PRESIDÊNCIA DA REPÚBLICA
Comitê Nacional de Cibersegurança

Ata da 9ª Reunião Ordinária (RO-001-26)

Em 25 de março de 2026, das 14h20 às 16h45, reuniu-se no Palácio do Planalto, 4º Andar, Sala 98, o Pleno do Comitê Nacional de Cibersegurança (CNCiber) para sua Nona Reunião Ordinária (RO-001-26).

1. PROCEDIMENTOS

1.1 Verificação do Quórum

Às 14h20 o Presidente do CNCiber abriu a RO-001-26 do CNCiber.

Em atendimento ao disposto no Decreto 11.856, de 26 de dezembro de 2023, que instituiu o CNCiber, procedeu-se, em primeira chamada, a verificação do quórum para a reunião. Constatou-se a presença de titulares e/ou suplentes de 22 das 25 instituições que compõem o CNCiber, cumprindo a disposição do Decreto 11.856 quanto ao quórum para reuniões do CNCiber. Também presentes estavam representantes da ABIN e do TCU, instituições convidadas.

1.2 Aprovação da Ata da RO-004-25

Procedeu-se, em seguida, à aprovação da ata da RO-004-25.

A referida ata fora aprovada *ad referendum* pelo Presidente do CNCiber após o envio da minuta aos membros e decorrido o prazo de manifestações, tendo sido efetuados ajustes por solicitação do representante do MGI.

O Presidente, então, solicitou aos membros que confirmassem a referenda feita com relação à ata, a qual foi aprovada por unanimidade.

1.3 Aprovação da Pauta da RO-001-26

Procedeu-se, então, à aprovação da pauta previamente enviada aos participantes, acrescida de um item (13) por sugestão do GSI, além de uma mudança na ordem dos itens 11 e 12 da pauta original para as posições 7 e 8, respectivamente, solicitada pelo representante da FIESP, ficando a pauta final conforme transcrita a seguir.

1. *Verificação do quórum.*
2. *Aprovação da ata da RO-004-25.*
3. *Aprovação da pauta da RO-001-26.*
4. *Informe sobre o Marco Legal da Cibersegurança em tramitação no Senado.*
5. *Informe sobre o Anteprojeto da Lei Geral da Cibersegurança aprovado pelo CNCiber.*
6. *Deliberação sobre proposta de dar publicidade, fundamentada no princípio da transparência e publicidade da coisa pública, ao Anteprojeto da Lei Geral da Cibersegurança aprovado pelo CNCiber, bem como às propostas de ANCiber; e*
7. *Deliberação sobre proposta de realização de Audiências Públicas sobre as propostas (referidas no item 11), a serem capitaneadas pelo CNCiber.*
8. *Informe sobre Auditoria Operacional do TCU sobre Fraudes usando a Imagem do Governo.*
9. *Deliberação sobre a conclusão dos trabalhos do GTT Cibereducação-Estratégias e encerramento do GTT.*

10. *Deliberação sobre a proposta de criação de um novo GTT para continuidade dos trabalhos de dos GTTs Cibereducação anteriores.*
11. *Deliberação sobre a conclusão dos trabalhos do GTT P-Ciber-Estruturante e encerramento do GTT.*
12. *Informe sobre o andamento dos trabalhos do GTT Maturidade.*
13. *Deliberação sobre a proposta de criação de um GTT P-Ciber-Antipersonificação, para a proposição de Iniciativas Estratégicas para o Combate a Fraudes baseadas em Personificação Governamental, a serem incluídas no P-Ciber.*

A pauta foi aprovada por unanimidade.

1.4 Informe sobre o Marco Legal da Cibersegurança em tramitação no Senado.

O Presidente do CNCiber informou ao pleno que o Marco Legal da Cibersegurança em discussão no Senado está na Comissão de Ciência e Tecnologia daquela Casa, com relator designado, para deliberação em caráter terminativo. Isso significa dizer que após aprovação nessa Comissão o PL será considerado aprovado pelo Senado e irá para a Câmara dos Deputados para deliberação como casa revisora. Caso sofra alterações na Câmara retornará ao Senado para nova aprovação.

Informou também que O PL em questão é bastante diverso daquela minuta de anteprojeto proposta e aprovada por unanimidade pelo CNCiber na RO-004-25, e se beneficiaria muito da mesclagem dos dois textos. Disse que segundo informações da Secretaria-Executiva da Frente Parlamentar de Apoio à Cibersegurança e à Defesa Cibernética (FrenCyber), haveria disposição da casa na avaliação da possibilidade de ajustes ao texto antes da deliberação na CCT.

1.5 Informe sobre o Anteprojeto da Lei Geral da Cibersegurança aprovado pelo CNCiber.

O Presidente do CNCiber informou ao pleno que a minuta do Anteprojeto de Lei aprovada pelo CNCiber na RO-004-25 foi remetida à CC/SAEJ logo após a reunião que o aprovou. Alguns pontos foram ajustados entre a SE-CNCiber e a SAEJ. Dias depois a SE-CNCiber e o GSI enviaram à SAEJ/CC uma proposta de um anteprojeto unificado, incorporando ao texto do Marco Legal em discussão no Senado as propostas da minuta aprovada pelo CNCiber. Informou também que foi solicitada uma reunião, entre o GSI, a CC, o MGI e a SRI para verificar as alternativas de envio dos diferentes textos ao Senado antes da deliberação terminativa na CCT, mas que tal reunião ainda não ocorreu.

1.6 Deliberação sobre proposta de dar publicidade ao Anteprojeto da Lei Geral da Cibersegurança aprovado pelo CNCiber, bem como às propostas de ANCiber

O Presidente do CNCiber informou ao pleno que a FIESP apresentou proposta de dar publicidade, fundamentada no princípio da transparência e publicidade da coisa pública, ao Anteprojeto da Lei Geral da Cibersegurança aprovado pelo CNCiber, bem como às propostas de ANCiber.

Solicitou, em seguida, que o representante da FIESP explicasse a proposta. O representante da FIESP argumentou que um grande esforço foi realizado pelo CNCiber para a discussão e elaboração das propostas em questão. Que entende que o CNCiber é um órgão consultivo, de sorte que suas propostas podem ser adaptadas, ou até desconsideradas, pelo decisor. Mas que o trabalho feito deve ser publicizado, em alinhamento com os princípios da transparência e publicidade da coisa pública, de sorte que a sociedade possa conhecer e opinar sobre o trabalho realizado.

Seguiram-se manifestações favoráveis dos representantes da Casa Civil, da ANATEL, do MJSP, da FGV, da ASSESPRO, do IASP, do MGI e do MRE. Nas manifestações foi observado que se trata de uma minuta não vinculativa, mas que contém muitos detalhes que podem ser úteis, por exemplo, para

avaliação pelos legisladores durante o debate que ocorre no Senado, bem como por eventuais setores da sociedade que possam ser afetados pela proposta.

Findas as manifestações, a proposta foi aprovada por unanimidade.

A SE-CNCiber informou, então, que tão logo seja publicada a ata da RO-001-25 os documentos gerados pelos diferentes grupos de trabalho serão disponibilizados na página oficial do CNCiber.

1.7 Deliberação sobre proposta de realização de uma Audiência Pública sobre a minuta da Lei Geral da Cibersegurança e as propostas alternativas de ANCiber

O Presidente do CNCiber informou ao pleno que a apresentou proposta de realização de uma audiência pública, capitaneada pelo CNCiber, para avaliação do Anteprojeto da Lei Geral da Cibersegurança e das alternativas de ANCiber.

Solicitou, em seguida, que o representante da FIESP explicasse a proposta. O representante da FIESP argumentou que o princípio já fora discutido no item anterior, mas que além de dar publicidade ao tema seria possível coletar contribuições da sociedade para as propostas.

A representante do IASP argumentou que, sendo dada a devida publicidade aprovada no item 6 da pauta, entendia que audiências públicas seriam realizadas no Congresso, não sendo necessário que o CNCiber se ocupasse dessa tarefa.

O representante da ANATEL informou que a realização de uma audiência pública implica em estruturar um processo de reposta a cada uma das sugestões recebidas, com eventual alteração do texto apresentado e que, nesse ponto, concordava que o melhor seria não realizar uma Audiência Pública, mas talvez uma apresentação da minuta aprovada. Em suas palavras, uma explicação de "como e porque chegamos a essas propostas", facilitando a análise do conteúdo por aqueles que estiverem interessados.

Seguiu-se um rápido debate sobre o tema e o Presidente propôs que a SE-CNCiber avaliasse as opções de apresentação das minutas e propostas à sociedade, elaborasse uma proposta e solicitasse a anuência dos membros do CNCiber, para então dar prosseguimento à ação.

A proposta foi aprovada por unanimidade.

1.8 Informe sobre Auditoria Operacional do TCU sobre Fraudes usando a Imagem do Governo

O Presidente informou que o TCU encaminhou processo de Tomada de Contas em andamento a diferentes órgãos, alguns dos quais representados no CNCiber. Embora o GSI não seja um órgão diretamente relacionado ao tema, o TCU entendeu por incluí-lo no processo, enquanto órgão que exerce a Presidência do CNCiber e atua como SE-CNCiber.

Informou que uma das medidas propostas contidas no documento consiste em **determinar** a publicação do P-Ciber, possivelmente incluindo iniciativas estratégica para combate a golpes efetuados por meio da personificação de órgãos públicos.

O representante do TCU fez uma breve explanação sobre o processo de deliberação do TCU, informando que o relatório fora enviado para comentário pelos órgãos citados, que depois seria eventualmente ajustado pelos auditores com base nos comentários recebidos, então submetido ao Min. Relator, e então ao Pleno do TCU. Somente a partir de então ele passa a ter caráter vinculante.

1.9 Deliberação sobre a conclusão dos trabalhos do GTT Cibereducação-Estratégias e encerramento do GTT.

O Presidente informou que o referido GTT foi instituído na RO-003-25 com a finalidade de complementar as propostas do GTT Cibereducação, e foi coordenado pela Profa. Érica Galindo, da Casa Civil. Como a Profa. Se encontrava ausente, por motivo de saúde, solicitou que um dos membros do GTT fizesse a apresentação do relatório dos trabalhos do GTT.

A representante do IPCD fez uma explanação dos trabalhos realizados, apontando que após o primeiro GTT Cibereducação ter feito um extenso trabalho de curadoria dos materiais de cibereducação existentes no País, o presente GTT estudou diversas estratégias para levar esses materiais aos diferentes públicos-alvo (crianças e adolescentes, pessoas neurodivergentes, idosos e mulheres) vítimas preferenciais de cibercrimes. Explicou que o GTT trabalhou diversas questões, mas que constatou que o próximo passo é aprofundar o debate com foco em cada um dos públicos-alvo citados. Informou que o GTT entendeu que crianças e adolescentes deveriam ser o primeiro público em foco. Observou também que o GTT constatou que essa continuidade dos debates é um reflexo e uma evidência da natureza continuada da necessidade da cibereducação. Por fim, disse que por todas essas razões propunham a criação de um novo GTT Cibereducação-Crianças e Adolescentes, a ser discutido em seguida.

O Presidente então colocou em deliberação a aprovação do relatório e o encerramento do GTT.

Ambos foram aprovados por unanimidade.

1.10 Deliberação sobre a Proposta de criação de um novo GTT para continuidade dos trabalhos dos GTTs Cibereducação

Passou-se à discussão da proposta de um novo GTT Cibereducação com foco em estratégias de cibereducação para crianças e adolescentes, com a mesma duração e integrado pelas mesmas instituições do GTT anterior, acrescido por outras instituições que demonstrassem interesse.

Os representantes do MGI e da ASSEPRO demonstraram interesse em participar.

Dessa forma, o GTT será integrado por:

1. Agência Nacional de Telecomunicações, que o coordenará;
2. Casa Civil da Presidência da República;
3. Ministério da Gestão e Inovação em Serviços Públicos;
4. Comitê Gestor da Internet no Brasil - CGI.Br;
5. Federação das Indústrias do Estado de São Paulo - FIESP (setor empresarial);
6. Instituto Peck de Cidadania Digital - IPCD (setor sociedade civil);
7. Instituto dos Advogados de São Paulo - IASP (setor sociedade civil);
8. Centro de Pesquisa e Desenvolvimento em Telecomunicações - CPqD (setor científico, tecnológico e de inovação);
9. Fundação Getúlio Vargas - FGV (setor científico, tecnológico e de inovação);
10. Rede Nacional de Ensino e Pesquisa - RNP (setor científico, tecnológico e de inovação); e
11. Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação - ASSESPRO.

Como o número de participantes superou o limite regimental, o Pleno do CNCiber autorizou a excepcionalidade.

A proposta foi aprovada por unanimidade.

1.11 Deliberação sobre a conclusão dos trabalhos do GTT P-Ciber-Estruturante e encerramento do GTT

O Presidente informou que o referido GTT foi instituído na RO-003-25 com a finalidade de complementar as propostas do GTT Cibereducação, e foi coordenado conjuntamente pelo GSI e pelo MGI. Solicitou então ao SE-CNCiber, que representou o GSI na Coordenação do GTT, que apresentasse o relatório.

O Coordenador informou que a criação desse GTT fora proposta com vistas a complementar as 127 Iniciativas Estratégicas propostas pelos GTT P-Ciber com ações com características de mais longa duração e preferencialmente que fossem interinstitucionais ou de abrangência nacional. Acrescentou que um dos pontos mais relevantes do trabalho do GTT anterior foi o de estipular um mecanismo de atualização do P-Ciber, que seria essencial para as próximas etapas. Informou que o grupo discutir diversas questões, tendo chegado a um conjunto d e18 Iniciativas Estratégicas Estruturantes (IEEs) que complementavam as 127 Iniciativas Estratégicas Institucionais (IEIs) originalmente propostas. Complementou informando que as próximas etapas consistem na formatação do P-Ciber com as IEIs e IEEs aprovadas, submissão do P-Ciber à anuência dos 15 órgãos governamentais do CNCiber e posterior publicação.

Finda a apresentação, o Presidente colocou em deliberação a aprovação do relatório e o encerramento do GTT.

Ambos foram aprovados por unanimidade.

1.12 Informe sobre o andamento dos trabalhos do GTT Maturidade

O presidente informou que o GTT Maturidade foi instituído na RO-003-25, e foi coordenado conjuntamente pelo GSI e pelo MGI. Solicitou então ao SE-CNCiber, que representou o GSI na Coordenação do GTT, que apresentasse o andamento.

O Coordenador informou que o vem trabalhando com afinco na elaboração de um Modelo de Maturidade (denominado CIMBRA – Ciber Maturidade Brasileira) Nacional (CIMBRA-N) e outro Institucional (CIMBRA-I). Informou que o CIMBRA hoje apresenta 6 níveis de maturidade (0-Inicial, 1-Fundamental, 2-Básico, 3-Médio, 4-Evoluído e 5-Avançado). Informou que o modelo foi concebido com 3 níveis hierárquicos.

Abordando inicialmente o CIMBRA-N, explicou que os 3 níveis são Eixos, Vetores e Aspectos, que são avaliados com base em Evidências explicitadas. Explicou que são 8 Eixos, desdobrados em 35 Vetores, subdivididos em 92 Aspectos, os quais podem ser verificados por 411 Evidências. Informou que o trabalho no CIMBRA-N está bastante avançado, restando a finalização da alocação das Evidências aos correspondentes Aspectos, o que por vezes implica em alterar os Aspectos e, eventualmente, um ou outro Vetor. Que esse trabalho deve ser finalizado no início de Abril, de sorte que em fins de abril pode ser possível a realização de um piloto do modelo (versão Alfa) com um conjunto de cerca de 12 instituições respondentes. Que em seguida, feitos os ajustes necessários, pode ser feito novo piloto (Beta) com cerca de 35 instituições, para nova validação e ajustes, a ocorrer em maio ou junho. E que assim seria possível a realização da primeira avaliação completa nacional com o novo modelo em meados do 2º semestre de 2026. Informou que o GSI estuda a possibilidade de realizar uma terceira avaliação com o modelo CMM Oxford nesse período. A primeira foi em 2020, a segunda em 2023, e a terceira estava prevista para 2026. A realização dessa avaliação em paralelo com a primeira do CIMBRA-N proveria parâmetros de comparação entre os dois modelos.

Passando para o CIMBRA-I, explicou que, no presente momento, os 3 níveis hierárquicos do modelo

são denominados Eixos, Processos e Ações. São atualmente 14 Eixos, desdobrados em 66 Processos, subdivididos em 469 Ações. A título de comparação, explicou que o PPSI tem 2 níveis, sendo 18 Controles subdivididos em 153 Salvaguardas. Comentou que o grande objetivo e desafio, no momento, é a integração do CIMBRA-I com o PPSI. A representante do MGI, também Coordenadora do GTT, exemplificou que o PPSI hoje não contempla TO (Tecnologia Operacional), que está presente no CIMBRA-I, sendo necessário avaliar a melhor forma de complementar o PPSI para encaixá-lo nesse contexto mais amplo. O SE-CNCiber continuou explicando que o CIMBRA-I foi pensado para se integrar ao CIMBRA-N, de forma a permitir a geração de dados para o estabelecimento de Políticas Públicas Orientadas por Evidências. Avaliou que seja possível o GTT apresentar o CIMBRA-I em junho (no máximo em outubro), posto que com o fim do desenvolvimento do CIMBRA-N as atenções ficarão focadas no CIMBRA-I.

Por fim, explicou que o CIMBRA-I, como concebido, permite a análise dos dados de maturidade coletados por diferentes dimensões: Instituição, Setor, Porte, Eixo, Processo ou Ação. Que interligando esses dados com os dados de interdependência da cadeia de suprimentos é possível identificar os elos mais fracos de toda a cadeia, possibilitando uma atuação para o robustecimento desses pontos fracos, elevando a maturidade do conjunto como um todo.

Seguiu-se uma breve sessão de perguntas e respostas sobre alguns detalhes dos modelos.

1.13 Deliberação sobre a proposta de criação de um GTT Antipersonificação.

O Presidente informou que paralelamente ao trabalho de publicação do P-Ciber deliberado anteriormente, o GTT proposto poderá estudar a conveniência e oportunidade de incluir iniciativas estratégicas para tratar do problema público dos golpes por meio da personificação de sites governamentais. Caso decida pela aprovação de algumas IEs sobre o tema, elas serão incorporadas ao P-Ciber em seguida, seguindo o rito de anuência e publicação previsto.

Assim, a proposta prevê um GTT P-Ciber-Antipersonificação com as seguintes características:

> *GTT P-Ciber-Antipersonificação, para a proposição de Iniciativas Estratégicas para o Combate a Fraudes baseadas em Personificação Governamental, a serem incluídas no P-Ciber.*
>
> *a) Duração de 60 dias*
> *b) Coordenado conjuntamente pelo GSI e MJSP*
> *c) Participação da CC, MD, MGI, MCom, ANATEL, BACEN, CGI e outras entidades que tenham interesse ou expertise na temática.*

O Presidente solicitou ao representante do TCU que fizesse uma breve explanação do problema tratado pelo TCU.

O representante do TCU fez uma breve explicação da situação e da necessidade de atacá-la.

O representante do MJSP manifestou que o problema em tela tem duas vítimas: o cidadão atingido, diretamente prejudicado, e o governo, que fica com sua imagem arranhada. Explicou que inclusive a Polícia Federal já foi vitimada por personificação indevida. Por fim, concordou com a Coordenação conjunta do GTT.

Além dos membros sugeridos pelo GSI na proposta, também manifestaram interesse em participar o MRE, o MCTI, a ASSESPRO, CONEXIS-BRASSCOM e CPqD. Como o total de participantes supera o limite regimental, o CNCiber deliberou por autorizar a excepcionalidade.

A proposta de criação do GTT foi aprovada por unanimidade.

2. ENCERRAMENTO

Não havendo mais temas a tratar, a RO-001-26 foi declarada encerrada pelo Presidente.

3. ANEXOS

Anexei a essa ata:

1. O Relatório do GTT Cibereducação-Estratégias aprovado pelo CNCiber.
2. O Relatório do GTT P-Ciber-Estruturante aprovado pelo CNCiber.

MARCELO ANTONIO OSLLER MALAGUTTI

Secretário-Executivo do CNCiber

ESTRATÉGIAS DE CIBEREDUCAÇÃO

Relatório final do GTT instituído pela Resolução CNCIBER Nº 15, de 13/10/2025

BRASÍLIA – 2026

Sumário

1 Apresentação

1.1 Contexto de criação do GTT

Por meio da Resolução CNCIBER nº 15, de 13/10/25, foi instituído o grupo de trabalho temático para elaboração de estratégias de divulgação de materiais educativos de Cibersegurança. A criação deste GTT é um desdobramento direto dos resultados alcançados e das lacunas identificadas pelo GTT precedente, estabelecendo um ciclo contínuo de fortalecimento da cultura de segurança digital no Brasil.

O GTT anterior foi instituído pela Resolução CNCiber nº 9, de 26/5/25, com a missão de identificar ou elaborar materiais educativos de cibersegurança e planejar estratégias de difusão. Durante seu período de atuação, aquele grupo realizou um extenso diagnóstico que resultou na curadoria de materiais, identificação de um vasto volume de conteúdos já disponíveis na sociedade e em órgãos públicos. Embora houvesse abundância de material técnico, não houve tempo hábil para o desenvolvimento detalhado de estratégias de comunicação e disseminação eficazes para os diversos públicos-alvo.

Neste cenário, diante da necessidade de transformar o acervo curado em ações práticas de conscientização, o CNCiber instituiu este novo GTT focado especificamente na elaboração de estratégias de difusão de materiais educativos de Cibersegurança.

1.2 Delimitação do escopo e exclusões

A definição do escopo de atuação deste GTT seguiu critérios de viabilidade técnica, impacto social e conformidade com os prazos estabelecidos para a entrega de resultados. Nesse contexto, tanto a Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 11.856, de 26/12/2023, quanto a Estratégia Nacional de Cibersegurança (E-Ciber), instituída pelo Decreto nº 12.573, de 4/8/2025, reconhecem a necessidade de promover a segurança digital de diferentes segmentos da sociedade, com destaque para crianças e adolescentes como públicos prioritários.

Considerando, contudo, a diversidade e as especificidades dos grupos mencionados nesses instrumentos, o escopo deste GTT foi delimitado de forma estratégica, a fim de assegurar maior efetividade às ações propostas.

Ressalta-se que, o grupo realizou um levantamento, anexo ao presente documento, com insumos para realizar um diagnóstico e mapeamento inicial. Após esta fase, o GTT optou por concentrar seus esforços iniciais no público de crianças e adolescentes, especificamente nas faixas de 12 a 15 anos (Ensino Fundamental II) e 16 a 18 anos (Ensino Médio), fundamentando-se nos seguintes aspectos:

- Alcance em larga escala. A possibilidade de atingir um universo expressivo de crianças e adolescentes por meio da rede escolar pública e privada.

- Articulação institucional. A existência de canais de diálogo estabelecidos com órgãos centrais de governança, como o Ministério da Educação (MEC) e as secretarias estaduais de educação, facilitando a implementação das estratégias de difusão.

- Base de evidências. Dados da pesquisa TIC Kids Online Brasil e diretrizes do Programa Escola que Protege que apontam estas faixas etárias como crítica para a prevenção de violências e riscos digitais.

- Base metodológica replicável. O trabalho de identificação e classificação de riscos digitais desenvolvido para este público servirá como base conceitual e metodológica para futuras ações destinadas aos outros segmentos identificados.

Embora o foco atual tenha sido o público infantojuvenil, as discussões realizadas no âmbito do GTT ratificaram a necessidade urgente de contemplar outros grupos em situação de vulnerabilidade previstos na E-Ciber, os quais demandam expertises específicas e estratégias de comunicação distintas, tais como:

- Pessoas idosas (60+) que requer linguagem adaptada e canais de disseminação específicos para a inclusão digital segura.

- Pessoas neurodivergentes que necessitam de materiais acessíveis e metodologias que considerem suas particularidades de processamento de informação.

Para além dos segmentos prioritários já previstos na PNCiber e E-Ciber, a síntese das pesquisas analisadas por este GTT indica que o grupo de mulheres também apresenta uma combinação crítica de vulnerabilidade e exposição a ameaças específicas no ambiente digital. Dados e estimativas revelam um cenário alarmante que demanda atenção institucional dedicada, evidenciando que, somente em 2024, 1,6 milhão de mulheres tiveram fotos e vídeos íntimos vazados na internet sem seu consentimento, enquanto 8,5 milhões foram vítimas de *stalking*[1]. Tais indicadores reforçam a urgência da elaboração de estratégias de proteção e conscientização voltadas especificamente a este segmento.

[1] FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Visível e invisível: a vitimização de mulheres no Brasil. 5. ed. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em:

Assim, dada a expertise necessária para cada um desses segmentos de públicos, este GTT sugere a proposição de novos grupos de trabalho técnicos para cada um dos segmentos apresentados — idosos, neurodivergentes e mulheres —, incluindo especialistas técnicos nas várias áreas. Também se sugere como possibilidade a criação de GTT liderado pela SECOM para elaborar uma estratégia unificada de uso dos canais governamentais para a difusão de conteúdos de cibersegurança a toda a sociedade.

1.3 O GTT P-Ciber-Educação

O Grupo de Trabalho Técnico (GTT) Educação-Estratégias desenvolveu suas atividades entre 22/10/2025 e 05/03/2026, com o objetivo central de elaborar estratégias para a difusão de materiais educativos em cibersegurança. O grupo adotou um regime de reuniões quinzenais de 1h hora de duração cada, estruturando suas entregas em torno da curadoria de materiais existentes e do desenvolvimento de novos modelos de disseminação.

O percurso do GTT foi marcado por quatro fases principais de amadurecimento descritas nas seções a seguir.

1.3.1 Fase 1 - Diagnóstico e Mapeamento Inicial (Out/Nov.25)

As primeiras reuniões focaram no levantamento de materiais produzidos pelo GTT anteriores e na identificação de públicos prioritários. Destaca-se a apresentação da representante da Anatel em 05/11, que trouxe um panorama dos grupos mais suscetíveis a riscos cibernéticos, fundamentando a escolha dos alvos das ações.

1.3.2 Fase 2 - Integração com tecnologias emergentes (Nov.25)

Em 26/11, o grupo aprofundou o debate sobre a relação entre Inteligência Artificial (IA) e Cibersegurança, com apresentação do representante do CPQD. Essa discussão revelou a necessidade futura de um GT específico para IA, mas, para o escopo atual, serviu para refinar os riscos digitais que seriam abordados nos materiais educativos.

1.3.3 Fase 3 - Definição de foco e segmentação (Dez.25)

Após análise técnica, o grupo optou por priorizar o público de crianças e adolescentes, devido às evidências disponíveis sobre a gravidade do problema; à clareza dos canais de disseminação (como a rede escolar); à gama de materiais

https://forumseguranca.org.br/wp-content/uploads/2025/03/relatorio-visivel-e-invisivel-5ed-2025.pdf. Acesso em: 5 mar. 2026.

disponíveis para utilização direta nas ações da estratégia; à priorização do público nas políticas públicas vigentes (Política Nacional de Cibersegurança e Estratégia Nacional de Cibersegurança); e à demanda da sociedade por ações na temática. Em 03/12, decidiu-se que a abordagem para outros grupos, como pessoas neurodivergentes e idosos, seria adaptada posteriormente com base na metodologia que viesse a ser desenvolvida para o público infantil.

Adicionalmente, restou claro para o grupo que ações para pessoas neurodivergentes demandam o engajamento de especialistas na temática a fim de compreender melhor eventuais diferentes riscos a que esse grupo está exposto no ambiente digital, assim como diferentes necessidades em termos de conscientização (recursos, veículos, materiais, etc), também considerando que o grupo abrange pessoas com diversas diferenças neurológicas e que, portanto, uma única estratégia pode não ser viável para o grupo com um todo.

1.3.4 Fase 4 - Consolidação de Modelos e Reclassificação (Jan.26)

As reuniões finais focaram na criação de documentos de proposta de modelo de estratégia e na reclassificação técnica de materiais produzidos no GTT anterior. O grupo trabalhou na catalogação por risco digital, faixa etária e tipo de uso do material.

1.4 Metodologia de trabalho do GTT

Para garantir a qualidade técnica e a viabilidade das propostas, o GTT utilizou as seguintes frentes metodológicas:

- Curadoria especializada. Foi realizada uma revisão e catalogação de materiais destinados a cidadãos, professores e setores público/privado, produzidos pelos GTT criado pela Resolução CNCIBER nº 9, de 26/5/25.
- Divisão multidisciplinar de tarefas. Foi realizada uma distribuição alternada de itens de estudo entre os membros para evitar sobrecarga e garantir múltiplas perspectivas, resultando em diversas apresentações realizadas sobre temas relacionados à temática de Cibereducação, conforme mencionado na seção anterior.
- Ferramentas de apoio. Foram utilizadas ferramentas como o NotebookLM para a criação de infográficos e sistematização de textos de insumo para IA visando modernizar a apresentação dos resultados durante os trabalhos do grupo.

- Participação colaborativa. O cronograma de reuniões foi mantido mesmo em períodos de férias, garantindo a continuidade do fechamento dos documentos e a consolidação da nova categorização dos materiais que integram a Campanha Nacional Boas Conexões (CNBC), detalhada nas seções 2 e 3 deste documento.

1.5 A proposta elaborada

Com resultado do trabalho realizado, o grupo propõe a realização da **Campanha Nacional Boas Conexões (CNBC)**, abrangendo os sistemas de ensino municipais, estaduais, distrital e federal, conforme os arts. 12 (IX), 16, 17 e 18 da Lei nº 9.394/1996 (LDB), com execução prioritária nas unidades que atendem estudantes do ensino fundamental II e do ensino médio.

No contexto escolar, o ECA Digital reforça o dever das instituições de ensino de atuar de forma preventiva, educativa e protetiva, promovendo ações de conscientização, orientação e mediação de conflitos relacionados ao uso das tecnologias digitais, especialmente diante de práticas como *cyberbullying*, assédio online, exposição indevida de imagem, violência digital e outros riscos de conduta e contato.

A implementação de campanhas educativas estruturadas, continuadas e mediadas por professores e equipes pedagógicas, como a proposta neste documento, encontra respaldo direto no ECA Digital, ao contribuir para:

- a promoção da convivência digital respeitosa;
- o desenvolvimento de competências para identificação de riscos e violências online;
- o fortalecimento de canais de apoio, acolhimento e encaminhamento;
- a prevenção de danos à saúde mental, à dignidade e aos direitos fundamentais de crianças e adolescentes.

Essa abordagem reafirma o papel da escola como espaço central de proteção, formação cidadã e promoção de direitos no ambiente digital, em consonância com este importante marco legal e com as diretrizes da Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 11.856, de 26 de dezembro de 2023[2], e da Estratégia

2 BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em 04/03/2026

Nacional de Cibersegurança (E-Ciber), aprovada pelo Decreto nº 12.573, de 4 de agosto de 2025[3].

Nesse sentido, a campanha pode ser estruturada de forma faseada e integrada, iniciando-se por uma etapa de sensibilização e informação mediada pelos educadores, com a disponibilização de materiais pedagógicos, bem como de orientações para a utilização, conforme listagem anexa.

Em seguida, a campanha deve avançar para uma fase de apropriação e reflexão, por meio da realização de outras atividades mediadas no ambiente escolar, como debates orientados, rodas de conversa e oficinas, conduzidas por professores e equipes pedagógicas, com o objetivo de estimular o diálogo, a reflexão crítica e o desenvolvimento de habilidades socioemocionais relacionadas às interações digitais.

Como etapa de engajamento criativo e protagonismo juvenil, recomenda-se o lançamento de premiação voltada à produção de vídeos curtos, com duração de até um minuto, por estudantes das escolas públicas. A iniciativa deve incentivar a expressão criativa e coletiva dos estudantes, culminando em processo de seleção e premiação das melhores produções, respeitando o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) e a vinculação de todo uso de dados ao superior interesse da criança e do adolescente.

A campanha poderia contemplar, ainda, uma fase de reconhecimento e divulgação dos resultados, com a publicização das produções selecionadas e o compartilhamento de boas práticas no âmbito das redes de ensino, de modo a ampliar o alcance das mensagens e fortalecer a cultura de cibersegurança nas comunidades escolares.

Recomenda-se que a campanha seja coordenada nacionalmente pelo Ministério da Educação, em articulação com as secretarias estaduais, distrital e municipais de educação e demais órgão e instituições interessadas. Ainda que seja integrada a políticas e programas já existentes, como o Programa Escola que Protege, de modo a evitar sobreposição de iniciativas e assegurar coerência institucional. A execução local deve ocorrer no âmbito das unidades escolares, com apoio das equipes pedagógicas e das redes de ensino.

A estratégia deve contar, ainda, com a articulação de uma rede de apoio e encaminhamento, envolvendo serviços psicossociais, conselhos tutelares e organizações

3 BRASIL. Decreto nº 12.573, de 6 de agosto de 2025. Institui a Institui a Estratégia Nacional de Cibersegurança. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em 04/03/2026

especializadas, para orientação, acolhimento e encaminhamento de casos identificados no contexto escolar.

2 Campanha Nacional Boas Conexões (CNBC)

2.1 Problema e diagnóstico

O uso crescente de tecnologias digitais por crianças e adolescentes ampliou a exposição desse grupo a diversos riscos no ciberespaço. O acesso precoce a dispositivos conectados, plataformas digitais e redes sociais cria oportunidades relevantes para aprendizagem, socialização e desenvolvimento de competências digitais. Entretanto, esse mesmo processo também expõe esse público a uma série de riscos e vulnerabilidades que exigem respostas estruturadas de políticas públicas e estratégias educacionais.

Relatórios internacionais sobre proteção infantil no ambiente digital destacam que a segurança online das crianças e adolescentes constitui um desafio crescente para governos, escolas, famílias e empresas de tecnologia[4]. A digitalização trouxe novas formas de exposição a violência, exploração e práticas abusivas, tornando necessário compreender como crianças utilizam tecnologias digitais, quais riscos enfrentam e quais mecanismos podem ser implementados para reduzir tais vulnerabilidades. Nesse contexto, a proteção infantil no ambiente digital requer uma abordagem multidimensional que combine, entre outros instrumentos, educação e regulação (em sentido amplo).

No campo regulatório, em resposta a essa realidade, a PNCiber estabelece como um de seus objetivos o fortalecimento da atuação diligente de crianças e adolescentes no ambiente digital, pautando-se, como princípio norteador, na garantia dos direitos fundamentais.

A PNCiber tem como instrumento a E-Ciber, que detalha as iniciativas para implementar os objetivos da política incluindo a proteção e a conscientização do cidadão, de forma a criar condições seguras para o uso dos serviços digitais, especialmente por pessoas em situação de vulnerabilidade, como crianças e adolescentes.

A E-Ciber prevê, entre outras medidas, ações de incentivo à atuação segura no ciberespaço, capacitação de professores em cibersegurança; inclusão de temas relacionados à cibersegurança nos currículos de todos os níveis educacionais; e promoção da prevenção e do combate aos cibercrimes, às fraudes digitais e a outras práticas maliciosas no ciberespaço por meio de atuação multisetorial.

[4] UNITED NATIONS CHILDREN'S FUND (UNICEF). **Child safety online: global challenges and strategies**. Florence: UNICEF Office of Research – Innocenti, 2012. Disponível em: https://www.unicef.org/media/66821/file/Child-Safety-Online.pdf. Acesso em: 04/03/2026

Complementarmente, o Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025)[5] reconhece que o ambiente digital integra o contexto de desenvolvimento, socialização e aprendizagem de crianças e adolescentes, atribuindo responsabilidade compartilhada entre órgãos públicos, escolas, famílias, plataformas digitais e sociedade na promoção de ambientes seguros e adequados à condição peculiar de desenvolvimento desse público.

Quanto à educação, essa deve ser compreendida como parte de um campo mais amplo de literacia digital, que envolve processos de educação, formação e capacitação voltados ao uso seguro, crítico e responsável das tecnologias digitais[6]. A literacia digital não se limita à aquisição de habilidades técnicas operacionais, mas compreende o desenvolvimento de conhecimentos, competências e capacidades que permitem aos indivíduos compreender e utilizar tecnologias digitais de maneira informada e responsável.

Nesse âmbito, destaca-se também o conceito de ciber-higiene utilizado na literatura de cibersegurança para descrever o conjunto de práticas e comportamentos rotineiros que contribuem para a proteção de ativos digitais e usuários que devem ser integradas por meio da educação[7]. Tais práticas incluem, entre outras, o uso adequado de mecanismos de autenticação, a gestão segura de credenciais, a verificação da confiabilidade de mensagens e *links* recebidos, a proteção da privacidade em redes sociais e a adoção de cuidados durante a navegação e o compartilhamento de informações.

Estudos indicam que níveis mais elevados de ciber-higiene estão associados a maior capacidade de processamento crítico de informações online e à adoção de comportamentos digitais mais seguros, reduzindo a probabilidade de exposição a ameaças como fraudes, *phishing* e outros ataques baseados em engenharia social[8].

Dessa forma, iniciativas educacionais voltadas à promoção da cibersegurança devem buscar não apenas ampliar o conhecimento sobre riscos digitais, mas também

5 BRASIL. Lei nº 15.211, de 23 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm. Acesso em 04/03/2026

6 Belli, Luca; Medeiros, Breno; Couto, Natália; Bakonyi, Erica; Gaspar, Walter; Lage, Daniel. Governança e regulação da cibersegurança no Brasil: proteção da infraestrutura crítica, segurança da informação e construção da soberania digital. Rio de Janeiro: Lumen Juris, 2026. Disponível em: https://direitorio.fgv.br/publicacao/governanca-e-regulacao-da-ciberseguranca-no-brasil. Acesso em 04/03/2026.

7 Ibidem, p. 127.

8 VISHWANATH, Arun et al. Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, v. 128, p. 113160, 2020. Disponível em: https://doi.org/10.1016/j.dss.2019.113160. Acesso em 04/03/2026.

incentivar a incorporação de práticas de ciber-higiene no cotidiano de crianças e adolescentes, contribuindo para o desenvolvimento de hábitos digitais seguros desde as etapas iniciais da formação escolar.

Diante desse contexto, a seção seguinte apresenta as principais categorias de ameaças digitais consideradas no âmbito desta estratégia.

2.2 Riscos digitais

2.2.1 Eixos de riscos

Esta ação considera dois eixos de riscos que exigem monitoramento constante para garantir a integridade dos estudantes e a efetividade da política pública, conforme detalhamento a seguir.

2.2.1.1 Riscos associados ao público-alvo

A exposição contínua a ambientes digitais hostis sem a devida mediação acarreta consequências severas, que justificam a priorização desta iniciativa[9]. Entre as principais, destacam-se:

- Impacto psicossocial: aumento de quadros de ansiedade, depressão, isolamento social e, em casos extremos, autolesão, decorrentes de situações de humilhação pública, *cyberbullying* e perseguição online[10,11].

- Evasão e rendimento escolar: o ambiente escolar, quando percebido como inseguro ou associado à extensão da violência virtual, pode levar à recusa escolar, queda no desempenho cognitivo e abandono dos estudos[12].

[9] COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil: TIC Kids Online Brasil 2024. Disponível em: https://cgi.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf.

[10] BOTTINO, Sara Mota Borges et al. Cyberbullying and adolescent mental health: systematic review. Cadernos de Saúde Pública, v. 31, n. 3, p. 463-475, 2015. Disponível em: https://doi.org/10.1590/0102-311X00036114. Acesso em 05/03/2026.

[11] FERREIRA, Taiza Ramos de Souza Costa; DESLANDES, Suely Ferreira. Cyberbulling: conceituações, dinâmicas, personagens e implicações à saúde. Ciência & Saúde Coletiva, v. 23, n. 10, p. 3369-3379, 2018. Disponível em: https://doi.org/10.1590/1413-812320182310.13482018. Acesso em 05/03/2026.

[12] KOWALSKI, Robin M.; LIMBER, Susan P. Psychological, physical, and academic correlates of cyberbullying and traditional bullying. Journal of Adolescent Health, v. 53, n. 1, p. S13-S20, 2013. Disponível em: https://doi.org/10.1016/j.jadohealth.2012.09.018. Acesso em 05/03/2026.

- Normalização da violência: o risco de dessensibilização dos estudantes frente ao discurso de ódio, naturalizando comportamentos agressivos como forma padrão de interação social, fenômeno que agrava a escalada da violência escolar[13,14].

2.2.1.2 LACUNAS ESTRUTURAIS E DESAFIOS DE IMPLEMENTAÇÃO

Para mitigar falhas na execução, é necessário reconhecer e atuar sobre as lacunas existentes na rede de ensino.

- Desigualdade de acesso e letramento: a disparidade no acesso a dispositivos e na fluência digital entre diferentes regiões e níveis socioeconômicos podem comprometer o alcance uniformizado da campanha[15].

- Preparo da equipe pedagógica: a ausência de formação continuada específica sobre cultura digital para professores pode gerar insegurança na mediação de conflitos, exigindo materiais de apoio robustos e autoexplicativos[16].

- Engajamento familiar: a dificuldade de integração entre a escola e as famílias na supervisão das atividades online representa um ponto crítico de governança, demandando estratégias de comunicação que ultrapassem os muros da escola e fortaleçam a corresponsabilidade na proteção dos estudantes[16].

Além dos impactos psicossociais e das lacunas estruturais já identificadas, o ambiente digital impõe um conjunto amplo e interconectado de riscos específicos a crianças e adolescentes, que demandam abordagem integrada na formulação de políticas públicas.

---

[13] CARA, D. (Relator). Ataques às escolas no Brasil: análise do fenômeno e recomendações para a ação governamental. Brasília, DF: Ministério da Educação (MEC), 2023. Disponível em: https://www.gov.br/mec/pt-br/acesso-a-informacao/participacao-social/grupos-de-trabalho/prevencao-e-enfrentamento-da-violencia-nas-escolas/resultados/relatorio-ataque-escolas-brasil.pdf. Acesso em: 05/03/2026.

[14] QUEIROZ, C.; FRAIZ, V. Violência escolar aumenta nos últimos 10 anos no Brasil. Revista Pesquisa FAPESP, São Paulo, ed. 350, abr. 2025. Disponível em: https://revistapesquisa.fapesp.br/violencia-escolar-aumenta-nos-ultimos-10-anos-no-brasil/. Acesso em: 05/03/2026.

[15] COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: TIC Educação 2023. São Paulo: Núcleo de Informação e Coordenação do Ponto BR (NIC.br), 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20241119194257/tic_educacao_2023_livro_completo.pdf . Acesso em: 05/03/2026.

[16] Comitê Gestor da Internet no Brasil. TIC Kids Online Brasil PESQUISA SOBRE O USO DA INTERNET POR CRIANÇAS E ADOLESCENTES NO BRASIL. São Paulo. 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf. Acesso em 05/03/2026.

2.2.2 CATEGORIAS DE RISCOS

Conforme mencionado, o uso intensivo da internet e de dispositivos digitais por crianças e adolescentes amplia significativamente sua exposição a diferentes tipos de ameaças no ambiente online. Essas ameaças, que não são homogêneas, podem manifestar-se de diversas formas e envolver diferentes tipos de comportamentos e impactos no bem-estar físico e psicológico, aprendizagem e na convivência escolar de crianças e adolescentes[17] [18].

A literatura analisa as ameaças digitais enfrentadas por crianças e adolescentes e identificou um conjunto recorrente de categorias relacionadas à riscos que permitem compreender o cenário de forma sistemática[19] [20]. Entre essas categorias destacam-se os riscos de conteúdo, de contato, de conduta, de consumo, econômicos e de privacidade, os quais podem se manifestar isoladamente ou de forma combinada nas experiências digitais de crianças e adolescentes. As categorias de riscos são apresentadas no quadro a seguir.

Categoria do risco	Descrição
CR1. Riscos de conteúdo	• Os riscos de conteúdo referem-se à exposição a materiais inadequados ou potencialmente prejudiciais ao desenvolvimento infantil. • Esses conteúdos podem incluir material violento, pornográfico ou discriminatório, bem como informações que incentivem comportamentos nocivos, como o consumo de drogas, automutilação ou práticas perigosas.

[17] **2º Boletim técnico "Escola que Protege: dados sobre bullying e cyberbullying"**. 1. ed. Curitiba: Ministério da Educação, 2025. Disponível em: https://www.gov.br/mec/pt-br/escola-que-protege/segundo-boletim-tecnico-escola-que-protege.pdf Acesso em 04/03/2026. FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 04/03/2026.

[18] Comitê Gestor da Internet no Brasil. TIC Kids Online Brasil PESQUISA SOBRE O USO DA INTERNET POR CRIANÇAS E ADOLESCENTES NO BRASIL. São Paulo. 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf Acesso em 04/03/2026. BRASIL. Ministério da Educação. Secretaria de Educação Continuada, Alfabetização de Jovens e Adultos, Diversidade e Inclusão (SECADI).

[19] QUAYYUM, Farzana; CRUZES, Daniela S.; JACCHERI, Letizia. Cybersecurity awareness for children: A systematic literature review. **International Journal of Child-Computer Interaction**, v. 30, p. 100343, 2021. Disponível em: https://doi.org/10.1016/j.ijcci.2021.100343 Acesso em 04/03/2026

[20] Livingstone, Sonia; Stoilova, Mariya. The 4Cs: Classifying online risk to children. 2021. Disponível em: https://www.researchgate.net/publication/349888588_The_4Cs_Classifying_online_risk_to_children Acesso em 04/03/2026.

	• A facilidade de acesso a diferentes plataformas digitais amplia a probabilidade de que crianças e adolescentes entrem em contato com esse tipo de material, muitas vezes sem a mediação ou orientação adequada de adultos.
CR2. Riscos de contato	• Os riscos de contato dizem respeito às interações online entre crianças e outros usuários que podem representar ameaça à sua segurança ou integridade. • Entre os exemplos mais frequentes estão o contato com desconhecidos, o aliciamento online (*grooming*), tentativas de manipulação emocional ou exploração sexual, além de práticas de perseguição digital (*cyberstalking*). • Esses riscos são frequentemente facilitados pela anonimidade e pela assimetria de poder entre adultos e crianças em ambientes digitais.
CR3. Riscos de conduta	• Os riscos de conduta estão associados aos comportamentos adotados pelos próprios usuários no ambiente digital, incluindo *cyberbullying*, disseminação de discursos ofensivos, compartilhamento de informações pessoais ou participação em práticas que possam causar danos a si mesmos ou a outros. • Essas situações podem ocorrer tanto na condição de vítima quanto de autor, refletindo a dinâmica interativa das plataformas digitais.
CR4. Riscos econômicos (ou riscos de consumo ou contrato)	• Os riscos econômicos envolvem situações em que crianças e adolescentes são expostos a fraudes, golpes financeiros ou práticas comerciais enganosas no ambiente digital. • Esses riscos podem incluir tentativas de *phishing*, roubo de identidade, golpes em plataformas digitais, compras não autorizadas em aplicativos ou jogos online e outras práticas fraudulentas que exploram a inexperiência dos usuários mais jovens.

CR5. Riscos à privacidade	• Os riscos relacionados à privacidade e à proteção de dados decorrem da coleta, uso ou compartilhamento indevido de informações pessoais no ambiente digital. • Crianças e adolescentes frequentemente compartilham dados pessoais, fotografias, localização ou outras informações sensíveis sem plena compreensão das possíveis consequências desse comportamento. • A exposição dessas informações pode gerar diversos tipos de vulnerabilidades, incluindo uso indevido de dados, roubo de identidade, chantagem digital ou exploração comercial de informações pessoais.

2.2.3 DIMENSÕES DE RISCOS

Diante da multiplicidade e complexidade dos riscos digitais identificados na literatura, a estratégia delineada neste documento adota um recorte analítico deliberado, organizado em três dimensões principais de risco. Essa opção metodológica busca simplificar a abordagem pedagógica da temática no contexto educacional, sem prejuízo da abrangência das diferentes ameaças presentes no ambiente digital.

Para fins deste trabalho, algumas categorias tradicionalmente tratadas de forma independente na literatura consultada[21] foram organizadas em três dimensões principais. Assim, os riscos de conduta e contato foram agrupados em um eixo único. Os riscos relacionados à privacidade e à exposição de dados pessoais foram considerados como riscos transversais, podendo incidir em qualquer um dos eixos, motivo pelo qual não foram abordados em uma categoria em apartado. E os riscos econômicos são tratados com a nomenclatura de riscos de consumo, abrangendo situações como fraudes digitais, golpes online, práticas comerciais enganosas e compras indevidas em ambientes digitais, conforme a tabela de referência a seguir.

Dimensão do risco	**Categorias de riscos**
D1. Conduta & contato	CR2. Riscos de contato CR3. Riscos de conduta

[21] Ibidem.

D2. Conteúdo	CR1. Riscos de conteúdo
D3. Consumo	CR4. Riscos econômicos

A partir dessa organização, para cada uma das dimensões de riscos foi desenvolvida uma frente temática específica, que detalha ações pedagógicas, educativas e preventivas adaptadas às características e vulnerabilidades do público-alvo.

Essa abordagem permitirá enfrentar de forma estruturada ameaças de alta incidência no contexto escolar, com impactos diretos sobre o bem-estar, a convivência, a permanência e o desempenho educacional dos estudantes, contribuindo para a promoção de experiências digitais seguras, responsáveis e conscientes.

2.2.4 GRADAÇÃO DE RISCOS E FLUXO DE RESPOSTA

O delineamento da severidade dos incidentes no ambiente digital e a definição de seus respectivos fluxos de encaminhamento encontram amparo transversal no Sistema de Garantia de Direitos. O Estatuto da Criança e do Adolescente a Lei de Diretrizes e Bases da Educação Nacional e a Lei nº 14.811/2024 atuam de forma conjunta em todos os estágios do conflito, desde a prevenção primária e mediação pedagógica até a responsabilização criminal e proteção integral.

A estruturação de fluxos claros de encaminhamento responde à necessidade de articular a escola com a rede de proteção, reconhecendo os limites da atuação estritamente educacional. O encaminhamento não se configura como uma transferência de responsabilidades, mas sim como o acionamento de uma rede intersetorial (composta por saúde, assistência social, conselho tutelar e justiça) essencial para garantir o cuidado integral da vítima e a intervenção adequada junto ao agressor. Essa ação é imperativa não apenas para evitar a omissão institucional frente a violações de direitos, mas para assegurar que as respostas sejam céleres, especializadas e proporcionais à gravidade de cada caso.

Dessa forma, a atuação das instituições de ensino deve observar uma gradação de riscos estruturada nos níveis descritos na tabela a seguir que estabelece a gradação de riscos e o fluxo de respostas, em estrita observância às diretrizes da Lei nº 14.811/2024, detalhando os níveis de severidade e as medidas que devem ser tomadas por órgãos e entidades (como escolas, conselhos e polícia) diante de cada nível de risco digital detectado.

Nível	Descrição	Encaminhamento
N1. Conflitos de convivência digital e uso inadequado	Desentendimentos pontuais, divergências de opinião ou práticas iniciais de risco de consumo.	São passíveis de mediação pedagógica interna visando o restabelecimento do diálogo e a orientação educativa.
N2. Intimidação sistemática (Cyberbullying) e exposição moderada	Ações intencionais, repetitivas e sem motivação evidente que causam sofrimento à vítima, ou situações de dependência de jogos e vazamento de dados que afetam o bem-estar.	Exigem intervenção da gestão escolar, acolhimento e envolvimento das famílias.
N3. Infrações, crimes digitais e exploração	Casos graves que envolvem ameaças à integridade física, divulgação de cenas de nudez, racismo, homofobia, incitação à violência, aliciamento, fraudes financeiras severas ou exploração sexual infantil.	Demandam acionamento imediato da rede de proteção (Conselho Tutelar, Ministério Público e autoridades policiais).

2.2.5 CLASSIFICAÇÃO DOS RISCOS E VIOLÊNCIAS NO AMBIENTE DIGITAL

A compreensão e a categorização das violências e ameaças no ambiente digital exigem um alinhamento com metodologias consolidadas internacionalmente e adotadas por órgãos oficiais brasileiros. Para garantir a precisão conceitual e orientar as intervenções pedagógicas de forma fundamentada[22], a tipologia de riscos apresentada a seguir baseia-se na classificação utilizada neste documento (Conduta e Contato, Conteúdo e Consumo).

Natureza da agressão e da interação de risco	Descrição
Conduta e Contato	• Agressão visual e Exposição: produção, manipulação ou compartilhamento de figurinhas (*stickers*), memes depreciativos, vídeos ou imagens adulteradas (*deepfakes*) e exposição de mídia íntima não consentida.

[22] Comitê Gestor da Internet no Brasil. TIC Kids Online Brasil PESQUISA SOBRE O USO DA INTERNET POR CRIANÇAS E ADOLESCENTES NO BRASIL. São Paulo. 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf Acesso em 04/03/2026. BRASIL. Ministério da Educação. Secretaria de Educação Continuada, Alfabetização de Jovens e Adultos, Diversidade e Inclusão (SECADI).

	• Exclusão social: criação de grupos, fóruns ou páginas com o intuito deliberado de isolar, ignorar, ridicularizar ou segregar determinados estudantes do convívio digital coletivo. • Intimidação sistemática (Cyberbullying): a junção repetitiva e intencional das agressões citadas acima, incluindo apelidos pejorativos e perseguição continuada, configurando violência escolar tipificada na legislação brasileira. • Violação de identidade (Personificação): criação de perfis falsos (fakes) para se passar por terceiros com o intuito de difamar ou constranger a vítima perante seus pares. • Assédio e Aliciamento (*Grooming*): abordagens indesejadas, frequentemente realizadas por estranhos ou perfis falsos, com o objetivo de obter vantagens, cooptação para atividades ilícitas ou exploração sexual infantil. • Extorsão e Perseguição: chantagem envolvendo o vazamento de imagens íntimas (*sextortion*) e o monitoramento obsessivo e intimidador da vítima nos ambientes digitais (*cyberstalking*).
Conteúdo	• Consumo de material violento ou extremista: exposição a vídeos, fóruns ou imagens que exibam violência explícita, crueldade contra animais, ou que promovam a radicalização e a cooptação por grupos extremistas. • Incentivo a comportamentos nocivos: contato com informações e "desafios virais" (*challenges*) que estimulem a automutilação, distúrbios alimentares, uso de substâncias ilícitas ou práticas que coloquem a vida e a integridade física em risco. • Exposição a material pornográfico: acesso (intencional ou acidental, muitas vezes impulsionado por algoritmos) a conteúdos adultos ou de sexualização precoce, incompatíveis com o estágio de desenvolvimento psicossocial da criança ou do adolescente. • Desinformação e Manipulação (*Fake News*): consumo de notícias falsas, teorias da conspiração ou conteúdos manipulados que prejudicam a segurança informacional, a compreensão da realidade e o desenvolvimento do pensamento crítico do estudante.

Consumo	• Engenharia Social e Fraudes (*Phishing*): táticas de manipulação para o roubo de credenciais (senhas) e dados pessoais por meio de e-mails falsos, links maliciosos ou mensagens enganosas em redes sociais. • Golpes Financeiros e de Comércio Eletrônico: fraudes envolvendo aplicativos bancários, clonagem de aplicativos de mensagens para pedidos de transferências financeiras, emissão de boletos falsos e compras em sites não verificados. • Exploração Comercial Abusiva: indução a compras não autorizadas ou compulsivas em aplicativos e jogos online (como microtransações e *loot boxes*), além da exposição a publicidade velada voltada ao público infantil. • Exposição Indevida de Dados Pessoais (*Oversharing*): compartilhamento excessivo ou desprotegido de informações sensíveis (localização, rotina, documentos pessoais) que comprometem a privacidade e facilitam o roubo de identidade. • Vulnerabilidades de Acesso e Infraestrutura: riscos associados à falta de higiene cibernética, como o uso de redes Wi-Fi públicas desprotegidas para transações, ausência de autenticação em duas etapas (2FA), negligência com backups e infecção por malwares via downloads não seguros.

2.3 Objetivos gerais e resultados esperados

A CNBC tem como propósito central:

- Conscientizar crianças e adolescentes sobre os riscos digitais, abrangendo as dimensões de conteúdo, conduta e contato, além das vulnerabilidades relacionadas ao consumo, aos riscos econômicos e à privacidade.
- Estimular comportamentos pautados no respeito, na empatia, na segurança informacional e no uso seguro e responsável das tecnologias digitais.
- Desenvolver a capacidade crítica de identificação de situações de risco, violência online, fraudes e exploração, fortalecendo o conhecimento dos canais adequados de orientação, apoio e denúncia.

- Apoiar professores, famílias e escolas na atuação preventiva, educativa e de mediação no ambiente digital, concretizando, no âmbito educacional, os deveres previstos no Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025).

Como resultado direto destas ações, espera-se:

- Ampliação da literacia digital: o fortalecimento do conhecimento e das habilidades práticas para identificar conteúdos nocivos e prevenir situações de violência online.

- Cultura de cibersegurança: a consolidação de comportamentos pautados na proteção de dados pessoais, privacidade e segurança informacional.

- Convivência digital ética: o estímulo a interações mais saudáveis, empáticas e respeitosas entre pares no ambiente virtual.

- Autonomia e proteção: o pleno domínio sobre os canais de orientação, apoio e denúncia, incentivando o uso seguro, consciente e responsável das tecnologias digitais.

Com base nos objetivos delineados, apresenta-se a seguir o modelo estrutural da CNBC, onde se descreve a arquitetura da campanha e as ferramentas metodológicas que viabilizarão o alcance dos resultados esperados para o público infantojuvenil.

3 Estruturação da CNBC

A CNBC está estruturada por eixos temáticos que correspondem às dimensões de riscos identificados para crianças e adolescentes no ambiente digital. Cada eixo temático será detalhado com objetivos específicos, temas abordados, públicos-alvo, materiais pedagógicos recomendados, fases de implementação e indicadores de acompanhamento.

Os materiais utilizados na campanha constituem insumos diversificados, produzidos por órgãos públicos, instituições de ensino, organizações da sociedade civil e parceiros do setor privado, de forma a integrar conhecimentos, boas práticas e experiências já consolidadas na promoção da segurança digital e da convivência respeitosa online.

Essa estrutura permite que a campanha seja aplicada de forma consistente e adaptável às diferentes realidades locais e faixas etárias, garantindo a coerência pedagógica e o alinhamento às diretrizes da PNCiber e da E-Ciber.

3.1 Eixos temáticos

3.1.1 Eixo 1: Riscos de conduta e contato

▸ Objetivo específico	Prevenir o *cyberbullying* e outras formas de violência digital, promovendo a convivência digital respeitosa e amigável entre estudantes. Este eixo visa fortalecer a capacidade de identificação de riscos e situações de violência online, além de orientar sobre os encaminhamentos adequados conforme a severidade das ocorrências. Para fins de contextualização, apresenta-se a seguir uma breve classificação da violência digital.
▸ Natureza da agressão	• Agressão visual e Exposição • Exclusão social • Intimidação sistemática (*Cyberbullying*) • Violação de identidade (Personificação) • Assédio e Aliciamento (*Grooming)* • Extorsão e Perseguição
▸ Severidade e encaminhamento (Lei nº 14.811/2024)	• Nível 1 – Conflitos de convivência digital: divergências pontuais, tratáveis via mediação pedagógica. • Nível 2 – Cyberbullying: ações repetitivas que causam sofrimento, exigindo intervenção escolar, acolhimento e envolvimento das famílias. • Nível 3 – Infrações e crimes digitais: casos graves com ameaça física, divulgação de cenas de nudez, racismo, homofobia ou incitação à violência; acionamento imediato da rede de proteção.

▸ Período de execução	Idealmente a campanha pode ter a duração de 7 meses.
▸ Público-alvo prioritário	**PRIORITÁRIO** O público-alvo prioritário da presente campanha são estudantes de 12 a 15 anos (Ensino Fundamental II) e de 16 a 18 anos (Ensino Médio). **COMPLEMENTAR** Além do grupo prioritário, a campanha contempla públicos estratégicos para fins de prevenção e apoio institucional, quais sejam: • Crianças de 9 a 11 anos (caráter preventivo); • Professores e equipes pedagógicas (mediação, identificação precoce e encaminhamento de casos). Ressalta-se que os materiais e as atividades deverão ser adaptados às faixas etárias específicas, a fim de garantir maior engajamento e efetividade.

Quanto aos materiais indicados a este eixo temático da CNBC, a tabela a seguir apresenta a relação de materiais de apoio indicados para a sua implementação. Os conteúdos foram selecionados com base na aderência ao objetivo específico do eixo e organizados por faixa etária, de modo a subsidiar ações pedagógicas de prevenção, conscientização e enfrentamento da violência no ambiente digital.

Conforme a natureza de cada material, estes poderão ser impressos e distribuídos a estudantes e professores, utilizados em atividades formativas ou empregados como insumos para planejamento pedagógico, mediação de casos e aprofundamento temático pelas equipes escolares.

Faixa etária	**Material**	**Entidade elaboradora**
9 a 12; 16 a 18	Cartilha de Segurança para Internet - Fascículo Autenticação[23]. Acesso: https://cartilha.cert.br/fasciculos/#autenticacao	CERT.br/NIC.br

[23] As cartilhas do CERT.br/NIC.br listadas neste documento também podem ser consultadas no portal do Centro de Excelência em Privacidade e Segurança (CEPS GOV.BR), no endereço https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/cert.br.

9 a 12; 16 a 18	Cartilha de Segurança para Internet - Fascículo Backup. Acesso: https://cartilha.cert.br/fasciculos/#backup	CERT.br/NIC.br
9 a 12; 16 a 18	Cartilha de Segurança para Internet - Fascículo Boatos. Acesso: https://cartilha.cert.br/fasciculos/#boatos	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Celulares e Tablets. Acesso: https://cartilha.cert.br/fasciculos/#celulares-e-tablets	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Códigos Maliciosos. Acesso: https://cartilha.cert.br/fasciculos/#codigos-maliciosos	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Comércio via Internet. Acesso: https://cartilha.cert.br/fasciculos/#comercio-via-internet	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Computadores. Acesso: https://cartilha.cert.br/fasciculos/#computadores	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Furto de Celular. Acesso: https://cartilha.cert.br/fasciculos/#furto-de-celular	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Phishing e Outros Golpes. Acesso: https://cartilha.cert.br/fasciculos/#phishing-golpes	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Proteção de Dados. Acesso: https://cartilha.cert.br/fasciculos/#protecao-de-dados	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Redes. Acesso: https://cartilha.cert.br/fasciculos/#redes	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Redes Sociais. Acesso: https://cartilha.cert.br/fasciculos/#redes-sociais	CERT.br/NIC.br
12 a 15; 16 a 18	Curso Cidadão Digital (Safernet Brasil) Acesso: https://ead.safernet.org.br/cidadaodigital/	SaferNet
12 a 15; 16 a 18	Caderno de aulas completo - Projeto da Disciplina Cidadania Digital (Safernet Brasil) Acesso: https://bit.ly/caderno-cidadania-digital	SaferNet
12 a 15; 16 a 18	Planos de aula - Projeto da Disciplina Cidadania Digital (Safernet Brasil) Acesso: https://cidadaniadigital.org.br/planos	SaferNet

12 a 15; 16 a 18	Em busca do bem-estar digital Acesso: https://cidadaodigital.org.br/em-busca-do-bem-estar-digital/	SaferNet
9 a 11; 12 a 15; 16 a 18	Cartilha - Conhecendo para prevenir*: bullying* e *cyberbullying* Acesso: https://alessandraborelli.com.br/material-educativo/bullying-cyberbullying/	Nethics
12 a 15; 16 a 18	Cuidado ao acessar QR Codes Acesso: https://cidadaonarede.nic.br/videos/cuidado-ao-acessar-qr-codes/	NIC.br
16 a 18	O que é infostealer? Acesso: https://cidadaonarede.nic.br/videos/o-que-e-infostealer/	NIC.br
9 a 11; 12 a 15; 16 a 18	Proteja-se de Golpes no WhatsApp Acesso: https://cidadaonarede.nic.br/videos/proteja-se-de-golpes-no-whatsapp/	NIC.br
12 a 15; 16 a 18	Cuidado com Wi-Fi público Acesso: https://cidadaonarede.nic.br/videos/cuidado-com-redes-wi-fi-publicas/	NIC.br
12 a 15; 16 a 18	O que é Phishing? Acesso: https://cidadaonarede.nic.br/videos/o-que-e-phishing/	NIC.br
16 a 18	Segurança no Internet Banking Acesso: https://cidadaonarede.nic.br/videos/seguranca-no-internet-banking/	NIC.br
16 a 18	O que é Ransomware? Acesso: https://cidadaonarede.nic.br/videos/o-que-e-ransomware/	NIC.br
9 a 11; 12 a 15; 16 a 18	Proteja seu smartphone Acesso: https://cidadaonarede.nic.br/videos/proteja-seu-smartphone/	NIC.br
12 a 15; 16 a 18	Sites de compras seguros Acesso: https://cidadaonarede.nic.br/videos/verifique-a-seguranca-de-sites-de-compras/	NIC.br
12 a 15; 16 a 18	Vazamento de dados Acesso: https://cidadaonarede.nic.br/videos/vazamento-de-dados-o-que-fazer/	NIC.br

9 a 12	Livro de atividades sobre segurança on-live trabalhe com Sango. Acesso: https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/0c5ad7e8ba70dd82bfb000fad74a5bc8	UIT [24]
9 a 12	Livro de atividades de segurança on-live guia do professor. Acesso: https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/e26475e3b3f2f2f845e0d70e8079bea4	UIT
9 a 12	Livro “On-line com Sango”. Acesso: https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/a7808b2af21b453ae0d700d8586c7af3	UIT
9 a 12; 12 a 15	Guia Internet Segura - crianças de 8 a 12 anos. Acesso: https://internetsegura.br/pdf/guia-internet-segura.pdf	NIC.br
9 a 12	Jogos de Tabuleiro: “Comportamento Seguro” e “Segurança Online”. Acesso: https://internetsegura.br/tabuleiro/	NIC.br
12 a 15; 16 a 18	Guia #Internet com Responsa - Cuidados e Responsabilidades no Uso da Internet. Acesso: https://internetsegura.br/pdf/internet_com_responsa.pdf	NIC.br
12 a 15; 16 a 18	Guia #InternetComResponsa na sua sala de aula. Acesso: https://internetsegura.br/pdf/guia_internet_com_responsa_na_sua_sala_de_aula.pdf	NIC.br
12 a 15	Jogo SerDigi. Acesso: https://images.serpro.gov.br/Web/ServicoFederalDeProcessamentoDeDadosSerp/%7B375f7455-fe7e-4625-9444-a1c84756fc49%7D_Game-Cartas-SerDigi-02-2025_compressed_1_(1).pdf	SERPRO
12 a 15; 16 a 18	Palavras Cruzadas: Proteção de Dados. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=protecao	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Backup. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=backup-1	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Boatos. Acesso: https://www.gov.br/governodigital/pt-	CEPS GOV.BR

[24] União Internacional de Telecomunicações

	br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=boatos	
12 a 15; 16 a 18	Palavras Cruzadas: Códigos Maliciosos. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=codigos-1	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Comércio via Internet. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=comercio	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Furto de Celular. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=furto	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Phishing e Outros Golpes. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=phishing	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Proteção de Dados. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=protecao	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Banco via Internet. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=bancoviainternet	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Computadores. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=computadores	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Privacidade. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=privacidade	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Redes. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=redes	CEPS GOV.BR

12 a 15; 16 a 18	Palavras Cruzadas: Redes Sociais. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=sociais	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Vazamento de Dados. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=vazamento	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Celulares e Tablets. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=celulares	CEPS GOV.BR
12 a 15; 16 a 18	Labirinto - Internet com Responsa. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=labirinto-responsa	CEPS GOV.BR
12 a 15; 16 a 18	Labirinto - Internet com responsa vai às compras. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=labirinto-compras	CEPS GOV.BR
12 a 15; 16 a 18	Wordle - Internet com responsa #fikdik. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=wordle-game	CEPS GOV.BR
12 a 15; 16 a 18	Quis – Furto de Celular. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=furto-de-celular	CEPS GOV.BR
12 a 15; 16 a 18	Jogos Educativos: Golpes Cibernéticos, Phishing Mails, Jogo do Virus, Segurança Ninja, Malware Lab, Cyber Bomber e outros. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos	CEPS GOV.BR

3.1.2 EIXO 2: RISCOS DE CONTEÚDO

▸ Objetivo específico	Promover a capacidade crítica dos estudantes para identificar, analisar e reagir adequadamente a conteúdos inadequados ou potencialmente prejudiciais no ambiente digital, fortalecendo a segurança informacional e a autonomia no uso de plataformas digitais.
▸ Natureza da agressão	• Consumo de material violento ou extremista • Incentivo a comportamentos nocivos • Exposição a material pornográfico • Desinformação e Manipulação (Fake News)
▸ Período de execução	Idealmente a campanha pode ter a duração de 7 meses.
▸ Público-alvo prioritário	**PRIORITÁRIO** O público-alvo prioritário da presente campanha são estudantes de 12 a 15 anos (Ensino Fundamental II) e de 16 a 18 anos (Ensino Médio). **COMPLEMENTAR** Além do grupo prioritário, a campanha contempla públicos estratégicos para fins de prevenção e apoio institucional, quais sejam: • Crianças de 9 a 11 anos (caráter preventivo); • Professores e equipes pedagógicas (mediação, identificação precoce e encaminhamento de casos). Ressalta-se que os materiais e as atividades deverão ser adaptados às faixas etárias específicas, a fim de garantir maior engajamento e efetividade.

Os conteúdos foram selecionados com base na aderência ao objetivo específico do eixo, contemplando iniciativas institucionais de educação digital, vídeos educativos, cursos estruturados, planos de aula e materiais de orientação técnica elaborados por órgãos públicos e entidades especializadas.

Os materiais abordam, entre outros temas:

- identificação de vídeos adulterados e conteúdos manipulados;
- compreensão de desinformação e práticas enganosas;
- uso seguro de tecnologias emergentes, incluindo inteligência artificial;

- noções de proteção digital, como antivírus, backups e atualização de sistemas;
- desenvolvimento de competências de cidadania digital e pensamento crítico.

Organizados por faixa etária, esses recursos poderão ser utilizados em diferentes formatos pedagógicos, tais como exibição de vídeos seguida de debate orientado, oficinas práticas, aplicação de planos de aula estruturados, cursos complementares e atividades interdisciplinares.

Faixa etária	Material	Entidade elaboradora
12 a 15; 16 a 18	Vida de Influencer: Teatro Educativo sobre Proteção Digital para Crianças e Adolescentes. Acesso: https://www.youtube.com/watch?v=Yr9RWKL0qJI&list=PLOmVJ5Ex3R10wEUM3edKTSErojXs_07xg&index=22	Anatel
12 a 15; 16 a 18	Curso Cidadão Digital (Safernet Brasil). Acesso: https://ead.safernet.org.br/cidadaodigital/	SaferNet
12 a 15; 16 a 18	Caderno de aulas completo - Projeto da Disciplina Cidadania Digital (Safernet Brasil). Acesso: https://bit.ly/caderno-cidadania-digital	SaferNet
12 a 15; 16 a 18	Planos de aula - Projeto da Disciplina Cidadania Digital (Safernet Brasil). Acesso: https://cidadaniadigital.org.br/planos	SaferNet
12 a 15; 16 a 18	Guia prático para educadores: caminhos para prevenir e mediar agressões online entre estudantes (Safernet Brasil). Acesso: https://cidadaodigital.org.br/guia-pratico-para-educadores-caminhos-para-prevenir-e-mediar-agressoes-online-entre-estudantes	SaferNet
12 a 15; 16 a 18	Identifique vídeos adulterados. Acesso: https://cidadaonarede.nic.br/videos/identifique-videos-adulterados/	NIC.br[25]
9 a 11; 12 a 15; 16 a 18	Importância do Backup. Acesso: https://cidadaonarede.nic.br/videos/backup-a-importancia-de-ter-copias-de-seguranca/	NIC.br
16 a 18	O que é Ransomware? Acesso: https://cidadaonarede.nic.br/videos/o-que-e-ransomware/	NIC.br
9 a 11; 12 a 15; 16 a 18	Antivírus: por que usar? Acesso: https://cidadaonarede.nic.br/videos/antivirus-por-que-usar/	NIC.br
12 a 15; 16 a 18	Atualização de Softwares. Acesso: https://cidadaonarede.nic.br/videos/atualizacao-de-softwares-e-sistemas/	NIC.br

[25] Núcleo de Informação e Coordenação do Ponto BR

12 a 15; 16 a 18	Links encurtados. Acesso: https://cidadaonarede.nic.br/videos/o-perigo-dos-links-encurtados/	NIC.br

3.1.3 EIXO 3: RISCOS DE CONSUMO

▸ Objetivo específico	Promover a segurança no consumo digital e fortalecer a capacidade dos estudantes de identificar e prevenir fraudes, golpes, práticas comerciais enganosas e riscos relacionados à exposição indevida de dados pessoais no ambiente online. O eixo busca desenvolver competências para o uso seguro de dispositivos, aplicativos bancários, plataformas de comércio eletrônico e redes sociais, incentivando práticas responsáveis de proteção patrimonial, privacidade e bem-estar digital. Também pretende orientar sobre medidas preventivas, tais como autenticação segura, reconhecimento de tentativas de *phishing*, verificação de sites de compras, cuidado com redes Wi-Fi públicas, uso adequado de backups e atualização de sistemas, bem como encaminhamentos adequados em caso de incidentes digitais.
▸ Natureza da agressão	• Engenharia Social e Fraudes (*Phishing*) • Golpes Financeiros e de Comércio Eletrônico • Exploração Comercial Abusiva • Exposição Indevida de Dados Pessoais (*Oversharing*) • Vulnerabilidades de Acesso e Infraestrutura
▸ Período de execução	Idealmente a campanha pode ter a duração de 7 meses.
▸ Público-alvo prioritário	**PRIORITÁRIO** O público-alvo prioritário da presente campanha são estudantes de 12 a 15 anos (Ensino Fundamental II) e de 16 a 18 anos (Ensino Médio). **COMPLEMENTAR** Além do grupo prioritário, a campanha contempla públicos estratégicos para fins de prevenção e apoio institucional, quais sejam: • Crianças de 9 a 11 anos (caráter preventivo); • Professores e equipes pedagógicas (mediação, identificação precoce e encaminhamento de casos).

	Ressalta-se que os materiais e as atividades deverão ser adaptados às faixas etárias específicas, a fim de garantir maior engajamento e efetividade.

A tabela a seguir apresenta a relação de materiais de apoio indicados para a implementação da CNBC, com foco no terceiro eixo temático. Os conteúdos foram selecionados com base na aderência ao objetivo específico do eixo e contemplam cartilhas técnicas, vídeos educativos, cursos estruturados e guias de boas práticas elaborados por órgãos especializados em segurança da informação e cidadania digital.

Os materiais abordam, entre outros temas:

- autenticação segura e uso de senhas fortes;
- proteção de dispositivos móveis e computadores;
- *phishing*, *infostealers*, *ransomware* e outros códigos maliciosos;
- golpes em aplicativos de mensagens e redes sociais;
- comércio eletrônico seguro e verificação de sites de compras;
- segurança em internet banking e pagamentos digitais;
- proteção de dados pessoais e resposta a vazamentos;
- uso seguro de QR Codes e redes Wi-Fi públicas;
- boas práticas no uso de inteligência artificial e tecnologias emergentes.

Organizados por faixa etária, os recursos possibilitam abordagem progressiva do tema, desde noções iniciais de proteção de dispositivos (9 a 11 anos) até discussões mais aprofundadas sobre fraudes financeiras, proteção patrimonial e governança digital (16 a 18 anos).

Conforme a natureza de cada material, estes poderão ser:

- utilizados em atividades de conscientização em sala de aula;
- incorporados a oficinas práticas sobre segurança digital;
- empregados como insumos para formação de professores;
- distribuídos em formato impresso ou digital como material de apoio preventivo;
- utilizados como base para estudos de caso e simulações pedagógicas de golpes e fraudes.

A diversidade de entidades elaboradoras assegura consistência técnica, atualização temática e alinhamento às melhores práticas nacionais em segurança digital.

Faixa etária	Material	Entidade elaboradora
9 a 12; 16 a 18	Cartilha de Segurança para Internet - Fascículo Autenticação[26]. Acesso: https://cartilha.cert.br/fasciculos/#autenticacao	CERT.br/NIC.br
9 a 12; 16 a 18	Cartilha de Segurança para Internet - Fascículo Backup. Acesso: https://cartilha.cert.br/fasciculos/#backup	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Boatos. Acesso: https://cartilha.cert.br/fasciculos/#boatos	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Celulares e Tablets. Acesso: https://cartilha.cert.br/fasciculos/#celulares-e-tablets	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Códigos Maliciosos. Acesso: https://cartilha.cert.br/fasciculos/#codigos-maliciosos	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Comércio via Internet. Acesso: https://cartilha.cert.br/fasciculos/#comercio-via-internet	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Computadores. Acesso: https://cartilha.cert.br/fasciculos/#computadores	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Furto de Celular. Acesso: https://cartilha.cert.br/fasciculos/#furto-de-celular	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Phishing e Outros Golpes. Acesso: https://cartilha.cert.br/fasciculos/#phishing-golpes	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Proteção de Dados. Acesso: https://cartilha.cert.br/fasciculos/#protecao-de-dados	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Redes. Acesso: https://cartilha.cert.br/fasciculos/#redes	CERT.br/NIC.br
12 a 15; 16 a 18	Cartilha de Segurança para Internet - Fascículo Redes Sociais. Acesso: https://cartilha.cert.br/fasciculos/#redes-sociais	CERT.br/NIC.br
12 a 15; 16 a 18	Curso Cidadão Digital (Safernet Brasil). Acesso: https://ead.safernet.org.br/cidadaodigital/	SaferNet
12 a 15; 16 a 18	Caderno de aulas completo - Projeto da Disciplina Cidadania Digital (Safernet Brasil). Acesso: https://bit.ly/caderno-cidadania-digital	SaferNet

[26] As cartilhas do CERT.br/NIC.br listadas neste documento também podem ser consultadas no portal do Centro de Excelência em Privacidade e Segurança (CEPS GOV.BR), no endereço https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/cert.br.

12 a 15; 16 a 18	Planos de aula - Projeto da Disciplina Cidadania Digital (Safernet Brasil). Acesso: https://cidadaniadigital.org.br/planos	SaferNet
12 a 15; 16 a 18	Em busca do bem-estar digital. Acesso: https://cidadaodigital.org.br/em-busca-do-bem-estar-digital/	SaferNet
12 a 15; 16 a 18	Cuidado ao acessar QR Codes. Acesso: https://cidadaonarede.nic.br/videos/cuidado-ao-acessar-qr-codes/	NIC.br
16 a 18 anos	O que é infostealer? Acesso: https://cidadaonarede.nic.br/videos/o-que-e-infostealer/	NIC.br
9 a 11; 12 a 15; 16 a 18	Proteja-se de Golpes no WhatsApp. Acesso: https://cidadaonarede.nic.br/videos/proteja-se-de-golpes-no-whatsapp/	NIC.br
12 a 15; 16 a 18	Cuidado com Wi-Fi público. Acesso: https://cidadaonarede.nic.br/videos/cuidado-com-redes-wi-fi-publicas/	NIC.br
12 a 15; 16 a 18	O que é Phishing? Acesso: https://cidadaonarede.nic.br/videos/o-que-e-phishing/	NIC.br
16 a 18	Segurança no Internet Banking. Acesso: https://cidadaonarede.nic.br/videos/seguranca-no-internet-banking/	NIC.br
16 a 18	O que é Ransomware? Acesso: https://cidadaonarede.nic.br/videos/o-que-e-ransomware/	NIC.br
9 a 11; 12 a 15; 16 a 18	Proteja seu smartphone. Acesso: https://cidadaonarede.nic.br/videos/proteja-seu-smartphone/	NIC.br
12 a 15; 16 a 18	Sites de compras seguros. Acesso: https://cidadaonarede.nic.br/videos/verifique-a-seguranca-de-sites-de-compras/	NIC.br
12 a 15; 16 a 18	Vazamento de dados. Acesso: https://cidadaonarede.nic.br/videos/vazamento-de-dados-o-que-fazer/	NIC.br
12 a 15; 16 a 18	Palavras Cruzadas: Proteção de Dados. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=protecao	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Backup. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=backup-1	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Boatos. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-	CEPS GOV.BR

	e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=boatos	
12 a 15; 16 a 18	Palavras Cruzadas: Códigos Maliciosos. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=codigos-1	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Comércio via Internet. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=comercio	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Furto de Celular. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=furto	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Phishing e Outros Golpes. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=phishing	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Proteção de Dados. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=protecao	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Banco via Internet. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=bancoviainternet	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Computadores. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=computadores	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Privacidade. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=privacidade	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Redes. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=redes	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Redes Sociais. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=sociais	CEPS GOV.BR
12 a 15; 16 a 18	Palavras Cruzadas: Vazamento de Dados. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=vazamento	CEPS GOV.BR

12 a 15; 16 a 18	Palavras Cruzadas: Celulares e Tablets. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=celulares	CEPS GOV.BR
12 a 15; 16 a 18	Labirinto - Internet com Responsa. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=labirinto-responsa	CEPS GOV.BR
12 a 15; 16 a 18	Labirinto - Internet com responsa vai às compras. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=labirinto-compras	CEPS GOV.BR
12 a 15; 16 a 18	Wordle - Internet com responsa #fikdik. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=wordle-game	CEPS GOV.BR
12 a 15; 16 a 18	Quis – Furto de Celular. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos/game?url=furto-de-celular	CEPS GOV.BR
12 a 15; 16 a 18	Jogos Educativos: Golpes Cibernéticos, Phishing Mails, Jogo do Virus, Segurança Ninja, Malware Lab, Cyber Bomber e outros. Acesso: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/centro-de-excelencia-em-privacidade-e-seguranca/jogos	CEPS GOV.BR

3.2 Fases da campanha

Cada eixo temático da CNBC deverá ser viabilizado por meio de etapas sucessivas e articuladas, de modo a assegurar coerência pedagógica, efetividade das ações e adequada avaliação dos resultados, conforme segue.

3.2.1 Fase 1 – Planejamento e preparação

▸ Duração	Meses 1 a 3
▸ Coordenação nacional	Ministério da Educação (MEC)
▸ Atores	Secretarias estaduais, distrital e municipais de educação e a Secretaria de Educação Profissional e Tecnológica.

Nesta fase, serão realizadas a definição do escopo da campanha, a seleção e a consolidação dos materiais a serem utilizados, bem como a validação pedagógica dos conteúdos.

Caberá à coordenação nacional, estabelecer diretrizes gerais, cronograma e orientações para implementação (incluindo a orientação para utilização dos materiais indicados e/ou elaboração de materiais a partir dos existentes, bem como a adaptação às faixas etárias de crianças e adolescentes abrangidos pela campanha), enquanto as secretarias de educação apoiarão a adequação dos materiais às realidades locais e a articulação com as redes de ensino.

3.2.2 Fase 2 – Sensibilização e disseminação de conteúdos

▸ Duração	Meses 3 a 5
▸ Coordenação	Secretarias de educação e Ministério da Educação (MEC)
▸ Atores	Unidades escolares e assessorias de comunicação.

Esta fase tem como objetivo promover a conscientização inicial da comunidade escolar sobre os riscos digitais de que trata o respectivo eixo temático.

As ações incluem a distribuição dos materiais pedagógicos às escolas, a divulgação dos conteúdos em plataformas educacionais e canais institucionais, o envio de comunicados às famílias e a orientação às unidades escolares quanto ao uso dos materiais em atividades pedagógicas.

3.2.3 Fase 3 – Atividades mediadas no ambiente escolar

▸ Duração	Meses 5 e 6
▸ Coordenação	Unidades escolares
▸ Atores	Profissionais da educação escolar básica, conforme art. 61 da LDB, a exemplo de professores, equipes pedagógicas, gestores, entre outros.

Nesta etapa, os materiais da campanha serão utilizados em atividades mediadas no ambiente escolar, como debates orientados, rodas de conversa, oficinas e outras ações pedagógicas.

O foco é estimular a reflexão crítica, o diálogo entre os estudantes e o desenvolvimento de competências relacionadas à convivência digital respeitosa, com mediação de professores e equipes pedagógicas.

3.2.4 Fase 4 – Engajamento criativo e premiação

▸ Duração	Mês 6
▸ Coordenação	Ministério da Educação (MEC) e secretarias de educação
▸ Atores	Unidades escolares e estudantes.

▸ Atividades	Prêmio Boas Conexões – produção de vídeos de até 1 minuto pelos estudantes; orientação, seleção e premiação.

Como etapa de engajamento e protagonismo juvenil, poderia ser lançado, na primeira semana do mês, o “Prêmio Boas Conexões”, incentivando a produção de vídeos curtos de até 1 minuto pelos estudantes, com foco na temática de que trata cada eixo.

Caberá às escolas orientar e apoiar a produção dos materiais, enquanto a coordenação da campanha conduzirá o processo de seleção e premiação. A premiação poderia ocorrer no final do ano letivo.

3.2.5 Fase 5 – Divulgação dos resultados e devolutiva

▸ Duração	2 meses após o término da campanha
▸ Coordenação	Ministério da Educação (MEC)
▸ Atores	Secretarias de educação e assessorias de comunicação.

Nesta fase, serão divulgados os resultados da campanha e as produções selecionadas, por meio de portais institucionais, plataformas educacionais e outros canais oficiais. A divulgação visa reconhecer o engajamento dos estudantes e das escolas, disseminar boas práticas e ampliar o alcance das mensagens da campanha junto à sociedade.

Quanto à premiação, sugere-se que tenha caráter predominantemente educativo, formativo e de reconhecimento institucional, de modo a valorizar o protagonismo juvenil, o trabalho coletivo e o engajamento das comunidades escolares na promoção da convivência digital amigável, na prevenção do *cyberbullying* e temáticas específicas de cada eixo da CNBC.

Como primeira possibilidade, recomenda-se a adoção de premiação simbólica e institucional, por meio da concessão de troféus, placas ou certificados aos três primeiros colocados, bem como o reconhecimento público das produções selecionadas, com divulgação em portais e canais institucionais. Essa modalidade contribui para a valorização dos estudantes, professores orientadores e unidades escolares, sem estimular competição excessiva.

Como segunda possibilidade, sugere-se a oferta de premiação educativa e cultural, contemplando a disponibilização de kits educativos ou culturais e a realização de experiências formativas, como oficinas criativas, atividades educativas ou laboratórios de produção audiovisual voltados aos estudantes participantes. Essa modalidade tem potencial de ampliar os efeitos pedagógicos da campanha e de estimular a continuidade das ações no ambiente escolar.

Como terceira possibilidade, poderá ser considerada a adoção de premiação de caráter financeiro indireto, destinada às escolas ou redes de ensino responsáveis pelas produções selecionadas, com finalidade exclusivamente educativa ou cultural, observadas as normas aplicáveis à administração pública. Essa alternativa permite o fortalecimento das ações institucionais nas unidades escolares, evitando a concessão direta de valores a estudantes.

A definição das modalidades de premiação a serem adotadas deverá observar critérios pedagógicos, a adequação ao público infanto-juvenil, a viabilidade administrativa e a coerência com os objetivos da campanha, podendo ser utilizadas de forma isolada ou combinada, conforme decisão da coordenação da iniciativa. Ademais a premiação poderia ser estabelecida com recorte para unidade escolar e sistemas de ensino, que culminariam em premiação nacional geral.

3.2.6 Fase 6 – Monitoramento e avaliação

▸ Duração	Sem duração delimitada
▸ Coordenação	Ministério da Educação (MEC)
▸ Atores	Secretarias de educação e unidades escolares.

Sugere-se que o monitoramento e a avaliação da campanha tenham como finalidade acompanhar a execução das ações previstas e aferir sua efetividade, de modo a subsidiar eventuais ajustes ao longo da implementação e contribuir para a consolidação de boas práticas ao final do período.

Para a mensuração do alcance da campanha, recomenda-se considerar indicadores como o número de escolas participantes, a quantidade de materiais distribuídos, a estimativa de público alcançado e os acessos aos conteúdos disponibilizados em meios digitais, possibilitando avaliar a abrangência das ações nos diferentes territórios e canais de divulgação.

No que se refere ao engajamento, propõe-se observar a utilização dos materiais em sala de aula, a participação dos estudantes nas atividades desenvolvidas e os relatos qualitativos de professores e equipes pedagógicas, com vistas a aferir o nível de envolvimento da comunidade escolar com a temática da convivência digital.

Quanto aos resultados, sugere-se avaliar a compreensão dos estudantes acerca do tema do *cyberbullying*, a capacidade de identificação de riscos e situações de violência digital e o conhecimento dos canais de orientação, apoio e denúncia, de forma a verificar os efeitos educativos da campanha.

A avaliação poderá ser realizada por meio de instrumentos variados, tais como questionários aplicados a estudantes e professores, relatórios elaborados pelas unidades escolares e análise de métricas digitais relativas ao acesso e à interação com os conteúdos divulgados.

Recomenda-se que o monitoramento ocorra de forma contínua ao longo da execução da campanha, com a realização de uma avaliação consolidada ao final do período, possibilitando a elaboração de diagnóstico geral, a identificação de aprendizados e a formulação de recomendações para o aprimoramento de iniciativas futuras.

Referências

Belli, Luca; Medeiros, Breno; Couto, Natália; Bakonyi, Erica; Gaspar, Walter; Lage, Daniel. Governança e regulação da cibersegurança no Brasil: proteção da infraestrutura crítica, segurança da informação e construção da soberania digital. Rio de Janeiro: Lumen Juris, 2026. Disponível em: https://direitorio.fgv.br/publicacao/governanca-e-regulacao-da-ciberseguranca-no-brasil. Acesso em 04/03/2026.

BORELLI, Alessandra; ZAMPERLIN, Emelyn. *Bullying e cyberbullying: cartilha*. São Paulo: Opice Blum Academy / Nethics Educação Digital, [2021]. Disponível em: https://opiceblumacademy.com.br/wp-content/uploads/2021/04/CARTILHA-CYBERBULLYING2-obac.pdf. Acesso em: 5 mar. 2026.

BOTTINO, Sara Mota Borges et al. Cyberbullying and adolescent mental health: systematic review. Cadernos de Saúde Pública, v. 31, n. 3, p. 463-475, 2015. Disponível em: https://doi.org/10.1590/0102-311X00036114. Acesso em 05/03/2026.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 4 mar. 2026.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 5 mar. 2026.

BRASIL. Lei nº 9.394, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da educação nacional. Diário Oficial da União: seção 1, Brasília, DF, 23 dez. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 5 mar. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) — Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 mar. 2026.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15211.htm. Acesso em: 5 mar. 2026.

BRASIL. Ministério da Educação. Secretaria de Educação Continuada, Alfabetização de Jovens e Adultos, Diversidade e Inclusão (SECADI). 2º Boletim técnico “Escola que Protege: dados sobre bullying e cyberbullying”. 1. ed. Curitiba: Ministério da Educação, 2025.

Disponível em: https://www.gov.br/mec/pt-br/escola-que-protege/segundo-boletim-tecnico-escola-que-protege.pdf. Acesso em: 4 mar. 2026.

BRASIL. Resolução CNCiber nº 15, de 13 de outubro de 2025. Institui o grupo de trabalho temático para elaboração de estratégias de divulgação de materiais educativos de Cibersegurança. Disponível em: https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber/resolucos/resolucao-cnciber-no-15-de-13-de-outubro-de-2025.pdf. Acesso em: 5 mar. 2026.

BRASIL. Resolução CNCiber nº 9, de 26 de maio de 2025. Institui o grupo de trabalho temático para identificação ou elaboração de materiais educativos de Cibersegurança e estratégias de difusão desses materiais. Disponível em: https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber/resolucoes/resolucao-cnciber-no-9-de-26-de-maio-de-2025-gtt-cibereducacao.pdf . Acesso em: 5 mar. 2026.

CARA, D. (Relator). Ataques às escolas no Brasil: análise do fenômeno e recomendações para a ação governamental. Brasília, DF: Ministério da Educação (MEC), 2023. Disponível em: https://www.gov.br/mec/pt-br/acesso-a-informacao/participacao-social/grupos-de-trabalho/prevencao-e-enfrentamento-da-violencia-nas-escolas/resultados/relatorio-ataque-escolas-brasil.pdf. Acesso em: 05/03/2026.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Pesquisa sobre o Uso da Internet por Crianças e Adolescentes no Brasil: TIC Kids Online Brasil 2024. São Paulo: Núcleo de Informação e Coordenação do Ponto BR (NIC.br), 2025.

COMITÊ GESTOR DA INTERNET NO BRASIL. TIC Kids Online Brasil: pesquisa sobre o uso da internet por crianças e adolescentes no Brasil. São Paulo: CGI.br, 2024. Disponível em: https://cetic.br/media/docs/publicacoes/2/20250512154312/tic_kids_online_2024_livro_eletronico.pdf. Acesso em: 4 mar. 2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/279. Acesso em: 4 mar. 2026.

FERREIRA, Taiza Ramos de Souza Costa; DESLANDES, Suely Ferreira. Cyberbulling: conceituações, dinâmicas, personagens e implicações à saúde. Ciência & Saúde Coletiva, v. 23, n. 10, p. 3369-3379, 2018. Disponível em: https://doi.org/10.1590/1413-812320182310.13482018. Acesso em 05/03/2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Visível e invisível: a vitimização de mulheres no Brasil. 5. ed. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2025/03/relatorio-visivel-e-invisivel-5ed-2025.pdf. Acesso em: 5 mar. 2026.

KOWALSKI, Robin M.; LIMBER, Susan P. Psychological, physical, and academic correlates of cyberbullying and traditional bullying. Journal of Adolescent Health, v. 53, n. 1, p. S13-S20, 2013. Disponível em: https://doi.org/10.1016/j.jadohealth.2012.09.018. Acesso em 05/03/2026.

LIVINGSTONE, Sonia; STOILOVA, Mariya. The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburgo: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence, 2021.

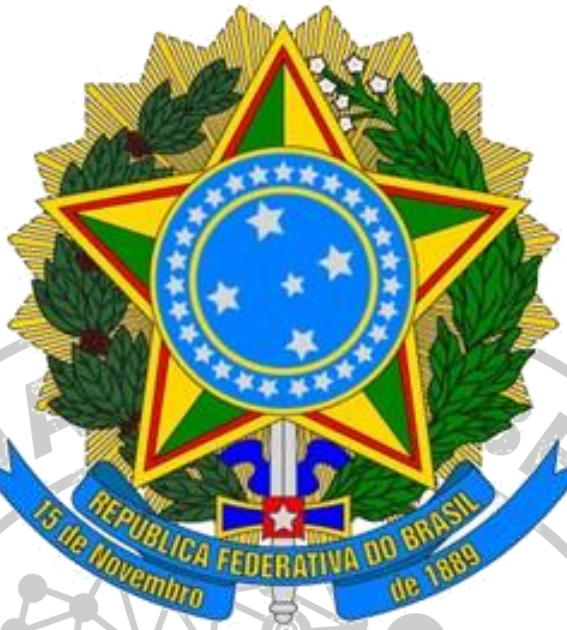
ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Comitê dos Direitos da Criança. Comentário Geral nº 25 (2021) sobre os direitos das crianças em relação ao ambiente digital (Documento CRC/C/GC/25).

QUEIROZ, Christina. Violência escolar aumenta nos últimos 10 anos no Brasil. *Revista Pesquisa FAPESP*, São Paulo, ed. 350, abr. 2025. Disponível em:https://revistapesquisa.fapesp.br/violencia-escolar-aumenta-nos-ultimos-10-anos-no-brasil/. Acesso em: 05/03/2026.

QUAYYUM, Farzana; CRUZES, Daniela S.; JACCHERI, Letizia. Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, v. 30, p. 100343, 2021. Disponível em: https://doi.org/10.1016/j.ijcci.2021.100343. Acesso em 04/03/2026.

UNITED NATIONS CHILDREN'S FUND (UNICEF). Child safety online: global challenges and strategies. Florence: UNICEF Office of Research – Innocenti, 2012. Disponível em: https://www.unicef.org/media/66821/file/Child-Safety-Online.pdf. Acesso em: 4 mar. 2026.

VISHWANATH, Arun et al. Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, v. 128, p. 113160, 2020. Disponível em: https://doi.org/10.1016/j.dss.2019.113160. Acesso em: 04/03/2026.



Presidência da República

Comitê Nacional de Cibersegurança (CNCiber)

Plano Nacional de Cibersegurança (P-Ciber – Estruturante)

Brasília - 2026

COMITÊ NACIONAL DE CIBERSEGURANÇA
CNCiber

SUMÁRIO

1 APRESENTAÇÃO

1.1 Introdução

Com o objetivo de melhorar a cibersegurança e a ciber-resiliência do país e promover a cooperação nacional e internacional, foi instituída, em 2023, a Política Nacional de Cibersegurança (PNCiber) [1], que criou o Comitê Nacional de Cibersegurança (CNCiber) com uma natureza multidisciplinar, envolvendo representantes do governo, academia, sociedade civil, e empresariado para acompanhar a implementação e evolução dessa política pública, responsável pela presente estratégia. A PNCiber também estabeleceu seus dois instrumentos: a Estratégia Nacional de Cibersegurança (E-Ciber)[2] e o Plano Nacional de Cibersegurança (P-Ciber).

1.2 O GTT P-Ciber-Estruturante

Concluído o GTT-P-Ciber[3], que elaborou a primeira versão do P-Ciber contemplando mais de uma centena de Iniciativas Estratégicas (IEs), o CNCiber entendeu ser necessária a criação de um novo GTT[4] para identificar Iniciativas Estratégicas Estruturantes, as quais, por sua natureza, perpassariam mais de uma Ação Estratégica (AE) da E-Ciber.

Esse grupo de trabalho foi constituído por representantes das seguintes instituições:

- Gabinete de Segurança Institucional da Presidência da República (coordenação);
- Ministério da Gestão e da Inovação em Serviços Públicos (coordenação);
- Casa Civil da Presidência da República;
- Ministério da Ciência, Tecnologia e Inovação;
- Ministério das Comunicações;
- Ministério do Desenvolvimento, Indústria, Comércio e Serviços;
- Ministério da Educação;
- Ministério da Justiça e Segurança Pública;

[1] Decreto Nº 11.856, em 26 de dezembro de 2023.

[2] Instituída pelo Decreto 12.573, de 4 de agosto de 2025.

[3] Criado por meio da Resolução CNCiber nº 8, de 26 de maio de 2025.

[4] Criado por meio da Resolução CNCiber nº 14, de 8 de outubro de 2025.

- Confederação das Associações das Empresas Brasileiras de Tecnologia da Informação -ASSEPRO (setor empresarial);
- Instituto dos Advogados de São Paulo - IASP (setor sociedade civil);
- Federação das Indústrias do Estado de São Paulo - FIESP (setor empresarial);
- Conexis/Brasscom (setor empresarial); e
- Rede Nacional de Ensino e Pesquisa - RNP (setor científico, tecnológico e de inovação).

1.3 Da Metodologia de Elaboração do P-Ciber-Estruturante

O GTT reuniu-se por 16 vezes, com uma média de 10 a 12 participantes por reunião, totalizando mais de 250 pessoas.hora aplicadas para deliberar sobre as propostas de IE-Estruturantes e sua pertinência ao objeto do GTT.

O GTT P-Ciber-Estruturante definiu que as IE-Estruturantes seriam acrescidas ao P-Ciber originalmente elaborado. Para diferenciar as duas categorias de IEs, adotou-se a denominação de IEs Institucionais (IEIs) para o conjunto de iniciativas do P-Ciber original, e IEs Estruturantes (IEEs) para o novo conjunto.

1.4 Da Publicação

O GTT decidiu que a publicação dessas IEEs dar-se-á no mesmo contexto da publicação do P-Ciber com as IEIs originais, com uma marcação distintiva das IEEs de forma a diferenciá-las das IEIs originais. Decidiu-se, também, que as IEEs não serão vinculadas a uma AE específica, dada sua natureza multivariada.

As IEEs serão publicadas integradas ao P-Ciber e seguirão o mesmo processo de atualização originalmente proposto.

2 INICIATIVAS ESTRATÉGICAS ESTRUTURANTES (IEE)

A seguir apresenta-se o conjunto de 19 IE-Estruturantes identificadas pelo GTT, todas entendidas como tendo possibilidade real de implementação, mesmo considerada a severa limitação posta pela grave situação fiscal do País.

2.1 IEE 01 - Cibereducação-Estratégias

Proponente: CNCiber	**Prazo:** 2026-2031
Responsável: CNCiber e instituições apoiadoras	
Descrição: Proposição de estratégias para a disseminação dos materiais de cibereducação disponibilizados pelo governo e outras instituições no Brasil.	
Motivação: Identificou-se a inexistência de uma cultura disseminada de cibersegurança e ciber-higiene. Paradoxalmente, verificou-se a existência de vasta gama de materiais de cibereducação em diferentes níveis de profundidade e voltados a públicos diversos, cuja disseminação é muito limitada. Assim, busca-se a proposição e implementação de estratégias de disseminação desses materiais para o atingimento de um público mais amplo.	
Implementação: Divulgação dos materiais didáticos existentes ou a serem elaborados por meio de diferentes veículos de comunicação, articulados pelo CNCiber, Casa Civil e GSI, destinados a públicos específicos e avaliação do resultado alcançado.	
Recursos: Não há previsão de dotação orçamentária específica no presente momento.	

2.2 IEE 02 - Programa de Fortalecimento da Cibersegurança

Proponente:	**Prazo:**
MGI	2026-2031

Responsável:

CNCiber: análise e reconhecimento das iniciativas estratégicas institucionais submetidas;

Instituições públicas e privadas: submissão de iniciativas e projetos;

Secretaria-executiva do CNCiber: gestora do programa.

Descrição:

Implementar o Programa de Fortalecimento da Cibersegurança, estimulando a criação e execução de iniciativas estratégicas institucionais alinhadas às ações estratégicas da E-Ciber.

Motivação:

Para estimular a criação de iniciativas para a implementação de ações estratégicas dos 4 eixos da E-Ciber em todo o País, além de fortalecer a maturidade cibernética, articular governo, setor produtivo, academia e sociedade, criar uma cultura nacional de cibersegurança, padronizar práticas e promover maior resiliência contra riscos e ameaças digitais.

Implementação:

As instituições enviarão propostas de iniciativas de forma contínua, que serão analisadas e validadas conforme as diretrizes da E-Ciber. As iniciativas aprovadas serão padronizadas e divulgadas para estimular sua expansão e adesão em todo o País.

Recursos:

Não há previsão de dotação orçamentária específica no presente momento.

2.3 IEE 03 - Selo "Brasil Ciberseguro"

Proponente:	**Prazo:**
MGI	2026-2031

Responsável:

CNCiber: análise e reconhecimento das iniciativas estratégicas institucionais submetidas;

Instituições públicas e privadas: submissão de iniciativas e projetos;

Secretaria-executiva do CNCiber: gestora do programa.

Descrição:

O selo "Brasil Ciberseguro" será um reconhecimento nacional para organizações que adotarem iniciativas estratégicas de cibersegurança alinhadas à Estratégia Nacional de Cibersegurança.

Motivação:

Para estimular e comprovar o compromisso contínuo com ações estratégicas da E-Ciber, fortalecendo proteção, resiliência, cooperação e governança.

Implementação:

A obtenção do selo ocorre mediante o cumprimento dos critérios estabelecidos e a comprovação das iniciativas alinhadas a cada eixo da E-Ciber. A avaliação resulta na concessão de quatro tipos de selos - um para cada eixo estratégico - distribuídos em três categorias (bronze, prata e ouro), definidas conforme a quantidade de iniciativas implementadas pela instituição.

O selo passa a ser aplicável a partir da publicação do P-Ciber e pode ser solicitado pelas instituições à medida que comprovarem suas iniciativas estratégicas institucionais de cibersegurança.

Recursos:

Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.

2.4 IEE 04 - Modelo de Maturidade Nacional

Proponente: CNCiber	**Prazo:** 2026-2031
Responsável: CNCiber	
Descrição: Proposição de um modelo de avaliação da maturidade nacional em cibersegurança.	
Motivação: Hoje utilizamos modelos desenvolvidos em outros países, com realidade e cultura institucional muito distinta daquela brasileira e regional. Adicionalmente, na avaliação feita hoje passa-se grande quantidade de dados e informações relevantes para instituições estrangeiras. Ademais, as avaliações existentes apenas incidentalmente proveem informações que possam alimentar a avaliação de políticas públicas para a melhoria da cibersegurança e ciber-resiliência nacionais. Assim, entende-se adequado o desenvolvimento de um modelo de maturidade nacional para sanar as limitações dos modelos hoje usados.	
Implementação: Consolidação e adaptação de modelos internacionalmente reconhecidos como o CMM de Oxford e o GCI da UIT às condições nacionais.	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.5 IEE 05 - Modelo de Maturidade Institucional

Proponente: CNCiber	**Prazo:** 2026-2031
Responsável: CNCiber	
Descrição: Proposição de um modelo de avaliação da maturidade institucional em cibersegurança.	
Motivação: Não dispomos de um modelo de avaliação de maturidade institucional aplicável a instituições provedoras de serviços essenciais e operadores de infraestruturas críticas. O modelo hoje utilizado na APF, o PPSI, pode vir a ser acrescido dessas características. Necessitamos também de um modelo que possa gerar informações agregáveis nacionalmente e setorialmente para alimentar o modelo nacional e permitir a avaliação da efetividade das políticas públicas de cibersegurança ao longo do tempo.	
Implementação: Consolidação e adaptação de modelos de maturidade institucional internacionalmente reconhecidos como o C2M2 2.1 e o CSF 2.0 e com o modelo de conformidade CIS 8.1 e o PPSI 2.0.	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.6 IEE 06 - Lei Geral da Cibersegurança/Marco Legal da Cibersegurança

Proponente: CNCiber	**Prazo:** 2026-2031
Responsável: CNCiber, GSI, CC e SRI	
Descrição: Proposição de um anteprojeto de Lei Geral da Cibersegurança integrado ao Marco Legal em discussão no Senado Federal	
Motivação: O CNCiber tem sdo taxativo na necessidade de uma marco legal que oriente as atividades de regulação, fiscalização, coordenação e controle da atividade de cibersegurança nacional. O Poder Executivo Federal elabora, desde fevereiro de 2023, um anteprojeto de lei para a organizar as competências e responsabilidades pela cibersegurança nacional, com uma proposta anuída por unanimidade no CNCiber em dezembro de 2025, que agora precisa ser encaminhada ao Congresso Nacional e integrada ao projeto de lei em tramitação no Senado Federal.	
Implementação: Consolidação da proposta aprovada pelo CNCiber com a Casa Civil, SRI e Congresso Nacional	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.7 IEE 07 - Órgão de Governança

Proponente: CNCiber	**Prazo:** 2026-2031
Responsável: CNCiber, GSI, CC e SRI	
Descrição: Proposição de um órgão de governança da cibersegurança nacional para coordenar a implementação das políticas públicas nacionais de cibersegurança	
Motivação: Uma das principais carências identificadas na implementação das políticas públicas de cibersegurança é a falta de um órgão responsável pela coordenação centralizada dessas políticas, com capacidade de regulação, fiscalização, coordenação e controle.	
Implementação: Proposição de um órgão de governança para assumir a atribuição de autoridade nacional de cibersegurança com base nos estudos elaborados pelo CNCiber.	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.8 IEE 08 - Hotsite do P-Ciber

Proponente:	**Prazo:**
GSI	2026-2031
Responsável: SE-CNCiber, por meio da Assessoria de Comunicação Social do GSI/PR.	
Descrição: Criação de uma solução digital para a disponibilização do conteúdo do P-Ciber, integrado à E-Ciber, para toda a sociedade, em consonância com os princípios da publicidade e da transparência ativa.	
Motivação: A necessidade decorre não somente dos princípios já mencionados, mas também para permitir o claro entendimento de uma metodologia governamental que adota a tríade política-estratégia-plano aplicada ao caso concreto da cibersegurança. Esta solução digital é arquitetada de forma que o usuário entenda claramente o encadeamento e a razão de ser de cada iniciativa estratégica existente ou, metaforicamente, como cada tijolo contribui para a construção do edifício. Ademais, esta forma de publicação dos trabalhos é muito mais flexível a adaptável do que as publicações impressas tradicionais, possibilitando sua atualização constante, à medida que novas iniciativas surjam ou que as mais antigas sejam completadas e retiradas do sítio eletrônico, por exemplo.	
Implementação: O conteúdo a ser exposto no sítio eletrônico será o próprio P-Ciber. Algumas estratégias de divulgação para conteúdos análogos foram examinados em alguns países e avaliados como benchmarks, tendo a solução digital suíça (https://digital.swiss/en/) sido considerada a mais adequada às finalidades brasileiras em razão de sua objetividade e simplicidade de projeto.	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.9 IEE 09 - Fundos Setoriais para Estímulo à Cibersegurança

Proponente: CNCiber	**Prazo:** 2026-2031
Responsável: CNCiber, GSI, CC, SRI e ORSs	
Descrição: Proposição de adaptações normativas (legais ou infralegais) para explicitar a possibilidade de utilização de fundos setoriais existentes para projetos de melhoria da cibersegurança e ciber-resiliência nos respectivos setores	
Motivação: Um dos principais óbices apontados pelos administradores públicos e privados é a dificuldade na obtenção de recursos para a implementação de programas ou projetos de cibersegurança. A viabilização do uso de fundos setoriais existentes para tais projetos pode dinamizar a implementação desses projetos.	
Implementação: Proposição de alterações legais e infralegais para explicitar a possibilidade de utilização de recursos dos fundos setoriais para atividades de cibersegurança.	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.10 IEE 10 - Fortalecimento de ISACs

Proponente:	**Prazo:**
GSI	2026-2031
Responsável: GSI	
Descrição: Adoção de ações em variadas frentes com vistas a concretizar as iniciativas propostas na Portaria GSI/PR nº 148, de 8 de abril de 2025, a qual "Institui a Diretriz de Estímulo à Criação e Operação de Centros de Análise e Compartilhamento de Informações (Information Sharing and Analysis Centers - ISACs). "	
Motivação: A necessidade decorre de que tais organizações têm natureza privada e frequentemente surgem pela associação voluntária de operadores de infraestruturas críticas de um país. Esta associação, especialmente quando incentivada pelo Governo, traz muitos benefícios em cibersegurança para os países em que elas já existem, principalmente pelo fato de que a atuação colaborativa especializada no compartilhamento de inteligência de ameaças cibernéticas aumenta grandemente a resiliência em uma área específica de serviço essencial ou de infraestrutura crítica. Outro ponto importante a considerar é o alto percentual de presença de tecnologia operacional (TO), área que ainda conta com reduzido número de profissionais e especialistas dedicados à cibersegurança, e que, portanto, podem ter sua atuação potencializada pela atuação coordenada e/ou centralizada.	
Implementação: A atuação proativa da SSIC/GSI monitora o surgimento destas iniciativas pelo país e, no momento certo, faz o convite formal para adesão à ReGIC. O CNCiber instituiu um guia para a criação e operação de ISAC com orientações práticas neste sentido, e tem revisado e chancelado materiais informativos produzidos pelas organizações já existentes. O objetivo é que todos os setores de serviços essenciais e de operadores de infraestruturas críticas contem com tais centros em médio prazo.	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.11 IEE 11 - Programa de Apoio a PMEs

Proponente:	**Prazo:**
GSI	2026-2031

Responsável:

GSI, BNDES, SEBRAE, SERASA e FIESP.

Descrição:

Será desenvolvido um produto financeiro de mercado na forma de empréstimo bancário para que as PME interessadas possam aderir para empregar recursos no fortalecimento de sua postura de cibersegurança, aperfeiçoando processos, tecnologias e equipamentos, além de capacitar colaboradores em proteção cibernética.

Motivação:

O foco nesta significativa parcela do empresariado brasileiro decorre do fato de que cerca de 2/3 das empresas deste porte fecham suas portas em até 6 meses após serem vítimas de ataques cibernéticos, com significativos prejuízos para o mercado de trabalho e a economia nacional. Tais empresas frequentemente não contam com recursos disponíveis para investir em cibersegurança, de forma que aceitam um risco alto sem qualquer alternativa. Sua fragilidade no ambiente digital também as coloca em desvantagem em termos concorrenciais como integrantes de cadeia de suprimento, visto que as grandes empresas contratantes, igualmente preocupadas com sua cibersegurança, tendem a não incluir elos em sua cadeia de produção que não coadunem com as melhores práticas em cibersegurança.

Implementação:

Após o interesse do empresário manifestado nas respostas do questionário, será realizada uma capacitação gratuita a ser oferecida pelos estudantes e graduados do programa Hackers do Bem, da RNP. Esta interação possibilitará maior compreensão e confiança nos investimentos que o empresário fará na cibersegurança de seu negócio, além de abrir perspectivas profissionais mais amplas aos formandos do programa.

Recursos:

Os recursos materiais e humanos já se encontram descritos. Espera-se atingir, nesta primeira versão, cerca de 10 mil PME no país.

2.12 IEE 12 - Cibersegurança de Tecnologias Computacionais Emergentes (TCEs)

Proponente:	**Prazo:**
ANATEL MCTI	2026-2031
Responsável: CNCiber e Orgãos Públicos com atuação (e/ou recursos) para fomentar a PD&I e FRH (Ministérios, como MCTI, MCOM, MGI ou MD; Agências e/ou Autarquias Especiais: como Anatel ou ITI; ou instituições privadas parceiras do setor Público: RNP); além de organizações que trabalham no desenvolvimento dessas tecnologias.	
Descrição: Desenvolvimento e Implementação de programa para fomentar estudos e projetos sobre riscos, desafios e oportunidades trazidos pelas TCEs para a cibersegurança; para incentivar a adoção de TCEs para a promoção de cibersegurança; e para assegurar que cibersegurança seja prioridade no desenvolvimento de TCEs no país.	
Motivação: As TCEs (por exemplo IA, computação quântica e internet das coisas) trazem novos riscos e desafios para a promoção de cibersegurança ao mesmo tempo que a sua utilização para ações de prevenção, tratamento e resposta a incidentes cibernéticos traz oportunidades que precisam ser estudadas, compreendidas e aproveitadas. Além disso, os próprios aspectos de cibersegurança da tecnologia em si necessariamente precisam ser entendidos e fomentados.	

Implementação:

Criação de um Programa amplo e abrangente, com diretrizes e ações de fomento para incentivar que organizações dos setores público e privado, bem como a academia, no âmbito das suas competências, desenvolvam ações e projetos, com ênfase em quatro eixos:

a) mapeamento de riscos, impactos e oportunidades ensejadas pelas tecnologias emergentes em cibersegurança;

b) avanços (e novos desafios) em cibersegurança que poderão ser viabilizados com essas novas tecnologias;

c) mapear e priorizar iniciativas que possam acelerar a utilização dessas tecnologias para a promoção da cibersegurança em prol da Sociedade Brasileira;

d) parcerias com governos e centros de pesquisa estrangeiros para o desenvolvimento e aplicação de TCEs no Brasil.

Recursos:

Não existe, no momento, previsão orçamentária. Por outro lado, em tese há alternativas legislativas que viabilizariam a criação de um programa com a amplitude exigida para que o Plano Nacional proposto pelo CNCiber alcance um impacto equiparável ao Plano Brasileiro de IA. Nesse sentido, poderiam ser previstos recursos de fundos existentes (FNDCT, FNDIT, FUNTTEL ou FUST), para fomentar a PD&I e a FRH nas novas tecnologias, que ditarão os rumos da Cibersegurança, desde que esses fossem eventualmente fortalecidos com novos recursos. E uma possibilidade concreta pode advir, da criação do REDATA (ora em apreciação pelo Congresso Nacional), caso sejam promovidos ajustes com o foco sugerido.

2.13 IEE 13 - Programa Nacional de Certificação e Selo de Cibersegurança de Produtos e Serviços

Proponente:	**Prazo:**
MJSP	2026-2031
Responsável: CNCiber, Autoridade Nacional de Cibersegurança e ORSs.	
Descrição: Criação de um Programa Nacional de Certificação e Selo de Cibersegurança para produtos e serviços de tecnologia da informação utilizados pela Administração Pública e por provedores de serviços essenciais e operadores de infraestruturas críticas, atestando conformidade com requisitos mínimos de cibersegurança reconhecidos nacionalmente.	
Motivação: Ausência de critérios nacionais uniformes para avaliar a cibersegurança de produtos e serviços de TI e TO. Risco sistêmico decorrente da aquisição de soluções inseguras ou não auditadas. Necessidade de reduzir vulnerabilidades na cadeia de suprimentos digital. Dependência de certificações estrangeiras, nem sempre adequadas ao contexto regulatório brasileiro.	

Implementação:

O programa deve harmonizar e atuar em sinergia com processos de certificação de produtos implementados por órgãos reguladores setoriais, a exemplo daquele da ANATEL, os quais consideram requisitos de segurança cibernética para fins de avaliação de conformidade de equipamentos. Dessa forma, produtos e serviços de TI e TO deverão atender requisitos e padrões nacional e setorialmente reconhecidos, aprimorando a segurança da cadeia de suprimentos para agentes regulados. O programa e seus processos devem ser desenvolvidos de forma a otimizar fluxos e maximizar a eficiência, buscando não inibir a inovação e não criar barreiras de mercado.

Diretrizes:

a) certificação por organismos acreditados;

b) critérios técnicos baseados em padrões nacionais e internacionais;

c) integração com políticas de compras públicas;

d) priorização de soluções que integrem tecnologias desenvolvidas no País.

Recursos:

Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.

2.14 IEE 14 - Cadastro Nacional de Talentos em Cibersegurança (CNTCiber)

Proponente: MJSP	**Prazo:** 2026-2031
Responsável: CNCiber o ORSs	
Descrição: Estabelecimento de um banco de talentos em cibersegurança para acionamento de especialistas em caso de interesse público.	
Motivação: Incidentes cibernéticos sistêmicos podem exceder rapidamente a capacidade de resposta das instituições afetadas. Escassez de profissionais altamente especializados em momentos críticos. Necessidade de resposta coordenada e imediata em situações de grande relevância e interesse público. Boas práticas internacionais indicam a importância de cadastros técnicos estratégicos. Fortalecimento da cooperação público-privada em cenários de interesse público.	

Implementação: I - Cadastro de especialistas e qualificações; II - Estabelecimento de: a) termos de confidencialidade; b) regras de prevenção de conflitos de interesse; c) responsabilidades durante atuação. III - Integração com: a) GSI; b) MCTI; c) MEC; d) RNP; e) MGI; f) CSIRTs setoriais; g) outras instituições que qualifiquem profissioanis de cibersegurança. IV - Participação em treinamentos e simulações periódicas.
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.

2.15 IEE 15 - Exercício Cibernético Nacional de Resiliência Sistêmica (Complementar ao Guardião Cibernético)

Proponente: MJSP	**Prazo:** 2026-2031
Responsável: CNCiber, GSI e MD	
Descrição: Realizar anualmente um exercício de nível estratégico-executivo focado na simulação de falhas em múltiplas cadeias de suprimentos interconectadas (ex: falha de fornecedor de nuvem que afeta bancos e energia), envolvendo a alta gestão e reguladores, indo além da resposta tática e operacional.	
Motivação: Incidentes reais tendem a gerar efeitos em cascata entre setores interdependentes Exercícios exclusivamente técnicos são insuficientes para testar decisões estratégicas Necessidade de envolver alta gestão, reguladores e tomadores de decisão Fortalecer a coordenação interinstitucional em crises complexas Identificar falhas de governança antes de eventos reais	
Implementação: Ciclo estruturado do exercício: a) planejamento e definição de cenários realistas; b) treinamentos simulados (tabletop) com alta gestão; c) exercício técnico-operacional envolvendo CSIRTs e SOCs; d) relatório de lições aprendidas; e) publicação de síntese pública com salvaguardas de sigilo; f) Integração com exercícios já existentes (Guardião Cibernético).	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento. Possivelmente, fundos setoriais poderiam ser adequados para a realização dessas iniciativas, em conjunto com a iniciativa "Fundos Setoriais para a Cibersegurança".	

2.16 IEE 16 - Continuidade e Aprimoramento do Programa Hackers do Bem

Proponente: MCTI ANATEL	**Prazo:** 2026-2031
Responsável: MCTI, RNP, SENAI-SP, Softex e instituições públicas e privadas.	
Descrição: Assegurar a continuidade e aprimoramento do programa Hackers do Bem com a mobilização de recursos necessária para a continuidade do programa com novas edições, ampliação de vagas nas fases mais avançadas, incluindo parcerias para oportunizar vagas na residência tecnologia.	
Motivação: A lacuna de recursos humanos especializados é um dos maiores riscos em cibersegurança, com estimativas apontando gap de quase 5 milhões de profissionais globalmente, também afetando o país. Para além de uma necessidade doméstica, também pode se transformar em uma oportunidade de emprego e renda para milhares de brasileiros e produtos e serviços para o mercado global.	
Implementação: Mobilização de recursos para garantir a continuidade e o aprimoramento do programa.	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.17 IEE 17 - Continuidade e Aprimoramento do Exercício Guardião Cibernético

Proponente: GSI	**Prazo:** 2026-2031
Responsável: MD, GSI, CNCiber	
Descrição: Assegurar a continuidade e aprimoramento do Exercício Guardião Cibernético (EGC) com a mobilização de recursos necessária para a continuidade do exercício com novas edições e ampliação do número de participantes.	
Motivação: O histórico do EGC ao longo dos anos mostra a sua importância na consolidação de uma cultura de prontidão para ciberincidentes que possam afetar SEICs, bem como no planejamento da resiliência e da contingência decorrente das interdependências entre os diversos setores. O EGC é hoje um dos maiores exercícios de simulação e prontidão para ciberincidentes e cibercrises do mundo. Mas precisa ser ampliado para contemplar mais setores e mais instituições relacionadas a SEICs.	
Implementação: Mobilização de recursos para garantir a continuidade e o aprimoramento do exercício.	
Recursos: Não existe previsão orçamentária para a implementação dessa iniciativa no presente momento.	

2.18 IEE 18 - Fortalecimento do Programa de Privacidade e Segurança da Informação (PPSI)

Proponente: MGI	**Prazo:** 2026-2031
Responsável: MGI	
Descrição: Fortalecer o Programa de Privacidade e Segurança da Informação (PPSI), no tocante ao seu núcleo de cibersegurança, por meio da consolidação do modelo de maturidade, institucionalização da gestão de riscos como eixo de governança, padronização de controles e integração entre proteção de dados pessoais, segurança da informação e cibersegurança, com expansão a estados e municípios para promover harmonização nacional e cooperação federativa. A iniciativa observará a LGPD, a PNSI, a PNCiber e os eixos estratégicos da E-Ciber, incorporando diretrizes para uso de Inteligência Artificial (IA) e sua aplicação no aprimoramento do programa.	
Motivação: Reforçar a privacidade e a segurança da informação como fundamentos da transformação digital do Estado, assegurando proteção de dados, continuidade dos serviços e confiança institucional. O fortalecimento do PPSI consolidará modelo de governança baseado em riscos, elevando a maturidade, aprimorando a prevenção e resposta a incidentes e promovendo expansão estruturada a estados e municípios para harmonização de práticas e integração federativa. A utilização estratégica de IA no âmbito do programa ampliará a capacidade analítica e a qualidade da tomada de decisão, contribuindo para maior eficiência e padronização.	
Implementação: O fortalecimento do PPSI ocorrerá de forma contínua, com avaliação de maturidade alinhada à IEE 05 e aprimoramento da gestão de riscos conforme a LGPD, a PNSI e a PNCiber. Abrangerá a atualização de normativos, definição de responsabilidades, monitoramento de controles e capacitação, podendo ser adotado por estados e municípios para harmonização e integração federativa, bem como o uso de ferramentas de IA para apoiar a gestão, o monitoramento e o aprimoramento do programa.	
Recursos: Não há previsão de dotação orçamentária específica no presente momento.	