A ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA (E-Ciber)

2025

GABINETE DE SEGURANÇA INSTITUCIONAL

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

E-Ciber

Apresentação

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) apresenta a nova Estratégia Nacional de Cibersegurança (E-Ciber), regulamentada pelo Decreto 12.573/2025, que orienta os esforços para elevar a segurança e a resiliência cibernéticas nacionais.

A estratégia foi elaborada com base nas propostas do Comitê Nacional de Cibersegurança (CNCiber). O comitê é formado por 25 membros, sendo 16 representantes governamentais e 9 da sociedade civil. Estruturada em quatro eixos interligados, a E-Ciber promove:

(1) ações para ampliar a proteção e a conscientização de cidadãos e da sociedade, com iniciativas de educação formal e informal para todas as idades;

(2) o fortalecimento da segurança e da resiliência de serviços essenciais e infraestruturas críticas, apoiando a transformação digital em curso e mitigando riscos;

(3) a integração e a cooperação entre órgãos e instituições, no Brasil e no exterior; e

(4) medidas para garantir a soberania nacional e a governança da cibersegurança.

Trata-se da segunda estratégia nacional de cibersegurança do Brasil, que incorpora características de terceira geração, comparáveis às de nações líderes no setor, alinhando o País às mais avançadas práticas mundiais em conformidade com estudo do Banco Interamericano de Desenvolvimento (BID).

A E-Ciber estabelece 40 ações estratégicas, desdobradas em Planos Nacionais de Cibersegurança a serem periodicamente atualizados pelo CNCiber. O documento representa avanço significativo na área de cibersegurança, na resiliência de serviços essenciais e infraestruturas críticas e na consolidação da soberania digital do Brasil.

Gabinete de Segurança Institucional
Presidência da República

Confira o decreto 12.573/2025

SUMÁRIO

Estratégia Nacional de Cibersegurança (E-Ciber) 2025

Em 2023 foram instituídos a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança (CNCiber), envolvendo representantes do governo, da academia, da sociedade civil e do empresariado. O objetivo foi aprimorar a cibersegurança e a ciber-resiliência do País, bem como promover a cooperação nacional e internacional nesses temas.

Coube ao CNCiber elaborar a proposta que fundamentou a presente estratégia, que busca delinear os melhores rumos para a consecução dos objetivos estabelecidos na PNCiber. Para tanto, o Comitê elaborou um conjunto de prioridades visando a atender as necessidades mais urgentes do Brasil no campo da cibersegurança, com melhor e mais efetiva alocação de recursos, em curto e médio prazos, em um processo gradual e evolutivo. Cabe também ao CNCiber a gestão de riscos ao longo da implementação de toda essa política pública e, consequentemente, da E-Ciber. O Comitê vislumbra o estabelecimento de um órgão para a governança da cibersegurança nacional, o qual será responsável pela coordenação das ações e pela criação de mecanismos de regulação, fiscalização, coordenação e controle da temática no país, contemplando também a proteção de serviços essenciais e infraestruturas críticas e a gestão de cibercrises relevantes.

1 Panorama cibernético mundial

Em janeiro de 2023, o Fórum Econômico Mundial (WEF) apresentou seu Relatório de Riscos Globais, no qual afirma que "a tecnologia exacerbará as desigualdades, enquanto os riscos da cibersegurança continuarão sendo uma preocupação constante". Apontou, ainda, que o crime e a insegurança cibernéticos constituíam um novo elemento na lista dos 10 principais riscos globais mais graves da próxima década.

Já em janeiro de 2024, o WEF apresentou uma atualização desse relatório, no qual a cibersegurança subiu para o 5º lugar dentre os maiores riscos globais. Indicou também que os prejuízos mundiais decorrentes de ciberincidentes podem ser estimados na casa de 14% do Produto Interno Bruto (PIB) global que, projetados para o PIB brasileiro de 2024, correspondem a cerca de 1,5 trilhão de reais.

Na edição de 2025, o relatório apontou a ciberespionagem e a ciberguerra como a 5ª principal preocupação no horizonte de dois anos, percepção provavelmente influenciada pelo agravamento das tensões econômicas e políticas e pelos conflitos militares contemporâneos.

À medida que o ciberespaço desponta como arena preferencial de atividade criminosa transnacional e de competição e fricção geopolíticas, seus usos ofensivos e defensivos entram no cálculo estratégico de Estados e atores não estatais, com impactos na ordem internacional.

1.1 Ameaças

Ciberameaças têm a capacidade de colocar em risco grande número de indivíduos e organizações, inclusive as que detêm ou operam serviços essenciais e infraestruturas críticas, cujo papel central na sociedade acarreta elevado grau de sensibilidade.

Problemas graves e socialmente relevantes, como a fome e a dificuldade de acesso à eletricidade ou ao saneamento básico, são enfrentados por meio de esforços e priorização de investimentos. Já no contexto das ciberameaças, tipicamente existem oponentes motivados, com recursos e capacidade técnica variados, demandando ação e atenção permanentes por parte do Estado.

Alguns dos principais tipos de ameaças contra os serviços essenciais e infraestruturas críticas são: *phishing;* ataques de negação de serviço em larga escala; *ransomware;* vazamentos de informações privadas ou institucionais; ciberespionagem; interrupção de serviços e Ameaças Persistentes Avançadas (APTs). Essas ações maliciosas, perpetradas por atores estatais e não estatais, apresentam variados escopos, níveis de sofisticação e motivações. Podem responder a interesses políticos, religiosos, militares, econômicos, de inteligência, de sabotagem ou puramente criminosos.

O avanço de tecnologias emergentes, como a Inteligência Artificial e a Computação Quântica, tende a tornar esse cenário ainda mais desafiador, face às capacidades que tais inovações podem agregar aos agentes maliciosos.

O desenvolvimento de capacidades cibernéticas ofensivas, a depender de seu alcance, pode ter impactos comparáveis aos de ataques cinéticos e comprometer decisivamente interesses nacionais.

1.2 Contexto nacional

Em junho de 2022, a Lista de Alto Risco da Administração Pública (LAR), elaborada pelo Tribunal de Contas da União (TCU), apontou que "em 2021, 73,1% dos serviços públicos prestados pelo governo federal já eram totalmente digitais, o que corresponde a 3.598 serviços". Se considerados também aqueles parcialmente digitais, o percentual chega a 86,7%. "Esses números por si só mostram a dimensão dos riscos e o prejuízo que falhas de segurança e indisponibilidade de serviços podem acarretar".

Já a LAR de 2024 apontou aumento de 56% no número de ciberincidentes que afetaram a Administração Pública Federal, o que "levanta preocupações sobre a capacidade de as organizações públicas protegerem seus dados (estratégicos e pessoais) e manterem a prestação de serviços à sociedade brasileira", e que a cibersegurança, a autodeterminação e a capacidade de explorar econômica, estratégica e tecnologicamente seus dados pessoais e críticos são as três dimensões fundamentais da soberania digital.

De outra parte, as avaliações da maturidade brasileira em cibersegurança conduzidas em 2020 e em 2023, com base no Modelo de Maturidade em Cibersegurança da Universidade de Oxford, mostram que o Brasil, em todos os quesitos, encontra-se abaixo do ponto médio da escala, o estágio "Estabelecido". Ainda, conquanto tenha melhorado ligeiramente em 50% dos quesitos, manteve-se no mesmo nível em 29% e piorou em 21% deles, refletindo que o Brasil passasse de uma média de 40% de atendimento ao modelo em 2020 para 44% em 2023, patamar insuficiente para o nível de exposição digital da sociedade brasileira.

Para uma sociedade que busca a melhoria da qualidade de vida por meio da evolução tecnológica, tais números servem de alerta, evidenciando a premência de investimentos na área e a adoção de estrutura normativa e regulatória consistente. Ademais, ciberincidentes impactam duramente os direitos humanos, o exercício da cidadania, a economia e o desenvolvimento sustentável.

Não obstante, o Relatório do Índice Global de Cibersegurança de 2024 da União Internacional de Telecomunicações, reconhecendo os esforços de aprovação da PNCiber, a instituição do CNCiber e a promulgação da Convenção de Budapeste (convenção sobre o crime cibernético), dentre outras ações, posicionou o Brasil no grupo dos países-modelo em evolução nas áreas de medidas legais, técnicas, organizacionais, de conscientização e capacitação, e de cooperação internacional nessa matéria. Embora o índice não mensure a implementação de capacidades, tais marcos e iniciativas desenvolvidos no País traduzem uma evolução recente da maturidade do Estado brasileiro no tema.

1.3 Desafios

No contexto das ciberameaças, as organizações necessitam de meios para identificar, proteger, responder e recuperar-se de incidentes. Prevenção e reação adequadas irão demandar consciência situacional, cooperação e coordenação, que seriam mais bem encaminhadas por meio de uma estrutura de comando e controle centralizada.

O principal desafio a ser enfrentado pela sociedade brasileira referente à cibersegurança é estabelecer uma coordenação nacional das ações existentes, ou pretendidas, por diferentes atores públicos e privados, abrangendo todos os poderes e entes da Federação. Essa coordenação deve equacionar os riscos e as suas necessidades mais prementes, buscando sinergia no emprego dos limitados recursos humanos e materiais disponíveis, de modo a garantir a continuidade e a aceleração do processo de transformação digital vivenciado pelo País. Deve também buscar o aproveitamento das oportunidades criadas pelas tecnologias emergentes, como a utilização de ferramentas de inteligência artificial e aprendizado de máquina para analisar, identificar e responder aos ataques cibernéticos.

Outro desafio relevante é a escassez de dados e indicadores nacionais, consistentes e periódicos, que permitam o diagnóstico e o acompanhamento da evolução do contexto e do cenário, adequado às características, necessidades e condicionantes do País.

Além disso, é preciso melhorar a conscientização de gestores públicos e privados em relação aos riscos e ameaças do ciberespaço. A cibersegurança deve ser encarada como fator de estabilidade das sociedades modernas, um investimento que garante o bom funcionamento de todos os setores da economia e a continuidade dos negócios, minimizando a possibilidade de incidentes ou descontinuidade de serviços essenciais, com risco de paralisação e prejuízo das atividades da organização.

A E-Ciber contempla essas e outras questões relevantes para a elevação da maturidade nacional em cibersegurança, orientando as ações que o País deve seguir para se tornar mais seguro e resiliente às ameaças postas e vindouras. Ademais, sem deixar de usufruir dos benefícios que a tecnologia carreia para a sociedade e de inserir-se na crescente cadeia global de valor associada à cibersegurança.

1.4 Evolução da E-Ciber

A presente estratégia consiste na segunda versão do documento brasileiro nessa temática. Em linha com os resultados do Relatório do Índice Global de Cibersegurança de 2024 da União Internacional de Telecomunicações, a evolução da maturidade nacional pode ser depreendida da análise de alguns pontos, a exemplo daqueles refletidos na tabela a seguir, que apresenta um sumário comparativo da presente E-Ciber com sua predecessora.

TÓPICO	E-Ciber 2020	E-Ciber 2025	DESCRIÇÃO DA EVOLUÇÃO
Governança	Proposta de governança centralizada.	Governança se integra à soberania nacional como um dos 4 eixos temáticos da estratégia.	A nova estratégia propõe o desenvolvimento de mecanismos de regulação, fiscalização, coordenação e controle.
Desenvolvimento Tecnológico Nacional	Enfoque genérico no setor de cibersegurança.	Incentivo específico para tecnologias, soluções nacionais e redução do débito tecnológico em cibersegurança.	A nova abordagem fortalece a independência do Brasil e estimula a redução da dependência de tecnologias estrangeiras.
Inclusão e Diversidade	Não mencionada.	Inclusão de grupos sub-representados (crianças, adolescentes, idosos e neurodivergentes).	A nova estratégia incentiva a proteção de grupos vulneráveis.
Maturidade Cibernética	Avaliação esporádica.	Meta clara de atingir o nível 'Estabelecido' em todos os quesitos de maturidade.	A melhoria traz um acompanhamento estruturado da evolução do Brasil em cibersegurança.
Proteção de Serviços Essenciais e Infraestruturas Críticas	Foco em infraestruturas críticas.	Ampliação do enfoque para contemplar Serviços Essenciais e suas Infraestruturas Críticas.	Melhor preparação e resiliência dos serviços essenciais e infraestruturas críticas, incluindo padrões mínimos, seguros e certificação de produtos e serviços.
Orientação e oferta de apoio à inovação em PMEs e *Startups*	Incentivo à pesquisa e ao desenvolvimento.	Detalhamento de mecanismos para incentivar *startups* e PMEs.	A nova estratégia inclui ações específicas para criar um ambiente inovador para pequenas empresas.
Cooperação Internacional	Expansão de parcerias internacionais.	Intensificação de parcerias e intercâmbio com ênfase em construção de capacidades.	A estratégia de 2025 propõe o incremento das atividades de cooperação, para o fortalecimento conjunto de cibercapacidades.
Educação e Conscientização	Previsão de campanhas de conscientização.	Desenvolvimento de mentalidade de cibersegurança na sociedade, com ênfase em gestores públicos e privados.	A nova estratégia promove cultura de cibersegurança sustentável e enraizada na sociedade.

TÓPICO	E-Ciber 2020	E-Ciber 2025	DESCRIÇÃO DA EVOLUÇÃO
Comunicação e Resposta a Incidentes	Proposta de melhoria na comunicação entre setores.	Promoção da gestão de riscos e da proteção e resposta a ciberincidentes.	A melhoria favorece uma resposta mais ágil e eficaz, melhorando a capacidade de resposta a ciberincidentes.
Adoção de Tecnologias Emergentes	Incentivo genérico.	Redução do débito tecnológico do País em tecnologias emergentes e disruptivas.	A nova estratégia enfatiza a necessidade de ações governamentais afirmativas e incrementais para tal.
Vigência Ampliada	Vigência limitada a um período de 4 anos.	Vigência sem limite temporal, considerando objetivos e ações de curto, médio e longo prazos.	A nova estratégia considera e trata temas de horizonte mais amplo que aquele de 4 anos, o que constitui uma estratégia de longo prazo, ajustada por meio de planos anuais.

1.5 Objetivos a alcançar

A avaliação da eficácia da E-Ciber dar-se-á por meio do avanço dos quesitos do modelo brasileiro de maturidade em cibersegurança a ser proposto, que servirá de linha de base para essa estratégia.

Pretende-se que a E-Ciber permita que o Brasil em 5 anos obtenha ao menos o grau Estabelecido em todos os quesitos do modelo de maturidade, sem regredir naqueles em que já tenha igualado ou superado esse grau.

Os objetivos da E-Ciber desdobram aqueles da PNCiber:

- Garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade dos *hardwares, softwares* e dados utilizados para processamento, armazenamento e transmissão eletrônicos ou digitais de informações.
- Promover a soberania nacional, a priorização dos interesses nacionais e a diligência devida no ciberespaço.
- Estimular a adoção de medidas de proteção cibernética e gestão de riscos para prevenir, evitar, mitigar, reduzir e neutralizar vulnerabilidades, ataques e incidentes cibernéticos e seus impactos.
- Desenvolver a educação, a cultura e a capacitação técnico-profissional em cibersegurança na sociedade brasileira.
- Incrementar a atuação coordenada e o intercâmbio de informações de cibersegurança entre:

a) União, estados, Distrito Federal e municípios;

b) Poderes Executivo, Legislativo e Judiciário;

c) setor privado; e

d) sociedade em geral.

- Promover a autonomia produtiva e tecnológica na área de cibersegurança.
- Propiciar o desenvolvimento nacional de produtos, serviços e tecnologias voltados à cibersegurança.
- Intensificar o combate aos crimes cibernéticos.
- Implementar estratégias de colaboração para desenvolver a cooperação internacional.
- Fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à cibersegurança.

Assim, busca-se criar condições para articulação efetiva, no contexto da cibersegurança e ciber-resiliência, entre a União, os estados, o Distrito Federal e os municípios, os Poderes Executivo, Legislativo e Judiciário, o setor privado e a sociedade em geral. Portanto, abarca toda a nação, com especial atenção dedicada ao conjunto dos chamados "Serviços Essenciais".

1.6 Benefícios esperados

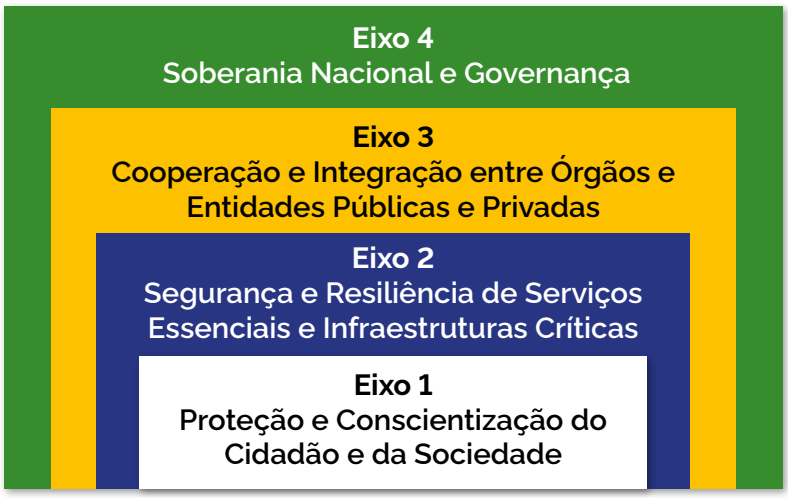
Estimativas de 2024 do Fórum Econômico Mundial apontam que as perdas financeiras com ciberofensas no Brasil em 2024 podem ter chegado a 14% do PIB global (cerca de 1,5 trilhão de reais, quando projetado para o Brasil) com severos impactos negativos sobre a arrecadação de impostos e tributos. Estudos recentes feitos especificamente para o Brasil pelo Instituto Nacional de Combate ao Cibercrime (INCC) indicam que esse número pode ter chegado a 18% do PIB (algo como 2,3 trilhões de reais). E esse valor cresce a cada ano.

Espera-se que a implantação da E-Ciber amplie a conscientização da sociedade, o preparo das instituições para a prevenção e a resiliência a ciberincidentes, em particular no tocante aos provedores de serviços essenciais e aos operadores de infraestruturas críticas, contendo a evolução dos prejuízos e reduzindo o risco da interrupção de serviços relevantes que possam gerar instabilidades na sociedade.

O decreto 12.573/2025 tem seu alcance normativo na esfera do Poder Executivo Federal e possui um efeito indutivo-colaborativo no âmbito dos demais poderes e na sociedade em geral.

2 Apresentação

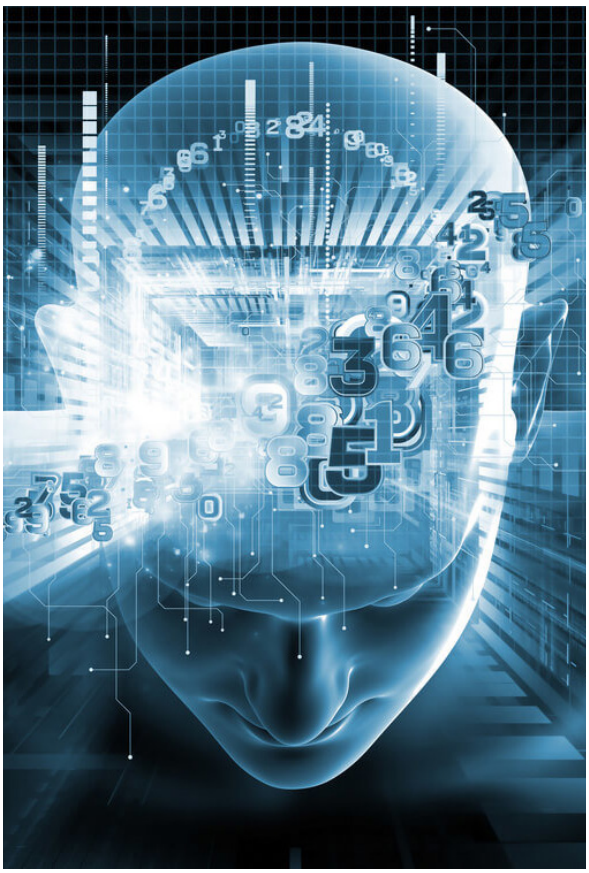
A E-Ciber 2025 foi desenvolvida considerando quatro Eixos Temáticos que se completam, apoiando-se uns nos outros, como representados na Figura 1.



Esses Eixos Temáticos agrupam um conjunto de Ações Estratégicas, a serem implementadas por meio de Iniciativas Estratégicas que serão detalhadas no Plano Nacional de Cibersegurança, conforme estabelece a PNCiber.

2.1 Eixo 1 – Proteção e conscientização do cidadão e da sociedade

A proteção e a conscientização do cidadão e da sociedade têm como objetivo garantir o uso seguro dos serviços digitais, com atenção especial às pessoas em situação de vulnerabilidade, como crianças e adolescentes, pessoas idosas e pessoas neurodivergentes. Para tanto, foram priorizadas as seguintes ações estratégicas:



- **Atuação segura no ciberespaço:** incentivo à adoção de comportamentos responsáveis e seguros por parte dos usuários ao utilizarem ferramentas digitais, com a promoção de práticas que reduzam ciber-riscos.
- **Apoio às vítimas:** promoção da ampliação de serviços de apoio às pessoas afetadas por crimes e outras práticas ilícitas no ambiente digital, com foco no acolhimento e na orientação.
- **Identificação e autenticação:** estímulo ao uso de mecanismos de identificação e autenticação de usuários conforme a necessidade de cada serviço digital, sempre respeitando a privacidade.
- **Capacitação de professores e gestores:** busca da qualificação de profissionais da educação, tanto da rede pública quanto privada, para habilitá-los a ensinarem tópicos relacionados à cibersegurança.
- **Cibersegurança na educação:** incentivo à inclusão de conteúdos sobre cibersegurança nos currículos escolares de todos os níveis, promovendo a formação de cidadãos digitalmente mais conscientes.
- **Participação em fóruns e eventos:** integração de estudantes, profissionais e pesquisadores em fóruns, congressos e atividades técnicas voltadas à cibersegurança.
- **Orientação a pequenas empresas:** orientação de *startups*, microempresas e empresas de pequeno porte quanto à gestão de ciber-riscos e à recuperação após ciberincidentes.
- **Planos de conformidade flexíveis:** avaliação de modelos adaptáveis de conformidade em cibersegurança para que órgãos públicos possam implementá-los de acordo com sua realidade.
- **Planos de contingência e testes:** incentivo ao desenvolvimento de planos institucionais de resposta a incidentes e à realização de testes e simulações para avaliar o nível de segurança cibernética.
- **Combate aos cibercrimes:** promoção da atuação integrada entre diferentes setores da sociedade para prevenir e combater crimes digitais, fraudes e outras ameaças no ciberespaço.

- **Divulgação de tratados internacionais:** disseminação da Convenção sobre o Crime Cibernético (Convenção de Budapeste) e de outros instrumentos nacionais e internacionais em vigor no País.
- **Ações contra o cibercrime:** apoio a iniciativas que aumentem a eficácia das operações de combate ao cibercrime, aprimorando investigações e respostas.
- **Canais de notificação:** estímulo ao aprimoramento legal e técnico das estruturas disponíveis para a denúncia de cibercrimes, visando a torná-las mais acessíveis e eficazes.
- **Capacitação de órgãos de persecução penal:** incentivo à formação contínua de profissionais que atuem em instituições responsáveis pela investigação e repressão ao cibercrime, para melhorar sua capacidade de atuação.

2.2 Eixo 2 – Segurança e resiliência de serviços essenciais e infraestruturas críticas

A segurança e a resiliência dos serviços essenciais e das infraestruturas críticas visam a oferecer instrumentos eficazes para prevenir e responder a ciberincidentes, buscadas por meio das seguintes ações estratégicas:

- **Promoção da gestão de riscos pelos reguladores:** estímulo para que entidades com funções regulatórias promovam a gestão de ciber-riscos e adotem medidas de proteção e resposta a ciberincidentes em seus respectivos setores.
- **Fortalecimento da regulação e controle:** desenvolvimento de mecanismos regulatórios, de fiscalização, de coordenação e de controle para garantir a segurança, a resiliência e a continuidade dos serviços essenciais, com foco especial na utilização segura de tecnologias da informação e operacionais.
- **Mecanismos de alerta de risco:** adoção de sistemas de alerta que avisem sobre riscos relevantes na prestação de serviços digitais, possibilitando respostas rápidas e eficazes.
- **Lista de alto risco de cibersegurança:** criação e manutenção de uma lista de alto risco que sirva como base para a gestão setorial de ciber-riscos.
- **Padrões mínimos para dados sensíveis:** estímulo à definição e adoção de padrões mínimos de cibersegurança para a proteção de dados relevantes e sensíveis, especialmente em contextos críticos.
- **Selo nacional de cibersegurança:** instituição de um selo nacional de certificação para indicar o nível de segurança de ciberativos, conferindo maior confiabilidade aos produtos, serviços e sistemas certificados.

- **Seguro contra ciberincidentes:** incentivo para que prestadores de serviços essenciais e operadores de infraestruturas críticas elevem suas medidas de resiliência, a exemplo da contratação de seguros específicos para cobrir danos decorrentes de ciberincidentes.
- **Exercícios e simulações:** promoção da realização periódica de exercícios e simulações, tanto em setores específicos quanto em contextos multissetoriais, com o objetivo de testar e fortalecer a ciber-resiliência dos serviços essenciais.
- **Aprimoramento normativo contínuo:** estímulo à constante atualização das normas relacionadas à cibersegurança, incluindo a definição de padrões mínimos de controle e a elaboração de guias técnicos.
- **Segurança na interoperabilidade de dados:** busca do fortalecimento da segurança na troca e no compartilhamento de dados entre sistemas, bem como nos canais digitais utilizados para a prestação de serviços.
- **Apoio às empresas brasileiras:** incentivos para que empresas nacionais busquem e utilizem produtos e serviços que estejam alinhados com padrões mínimos de cibersegurança, promovendo um ecossistema digital mais seguro.

2.3 Eixo 3 – Cooperação e integração entre órgãos e entidades públicas e privadas

A cooperação e a integração entre órgãos e entidades públicas e privadas visam a promover o debate e o intercâmbio de informações sobre cibersegurança, tanto no cenário nacional quanto internacional, com base nas seguintes ações estratégicas:

- **Criação de estruturas especializadas em cibersegurança:** estímulo ao estabelecimento de equipes de prevenção e resposta a incidentes cibernéticos, essenciais para atuação rápida em um cenário de ciberameaças crescentes. Ainda, a promoção da criação de centros de análise e compartilhamento de informações (ISACs, da sigla em inglês), os quais são instrumentos que geralmente contribuem para uma resposta coordenada. Também inclui o incentivo à instalação de laboratórios especializados, capazes de realizar testes, pesquisas e desenvolvimentos na área de cibersegurança.
- **Notificação nacional de ciberincidentes:** criação de um mecanismo unificado para a notificação de ciberincidentes no País, facilitando a resposta rápida, o mapeamento de ameaças e a coordenação entre atores públicos e privados.

- **Cooperação com instituições acadêmicas e agências:** fortalecimento das relações de confiança e colaboração entre instituições acadêmicas e agências nacionais e internacionais, buscando o desenvolvimento de ações conjuntas de cibersegurança e ciberdefesa, o fomento ao compartilhamento de informações e experiências, a promoção da divulgação coordenada de vulnerabilidades e a atuação no combate a cibercrimes e outros ilícitos no ambiente digital.
- **Fortalecimento da cibersegurança nos países vizinhos:** apoio à ampliação da capacidade de cibersegurança dos países do entorno estratégico do Brasil, por meio de iniciativas bilaterais ou multilaterais, com o objetivo de promover a estabilidade e a cibersegurança regionais.
- **Participação internacional do Brasil:** estímulo à presença ativa do Brasil em fóruns e organizações internacionais voltados à cibersegurança, favorecendo a troca de experiências, a definição de boas práticas e o alinhamento com padrões globais de proteção digital.

2.4 Eixo 4 – Soberania nacional e governança

A soberania nacional e a governança da cibersegurança têm como objetivo a proteção dos interesses da sociedade brasileira no ciberespaço e a garantia de um ambiente digital confiável, que favoreça o crescimento econômico e tecnológico do Brasil, pautando-se nas seguintes ações estratégicas:

- **Política Nacional de Cibersegurança:** atualização, divulgação e implementação da Política Nacional de Cibersegurança, conforme estabelecida pelo Decreto nº 11.856/2023, o qual orienta as ações estratégicas do País no campo da cibersegurança.
- **Modelo nacional de maturidade em cibersegurança:** elaboração de um modelo que permita medir a evolução do setor, avaliar o grau de maturidade em cibersegurança no Brasil e que também sirva de referência para ajustes no planejamento estratégico nacional.
- **Formação técnica e profissional:** ampliação da formação e capacitação técnica em cibersegurança em uma escala que atenda às demandas reais do País, incluindo a preparação de profissionais qualificados para atuar em todos os setores da economia.
- **Redução do débito tecnológico:** busca por ações afirmativas e progressivas para diminuir a dependência externa em tecnologias emergentes e disruptivas, fortalecendo a base tecnológica nacional.
- **Avaliação de conformidade em segurança:** estímulo ao desenvolvimento da capacidade de avaliar, de forma contínua, a conformidade em segurança de produtos, serviços e tecnologias ligados à cibersegurança, aumentando a confiabilidade e a qualidade das soluções utilizadas no País.

- **Sistemas seguros de troca de informações:** incentivo ao uso de sistemas seguros para o compartilhamento de informações sensíveis no campo da cibersegurança, promovendo maior proteção e integridade dos dados.
- **Incentivo ao setor privado:** apoio ao setor privado na criação e oferta de produtos, serviços e tecnologias voltadas à cibersegurança, com especial atenção às microempresas, pequenas empresas e *startups*.
- **Parcerias com institutos de pesquisa:** estímulo ao estabelecimento de parcerias com institutos brasileiros de pesquisa e desenvolvimento para o fortalecimento da produção científica e tecnológica nacional na área de cibersegurança, por meio de residências tecnológicas (estágios supervisionados em temas de cibersegurança).
- **Linhas de pesquisa e bolsas de estudo:** promoção da criação de linhas de pesquisa em cursos de graduação e pós-graduação *stricto sensu*, além da concessão de bolsas para formar especialistas e professores brasileiros em cibersegurança.
- **Desenvolvimento de soluções nacionais:** incentivo à produção de produtos, serviços e tecnologias nacionais que contribuam para o aprimoramento da cibersegurança no Brasil, reduzindo a dependência externa e promovendo a inovação local.

2.5 O Plano Nacional de Cibersegurança (P-Ciber)

A E-Ciber, enquanto estratégia nacional, tem um horizonte temporal não determinado e prevê que suas Ações Estratégicas serão desdobradas em Iniciativas Estratégicas de curto ou médio prazo, que deverão constar do Plano Nacional de Cibersegurança (P-Ciber). Este deve ser atualizado a cada um ou dois anos, com elaboração pelo CNCiber e aprovação pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) após anuência dos representantes dos órgão governamentais presentes no Comitê. O Plano conterá as iniciativas estratégicas discriminadas, seu cronograma de execução e a sua governança.

Expediente

Luiz Inácio Lula da Silva
Presidente

Geraldo Alckmin
Vice-presidente

Marcos Antonio Amaro dos Santos
Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República

Washington Rocha Triani
Secretário-Executivo do GSI/PR

Lincoln Bernardes Júnior
Secretário-Executivo Adjunto

Secretaria de Segurança da Informação e Cibernética

André Luiz Bandeira Molina
Secretário de Segurança da Informação e Cibernética

Luiz Fernando Moraes da Silva
Diretor do Departamento de Segurança Cibernética

Danielle Ayres
Diretora do Departamento de Segurança da Informação

Marcelo Antonio Osller Malagutti
Assessor Especial do Ministro

Assessoria

Marco Aurélio de Andrade Lima
Chefe de Gabinete do Ministro

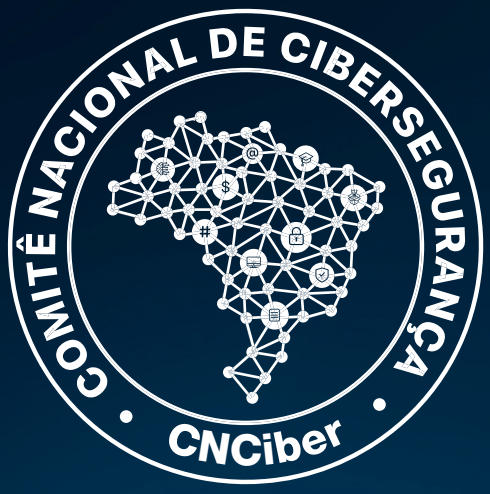
Cel (EB) R/1 Sergio Martins Rocha
Assessor Chefe Militar

Comunicação social

Heron Clementino de Andrade
Chefe da Assessoria Especial de Comunicação Social do GSI/PR

Design editorial
1º Ten EB Djalma Martins

Redação, revisão e tradução
Marcelo Antonio Osller Malagutti
Carlos Eduardo de Souza Gomes Fonseca
Maj EB Mayara Azeredo Alves
Primeiro-secretário **Reynaldo Collares**


COMITÊ NACIONAL DE CIBERSEGURANÇA
CNCiber