receptora cancelar ou alterar os dados de CNL de destino e enviar o BP para nova validação da EA. No segundo caso a Doadora terá novamente o prazo estabelecido no item 1.12 para autenticar o BP reenviado. Caso o BP permaneça no estado de CONFLITO por 30 (trinta) dias corridos, o registro será automaticamente cancelado pela EA.

1.20. Havendo a necessidade de remarcação da Janela de Migração, a Receptora deverá solicitar essa alteração à EA, com antecedência mínima de 3 (três) horas do início da nova Janela pretendida. Para o processo de remarcação de Janela de Migração aplicam-se as mesmas regras estabelecidas no item 1.3 desse documento.

Nota: A EA recusará a solicitação de remarcação de Janela de Migração que ocorra com menos do que 3 (três) horas do início da Janela de Migração previamente agendada.

1.21. A Receptora deverá realizar a fase de habilitação junto ao usuário e assinalar no BP que esta etapa foi concluída com sucesso.

1.21.1. A indicação no BP de conclusão da fase de habilitação pela Receptora deverá ocorrer desde o momento da solicitação da portabilidade até 3 (três) horas antes da Janela de Migração especificada no BP.

1.21.2. Caso a Receptora não indique no BP o sucesso na conclusão da fase de habilitação, a EA colocará automaticamente o BP no estado de SUSPENSO informando a ambas, Receptora e Doadora, da suspensão do processo de portabilidade.

NOTA I: A Receptora somente poderá solicitar à EA a suspensão de um BP quando for solicitado pelo cliente ou houver negociação entre as partes com anuência do mesmo.

NOTA II: A suspensão de um BP acarretará automaticamente na liberação do agendamento, da cota ocupada na Janela de Migração e do congelamento dos prazos para efeito de cálculo dos Indicadores de Qualidade da Portabilidade.

1.21.3. Caso o BP permaneça por 30 (trinta) dias corridos no estado de SUSPENSO, o mesmo será automaticamente cancelado pela EA.

1.22. Havendo a necessidade de atualização dos dados de CNL, EOT, informação de PTO ou reversão de PTO para um BP já Ativo, a Prestadora Receptora deverá utilizar-se de uma portabilidade Intrínseca para acerto do cadastro na BDR e BDO´s.

1.22.1. Estando o BP ainda em processo de portabilidade, o mesmo poderá ser cancelado para acerto dos dados em um novo BP.

1.23. Portabilidade de número único

1.23.1. Caso a Receptora precise portar um número único, a Doadora detentora do prefixo e milhar no Sistema de Plano de Numeração

deverá autenticar os BP´s, mesmo que os terminais não estejam ativados na sua rede, desde que se enquadre em uma das situações:

1.23.1.1. Tenha o número único ativo na sua rede em um ou mais CN´s para o mesmo cliente solicitante do(s) BP (s);

1.23.1.2. Tenha o número único (prefixo e milhar) compartilhado com uma ou mais Prestadoras para o mesmo usuário solicitante do(s) BP (s);

1.23.1.3. Tenha um bilhete de portabilidade ativo para um ou mais CN´s deste número único.

1.23.2. A Receptora deverá abrir BPs somente para os CN's das regiões em que atua. Os demais CN's que não foram portados não deverão ser comercializados para outro cliente que não seja o atual, ou seja, a detentora dos CN's deverá criar uma reserva;

1.23.3. A Receptora deverá fazer uma consulta prévia com a Doadora antes da criação dos BPs para combinar a portabilidade e identificar as áreas de atuação do cliente na Doadora;

1.23.4. As Prestadoras deverão analisar a proposta de portabilidade de números únicos com o intuito de evitar conflitos, para isso, devem ser realizados os seguintes procedimentos:

1.23.4.1. A Receptora deverá abrir uma solicitação do tipo "Número Único", no sistema SGCEAP – Módulo Incidentes Interprestadoras, informando obrigatoriamente os dados do cliente: CNPJ, CNL associado (utilizando o campo BP) e os números únicos;

1.23.4.2. A Receptora deverá formalizar no campo descrição os dados pertinentes e o prazo que serão realizadas as criações dos BPs e a Doadora deverá retornar com o contato e o prazo que irá autorizar;

1.23.4.3. Após a criação, a Doadora deverá autorizar os BPs criados, mesmo que não atue em todos os CN's solicitados.

1.23.5. Para os casos de portabilidade de números únicos que estiverem em conflito, deve ser seguido o processo de Incidentes Interprestadoras, através da abertura do tipo de incidente Rejeição por Número Inexistente.

1.23.6. A Receptora poderá portar parcialmente os números únicos, ativando na sua rede apenas os terminais portados nos CN´s solicitadas. Os demais terminais dos CN´s que não foram portados e encontram-se nas situações descritas, devem ser tratados conforme segue:

1.23.6.1. Números únicos ativos nos CN´s não portados - A Doadora detentora deverá negociar com o cliente se irá manter os números ativos na sua rede;

1.23.6.2. Números únicos não ativados nos CN´s não portados - A Doadora detentora deverá manter a reserva dos terminais, e estes não poderão ser comercializados para outro cliente que não seja o atual cliente da Receptora;

1.23.7. Caso a Receptora precise portar o restante dos terminais, a Doadora detentora deverá autenticar os BP´s dos terminais nas condições do item 1.23.1.

1.24. Portabilidade de FATB

1.24.1. A portabilidade de telefones rurais deve ter tratamento diferenciado em relação aos demais clientes do STFC, podendo o cliente rural manter o seu número dentro da área do mesmo CN, tanto na portabilidade interna como na portabilidade entre prestadoras.

1.24.2. No caso de portabilidade entre prestadoras, a autenticação por parte da doadora será feita de forma manual, devendo a prestadora doadora informar no BP o mesmo CNL informado pela prestadora receptora, de forma a não restringir a portabilidade entre áreas locais diferentes.

1.25. Processo de dupla autenticação de Portabilidade Numérica

1.25.1. Os usuários pessoas físicas (PF) de Prestadoras do Serviço Móvel Pessoal (SMP), receberão uma mensagem via SMS (*Short Message Service*) após a abertura e autorização do bilhete de portabilidade pela Prestadora Doadora. O usuário deverá necessariamente estar em posse de um aparelho telefônico com a referida linha ativa.

1.25.1.1. A continuidade da portabilidade será condicionada à resposta positiva desta mensagem pelo usuário.

1.25.1.2. Caso o usuário responda a mensagem negando a continuidade da portabilidade numérica referida, o bilhete será cancelado pela EA.

1.25.1.3. Caso o usuário não responda a mensagem dentro do tempo-limite (parametrizado) o bilhete entrará em conflito.

1.25.1.4. A prestadora Receptora poderá enviar uma nova mensagem ao usuário que ficar silente, assim que ultrapassado o tempo limite configurado.

1.25.2. Os usuários pessoas jurídicas (PJ) de Prestadoras do Serviço Móvel Pessoal (SMP), quando solicitada a portabilidade e tiver a quantidade limite de terminais (parametrizável) definida pelo GTOP, receberão uma mensagem via SMS (*Short Message Service*) após a abertura e autorização do bilhete de portabilidade pela Prestadora Doadora. O usuário deverá necessariamente estar em posse de um aparelho de telefonia com a referida linha ativa.

1.25.2.1. A continuidade da portabilidade será condicionada à resposta positiva desta mensagem pelo usuário.

1.25.2.2. Caso o usuário responda a mensagem negando a continuidade da portabilidade numérica referida, o bilhete será cancelado pela EA.

1.25.2.3. Caso o usuário não responda a mensagem dentro do tempo-limite (parametrizado) o bilhete entrará em conflito.

1.25.2.4. A prestadora Receptora poderá enviar uma nova mensagem ao usuário que ficar silente, assim que ultrapassado o tempo limite configurado.

1.25.3. Quando ultrapassada a quantidade limite de terminais pessoal jurídica (PJ), definida pelo GTOP, será enviado para o usuário um SMS informativo sobre o pedido de portabilidade numérica referido.

2. Mudança de endereço nas Prestadoras do STFC

2.1. É permitida a mudança de endereço com manutenção do Código de Acesso apenas se esta ocorrer dentro da mesma Área Local.

2.2. Somente nos casos de mudança de endereço que impliquem em alteração do CNL, a Prestadora responsável pela mudança deverá abrir um BP Intrínseco para fazer constar na BDR e BDO's a alteração da localidade.

2.2.1. No BP Intrínseco deve ser registrado como Doadora a mesma Prestadora que está abrindo a solicitação.

2.2.2. O BP Intrínseco não estará sujeito ao regime de Cotas de Janela de Migração, podendo ser agendado, também, em uma janela que esteja com sua cota previamente esgotada.

2.2.3. A abertura e o agendamento do BP Intrínseco devem somente respeitar o prazo mínimo de 3 (três) horas de antecedência da Janela de Migração.

NOTA: O procedimento de mudança de endereço assim como os respectivos prazos e regras são definidos pelo regulamento do STFC.

3. Habilitação de Código Não Geográfico Novo

3.1. A portabilidade de um CNG ativo deve ser tratada conforme descrito no item 1 desse documento.

3.2. Quando se tratar de ativação de um Novo CNG, previamente à abertura da solicitação de portabilidade, a Prestadora Receptora deve executar as seguintes ações:

3.2.1. Verificar na plataforma de portabilidade da EA se o prefixo do Novo CNG está incluído na relação de CNG's a 10 (dez) dígitos pré-existentes. Caso afirmativo o Novo CNG não poderá ser ativado;

3.2.2. Verificar se o prefixo do Novo CNG está incluído na relação da *Blacklist* de CNG disponibilizada no Portal de Documento eletrônico da EA, na qual é responsável pela gestão. Caso afirmativo, o novo CNG não poderá ser ativado;

3.2.3. Reservar e homologar o Novo CNG junto a Anatel através do Sistema de gestão do Plano de Numeração;

3.2.4. A Receptora abre um BP Intrínseco, onde deve ser registrado como Doadora a mesma Prestadora que está abrindo a solicitação.

NOTA: Para marcação da Janela de Migração do BP Intrínseco de um Novo CNG são válidos os requisitos estabelecidos nos itens 2.2.2 e 2.2.3.

3.3. Para a validação de um CNG a EA deverá realizar as seguintes pré-validações:

i. Verificar se o prefixo do CNG é existente e válido;
ii. Verificar se o CNG é pré-existente, podendo estar portado ou não; Caso seja pré-existente deverá proceder conforme descrito no item 1 desse documento.

Nota: A partir da abertura do BP Intrínseco o processo segue conforme o tratamento normal de ativação de um Código de Acesso contemplando as etapas previstas nos Itens 1 e 4 desse documento.

4. Atualização das Bases de Dados

4.1. Em cada Janela de Migração serão executados os seguintes procedimentos:

4.1.1. A EA atualiza a BDR no primeiro momento da Janela de Migração pré-estabelecida, e, simultaneamente, envia a mensagem em *broadcast* para atualização das BDO's de todas Prestadoras;

4.1.2. Durante a Janela de Migração a Receptora ativa o Número de Acesso portado, e a Doadora desativa o Número de Acesso portado,

encaminhando à EA, ambas as Prestadoras, a informação da data e hora da ativação e desativação, respectivamente;

NOTA: Não haverá sincronismo entre a ativação na Receptora e a desativação na Doadora, sendo que tais processos devem ser efetuados dentro do período de transição.

4.1.3. No caso de migração de um Código de Acesso portado para a Prestadora de Origem do Prefixo do Código de Acesso, a EA deverá excluir o registro de portabilidade da BDR e atualizar as BDO's. Contudo, a EA deverá manter o registro de movimentação do código em questão, além do respectivo BP, pelos prazos previstos no RGP;

NOTA: O processo de migração para a Prestadora de Origem não se aplica a CNG.

4.1.4. Tratando-se de CNG, finalizado o processo de portabilidade, a Receptora deverá proceder com a regularização do Acesso no Sistema de Plano de Numeração.

5. Cancelamento da Solicitação de Portabilidade

5.1. O cancelamento pode ser solicitado por iniciativa do cliente ou necessidade justificada da Receptora.

5.2. Todos os cancelamentos de BP deverão ser comunicados a EA seguidos de justificativa. As justificativas de cancelamento admitidas são:

i. Desistência do cliente;
ii. Indício de fraude;
iii. Não cumprimento da fase de habilitação.

5.3. A Receptora informa à EA o BP a ser cancelado, bem como o motivo do cancelamento.

5.4. A EA informa às Prestadoras Doadora e Receptora o cancelamento do BP.

Nota: A Doadora poderá confirmar o recebimento do cancelamento caso o BP já esteja autenticado.

5.5. O cancelamento a pedido do cliente após o prazo regulamentar de dois dias úteis é uma liberalidade das Prestadoras que farão o melhor esforço para evitar que o cliente fique sem serviço. Todavia, não constitui uma obrigação regulatória não devendo incidir sobre ela qualquer sanção. Neste caso, a Receptora poderá efetuar o cancelamento junto à EA desde que o pedido ocorra até 3 horas antes da Janela de Migração agendada.

5.6. Todo cancelamento implica na imediata liberação da cota alocada para o BP na Janela de Migração.

6. Desconexão de Código de Acesso Portado

6.1. O cliente pode, a qualquer momento, solicitar a desconexão do Código de Acesso portado.

6.2. A Receptora deve receber a solicitação do cliente para a desconexão do Código de Acesso portado e realizar as operações necessárias conforme regulamentação do STFC ou SMP. A Receptora deverá comunicar imediatamente à EA a data/hora da desconexão do Código de Acesso.

6.3. A EA devolverá o Código de Acesso à Prestadora de Origem 90 (noventa) dias corridos contados a partir da data de desconexão informada pela Receptora do último processo de portabilidade.

NOTA: É responsabilidade da Prestadora de Origem garantir a complementaridade do prazo de quarentena quando aplicável.

6.4. Em caso de desconexão de CNG não haverá processo devolução para a Prestadora de Origem, visto que os Códigos de Acesso desse tipo são geridos pela própria Anatel. Nesse caso a EA deverá apenas atualizar a BDR e BDO´s.

6.5. No caso de desconexão de CNG cabe à última Receptora, respeitado o prazo integral de quarentena, atualizar a EA e o SAPN devolvendo o código à Anatel.

6.6. É de responsabilidade da Receptora manter o Código de Acesso portado em suas bases de dados, permitindo possíveis reativações, caso este esteja sob ação judicial.

6.7. A retirada do Código de Acesso da base de números portados pela EA ocorrerá na primeira janela disponível respeitando o prazo de devolução estabelecido itens 6.3 e 6.5.

6.8. A Receptora ao reativar um Código de Acesso portado no período de quarentena deverá enviar um pedido de cancelamento da desconexão para a EA.

6.9. A EA, ao receber a informação de cancelamento da desconexão pela Receptora, comunicará às Prestadoras envolvidas, Receptora atual e a Prestadora de Origem, da reativação do Código de Acesso na atual Receptora.

6.10. Cabe a Receptora garantir que a reativação do Código de Acesso portado somente ocorra por solicitação do cliente titular do Código de Acesso enquanto esse estava ativo.

A Receptora ao realizar uma desconexão indevida de um Código de Acesso, poderá abrir um novo bilhete de portabilidade utilizando a marcação da *flag* de "Desconexão indevida" na GUI/NPAC e informar o bilhete de portabilidade anterior. Este procedimento poderá ser realizado a qualquer momento pela última Receptora. Os bilhetes com marcação do indicador de Desconexão Indevida não terão o processo de dupla autenticação com envio de SMS aos usuários.

7. Estorno de Terminal Portado

7.1. Esse processo aplica-se quando é solicitada a portabilidade de forma fraudulenta, equivocada ou ocorrer uma autenticação indevida por parte da Doadora resultando na migração indevida do Código de Acesso.

7.2. É responsabilidade da Receptora do Processo de Estorno a abertura do BP de Estorno, sendo que esse processo deve ser iniciado em até 30 dias corridos a partir da data de ativação do BP que está sendo estornado.

7.3. O BP a ser estornado será sempre aquele que ocasionou a portabilidade indevida, mesmo que tenha havido portabilidades anteriores ou posteriores para o mesmo Código de Acesso.

7.4. A Doadora no processo de estorno é a detentora atual do Acesso.

7.5. Após análise interna e constatação de que houve uma portabilidade indevida, a Receptora do Processo de Estorno deverá abrir o BP de Estorno e informar ao Cliente os prazos pertinentes a esse processo.

7.6. A Receptora do processo de Estorno deve enviar as seguintes informações para abertura do BP de Estorno pela EA:

7.6.1. Nome completo (Pessoa física) ou Razão Social;
7.6.2. CPF ou Documento de Identidade (Pessoa física) ou CNPJ (Pessoa
7.6.3. jurídica);
7.6.4. Código de Acesso a ser portado: CNG ou CN + Código de Acesso do usuário;
7.6.5. Código de identificação da Receptora;
7.6.6. Código de Identificação da Doadora;
7.6.7. CNL do endereço de destino, apenas para as Prestadoras do STFC;
7.6.8. A data/Janela em que ocorrerá a migração ou indicação da opção de antecipação automática de janela pela EA;

Nota: Especificamente para o caso de estorno o agendamento do BP poderá ocorrer para a primeira janela de Migração após o período de autenticação da Doadora.

7.6.9. EOT fiscal da Receptora;
7.6.10. RN1 da Receptora;
7.6.11. Tipo de acesso: Básico, Múltiplo ou CNG;
7.6.12. Se o BP é de estorno por fraude ou erro;

7.6.13. Número do protocolo de portabilidade que está sendo contestado;

7.6.14. Descrição do problema contendo um dos seguintes códigos abaixo:

i. NS+Código de Acesso de contato do cliente, onde o código NS significa: Cliente informa não ter solicitado portabilidade;
ii. CT+Código de Acesso de contato do cliente, onde o código CT significa: Conflito societário/familiar;
iii. SE+Código de Acesso de contato do cliente, onde o código SE significa: Cliente informa ter solicitado portabilidade de outro Código de Acesso.

7.7. Finalizado o registro da solicitação de estorno, a Receptora do processo de estorno envia à EA as informações descritas no item 7.6.

7.8. A partir da abertura do BP o processo segue conforme o tratamento normal de ativação de um acesso contemplando as etapas previstas nos Itens 1 e 4 desse documento.

7.9. Caso seja recusada a abertura do BP de estorno pela EA devido à existência de outro BP em andamento, a Receptora do processo de estorno deve abrir um incidente interprestadora, solicitando o cancelamento dessa portabilidade.

7.10. A Doadora terá até um dia útil, a partir do dia da solicitação, para autenticar o BP, confirmando ou não a Fraude ou Erro.

7.11. Havendo interesse da Receptora do Processo de Estorno em antecipar a Janela de Migração, esta deverá assinalar no BP essa necessidade. Havendo essa sinalização o BP será agendado automaticamente pela EA para a primeira Janela de Migração logo após a autenticação do BP pela Doadora, resguardando-se as 3h00min mínimas de antecedência da Janela de Migração.

7.12. A Doadora do processo de estorno, durante a fase de autenticação, deverá apresentar obrigatoriamente uma justificativa para a portabilidade indevida.

7.13. As Prestadoras envolvidas devem manter contato direto através de suas áreas de Anti-Fraude para facilitar o tratamento do processo de estorno.

7.14. Durante o período de análise do pedido de estorno a Doadora deve contatar o cliente visando esclarecer a possível situação de fraude ou erro.

7.15. A primeira solicitação de estorno de um Código de Acesso Pré-Pago Móvel deverá ser autorizada tacitamente conforme descrito no item 1.13.7. A partir da segunda solicitação de estorno envolvendo o mesmo Código de Acesso e Prestadoras, a Doadora do Processo de Estorno poderá negar o pedido de Estorno.

7.16. No caso de recusa, a Doadora do Processo de Estorno deve informar obrigatoriamente um dos seguintes códigos de justificativa:

i. “01”, que indica que houve uma validação positiva com o Cliente;
ii. “02”, que indica que o Cliente solicitou o estorno indevidamente.

7.17. Diante da recusa da Doadora do Processo de Estorno a EA deverá Informar à Receptora do Processo de Estorno que o mesmo foi negado pela Doadora. Caberá à Receptora do Processo de Estorno informar ao usuário (o)s motivo(s) da negativa.

NOTA: Havendo a necessidade por parte da Receptora do Processo de Estorno de contestação da recusa da Doadora do Processo de Estorno, deverá ser iniciado o Processo de Tratamento de Incidentes conforme descrito no item 11 deste documento.

7.18. Havendo a confirmação por parte da Doadora do Processo de Estorno quanto à ocorrência de Fraude ou Erro no Processo de Portabilidade que está sendo contestado, além de informar a EA a Doadora do Processo de Estorno deverá realizar as seguintes operações:

7.18.1. No caso de Fraude, bloqueia imediatamente todos os serviços do Código de Acesso. No caso de Erro o bloqueio deverá aguardar a conclusão da migração;

7.18.2. Caso o Código de Acesso em questão esteja sob mandato judicial, deverá ser dado início ao Processo de Quebra de Sigilo / Interceptação Judicial.

7.19. Ao receber a confirmação da Doadora do Processo de Estorno quanto à ocorrência de Fraude ou Erro no Processo de Portabilidade que está sendo

contestado a EA deverá Informar a Receptora do Processo de Estorno que esse foi aceito.

7.20. Ao receber a confirmação da EA quanto à ocorrência de Fraude ou Erro no Processo de Portabilidade que está sendo contestado, a Receptora do Processo de Estorno deverá realizar as seguintes operações:

7.20.1. Informar ao cliente que o Processo de Estorno foi aceito e que seu Código de Acesso e serviços associados serão normalizados após a conclusão do Processo de Estorno;

7.20.2. Iniciar seu processo interno de reativação a ser concluído durante a Janela de Migração estabelecida.

7.21. No horário de início da Janela de Migração agendada, deverão ser executadas as ações previstas no item 4 desse documento.

7.21.1. Finalizadas com sucesso as ações previstas no item 4 desse documento, a Receptora do Processo de Estorno deverá informar ao cliente que o Estorno foi concluído e seu Código de Acesso foi portado de volta com sucesso.

NOTA: Havendo alguma falha no processo de ativação do Código de Acesso deverá ser iniciado o Processo de Tratamento de Incidentes Pós-Portabilidade conforme descrito no item 3 do Anexo II desse documento.

7.22. É obrigação da Receptora do Processo de Portabilidade garantir que o solicitante seja realmente o titular do Código de Acesso, através da comprovação da titularidade da documentação apresentada pelo cliente. Assim, a princípio, a responsabilidade por qualquer fraude ou erro no processo de Portabilidade recai sobre as Receptoras.

7.23. Os bilhetes de portabilidade com indicativo de Estorno não passarão pelo processo de dupla autenticação com envio de SMS aos usuários.

8. Atualização de EOT

8.1. As Prestadoras devem manter atualizada a relação de EOT's cadastradas no GED da EA, conforme procedimento (https://ged.abrtelecom.com.br/documents/11085/11269/Processo+de+Atualiza%C3%A7%C3%A3o+de+EOTs_v3.ppt/58754ed0-8a57-45f9-aaf6-6c6a0ad6000c). Abaixo segue as principais ações:

NOTA: As atualizações devem ser incrementais, ou seja, somente as novas EOT's.

8.1.1. A Prestadora publica no GED o arquivo incremental de EOT's;

8.1.2. A EA realiza o batimento do arquivo publicado no GED com o Anexo V do DETRAF;

8.1.3. Caso não exista inconsistências no batimento descrito no item 8.1.2, a EA processa o arquivo publicado no GED e atualiza a tabela de referência da BDR. Caso contrário, a Prestadora será comunicada para corrigir as inconsistências encontradas;

8.1.4. A EA altera o nome do arquivo publicado no GED para "processado" e move o mesmo para o diretório de arquivos processados.

9. Disposições Gerais

9.1. Quando o Código de Acesso estiver sob interceptação judicial, toda e qualquer movimentação do mesmo deverá ser informada ao órgão competente.

9.2. Para realizar a portabilidade de um terminal no qual esteja retornando para Prestadora de origem, deve-se marcar a flag de PTO no bilhete de portabilidade.

10. Janelas de Migração e Cotas

10.1. Janela de Migração

10.1.1. Entende-se por Janela de Migração um período de 02h00min no qual todas as Prestadoras atualizam suas Bases de Referência efetivando as portabilidades previstas para ocorrerem nesse período.

10.2. Foram estabelecidas as seguintes Janelas de Migração para efetivação das portabilidades:

10.2.1. Janelas de Portabilidade nos dias úteis:

CÓDIGO	HORA INÍCIO	HORA FIM
J0	00h00min	02h00min
J1	08h00min	10h00min
J2	12h00min	14h00min
J3	16h00min	18h00min
J4	20h00min	22h00min
J5	22h00min	24h00min

10.2.2. Janelas de Portabilidade no sábado, domingo e feriados:

CÓDIGO	HORA INÍCIO	HORA FIM
J6	10h00min	12h00min
J7	14h00min	16h00min
J8	18h00min	20h00min

Nota1: Todas as Prestadoras do STFC ou SMP poderão figurar como Receptora ou Doadora em quaisquer Janelas de Migração, exceto na Janela J0. Excepcionalmente, nos casos de atendimento a portabilidades de Códigos de Acessos tipo CNG, Múltiplo, Número Único, Serviços de Emergências e Utilidade Pública, as Prestadoras do STFC poderão figurar nas segundas, quartas e sextas-feiras como Receptora ou Doadora na Janela J0.

Nota2: As seguintes datas são consideradas como feriados para o ambiente da portabilidade numérica: (i) segunda-feira de Carnaval, (ii) terça-feira de Carnaval, (iii) Sexta-Feira da Paixão, (iv) Corpus Christi, (v) 24 de dezembro, e, (vi) 31 de dezembro, além dos feriados nacionais, não facultativos, determinados pela legislação e divulgados anualmente pelo Ministério do Planejamento.

10.3. Critérios de Dimensionamento de Cotas de Janela de Migração.

10.3.1. As Janelas de Migração têm cotas pré-definidas que correspondem ao número máximo de portabilidades interprestadoras permitidas em cada Janela de Migração, tendo como referência para esse dimensionamento a capacidade instalada do sistema da EA.

10.3.2. O valor máximo de cotas por Janela é válido para todas as Janelas de Migração.

10.3.3. Todas as Janelas de Migração devem ter o valor máximo de cotas por janela

10.3.4. O valor máximo de cota será atualizado regularmente de forma ordinária e, excepcionalmente, de forma extraordinária.

10.3.5. Processo de Revisão Ordinária do Dimensionamento de Cotas.

10.3.5.1. A cada período de 2 (dois) meses, a EA deverá utilizar a seguinte fórmula para modificar o valor da cota das Janelas de Migração:

i. Valor de cota = Percentil 80 + 30%.

NOTA: Se o percentil 80 for inferior a 76% comparado ao limite atual, deverá ser considerado para o cálculo o percentil 90 mantendo o percentual de aumento de 30% do limite atual.

10.3.6. Para análise da necessidade de revisão do valor máximo de cotas será considerada a média de ocupação de todas as janelas no dia, de forma que os finais de semana e feriados com menor quantidade de Janelas tenham o mesmo peso dos dias úteis.

10.3.7. Por ter características diferenciadas de ocupação, a Janelas de Migração J0 não será contemplada no processo de revisão de cotas.

10.3.8. A EA e as Prestadoras afetadas pela atualização do valor máximo de cotas deverão disponibilizar seus sistemas e os recursos para o novo limite, um mês após a aplicação da fórmula.

10.4. Processo de Revisão Extraordinária do Dimensionamento de Cotas.

10.4.1. A Revisão Extraordinária será executada quando, num período de 08 (oito) dias consecutivos, em pelo menos 04 (quatro) dias distintos ocorrer a utilização de 85% da capacidade total do dia.

10.4.2. A EA deverá utilizar a seguinte fórmula para atualizar extraordinariamente o valor da cota:

i. Média aritmética do número de agendamentos do dia, que excedeu 85% do valor dimensionado.

10.4.3. As variações nos valores de cotas não poderão superar 15% do último valor aplicado pela fórmula da Revisão Ordinária.

10.4.4. A EA deve verificar diariamente se ocorreram as circunstâncias para se aplicar a Revisão Extraordinária. Caso haja necessidade de alteração do valor máximo de cotas por meio da Revisão Extraordinária, esse processo não voltará a ser verificado nos próximos 08 (oito) dias consecutivos.

10.4.5. As Prestadoras e EA deverão disponibilizar seus sistemas e recursos para atendimento ao novo valor máximo de cotas em até um dia após a aplicação da revisão.

11. Tratamento de Incidentes

11.1. O Processo de tratamento de incidentes tem como objetivo viabilizar a resolução das falhas ou quaisquer outros motivos que venham interromper ou não permitir a conclusão de uma portabilidade solicitada por um usuário, seja de responsabilidade das Prestadoras, do cliente ou EA, permitindo maior visibilidade, acompanhamento, controle, qualidade, minimização de impactos e riscos no processo de portabilidade, levando-se em consideração:

11.1.1. Incidentes abertos pelas Prestadoras para resolução de falhas de sistema ou de procedimento por parte das Prestadoras;

NOTA: São exemplos de solicitações: solicitação de celeridade no atendimento do BP, desativação de TN, estorno.

11.1.2. Incidentes interprestadoras para resolução de conflitos que impeçam a prosseguimento no processo de portabilidade;

11.1.3. Incidentes interprestadoras para resolução de falhas de Rede que ocorram após a conclusão da Portabilidade;

11.1.4. Solicitações registradas pelas Prestadoras para acompanhamento da Portabilidade de clientes especiais;

11.1.5. Solicitação de reserva de Janela de Migração para Manutenção Programada que possa vir a impactar o ambiente de portabilidade das Prestadoras ou EA;

11.1.6. Procedimento de Escalonamento de Incidentes entre as partes envolvidas com o objetivo de viabilizar a priorização da solução.

11.2. Incidentes interprestadoras

11.2.1. A EA deverá manter sistema para registro e acompanhamento da resolução dos conflitos entre Prestadoras que impeçam a prosseguimento no processo de portabilidade.

11.2.2. A Prestadora ofendida, ao identificar um problema antes da Janela de Migração e que impeça o processo de portabilidade, deve acionar a Prestadora ofensora através da abertura de incidente no Sistema de Tratamento de Incidentes da EA.

11.2.3. A EA deve gerar e enviar semanalmente para as Prestadoras um relatório consolidado dos incidentes abertos ou tratados no período de referência.

11.2.4. O Sistema de Tratamento de Incidentes da EA deverá enviar alerta e/ou notificações referente ao tempo de permanência dos incidentes em aberto, em função dos SLA´s previstos de resolução.

11.7.1.1. Os SLA's detalhados no quadro abaixo devem ser considerados em dias úteis contabilizando o período das 8h00min às 18h00min:

SEVERIDADE	SLA	ABRANGÊNCIA
Alta	12h00min	Iminência ou paralisação do serviço para o cliente.
Média	24h00min	Incidentes que impactam o andamento da solicitação de portabilidade.
Média Baixa	36h00min	Outros incidentes que não impactem o serviço do cliente ou o andamento da solicitação de portabilidade.
Baixa	48h00min	Incidentes que impactam o andamento da solicitação de portabilidade, relacionados à atualização de cadastro de base de dados da Anatel.

11.2.5. No caso de ocorrer impasse quanto à responsabilidade no tratamento do incidente a Entidade Administradora deverá ser acionada para busca de conciliação entre as partes envolvidas.

11.2.6. As Prestadoras devem manter atualizadas as bases de dados da Anatel que suportam o processo de solicitação de portabilidade.

11.2.7. A Anatel deve garantir a atualização de suas bases de dados que suportam a portabilidade de forma a não impactar o prazo para o cliente.

11.2.8. A Entidade Administradora deve fazer a gestão dos incidentes abertos pelas Prestadoras de forma a identificar possíveis ofensores, bem como agir junto a as Prestadoras e Fornecedores para solução definitiva do incidente.

11.2.9. As Prestadoras, ofensora e ofendida, devem manter atualizado o Sistema de Tratamento de Incidentes da EA durante todo o ciclo de vida do incidente.

11.3. Falhas de Rede

11.3.1. A EA deverá manter sistema para registro e acompanhamento das falhas de encaminhamento de rede identificadas pelas Prestadoras.

11.3.2. A Prestadora ofendida, ao identificar um problema de encaminhamento após a Janela de portabilidade, deve acionar a Prestadora ofensora através de processo de tratamento de falhas de encaminhamento já existentes entre Prestadoras e registrar o BA de Falha no Sistema de Tratamento de Falha de encaminhamento de rede da EA.

11.3.3. As Prestadoras, ofensora e ofendida, devem manter atualizado o Sistema de Tratamento de Falha de encaminhamento de rede da EA durante todo o ciclo de vida do BA de Falha.

11.3.4. A EA deve gerar e enviar semanalmente para as Prestadoras um relatório consolidado dos incidentes abertos ou tratados no período de referência.

11.3.5. O Sistema de Tratamento de Falha de encaminhamento de rede da EA deverá enviar alerta e/ou notificação referente ao tempo de permanência dos incidentes em aberto, em função do SLA previsto de resolução.

11.3.6. O SLA previsto para resolução de qualquer falha de encaminhamento de rede é de no máximo 3 (três) dias corridos.

11.4. Incidentes entre Prestadoras e EA

11.4.1. Deve ser previsto mais de um canal para abertura de incidente junto a Entidade Administradora pelas Prestadoras quando da detecção de alguma falha que impeça o processo de portabilidade e que não possa ser resolvida internamente pelas mesmas.

11.4.2. A EA deverá registrar as informações do Incidente aberto pelas Prestadoras gerando protocolo individual para cada acionamento bem como deve manter registrado em histórico todo o tratamento do Incidente.

11.4.3. A EA deverá priorizar no seu sistema de workflow o tratamento do incidente aberto pelas Prestadoras de acordo com a data e hora mais antiga e a severidade atribuída.

11.4.4. A EA quando da detecção de alguma falha no processo de portabilidade e que não possa ser resolvida internamente deve acionar as Prestadoras para abertura de Incidentes através dos canais fornecidos pelas mesmas.

11.4.5. A EA deve manter contato com as Prestadoras para identificação das causas das falhas relacionadas no incidente aberto.

11.4.6. A Prestadora deverá informar à EA as causas e a previsão para conclusão da resolução das falhas, caso as causas sejam internas da Prestadora.

11.4.7. A EA deve identificar as causas das falhas por meio da análise de arquivos de log´s, inclusive fornecidos pelas Prestadoras, e gerenciamento de hardware/software no sistema de portabilidade.

11.4.8. As Prestadoras e a EA devem utilizar-se de uma Requisição de Mudança, conforme previsto no processo de Gestão de Mudanças, para tratamento de qualquer necessidade de alterações no ambiente de portabilidade que sejam identificadas durante o processo de tratamento de incidentes.

11.4.9. A EA deve gerar e enviar periodicamente para as Prestadoras um relatório consolidado dos incidentes abertos ou tratados no período de referência.

11.4.10. A EA deve atender a solicitações de serviços que suportam o negócio e que não estejam relacionadas especificamente a uma falha.

11.4.11. A EA deve manter a Prestadora solicitante atualizada sobre o processo de recuperação do incidente para validação da solução empregada.

11.4.12. A EA deve fazer a gestão dos incidentes abertos de forma a identificar possíveis ofensores, bem como agir junto as Prestadoras e Fornecedores para solução definitiva do incidente.

11.4.13. A EA deve disponibilizar um mecanismo de *recovery* que atualize automaticamente os sistemas das Prestadoras após a correção da falha.

11.4.14. A EA deve disponibilizar um mecanismo que possibilite o sincronismo das informações das BDO com a BDR em caso de inconsistência nos dados identificada pelas Prestadoras.

11.4.15. A EA deve realizar o monitoramento e controle do processo de portabilidade prevendo a detecção pró-ativa de falhas, garantindo que as atualizações das BDO´s sejam realizadas por todas Prestadoras inclusive quanto à informação de data/hora de ativação e desativação dos terminais portados.

11.4.16. A partir da detecção de falhas ou acionamento das Prestadoras a EA deve garantir o registro do incidente, a classificação, o suporte inicial, diagnóstico, resolução e o encerramento do incidente.

11.4.17. A EA deve garantir a comunicação a todas as Prestadoras em caso de indisponibilidade geral dos serviços.

11.4.18. Devem ser previstos 3 graus de severidade para os incidentes, conforme o quadro abaixo:

SEVERIDADE	SLA (h)	ABRANGÊNCIA
1	02h00min	Situações críticas com alto nível de impacto no negócio e que afetam a maioria ou totalidade dos usuários.
2	04h00min	Situações críticas com médio nível de impacto no negócio e que afetam a maioria dos usuários ou alto nível de impacto no negócio afetando um determinado grupo de usuários.
3	08h00min	Situações com médio nível de impacto no negócio e que afetam um determinado grupo de usuários ou baixo nível de impacto no negócio.

11.5. Procedimentos de contingência

11.5.1. A EA deve disponibilizar ferramenta WEB e canal de Serviços para atendimento a solicitações de contingência pelas Prestadoras.

11.5.2. As Prestadoras devem utilizar ferramenta de contingência WEB da EA, mediante as dificuldades internas identificadas no momento de execução das atividades relacionadas ao BP e que não possam ser resolvidas internamente.

11.5.3. As Prestadoras poderão abrir incidente junto a EA para análise e, diante da viabilidade, execução das ações no BP que não possam ser realizadas diretamente pelas Prestadoras através da ferramenta de contingência WEB da EA.

11.5.4. A EA deve, sempre que possível, aplicar solução de contingência até o estabelecimento da solução definitiva.

11.5.5. A EA deve manter atualizadas as Prestadoras envolvidas na contingência em relação ao andamento das ações a serem executadas para a solução definitiva.

11.6. Acompanhamento de Portabilidades Especiais

11.6.1. As Prestadoras Receptoras poderão solicitar o acompanhamento de portabilidade de clientes especiais para a Prestadora Doadora de forma a garantir que todas as etapas do processo sejam pontualmente acompanhadas.

11.6.2. Entende-se por cliente especial descrito no item anterior os clientes que se enquadrem em pelo menos um dos requisitos abaixo:

11.6.3. Serviços de Utilidade Pública;

11.6.4. Migração de 100 (cem) ou mais acessos simultâneos de um mesmo cliente;

11.6.5. Código Não Geográfico.

11.6.6. A Entidade Administradora deve prover informações a respeito das Solicitações de Acompanhamento para todas as Prestadoras.

11.7. Processo de Manutenção Programada

11.7.1. Não faz parte do escopo deste processo o tratamento de interrupções emergenciais.

11.7.2. Deve ser observado o prazo mínimo de 15 (quinze) dias corridos para solicitação do bloqueio de Janela de Migração.

11.7.3. A solicitação de Bloqueio de Janela de Migração deverá ser realizada através da abertura de uma RdM, conforme processo de Gestão de Mudanças detalhado no anexo IV.

11.7.4. O bloqueio da Janela de Migração não poderá ser efetivado caso existam mais do que 2000 (dois mil) BP programados na respectiva janela ou mais do que 500 (quinhentos) BP´s programados para uma mesma operadora.

11.7.5. O número máximo de Janelas de Migração bloqueadas por mês deve obedecer à seguinte regra:

i. Dias úteis: 8 (oito) Janelas de Migração sendo no máximo 2 (duas) por semana e uma por dia para todas as Prestadoras;
ii. Finais de semana e feriados: 6 (seis) Janelas de Migração sendo no máximo 2 (duas) por final de semana;
iii. Uma operadora somente poderá solicitar o bloqueio de uma Janela de Migração nos dias úteis e 2 (duas) nos finais de semana no máximo.

11.7.6. A EA será a responsável pela gestão e controle do processo de bloqueio e desbloqueio de Janela de Migração para manutenção programada.

11.7.7. A solicitação de bloqueio de Janela de Migração somente deverá ser atendida pela EA se houver concordância de todas as Prestadoras que tenham BP´s programados como Receptora.

11.7.8. As Prestadoras Receptoras devem garantir a realocação de todos os BP´s que estejam programados em uma Janela de Migração bloqueada.

11.7.9. Caso não haja concordância de todas as Prestadoras Receptoras quanto ao bloqueio de uma determinada Janela de Migração e a solicitante do bloqueio desejar dar continuidade na manutenção programada esta deverá garantir a efetivação das portabilidades através de processos de contingência.

11.7.10. Qualquer Janela de Migração poderá ser bloqueada para efeito de manutenção programada observando-se os critérios descritos estabelecidos neste documento.

11.7.11. O desbloqueio de determinada Janela de Migração somente poderá ser atendido pela EA desde que seja solicitado com uma antecedência mínima de 5 (cinco) dias úteis antes da janela e pela operadora responsável pelo pedido de bloqueio da mesma.

11.7.12. O desbloqueio de Janela de Migração não elimina a cota consumida pela operadora quando da efetivação do bloqueio.

11.7.13. Deve haver concordância de todas Prestadoras quando ao desbloqueio de Janela de Migração.

11.7.14. A EA poderá solicitar o bloqueio de Janela de Migração para execução de manutenção programada obedecendo às regras estabelecidas neste documento referentes às Prestadoras.

11.8. Escalonamento

11.8.1. Entende-se por escalonamento a ação de acionamento de níveis hierárquicos superiores em caso de dificuldades da parte impactante na solução de incidentes.

11.8.2. As Prestadoras devem disponibilizar uma lista de contatos, que inclua Nome, E-mail, Telefones Fixo e Móvel, a ser utilizada pela EA e Prestadoras impactadas em casos de incidentes que necessitem de escalonamento.

11.8.3. Devem ser previstos três níveis de escalonamento interno nas Prestadoras que efetivamente corresponda à estrutura hierárquica que trata de Incidentes.

11.8.4. As Prestadoras devem disponibilizar contatos diferentes para cada nível de escalonamento.

11.8.5. Devem ser incluídos os representantes do GTOP e do GEX nos Níveis 2 (dois) e 3 (três) de escalonamento, respectivamente.

11.8.6. A EA deverá disponibilizar canal a ser utilizado pelas Prestadoras em casos de necessidade de escalonamento junto a esta Entidade, em função de incidente que for resolvido indevidamente pela Prestadora responsável ou que tenham excedido o SLA.

11.8.7. A EA deverá disponibilizar canal 24 (vinte e quatro) horas x 7 (sete) dias, por semana, a ser utilizado pelas Prestadoras em casos de necessidade de escalonamento junto a esta Entidade cuja solução é de sua responsabilidade em função de incidentes prioritários ou que tenham excedido o SLA.

11.8.8. As Prestadoras devem disponibilizar canal 24 (vinte e quatro) horas x 7 (sete) dias, por semana, a ser utilizado pela EA em caso de necessidade de escalonamento.

11.8.9. A EA deverá escalar a situação junto aos responsáveis em cada Prestadora, seguindo os níveis de escalonamento definidos, através de notificação via sistema ou contato direto.

11.8.10. As Prestadoras responsáveis deverão elaborar e apresentar à EA plano de ação para resolução definitiva do problema apontado bem como fechamento de eventuais pendências identificadas pela EA.

11.8.11. A EA deverá elaborar e apresentar às Prestadoras um Plano de Ação para resolução definitiva de problemas de sua responsabilidade.

12. Indicadores

12.1. O objetivo dessa seção é estabelecer as regras para apuração e validação dos resultados mensais dos Indicadores Operacionais previstos no Regulamento Geral de Portabilidade - RGP, Artigos. 49 §2º, 53 e 54, a saber:

TAP: Taxa de Autenticação da Portabilidade;
TIP: Taxa de Interrupção do serviço do cliente durante o Período de Transição da Portabilidade;
TEP: Taxa de Efetivação da Portabilidade.

12.2. Metas estabelecidas no RGP para os Indicadores Operacionais descritos no item 12.1 e regras de medição.

12.2.1. TAP - Taxa de Autenticação da Portabilidade.

i. 100% das Autenticações, considerando-se autorizações e recusas do BP, devem ocorrer em até 1 (um) dia, contabilizando a partir das 0h00mim do primeiro dia útil subsequente ao dia do pedido da portabilidade;
ii. O Indicador deve ser medido percentualmente a partir da relação entre o total de solicitações de portabilidade autenticadas no prazo e o total de solicitações de autenticação de portabilidade;
iii. O Indicador deve ser apurado individualmente para todas as Prestadoras envolvidas no processo de portabilidade como Doadora;
iv. Devem ser desconsideradas as Portabilidades Intrínsecas, para as quais não se faz necessário o processo de Autenticação;
v. Devem ser desconsideras todas as solicitações de portabilidade canceladas antes do término do prazo de autenticação, para as quais não haja registro de Autenticação da Doadora;
vi. São considerados ofensores deste indicador todos os eventos de perda de prazo de autenticação, ainda que o BP seja autorizado tacitamente pela EA por decurso de prazo;
vii. Os BPs devem ter seus eventos de “autenticação” computados no mês de sua ocorrência.
viii. Os bilhetes com status de Falha Parcial devem ser considerados como portados.

12.2.2. TIP: Taxa de Interrupção do serviço do cliente durante o Período de Transição de Portabilidade.

i. 99% dos períodos de transição devem ter duração máxima de 2h00mim;
ii. 100% dos períodos de transição devem ocorrer em no máximo 24h00mim;
iii. O Indicador deve ser medido percentualmente a partir da relação entre o total de transições realizadas dentro do período de interrupção de até 2h00mim e o total de portabilidades efetivadas e a relação entre o total de transições realizadas dentro do período de interrupção máximo de 24h00mim em relação ao total de portabilidade efetivadas;
iv. O indicador deve ser apurado individualmente para todas as Prestadoras envolvidas no processo de portabilidade como Receptora;

v. Serão consideradas como atendidas no prazo todas as transições cuja ativação na Receptora ocorra em até 02h00min após a desativação na Doadora ou quando a Receptora ativar o serviço do cliente dentro da Janela de Migração ou quando a Doadora desativar o serviço do cliente após a ativação na Receptora;
vi. Devem ser desconsideradas as portabilidades intrínsecas;
vii. Devem ser desconsideradas as portabilidades de estorno;
viii. Devem ser desconsideradas as portabilidades canceladas;
ix. Serão considerados como não atendidos no prazo os BP´s que, após o prazo de 5 (cinco) dias corridos da data da Janela de Migração, não considerando tal data, não possuam a informação de quando o serviço foi ativado na rede da Receptora;
x. Os bilhetes com status de Falha Parcial devem ser considerados como portados.

12.2.3. TEP: Taxa de Efetivação da Portabilidade

12.2.3.1. O cálculo da Taxa de Efetivação da Portabilidade deverá ser realizado segundo dois critérios de tempo:

12.2.3.1.1. Cômputo em dias úteis, conforme previsto no RGP, sendo válido para as Autorizadas do Serviço Telefônico Fixo Comutado (STFC) e Serviço Móvel Pessoal (SMP);

12.2.3.1.2. Cômputo em dias corridos, conforme previsto no Plano Geral de Metas de Universalização (PGMU), sendo válido apenas para as Concessionárias do STFC.

12.2.4. Taxa de Efetivação da Portabilidade para o critério estabelecido no item 12.2.3.

i. 95,00% dos processos de portabilidade devem ser efetivados em até 3 (três) dias úteis, contabilizados a partir das 00h00min do primeiro dia útil subsequente ao dia da abertura do BP;
ii. 100% dos processos de portabilidade devem ser efetivados em até 5 (cinco) dias úteis, contabilizados a partir das 00h00min do primeiro dia útil subsequente ao dia da abertura do BP;

iii. O Indicador deve ser medido percentualmente a partir da relação entre o total de solicitações de portabilidade efetivadas no prazo de 3 (três) e 5 (cinco) dias úteis e o total de solicitações de portabilidade efetivadas;
iv. O indicador deve ser apurado individualmente para todas as Prestadoras envolvidas no processo de portabilidade como Receptora;
v. Devem ser desconsiderados os finais de semanas e feriados estabelecidos;
vi. Deve ser considerado para efeito de apuração deste Indicador o período desde as 00h00min do primeiro dia útil subsequente ao dia da solicitação da portabilidade até o momento da ativação do serviço na rede da Receptora;
vii. Devem ser desconsideradas as portabilidades intrínsecas;
viii. Devem ser desconsideradas as solicitações canceladas;
ix. Devem ser desconsideradas as solicitações de estorno;
x. As solicitações agendadas a pedido do cliente e atendidas até o horário agendado devem ser consideradas como atendidas no prazo;
xi. Deve ser desconsiderado o período em que o BP estiver na condição de Suspenso ou Conflito;
xii. Os bilhetes com status de Falha Parcial devem ser considerados como portados.
xiii. Serão considerados como não atendidos no prazo os BP's que, após o prazo de 5 (cinco) dias corridos da data da Janela de Migração, não considerando tal data, não possuam a informação de quando o serviço foi ativado na rede da Receptora.

12.3. Quanto à validação dos Indicadores a serem apresentados pela Entidade Administradora, o processo deve ser composto dos seguintes passos:

12.3.1. A EA deverá apresentar para todas as Prestadoras e a Anatel, por meio de sistema próprio, os resultados mensais consolidados de todos os Indicadores;

12.3.2. As Prestadoras, de posse dos resultados mensais consolidados, farão a avaliação de conformidade dos indicadores, apresentando formalmente suas contestações à EA em caso de dúvidas ou não conformidades identificadas;

12.3.3. A EA avaliará a procedência da contestação, devendo sempre apresentar a argumentação técnica adequada a cada caso. Sendo considerada a contestação procedente, a EA deverá, ainda, corrigir os Indicadores

contestados, dando ciência a todas as Prestadoras envolvidas e a ANATEL;

12.3.4. O processo de contestação de indicadores descrito nos itens 3.2 e 3.3 desse Anexo poderá, também, ser utilizado pela ANATEL.

12.4. Disposições Gerais

12.4.1. Não é escopo deste documento o tratamento dos relatórios e indicadores de gestão da EA sobre seus Parceiros Técnicos contratados para operacionalização da portabilidade.

12.4.2. A EA deve disponibilizar Painel de Indicadores, desenvolver fluxo de análise, contestação e correção dos indicadores e gerá-los mensalmente conforme estabelecido neste documento.

12.4.3. As Prestadoras devem desenvolver um fluxo de tratamento de indicadores em seus sistemas e processos internos e validar mensalmente os resultados disponibilizados pela EA.

12.4.4. A Especificação Funcional que detalha a geração dos Indicadores e o processo de contestação encontra-se disponível no sistema GED da EA no diretório da versão atual do Manual Operacional.

12.4.5. A Especificação Funcional de que trata o item 12.4.5, assim como qualquer alteração na mesma, deve ser aprovada pelas Prestadoras e ANATEL.

13. Gestão de Mudanças

13.1. O Processo de Gestão de Mudanças tem como objetivo permitir que o ambiente de portabilidade seja alterado de forma padronizada a partir das necessidades das Prestadoras, EA e Parceiro Tecnológico da EA, com o emprego das melhores práticas de governança de TI do mercado, assegurando a eficiência e mitigando os impactos nesse ambiente.

13.2. O Processo de Mudança deve ser gerido pela EA, de forma a garantir o cumprimento de todas as etapas pelos Agentes do Processo, assim como deve

manter toda a documentação pertinente em meio magnético para consultas futuras.

13.3. A EA em conjunto com as Prestadoras deve estabelecer uma Política de Governança para controle do todo o processo desde o recebimento da solicitação de Mudança até a execução da RdM.

13.4. A EA deve manter um Sistema de Gestão de Mudanças com acesso pela Web que permita o registro da documentação pertinente e a administração do fluxo de análises e aprovações.

13.5. O Representante do Envolvido que desejar solicitar uma alteração no serviço deverá preencher a RdM descrevendo os requisitos de negócio que representam suas necessidades de Mudança e encaminhar por e-mail ao Gestor do Processo de Mudanças da EA.

13.6. A EA deve avaliar se a RdM está corretamente preenchida, ou com os dados mínimos para análise, observando se a Mudança proposta é pertinente.

NOTA: A avaliação sobre a pertinência da Mudança proposta será realizada pela EA com base nos requisitos de negócio estabelecidos na RdM. Quando necessário a EA poderá solicitar o auxílio do Comitê de Gestão de Mudanças para realizar essa análise em conjunto.

13.7. Com base na análise descrita no item 13.5, a EA decidirá pelo registro no Sistema de Gestão de Mudanças e abertura da RdM ou pelo retorno ao solicitante para revisão dos requisitos de negócio.

13.8. Durante o registro da solicitação no Sistema de Gestão de Mudanças a EA deverá classificar a RdM quanto a Urgência, Criticidade e Tipo, de acordo com as regras estabelecidas no item 13.18.

13.9. A partir da conclusão do processo de registro e geração da RdM os Representantes dos Envolvidos devem receber em suas caixas postais de e-mail a notificação de pendência de análise.

13.10. Os Representantes dos Envolvidos devem registrar seus pareceres nos formulários de análises estabelecidos, inclusive as análises de esforço, impactos e riscos.

13.11. Os Representantes dos Envolvidos devem fornecer esclarecimentos adicionais, quando solicitado, para elaboração das propostas de solução das RdM's pelo parceiro tecnológico da EA.

13.12. A EA deve organizar reuniões para leitura e entendimento da solicitação de Mudança dando suporte aos Representantes dos Envolvidos em suas análises internas e elaboração dos documentos de que trata o item 13.9.

13.13. A EA deve organizar reuniões de conciliação com vistas na obtenção de consenso quanto à lista de RdM's a serem submetidas para aprovação entre os Representantes dos Evolvidos e elaboração de proposta em comum, englobando uma avaliação custo-benefício proporcionado por cada RdM.

13.14. Os Representantes dos Envolvidos devem garantir o desenvolvimento interno, testes e homologação da solução técnica que atenda à solicitação de Mudança, conforme planejamento conjunto a ser elaborado.

13.15. Os Representantes dos Envolvidos devem realizar suas estimativas e análises técnicas em até 10 dias úteis a contar da data da disponibilização da RdM pela EA.

13.16. Os Representantes dos Envolvidos devem priorizar as Mudanças propostas com base nos requisitos funcionais das RdM's.

NOTA: Devem ser consideradas prioritárias as RdM's para atendimento a requisitos de negócio legais/regulatórios.

13.17. Os Representantes dos Envolvidos devem definir os prazos e planejar as demais etapas para execução das RdM´s com base na ordem de prioridade de cada Mudança Proposta.

13.18. Estrutura de classificação das RdM´s.

13.18.1. Quanto a Urgência

Nome	Meta de finalização	Descrição
Emergencial	O mais rápido possível	Solicitações geradas para instalação da solução de um incidente crítico, gerador de uma interrupção ou degradação do serviço, com alto impacto nos processos de negócio ou nas metas de qualidade do serviço e com abrangência que afeta a maioria dos usuários.
Programada	Conforme planejamento da Mudança	Solicitação de mudanças, independente do fator gerador, onde exista uma programação para seu desenvolvimento, teste e/ou instalação no ambiente produtivo do serviço.

13.18.2. Quanto ao impacto

NOTA: Para determinação do impacto, deve ser considerado o tempo de interrupção ou degradação do serviço, além da implicação em atraso no atendimento de outras demandas.

Nome	Continuidade da Operação	Negócios/Jurídico-Regulatório
Altíssimo	Provoca interrupção ou degradação da qualidade do serviço em períodos de atendimento de altas demandas de vendas (ex.: Natal, dias das mães, dias dos namorados, dias dos pais)	Seu atendimento resulta em atraso no atendimento de demandas regulatórias ou legais causando penalidades a clientes ou à prestadora de telecomunicações.
Alto	Provoca interrupção ou degradação da qualidade do serviço em períodos maiores que 8 horas contínuas ou interruptas.	Seu atendimento resulta em atraso no atendimento de todas as demandas programadas previamente.
Médio	Provoca interrupção ou degradação da qualidade do serviço em períodos de 1h e 1 minuto até 8 horas contínuas ou interruptas.	Seu atendimento resulta em atraso no atendimento de parte das demandas de outros clientes.
Baixo	Provoca interrupção ou degradação da qualidade do serviço em períodos de até 1 hora contínuas ou interruptas.	Seu atendimento resulta em atraso no atendimento de demandas somente do próprio solicitante.

Nenhum	Não há interrupção ou degradação da qualidade do serviço.	Não há atraso no atendimento de outras demandas.

13.18.3. Quanto ao Tipo

Nome	Descrição
Evolutiva	Mudança com objetivo de atender uma demanda visando melhorias, adequações ou conformidade nos processos do negócio ou da melhoria técnica funcional dos aplicativos e elementos integrantes do serviço.
Corretiva	Mudança com objetivo de aplicar a solução de um problema, incidente ou erro em ambiente produtivo, corrigindo o mesmo.
Manutenção Preventiva	Tem por objetivo a realização de manutenção programada do serviço, qual visa a manter a qualidade dos itens da estrutura técnica do serviço.
Manutenção Interna*	Objetiva formalizar e aprovar uma janela para trabalhos internos em uma Prestadora integrante do serviço

13.19. É de responsabilidade dos Representantes dos Envolvidos garantirem o registro de uma RdM para qualquer manutenção programada ou emergencial a ser realizada no ambiente interno de Portabilidade, comunicando a todos os envolvidos os impactos e riscos associados.

NOTA: As RdM's para manutenção no ambiente interno de portabilidade dos Representantes dos Envolvidos deverão ser classificadas como tipo "Manutenção Interna".

13.20. É responsabilidade do Conselho de Portabilidade da EA a aprovação final para a execução das RdM´s, podendo inclusive cancelar o processo ou solicitar a reavaliação tanto de escopo como de necessidade ao Comitê de Indústria.

13.21. A EA deve desenvolver um modelo de custos que permita a execução de RdM com interesse de pelo menos um dos Representantes do Envolvidos, desde que não haja impactos para os demais.

13.22. A Especificação Funcional que detalha todo o processo, agentes, responsabilidades, formulários e SLA envolvidos está disponível no link: http://ged.cleartech.com.br/gmud/Documentacao.

13.23. A figura abaixo mostra uma visão macro para o Processo de Gestão de Mudanças:

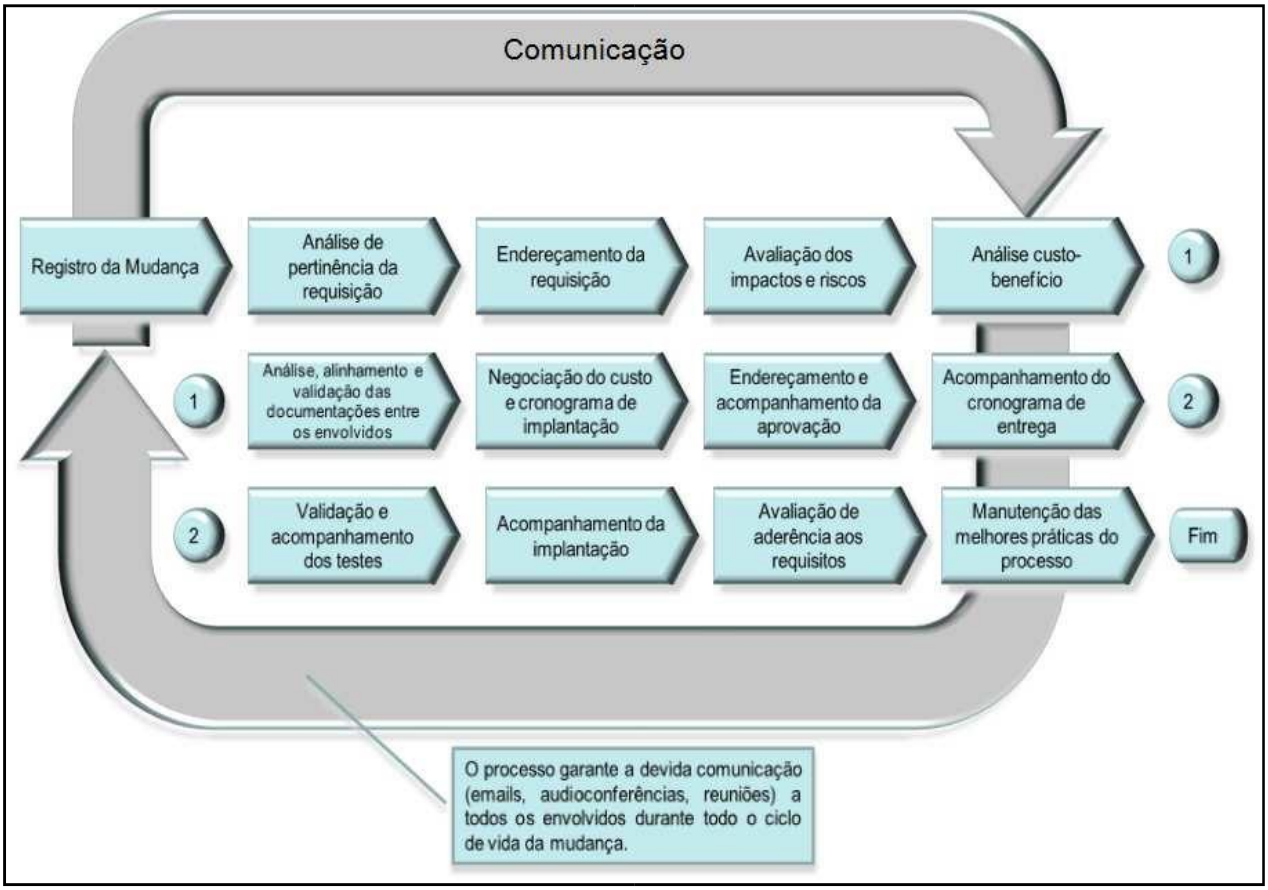


Figura 01 – Macro Processo de Gestão de Mudanças