Presidência da República
Casa Civil
Secretaria Especial para Assuntos Jurídicos

DECRETO Nº 12.573, DE 4 DE AGOSTO DE 2025

Institui a Estratégia Nacional de Cibersegurança.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, *caput*, inciso VI, alínea "a", da Constituição,

DECRETA:

Objeto e âmbito de aplicação

Art. 1º Fica instituída a Estratégia Nacional de Cibersegurança – E-Ciber, estruturada nos seguintes eixos temáticos:

I - proteção e conscientização do cidadão e da sociedade;

II - segurança e resiliência dos serviços essenciais e das infraestruturas críticas;

III - cooperação e integração entre os órgãos e entidades, públicas e privadas; e

IV - soberania nacional e governança.

§ 1º Os objetivos da Política Nacional de Cibersegurança, estabelecidos no art. 3º do Decreto nº 11.856, de 26 de dezembro de 2023, serão alcançados por meio da E-Ciber.

§ 2º Os eixos temáticos de que trata o *caput* serão implementados por meio de ações estratégicas específicas, as quais serão detalhadas no Plano Nacional de Cibersegurança, nos termos do disposto no art. 11.

Definições

Art. 2º Para fins do disposto neste Decreto, consideram-se:

I - ciberativos - *hardwares*, *softwares*, redes, dispositivos, aplicações, serviços, sistemas e dados utilizados para processar, armazenar ou transmitir informações por meio eletrônico ou digital;

II - 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;

III - cibercrime - crime praticado contra ou por meio de ciberativos;

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

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

VI - ciberofensa - conjunto de ações adotadas no ciberespaço em oposição a ciberativo;

VII - cibersegurança - conjunto de ferramentas, salvaguardas, diretrizes, abordagens de gestão de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias, entre outras medidas usadas para proteger o ciberespaço e os ciberativos do usuário e da organização;

VIII - ciberdefesa - conjunto de ações coordenadas pelo Ministério da Defesa, com a finalidade de assegurar a cibersegurança de ciberativos de interesse da defesa nacional e buscar superioridade no domínio cibernético sobre os ciberativos do responsável pela ciberofensa;

IX - ciber-risco - possibilidade de ocorrência de ciberincidente;

X - tecnologia da informação - conjunto de ciberativos destinados ao processamento de sistemas e de dados; e

XI - tecnologia operacional - conjunto de ciberativos destinados ao comando e ao controle de processos industriais de setores, como manufatura, telecomunicações, energia, medicina, gestão predial, entre outros.

Proteção e conscientização do cidadão e da sociedade

Art. 3º No âmbito da E-Ciber, a proteção e a conscientização do cidadão e da sociedade têm por objetivo criar condições seguras para o uso dos serviços digitais, especialmente por pessoas em situação de vulnerabilidade, tais como:

I - crianças e adolescentes;

II - pessoas idosas; e

III - pessoas neurodivergentes.

Art. 4º A proteção e a conscientização do cidadão e da sociedade abrangem, no mínimo, as seguintes ações:

I - incentivo à atuação segura no ciberespaço;

II - incentivo à expansão de serviços de apoio às vítimas de ilícitos praticados no ciberespaço;

III - promoção da identificação e da autenticação de usuários, conforme a necessidade e observado o respeito à privacidade;

IV - incentivo à capacitação de professores e gestores, públicos e privados, em cibersegurança;

V - incentivo à inclusão de temas relacionados à cibersegurança nos currículos de todos os níveis educacionais;

VI - incentivo à participação em fóruns e atividades acadêmicas, técnicas e profissionais relacionadas à cibersegurança;

VII - incentivo às iniciativas de orientação a microempresas, empresas de pequeno porte e *startups* na gestão de riscos e na retomada das atividades pós-incidentes cibernéticos;

VIII - avaliação de modelos de planos de conformidade em cibersegurança flexíveis para implementação por pessoas jurídicas de direito público;

IX - incentivo ao desenvolvimento de planos de contingência institucionais e à realização de testes e simulações para verificação do nível de cibersegurança no órgão ou na entidade;

X - promoção da prevenção e do combate aos cibercrimes, às fraudes digitais e a outras ações maliciosas no ciberespaço por meio de atuação multissetorial;

XI - divulgação da Convenção sobre o Crime Cibernético, promulgada pelo Decreto nº 11.491, de 12 de abril de 2023, e de instrumentos congêneres, nacionais e internacionais, relacionados a cibercrimes vigentes no País;

XII - promoção de ações que aumentem a efetividade das operações contra o cibercrime;

XIII - estímulo ao aprimoramento normativo e estrutural dos canais para notificação de cibercrimes; e

XIV - incentivo à capacitação e ao aprimoramento dos órgãos de persecução penal na repressão aos cibercrimes.

Segurança e resiliência dos serviços essenciais e das infraestruturas críticas

Art. 5º No âmbito da E-Ciber, a segurança e a resiliência dos serviços essenciais e das infraestruturas críticas têm por objetivo fornecer à sociedade instrumentos efetivos para prevenção e resposta a ciberincidentes.

Art. 6º A segurança e a resiliência dos serviços essenciais e das infraestruturas críticas abrangem, no mínimo, as seguintes ações:

I - estímulo às entidades dotadas de competências regulatórias para promover a gestão de riscos e adotar medidas de proteção e resposta a ciberincidentes nos seus setores;

II - desenvolvimento de mecanismos de regulação, fiscalização e controle destinados a aprimorar a segurança, a resiliência e a continuidade dos serviços essenciais e das infraestruturas críticas, em especial quanto à adoção de ferramentas de tecnologia da informação e de tecnologia operacional;

III - adoção de mecanismos de alerta de risco na prestação de serviços digitais;

IV - desenvolvimento e manutenção de lista de alto risco de cibersegurança a ser utilizada como fundamentação para a gestão de ciber-riscos setoriais;

V - estímulo à adoção de padrões mínimos de segurança para categorias de dados relevantes e sensíveis;

VI - criação e manutenção de selo nacional de certificação de alto nível de segurança de ciberativos;

VII - estímulo à adoção de mecanismos de mitigação de riscos, como seguros contra ciberincidentes, por prestadores de serviços essenciais e operadores de infraestruturas críticas;

VIII - incentivo à realização de exercícios e simulações setoriais e multissetoriais regulares destinados ao aprimoramento da resiliência dos serviços essenciais e das infraestruturas críticas;

IX - incentivo ao aprimoramento contínuo dos atos normativos relacionados à cibersegurança, inclusive em relação a padrões mínimos de controle e guias;

X - estímulo ao aperfeiçoamento da segurança na interoperabilidade de dados e de canais digitais; e

XI - incentivo às empresas brasileiras na contratação de produtos e serviços que adotem padrões mínimos de cibersegurança.

Cooperação e integração entre órgãos e entidades, públicas e privadas

Art. 7º No âmbito da E-Ciber, a cooperação e a integração entre órgãos e entidades, públicas e privadas, têm por objetivo promover o debate e o intercâmbio de informações relacionadas à cibersegurança em âmbito nacional e internacional.

Art. 8º A cooperação e a integração entre órgãos e entidades, públicas e privadas, abrangem, no mínimo, as seguintes ações:

I - estímulo à criação e ao desenvolvimento de:

a) equipes de prevenção e resposta a incidentes de cibersegurança;

b) centros de análise e compartilhamento de informações; e

c) laboratórios especializados em cibersegurança;

II - incentivo à criação de mecanismo nacional de notificação de ciberincidentes;

III - incentivo à cooperação e à construção da confiança entre instituições acadêmicas e agências, nacionais e internacionais, no âmbito da cibersegurança, com vistas a:

a) desenvolver ações de cibersegurança e de ciberdefesa;

b) compartilhar informações e experiências para o fortalecimento da cibersegurança;

c) divulgar, de forma coordenada, as vulnerabilidades de cibersegurança; e

d) combater cibercrimes e outros ilícitos cometidos no ciberespaço;

IV - apoio ao fortalecimento da capacidade de cibersegurança dos países do entorno estratégico brasileiro, por iniciativa bilateral ou multilateral; e

V - incentivo à participação do País em organizações e fóruns internacionais que tratem de cibersegurança.

Soberania nacional e governança

Art. 9º No âmbito da E-Ciber, a soberania nacional e a governança têm por objetivo atender e proteger os interesses da sociedade brasileira no ciberespaço e garantir um ambiente cibernético confiável que assegure o crescimento econômico e tecnológico do País.

Art. 10. A soberania nacional e a governança abrangem, no mínimo, as seguintes ações:

I - atualização, divulgação e implementação da Política Nacional de Cibersegurança, de que trata o art. 4º do Decreto nº 11.856, de 26 de dezembro de 2023;

II - elaboração de modelo nacional de maturidade em cibersegurança, que permita:

a) aferir a evolução do setor de cibersegurança; e

b) orientar as alterações necessárias ao planejamento estratégico do País;

III - formação e capacitação técnico-profissional em cibersegurança em escala compatível com as necessidades nacionais;

IV - redução do débito tecnológico do País em tecnologias emergentes e disruptivas por meio de ações governamentais afirmativas e incrementais;

V - incentivo ao desenvolvimento de capacidade de avaliação continuada de conformidade em segurança de produtos, em serviços e em tecnologias de cibersegurança;

VI - estímulo ao uso de sistema para troca segura de informações no âmbito da cibersegurança;

VII - incentivo ao setor privado na oferta de produtos, serviços, tecnologias em cibersegurança, especialmente para microempresas, empresas de pequeno porte e *startups*;

VIII - estímulo ao estabelecimento de parcerias com institutos brasileiros de pesquisa e desenvolvimento para ampliar as residências tecnológicas em cibersegurança;

IX - incentivo à criação de linhas de pesquisa para graduação e pós-graduação *stricto sensu* e concessão de bolsas de estudo para a formação de especialistas e de professores brasileiros em cibersegurança; e

X - incentivo ao desenvolvimento de produtos, serviços e tecnologias nacionais destinados ao aprimoramento da cibersegurança no País.

Plano Nacional de Cibersegurança

Art. 11. O Plano Nacional de Cibersegurança será proposto pelo Comitê Nacional de Cibersegurança, nos termos do disposto no art. 6º, *caput*, inciso I, do Decreto nº 11.856, de 26 de dezembro de 2023, e submetido à aprovação do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República.

§ 1º O Plano Nacional de Cibersegurança conterá:

I - as iniciativas estratégicas específicas de forma discriminada;

II - o cronograma de execução; e

III - a governança das ações e das atividades estabelecidas neste Decreto.

§ 2º A publicação do ato de que trata o *caput* ficará condicionada à anuência dos órgãos e das entidades públicas, de que trata o art. 7º, *caput*, incisos I a XV, do Decreto nº 11.856, de 26 de dezembro de 2023, integrantes do Comitê Nacional de Cibersegurança.

Revogação e vigência

Art. 12. Fica revogado o Decreto nº 10.222, de 5 de fevereiro de 2020.

Art. 13. Este Decreto entra em vigor na data de sua publicação.

Brasília, 4 de agosto de 2025; 204º da Independência e 137º da República.

LUIZ INÁCIO LULA DA SILVA
Marcos Antonio Amaro dos Santos

*