APRESENTAÇÃO

Este documento consiste em uma **minuta** de uma **Lei Geral da Cibersegurança** elaborada pelo Comitê Nacional de Cibersegurança (CNCiber).

O CNCiber, criado pelo Decreto 11.856, de 23 de dezembro de 2023, é um órgão consultivo, de sorte que suas propostas não têm caráter vinculante. Não obstante, dada a natureza multissetorial das 25 instituições que o integram, assim como o nível de especialização de seus membros na temática digital e da cibersegurança, são propostas fundamentadas no que há de mais moderno e atual na temática, de sorte que podem contribuir significativamente para o aprofundamento do debate nacional sobre os meios de se elevar o nível de cibersegurança e ciber-resiliência do Brasil.

A presente proposta resulta de um trabalho intenso, com centenas de horas de estudos, proposições e debates aplicadas na análise de alternativas e na elaboração de propostas que visam incorporar ao institucionalismo nacional as ferramentas necessárias para dotar o País dos instrumentos para continuar sua trajetória de digitalização crescente, com a segurança que nossa sociedade merece e demanda.

ANTEPROJETO DE LEI GERAL DE CIBERSEGURANÇA

Estabelece princípios, diretrizes e regras para a cibersegurança no Brasil e institui o Sistema Nacional de Cibersegurança.

O CONGRESSO NACIONAL decreta:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Seção I

Do objeto

Art. 1 º Esta Lei estabelece princípios, diretrizes e regras para a cibersegurança no Brasil e institui o Sistema Nacional de Cibersegurança.

Seção II

Das definições

Art. 2 º Para os fins desta Lei, considera-se:

I - agente de cibersegurança: pessoa natural ou jurídica, de direito público ou privado, responsável pela implementação ou execução de medidas de cibersegurança, conforme regulamentação da autoridade competente;

II - agente de cibersegurança obrigado: agente de cibersegurança que é obrigado a cumprir as disposições desta lei;

III - agente de cibersegurança voluntário: agente de cibersegurança que não é obrigado a cumprir as disposições desta lei;

IV - ambiente regulatório experimental ou *sandbox* regulatório: ambiente temporário controlado, criado pela autoridade nacional de cibersegurança, flexibilizando ou suspendendo a aplicabilidade do regramento vigente, para permitir a experimentação de inovações, sem sujeição a sanções imediatas;

V - autoridade competente de cibersegurança: autoridade nacional de cibersegurança ou autoridade setorial de cibersegurança, conforme o caso;

VI - autoridade nacional de cibersegurança: órgão ou entidade da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;

VII - autoridades setoriais de cibersegurança: órgãos ou entidades do Poder Público responsáveis por regular e fiscalizar atividades dos agentes de cibersegurança obrigados, dos provedores de serviços essenciais e operadores de infraestruturas críticas;

VIII - ciberameaça: circunstância ou evento, resultante de ciberofensa, com potencial para impactar, de forma adversa, indivíduos ou organizações, incluídos seus ativos, suas operações, suas funções, sua imagem ou sua reputação;

IX - ciberativos: *hardware, software*, redes, dispositivos, aplicações, serviços, sistemas ou dados utilizados para processar, armazenar ou transmitir informações por meio eletrônico ou digital;

X - ciberdefesa ou defesa cibernética: ações coordenadas com a finalidade de assegurar a cibersegurança de ativos de interesse da defesa nacional, obter dados para conhecimento de inteligência e buscar superioridade no ciberespaço sobre os ativos do oponente;

XI - ciberefeito: dano, permanente ou temporário, indisponibilidade ou limitação da operação, total ou parcial, ou mudança de comportamento de ciberativo ou não, resultante de ciberofensa;

XII - ciberespaço: ciberativos e seus usuários;

XIII - ciberincidente: ciberofensa combinada ao ciberefeito real ou potencial resultante de ciberofensa;

XIV - ciberofensa ou ciberataque: qualquer ato ou evento que comprometa a confidencialidade, integridade, disponibilidade, autenticidade ou resiliência de ciberativos, incluindo, mas não se limitando a infrações penais;

XV - cibersegurança: capacidade do Estado e da sociedade de proteger e garantir a segurança e a resiliência de ciberativos e seus usuários contra ciberameaças e ciberincidentes, compreendendo o conjunto articulado de ações preventivas, de resposta, de apuração de infrações, penais ou não, que possam comprometer a segurança nacional ou institucional, a ordem pública, a incolumidade das pessoas e o patrimônio;

XVI - equipe de prevenção, tratamento e resposta a ciberincidentes – ETIR: grupo de pessoas com a responsabilidade de prestar serviços relacionados à cibersegurança para uma instituição, pública ou privada;

XVII - ETIR setorial: ETIR de autoridade setorial de cibersegurança ou de agente de cibersegurança obrigado responsável por coordenar as atividades de cibersegurança e de centralizar as notificações de incidentes dos demais agentes do setor regulado;

XVIII - infraestruturas críticas: instalações, ativos e sistemas cuja destruição ou interrupção do funcionamento, total ou parcial, prejudique a prestação de serviços essenciais;

XIX - inteligência de ameaças: prática autorizada e regulamentada de coletar, analisar e disseminar informações sobre ciberameaças, com o objetivo de antecipar, prevenir e responder a ciberataques;

XX - invasão ética: prática autorizada e regulamentada de identificar, testar e explorar vulnerabilidades em ciberativos, com o objetivo de avaliar e fortalecer sua cibersegurança;

XXI - ISAC: centro de análise e compartilhamento de informações (*Information Sharing and Analysis Center* – ISAC), que funciona como plataforma neutra e segura para a coleta, análise e disseminação de informações sobre ameaças, vulnerabilidades e incidentes cibernéticos, promovendo a troca estruturada de dados e experiências, facilitando respostas mais rápidas e coordenadas a ciberincidentes, e permitindo a identificação precoce de tendências e ameaças emergentes;

XXII - plano de gestão de ciberincidentes: plano que orienta sobre a prevenção, o tratamento e a resposta a ciberincidentes;

XXIII - resiliência de serviços essenciais ou de infraestruturas críticas: capacidade de manutenção, ainda que degradada, da prestação de serviços essenciais ou do funcionamento de infraestruturas críticas, ou de sua recuperação, após a ocorrência de situação adversa;

XXIV - serviços essenciais: serviços indispensáveis ao atendimento das necessidades inadiáveis da sociedade que, quando não atendidas, colocam em perigo iminente a sobrevivência, a saúde ou a segurança do Estado ou da sociedade, provocando sério impacto social, ambiental, econômico, político ou internacional;

XXV - tecnologia computacional emergente (TCE): tecnologia da informação ou operacional provida por recurso tecnológico que, conquanto ainda em desenvolvimento ou implantação, apresenta elevado potencial para impactar significativamente diversos setores econômicos e sociais por apresentar inovações que oferecem novos modos de resolver problemas ou de aprimorar processos existentes; e

XXVI - usuário: pessoa natural ou jurídica que utiliza ciberativos que podem ser conectados direta ou indiretamente a outros ciberativos, ou que armazena, processa ou transmite dados.

Parágrafo único. Os serviços essenciais de que trata o inciso XXV do caput são os seguintes:

I - comunicações: telecomunicações, radiodifusão de sons e imagens e serviços postais;

II - defesa: atividades de defesa nacional;

III - defesa civil: gerenciamento de emergências e de calamidades públicas;

IV - educação: instituições de ensino fundamental, médio e superior, públicas ou privadas, hospitais universitários e centros de pesquisa;

V - energia: geração, distribuição e comercialização de energia elétrica, gás, hidrogênio, biocombustíveis, petróleo e derivados;

VI - espaço: serviços via satélite;

VII - finanças: transações bancárias, serviços financeiros, serviços de pagamento, investimentos e seguros;

VIII - governo digital: serviços eletrônicos ou digitais públicos, e de gerenciamento de ciberincidentes;

IX - infraestruturas digitais: centros de dados (*datacenters*), serviços de nuvem (*cloud computing*), provedores de infraestrutura de tráfego da Internet, serviços de nomes de domínio (*domain name services – DNS*) e de registro de nomes de domínios de topo (*top-level domains – TLD*), redes de distribuição de conteúdo (*content delivery networks – CDN*), prestadores de serviços de confiança (*a exemplo da certificação digital*), provedores de serviços gerenciados (*managed service providers – MSP*) e provedores de serviços de segurança gerenciados (*managed security service providers – MSSP*);

X - medicamentos e alimentos: produção, transformação, comercialização e distribuição;

XI - meio ambiente: proteção do meio ambiente, da fauna e da flora;

XII - nuclear: radiofármacos, instalações e combustíveis nucleares;

XIII - saneamento urbano: abastecimento de água, barragens, esgotamento sanitário, limpeza urbana e manejo dos resíduos sólidos;

XIV - saúde: atividades médicas, hospitalares, laboratoriais e funerárias, biossegurança, e bioproteção;

XV - segurança: justiça e segurança pública; e

XVI - transportes: controle de tráfego, transporte de pessoas e cargas nos modais aeroviário, aquaviário, ferroviário e rodoviário, e transporte público de passageiros.

Seção III

Dos princípios, objetivos e direitos

Art. 3 º A promoção da cibersegurança no Brasil tem os seguintes princípios:

I - a soberania nacional, a autonomia tecnológica e a priorização dos interesses nacionais;

II - inclusão digital e a educação em cibersegurança;

III - a apuração, a prevenção e a repressão de ciberincidentes e ciberataques, em especial quando dirigidos a serviços essenciais e infraestruturas críticas nacionais;

IV - a cooperação entre órgãos e entidades, públicas e privadas, nacionais e internacionais, em matéria de cibersegurança;

V - o desenvolvimento econômico, científico, tecnológico e a inovação;

VI - a livre iniciativa e a livre concorrência.

Art. 4 º. No contexto das ações de promoção da cibersegurança no Brasil, destacam-se especialmente os seguintes direitos e garantias fundamentais dos cidadãos:

I - a liberdade de expressão;

II - a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

III - a inviolabilidade do sigilo das comunicações, salvo por ordem judicial;

IV - a inviolabilidade e sigilo do fluxo de suas comunicações pela internet;

V - inviolabilidade e sigilo de suas comunicações privadas armazenadas;

VI - o acesso à informação; e

VII - o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Art. 5 º A promoção da cibersegurança no Brasil tem os seguintes objetivos:

XIV - fomentar as empresas e Instituições Científica, Tecnológica e de Inovação (ICTs) que desenvolvem, no País, produtos, serviços e tecnologias destinados à cibersegurança;

XV - estimular a aquisição pública de produtos, serviços e tecnologias destinados à cibersegurança

desenvolvidas por empresas e ICTs no País;

XVI - garantir a confidencialidade, a integridade, a autenticidade, a disponibilidade e o não repúdio dos dados utilizados para processamento, armazenamento e transmissão eletrônica ou digital de informações;

XVII - proteger as pessoas em contextos de maior exposição a riscos no ciberespaço, em especial:

a) crianças e adolescentes;

b) pessoas idosas; e

c) pessoas neurodivergentes;

XVIII - promover a prevenção, apuração e repressão de cibercrimes e de ciberofensas que ameacem a ordem pública, a incolumidade das pessoas e o patrimônio no ciberespaço;

XIX - estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, ciberincidentes e ciberataques;

XX - incrementar a resiliência das organizações públicas e privadas a ciberincidentes e ciberataques;

XXI - desenvolver a educação e a capacitação técnico-profissional em cibersegurança no País;

XXII - fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionados à cibersegurança;

XXIII - implementar e incrementar a atuação coordenada e o intercâmbio de informações de cibersegurança entre:

a) a União, os Estados, o Distrito Federal e os Municípios;

b) o Executivo, o Legislativo, o Judiciário e o Ministério Público;

c) o setor privado; e

d) a sociedade em geral;

XXIV - desenvolver mecanismos de regulação, fiscalização, coordenação e controle destinados a aprimorar a segurança e a resiliência cibernéticas nacionais, baseados na gestão dos riscos conforme a atividade; e

XXV - desenvolver a cooperação internacional em cibersegurança.

Seção IV

Do âmbito de aplicação

Art. 6º São agentes de cibersegurança obrigados:

I - operadores de infraestruturas críticas;

II - provedores de serviços essenciais; e

III - União, Estados, Distrito Federal e Municípios com mais de 100.000 (cem mil) habitantes.

§ 1º A aplicação desta Lei estende-se aos fornecedores diretos e indiretos que integram a cadeia

de suprimentos dos agentes de cibersegurança obrigados, devendo estes observar as normas e diretrizes expedidas pela autoridade competente de cibersegurança, em conformidade ao seu porte, natureza e grau de exposição a riscos.

§ 2º Os Municípios com menos de 100.000 (cem mil) habitantes observarão, no limite de suas condições orçamentárias, as disposições desta Lei.

§ 3º As Forças Armadas observarão as disposições desta Lei, respeitadas as especificidades da ciberdefesa.

§ 4º As instituições autorizadas a funcionar pelo Banco Central do Brasil observarão esta Lei, respeitadas as especificidades do seu setor, e a regulamentação do Banco Central do Brasil e do Conselho Monetário Nacional.

§ 5º Esta Lei aplica-se a qualquer agente de cibersegurança dos incisos I e II do **caput**, independentemente do país de sua sede, desde que:

I - a atividade seja realizada no território nacional;

II - a atividade tenha por objetivo a oferta ou o fornecimento de bens ou serviços de cibersegurança no território nacional;

III - o contratante esteja em território nacional; ou

IV - o objetivo da contratação inclua ciberativos que estejam em território nacional.

§ 7º As disposições desta Lei para os agentes de cibersegurança voluntários serão consideradas como boas práticas e não como obrigação legal.

§ 8º A aplicação da lei às micro e pequenas empresas, nos termos da Lei Complementar nº 123, de 14 de dezembro de 2006, será determinada pela autoridade competente de cibersegurança , respeitadas as especificidades e o porte.

CAPÍTULO II

DISPOSIÇÕES GERAIS

Seção I

Da gestão de riscos

Art. 7 º Os agentes de cibersegurança obrigados deverão adotar medidas técnicas, operacionais e organizacionais adequadas para:

I - gerir os riscos inerentes às suas atividades; e

II - minimizar ou mitigar o impacto de ciberincidentes nas suas atividades.

Parágrafo único. As medidas de que trata o *caput* deverão basear-se em uma abordagem sistêmica que:

I - contemple os riscos, a probabilidade de ocorrência de ciberincidentes e o impacto social e econômico, segundo critérios técnicos definidos pela autoridade competente de cibersegurança;

II - proteja os ciberativos, seu ambiente físico e os usuários diretamente vinculados a tais

sistemas;

III - garanta um nível de segurança adequado a cada risco identificado, considerando os avanços científicos, técnicos e tecnológicos mais recentes, inclusive internacionais, e os custos de sua implementação; e

IV - seja proporcional ao grau de exposição do agente de cibersegurança aos riscos e ao porte da sua organização .

Seção II

Das medidas de cibersegurança

Art. 8 º As medidas técnicas, operacionais e organizacionais a serem adotadas pelos agentes de cibersegurança obrigados, levando em consideração a matriz de risco aplicável, as especificidades de cada setor e o porte da organização, devem abranger, pelo menos, as seguintes áreas:

I - governança: estabelecimento da estrutura de governança, com definição formal de papéis e responsabilidades e gestão estratégica de riscos;

II - avaliação e auditoria: políticas e procedimentos para avaliação contínua da eficácia da gestão de riscos e um programa de auditorias internas ou externas para garantir a conformidade com requisitos legais e regulatórios;

III - gestão e proteção de ativos: classificação dos ciberativos e implementação de controles para sua proteção, incluindo o uso de criptografia e o estabelecimento de comunicações seguras;

IV - controle de acesso: políticas de controle de acesso, com a utilização de autenticação multifator e certificação digital;

V - segurança no ciclo de vida: incorporação de requisitos de segurança na aquisição, desenvolvimento e manutenção de ciberativos, incluindo o tratamento e a divulgação de vulnerabilidades;

VI - segurança:

a) de terceiros: gerenciamento dos riscos de segurança da cadeia de suprimentos (fornecedores e prestadores de serviços)

b) física: garantia da segurança das pessoas e instalações físicas;

VII - testes e monitoramento: realização de testes de cibersegurança contínuos para validação dos controles e detecção de atividades anômalas;

VIII - resposta a incidentes e crises: plano de resposta a incidentes de cibersegurança, testado e atualizado periodicamente, incluindo o tratamento dos ciberincidentes e a gestão de crises;

IX - continuidade de negócios e comunicações de emergência: manutenção da continuidade das operações, incluindo a recuperação de desastres e definição de protocolos para comunicação de emergência; e

X - conscientização e treinamento: conscientização e treinamento em cibersegurança, em diferentes níveis.

Parágrafo único: O agente de cibersegurança é responsável pela implementação das medidas de que trata os incisos do **caput**, inclusive no caso de sua opção pela contratação de empresa prestadora de serviços a terceiros para implementar tais medidas.

Art. 9 º Os agentes de cibersegurança obrigados devem adotar as medidas corretivas necessárias, adequadas e proporcionais, que sejam indispensáveis ao saneamento de suas falhas ou omissões.

Parágrafo único. As medidas corretivas de que trata o *caput* deverão ser atendidas nos prazos e nos termos previstos em regulamento exarado pela autoridade competente de cibersegurança.

CAPÍTULO III

DOS DEVERES DOS AGENTES DE CIBERSEGURANÇA OBRIGADOS

Seção I

Da interação com as autoridades competentes de cibersegurança

Art. 10 . Os agentes de cibersegurança obrigados, em conformidade com regulamentos exarados pela autoridade competente de cibersegurança, deverão:

I - designar e comunicar à autoridade competente de cibersegurança o responsável pela cibersegurança integrante da alta administração; e a equipe de ponto de contato permanente;

II - manter cadastro atualizado de suas informações;

III - notificar qualquer ciberincidente relevante à autoridade competente de cibersegurança;

IV - comunicar ao Centro Nacional de Cibersegurança-CENCiber vulnerabilidades relevantes identificadas em seus ciberativos; e

V - comunicar aos usuários dos seus serviços ciberincidentes relevantes;

§ 1º Regulamentação da autoridade competente de cibersegurança definirá prazos, procedimentos, forma de atendimento dos deveres relacionados à interação com a autoridade competente, inclusive para fins de classificação da relevância de ciberincidentes e de vulnerabilidades.

§ 2º A autoridade competente de cibersegurança resguardará o sigilo das informações e dados sobre o ciberincidente relevante notificado pelo agente de cibersegurança, podendo solicitar informações adicionais quando tiver conhecimento, ainda que por meios diversos do previsto no *caput*, inciso III.

Seção II

Da ETIR

Art. 11 . Compete aos agentes de cibersegurança obrigados e às autoridades setoriais de cibersegurança, nos termos das normas emitidas pela autoridade competente de cibersegurança:

I - instituir e implementar a sua ETIR;

II - comunicar imediatamente ao CENCiber, por meio de sua ETIR ou ISAC, sobre a existência de vulnerabilidades relevantes ou a ocorrência de ciberincidentes relevantes que impactem ou que possam impactar os serviços prestados ou contratados ou a operação da infraestrutura crítica;

III - promover ações de capacitação e profissionalização em cibersegurança para sua ETIR;

IV - manter a infraestrutura de sua ETIR atualizada; e

V - sanar, com urgência, as vulnerabilidades cibernéticas, em especial aquelas identificadas nos alertas e nas recomendações emitidos pelo CENCiber.

CAPÍTULO IV

DO FOMENTO AO ECOSSISTEMA DE CIBERSEGURANÇA NACIONAL

Art. 12 . A administração pública no âmbito da União, dos Estados, do Distrito Federal e dos Municípios poderá fomentar a inovação e o desenvolvimento produtivo e tecnológico em cibersegurança, na forma da legislação pertinente, pautado pelas seguintes diretrizes:

I - promoção da inovação nos setores produtivos, inclusive por meio da contratação de soluções inovadoras pelo Estado e da celebração de parcerias público-privadas;

II - investimento em pesquisa para o desenvolvimento de cibersegurança no País;

III - incentivo à produção local de componentes, equipamentos e soluções tecnológicas digitais;

IV - fomento ao desenvolvimento de produtos e serviços de cibersegurança no Brasil;

V - estímulo à inclusão de fornecedores nacionais na cadeia de valor global de cibersegurança.

Art. 13 O fomento à inovação e ao desenvolvimento produtivo e tecnológico em cibersegurança será realizado por meio dos seguintes instrumentos:

I - financiamento ou subvenção providos por instituições públicas de fomento;

II - encomendas tecnológicas;

III - contrato Público de Solução Inovadora (CPSI);

IV - concurso para a Inovação e Diálogo competitivo;

V - contratação direta de bens e serviços de cibersegurança desenvolvidos no País;

VI - incentivo à exportação de soluções e serviços de cibersegurança desenvolvidos no País;

VII - estímulo à adoção de padrões técnicos e certificações reconhecidas internacionalmente para facilitar a interoperabilidade e a aceitação de produtos brasileiros no exterior;

VIII - apoio à participação de empresas e instituições de pesquisa nacionais em projetos e consórcios internacionais de desenvolvimento de cibersegurança.

Parágrafo único. A implementação dos instrumentos previstos caput deverão conter cláusulas específicas que garantam a observância dos requisitos de segurança da cadeia de suprimentos, conforme orientações e diretrizes expedidas pela autoridade competente de cibersegurança.

CAPÍTULO V

DA GOVERNANÇA DA CIBERSEGURANÇA NACIONAL

Seção I

Do Sistema Nacional de Cibersegurança

Art. 14 . Fica instituído o Sistema Nacional de Cibersegurança - SNCiber, conjunto de órgãos e entidades da União, dos Estados, do Distrito Federal e dos Municípios, que atuam na promoção de cibersegurança, tendo como objetivos:

I - promover a harmonização e a colaboração entre os seus integrantes nos temas de cibersegurança;

II - subsidiar o Conselho Nacional de Cibersegurança no exercício das suas competências; e

III - compartilhar informações sobre:

a) medidas de prevenção, tratamento e resposta a ciberincidentes;

b) alertas sobre ameaças e vulnerabilidades cibernéticas;

c) fatos relacionados às suas competências regulatória e sancionatória; e

d) outros assuntos relacionados à cibersegurança.

Art. 15 . Integram o SNCiber:

I - o Gabinete de Segurança Institucional, como órgão central e coordenador;

II - a autoridade nacional de cibersegurança;

III - as autoridades setoriais de cibersegurança;

IV - os órgãos e as entidades públicos federais, estaduais, distritais e municipais que atuam na promoção de cibersegurança.

§ 1º Os integrantes do SNCiber participarão da Rede Nacional de Cibersegurança – RENCiber, que tem a finalidade de:

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

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;

III - divulgar informações sobre ciberataques;

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

V - promover a celeridade na resposta a ciberincidentes.

§ 2º O funcionamento da RENCiber será definido por meio de Regulamento da Autoridade Nacional de Cibersegurança.

§ 3º A secretaria-executiva SNCiber será exercida pelo Gabinete de Segurança Institucional da Presidência da República.

Seção II

Da Autoridade Nacional de Cibersegurança

Art. 16 . À autoridade nacional de cibersegurança compete a regulação, a fiscalização, a coordenação e o controle da cibersegurança no País.

Parágrafo único. As competências de que trata o caput são extensíveis à cibersegurança de tecnologias computacionais emergentes, exceto nos casos em que a legislação correspondente, quando houver, especifique o contrário.

Art. 17 . Caberá à autoridade nacional de cibersegurança no âmbito de suas competências:

I - emitir normas gerais sobre regras e padrões técnicos de cibersegurança;

II - monitorar o cumprimento das normas de que trata o inciso I, aplicando sanções em caso de infrações, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

III - expedir e reconhecer a certificação:

a) de produtos, serviços, tecnologias e esquemas de etiquetagem;

b) dos agentes de cibersegurança obrigados, conforme o nível de maturidade em cibersegurança; e

c) da cadeia de suprimentos dos agentes obrigados;

IV - promover a gestão de ciber-riscos por meio de:

a) disponibilização de documentos modelos;

b) formatação e execução de programas;

c) desenvolvimento de mecanismos de prevenção, monitoramento, detecção, análise e resposta a ciberincidentes; e

d) gerenciamento de crises cibernéticas;

V - gerir o CENCiber;

VI - promover e estabelecer mecanismos para prevenção, tratamento e resposta a ciberincidentes no País por meio das seguintes ações, dentre outras:

a) manutenção e operação de um centro de agregação e análise de informações sobre ataques e ciberincidentes;

b) suporte à prevenção, ao tratamento e à resposta a ciberincidentes nos serviços essenciais e infraestruturas críticas; e

c) suporte ao desenvolvimento das capacidades de prevenção, tratamento e resposta a ciberincidentes em todos os entes da federação;

VII - normatizar os procedimentos para a contratação ou realização, por agente de cibersegurança obrigado, das atividades de invasão ética e de inteligência de ameaças;

VIII - estimular a divulgação coordenada de vulnerabilidades e de informações de cibersegurança nos setores público e privado;

IX - cooperar com autoridades de cibersegurança, nacionais e, em coordenação com o Ministério das Relações Exteriores, internacionais, para:

a) a prevenção e tratamento de ciberameaças e ciberincidentes;

b) o desenvolvimento de capacidades de cibersegurança e ciber-resiliência; e

c) a divulgação de boas práticas e experiências brasileiras;

X - manter padrões e canais de comunicação seguros com setores de serviços essenciais e infraestruturas críticas para o compartilhamento de informações para prevenção e tratamento e resposta a ciberincidentes;

XI - contribuir para o desenvolvimento de uma cultura de cibersegurança no País; e

XII - estabelecer ambientes regulatórios experimentais para teste e observação de inovações, avaliação de seus riscos e benefícios, e posterior avaliação da necessidade de alteração do arcabouço regulatório; e

XIII - determinar, em caráter cautelar, por até 72 (setenta e duas) horas, o bloqueio de tráfego, a remoção de artefatos maliciosos, a desconexão ou o desligamento de ciberativos, desde que presentes os seguintes requisitos:

a) risco iminente de dano irreparável à confidencialidade, à integridade, à autenticidade ou à disponibilidade de ciberativos dos agentes de cibersegurança, ou à estabilidade do ciberespaço nacional; e

b) elevada possibilidade de aplicação de sanção por prática de atividade ilícita relacionada à cibersegurança.

XIV - definir, em conjunto com as autoridades setoriais de cibersegurança, as diretrizes relacionadas ao fomento às empresas e ICTs brasileiras que desenvolvem, no País, produtos, serviços e tecnologias nacionais destinados à cibersegurança;

XV - estabelecer diretrizes voltadas à capacitação e formação em proteção cibernética e gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, ciberincidentes e ciberataques.

Parágrafo único. A autoridade nacional de cibersegurança poderá emitir normas gerais diferenciadas para os agentes de cibersegurança obrigados, conforme as especificidades de cada setor, o porte da organização e a matriz de risco definida.

Seção III

Das Autoridades Setoriais de Cibersegurança

Art. 18 . Compete às autoridades setoriais de cibersegurança:

I - exercer competências regulatória, fiscalizatória e sancionatória, e de certificação e de representação internacional, para o respectivo setor, observadas as normas gerais expedidas pela autoridade nacional de cibersegurança, nos termos do § 1º deste artigo;

II - incentivar a adoção de padrões e de melhores práticas, e a adequada gestão do risco em cibersegurança em seu setor;

III - instituir ETIR setorial, nos termos das normas emitidas pela autoridade nacional de cibersegurança;

IV - notificar o CENCiber, por meio da ETIR setorial, quanto aos ciberincidentes de impacto relevante; e

V - identificar os serviços essenciais e as infraestruturas críticas de seu setor que requeiram atenção em termos de cibersegurança nacional.

§ 1º As autoridades setoriais de cibersegurança poderão dispor de forma diversa das normas gerais estabelecidas pela autoridade nacional de cibersegurança para o seu respectivo setor, podendo flexibilizar, dispensar ou aumentar o rigor das referidas normas, desde que devidamente motivado, devendo comunicar à autoridade nacional de cibersegurança sobre a decisão.

§ 2º No caso de flexibilização ou dispensa de normas gerais da autoridade nacional de cibersegurança, as autoridades setoriais de cibersegurança devem avaliar a eventual necessidade de adoção de medidas alternativas para alcançar a finalidade da norma geral.

§ 3º As autoridades setoriais de cibersegurança exercerão de forma plena as suas competências regulatória, fiscalizatória, sancionatória, de certificação e de representação internacional em cibersegurança, assegurando-se nesses casos competência residual à autoridade nacional de cibersegurança.

§ 4º O exercício da competência de representação internacional em cibersegurança, quando existente, não dispensa a necessidade de coordenação com o Ministério das Relações Exteriores.

Art. 19 O Banco Central do Brasil, o Conselho Monetário Nacional, o Conselho Nacional de Cibersegurança, a autoridade nacional de cibersegurança e o Gabinete de Segurança Institucional da Presidência da República manterão cooperação técnica contínua, incluindo a troca de experiências e a realização de estudos sobre o arcabouço regulatório internacional da cibersegurança no tocante ao setor supervisionado pelo Banco Central do Brasil.

Seção IV

Dos demais integrantes do Sistema Nacional de Cibersegurança

Art. 20 . Compete aos demais órgãos e entidades que atuam na promoção de cibersegurança implementar as normas gerais estabelecidas pela autoridade nacional de cibersegurança, no âmbito das suas competências.

Seção V

Do Conselho Nacional de Cibersegurança

Art. 21 . Fica instituído o Conselho Nacional de Cibersegurança – CNCiber com a finalidade de acompanhar a implementação desta Lei, da Política Nacional de Cibersegurança – PNCiber, da Estratégia Nacional de Cibersegurança – E-Ciber e do Plano Nacional de Cibersegurança – P-Ciber.

Art. 22 . Ao CNCiber compete:

I - propor atualizações para a PNCiber, E-Ciber; e P-Ciber.

II - avaliar e propor medidas, inclusive de educação, para incremento da cibersegurança no País;

III - formular propostas para o aperfeiçoamento da prevenção, da detecção, da análise e da resposta a ciberincidentes; e

IV - manifestar-se, mediante solicitação, sobre assuntos relacionados à cibersegurança; e

V - manifestar-se sobre ações de fomento às empresas e ICTs brasileiras que desenvolvem, no País, produtos, serviços e tecnologias destinados à cibersegurança.

Art. 23 . O CNCiber será composto por:

I - 1 representante do Gabinete de Segurança Institucional da Presidência da República, que o presidirá;

II - 1 representante da Autoridade Nacional de Cibersegurança;

III - 15 (quinze) representantes do Poder Executivo federal;

IV - 1 (um) representante do Senado Federal;

V - 1 (um) representante da Câmara dos Deputados;

VI - 1 (um) representante do Conselho Nacional de Justiça;

VII - 1 (um) representante do Conselho Nacional do Ministério Público;

VIII - 1 (um) representante do Comitê Gestor da Internet no Brasil;

IX - 3 (três) representantes de organizações da sociedade civil com atuação relacionada à cibersegurança;

X - 3 (três) representantes de instituições científicas, tecnológicas e de inovação relacionadas à área de cibersegurança;

XI - 3 (três) representantes do setor empresarial relacionados à área de cibersegurança;

XII - 1 (um) representante de prestadores de serviços essenciais ou operadores de infraestruturas críticas; e

XIII - 1 (um) representante de entidades estaduais e públicas de tecnologia da informação.

§ 1º A Secretaria-Executiva do CNCiber será exercida pelo Gabinete de Segurança Institucional da Presidência da República.

§ 2º Regulamento definirá sobre a representação dos órgãos e entidades Poder Executivo Federal, a suplência, o quórum de reunião e o quórum de aprovação das deliberações, a periodicidade das reuniões, a forma de edição do primeiro regimento interno, o mandato, e a forma de indicação dos representantes do § 2º, incisos IX, X, XI e XII.

Seção VI

Do Centro Nacional de Cibersegurança

Art. 24 . Fica instituído, no âmbito da autoridade nacional de cibersegurança, o Centro Nacional de Cibersegurança - CENCiber, órgão central da RENCiber, com as seguintes competências:

I - coordenar e acompanhar ações destinadas à gestão da prevenção, do monitoramento e do tratamento e resposta a ciberincidentes, inclusive no âmbito dos agentes de cibersegurança obrigados;

II - estimular a formação e a qualificação de recursos humanos na área de gestão de ciberincidentes;

III - promover o intercâmbio científico-tecnológico relacionado à gestão de ciberincidentes e ciberameaças com outros centros congêneres nacionais e internacionais;

IV - emitir alertas, recomendações, notificações, relatórios técnicos e estatísticos sobre vulnerabilidades e ciberincidentes, orientando as ETIRs quanto aos procedimentos de proteção e recuperação;

V - armazenar e analisar informações relativas a ameaças, ciberincidentes e tendências de vulnerabilidades cibernéticas;

VI - implementar mecanismos que permitam a avaliação dos danos reais e potenciais ocasionados por ciberincidentes;

VII - orientar as ETIRs dos agentes de cibersegurança obrigados e as ETIRs setoriais na verificação da conformidade dos controles estabelecidos de cibersegurança;

VIII - elaborar, atualizar e divulgar o plano de gestão de ciberincidentes para os agentes de cibersegurança obrigados;

IX - prover dados e informações de inteligência relativos a ciberameaças e ciberincidentes aos agentes de cibersegurança obrigados;

X - participar de operações interagências, entendidas como operações em conjunto com outras organizações, instituições ou entidades, com competências específicas, governamentais ou não, militares ou civis, públicas ou privadas, nacionais ou internacionais, com a finalidade de apoiar, no âmbito da cibersegurança, o objetivo das operações; e

XI - apoiar o Ministério da Defesa, sob demanda, nas operações de ciberdefesa ou defesa cibernética.

Parágrafo único. O CENCiber preservará o anonimato da pessoa física ou jurídica que comunicar uma vulnerabilidade.

CAPÍTULO V

DAS SANÇÕES ADMINISTRATIVAS

Art. 25 . Os agentes de cibersegurança obrigados, em razão das infrações cometidas às normas gerais emitidas pela autoridade nacional de cibersegurança, ficam sujeitos às seguintes sanções

administrativas:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2 % (dois por cento) do faturamento do último exercício da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - obrigação de fazer ou não fazer;

V - suspensão da distribuição de produtos ou fornecimento de serviços e tecnologias de cibersegurança a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

VI - proibição parcial ou total da distribuição de produtos ou fornecimento de serviços de cibersegurança a que se refere a infração; e

VII - proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas e de instituições financeiras públicas ou controladas pelo poder público, pelo prazo mínimo de 1 (um) e máximo de 5 (cinco) anos.

§ 1º Nos casos de empresas estrangeiras, responderá, solidariamente, pelo pagamento das multas de que trata o caput, incisos II e III, sua filial, sucursal, escritório ou estabelecimento situado no País.

§ 2º O disposto no caput, incisos I e IV, poderá ser aplicado às entidades e aos órgãos públicos.

Art. 26 . As sanções previstas no art. 24 serão aplicadas pela autoridade nacional de cibersegurança:

I - quando a infração não tiver sido apurada por autoridade setorial de cibersegurança;

II - após procedimento administrativo que possibilite a oportunidade da ampla defesa e contraditório; e

III - de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

a) a gravidade e a natureza da infração;

b) a boa-fé do infrator;

c) a vantagem auferida ou pretendida pelo infrator;

d) a condição econômica do infrator;

e) a reincidência;

f) o grau do dano causado;

g) a cooperação do infrator;

h) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano;

i) a adoção de política de boas práticas e governança em cibersegurança;

j) a pronta adoção de medidas corretivas; e

k) a proporcionalidade entre a gravidade da infração e a intensidade da sanção.

CAPÍTULO VI

DO ÓRGÃO DE GOVERNANÇA DA CIBERSEGURANÇA NACIONAL

[Designa ou institui órgão para exercer a atribuição de autoridade nacional de cibersegurança]

CAPÍTULO VII

DISPOSIÇÕES TRANSITÓRIAS

Art. 27 . Os agentes de cibersegurança obrigados. terão o prazo de 180 (cento e oitenta) dias para adequação às disposições legais, a contar da publicação das respectivas normas da autoridade nacional de cibersegurança e das autoridades setoriais de cibersegurança necessárias ao cumprimento dos deveres e obrigações constantes da Lei.

Art. 28 . Até que sejam ocupados os cargos destinados à a autoridade nacional de cibersegurança, o órgão a ser designado para esta função poderá efetuar, nos termos do art. 37, caput, inciso IX, da Constituição, e observado o disposto na legislação pertinente, contratação por tempo determinado, pelo prazo de vinte e quatro meses, do pessoal técnico imprescindível ao exercício de suas competências institucionais, limitado a sessenta pessoas, nos termos do art. 2º, caput, inciso VI, alínea "i", da Lei nº 8.745, de 9 de dezembro de 1993.

Art. 29 Parágrafo único. A contratação referida no *caput* poderá ser prorrogada, nos termos do disposto no art. 4º, parágrafo único, inciso IV, da Lei nº 8.745, de 9 de dezembro de 1993.

Art. 30 . O disposto no art. 2º da Lei nº 9.007, de 17 de março de 1995, aplica-se aos servidores, aos militares e aos empregados requisitados para a autoridade nacional de cibersegurança, limitado a sessenta pessoas, e até xx de xxxxxxxx de 202x.

Art. 31 . Esta Lei entra em vigor:

I - seis meses após sua publicação, em relação aos Capítulos xxxxxxx desta Lei; e

II - na data da sua publicação, para os demais dispositivos.

Art. 32 Brasília, de de 2025; º da Independência e º da República.