CAPÍTULO III
DOS OBJETIVOS

Art. 4º São objetivos da Política Nacional de Segurança da Informação:

I - contribuir para a segurança da informação, observados os direitos e as garantias fundamentais, especialmente em relação:

a) à proteção de dados pessoais, observada a legislação específica;

b) à segurança dos dados custodiados por órgãos e entidades públicos federais e entidades privadas prestadoras de serviços públicos; e

c) à gestão e à proteção adequadas do conhecimento sensível e das informações com restrição de acesso;

II - salvaguardar as infraestruturas críticas e os serviços essenciais;

III - estimular a gestão de riscos, a proteção e o controle da informação;

IV - incentivar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação;

V - aprimorar continuamente o arcabouço normativo relacionado à segurança da informação;

VI - incentivar a qualificação dos recursos humanos necessários à segurança da informação, com a promoção da inclusão e da diversidade;

VII - fortalecer a cultura e a educação em segurança da informação na sociedade;

VIII - construir uma rede abrangente, colaborativa, sistêmica e interoperacional relacionada à segurança da informação; e

IX - desenvolver a cooperação internacional em segurança da informação.

CAPÍTULO IV
DA ESTRUTURA DE GOVERNANÇA

Art. 5º O Gabinete de Segurança Institucional da Presidência da República coordenará as ações do Governo federal relativas à segurança da informação.

Art. 6º O Gabinete de Segurança Institucional instituirá, no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, o Comitê Gestor da Segurança da Informação, com a finalidade de acompanhar a implementação e a evolução da Política Nacional de Segurança da Informação.

Parágrafo único. O Comitê Gestor da Segurança da Informação será composto pelos gestores de segurança da informação dos órgãos e das entidades da administração pública federal.

CAPÍTULO V
DOS INSTRUMENTOS

Art. 7º São instrumentos da Política Nacional de Segurança da Informação:

I - a Estratégia Nacional de Segurança da Informação;

II - o Plano Nacional de Segurança da Informação; e

III - os normativos sobre segurança da informação editados pelo Gabinete de Segurança Institucional.

CAPÍTULO VI
DAS COMPETÊNCIAS

Art. 8º Competem ao Gabinete de Segurança Institucional os seguintes temas relacionados à segurança da informação:

I - coordenar as atividades de segurança da informação e das comunicações, inclusive quanto à formulação de políticas públicas;

II - elaborar diretrizes, estratégias, planos, normativos, requisitos metodológicos e recomendações;

III - promover programas destinados à formação e à qualificação de recursos humanos;

IV - coordenar e realizar ações destinadas à promoção da cultura de segurança da informação;

V - acompanhar a evolução tecnológica e as melhores práticas, em âmbito nacional e internacional; e

VI - estimular a cooperação internacional, em coordenação com o Ministério das Relações Exteriores.

Art. 9º Compete ao Sistema de Controle Interno do Poder Executivo Federal auditar a execução das ações da Política Nacional de Segurança da Informação de responsabilidade dos órgãos e das entidades da administração pública federal.

Art. 10. Compete aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação:

I - implementar a Política Nacional de Segurança da Informação;

II - instituir comitê interno de segurança da informação ou estrutura equivalente;

III - designar o gestor de segurança da informação;

IV - elaborar, publicar, implementar e revisar regularmente suas políticas de segurança da informação e suas normas internas de segurança da informação, observados os normativos sobre segurança da informação editados pelo Gabinete de Segurança Institucional;

V - estimular ações de conscientização e de capacitação de pessoas que atuem nos órgãos e nas entidades da administração pública federal em temas relacionados à segurança da informação;

VI - realizar a avaliação de conformidade com as normas relativas à segurança da informação;

VII - aplicar as ações corretivas e administrativas cabíveis nos casos de violação de sua política de segurança da informação, nos termos do disposto neste Decreto e na legislação;

VIII - coordenar as atividades desenvolvidas pelo gestor de segurança da informação, pelo encarregado pelo tratamento de dados pessoais, pelo gestor de segurança e credenciamento e pelo titular da unidade de tecnologia da informação;

IX - assegurar a transmissão do conhecimento e das responsabilidades por ocasião da substituição do gestor de segurança da informação; e

X - planejar e destinar recursos orçamentários para ações de segurança da informação.

Parágrafo único. Ao órgão de que trata o inciso II do *caput* compete propor a elaboração e as revisões da política de segurança da informação e das normas internas de segurança da informação do seu órgão ou da sua entidade.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 11. O Ministro de Estado Chefe do Gabinete de Segurança Institucional poderá editar atos complementares necessários à aplicação do disposto neste Decreto.

Art. 12. Ficam revogados:

I - o Decreto nº 9.637, de 26 de dezembro de 2018;

II - o art. 1º do Decreto nº 9.832, de 12 de junho de 2019;

III - o Decreto nº 10.641, de 2 de março de 2021; e

IV - o Decreto nº 10.849, de 28 de outubro de 2021.

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

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,

D E C R E T A :

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;

PRESIDÊNCIA DA REPÚBLICA • CASA CIVIL • IMPRENSA NACIONAL

LUIZ INÁCIO LULA DA SILVA
Presidente da República

RUI COSTA DOS SANTOS
Ministro de Estado Chefe da Casa Civil

AFONSO OLIVEIRA DE ALMEIDA
Diretor-Geral da Imprensa Nacional

DIÁRIO OFICIAL DA UNIÃO
Em circulação desde 1º de outubro de 1862

LARISSA CANDIDA COSTA
Coordenadora-Geral de Publicação, Produção e Preservação

ALEXANDRE MIRANDA MACHADO
Coordenador de Publicação do Diário Oficial da União

SEÇÃO 1 • Publicação de atos normativos
SEÇÃO 2 • Publicação de atos relativos a pessoal da Administração Pública Federal
SEÇÃO 3 • Publicação de contratos, editais, avisos e ineditoriais

www.in.gov.br ouvidoria@in.gov.br
SIG, Quadra 6, Lote 800, CEP 70610-460, Brasília - DF
CNPJ: 04196645/0001-00 Fone: (61) 3411-9450

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

Presidência da República

DESPACHOS DO PRESIDENTE DA REPÚBLICA

MENSAGEM

Nº 1.052, de 4 de agosto de 2025. Restituição ao Congresso Nacional de autógrafo do projeto de lei que, sancionado, se transforma na Lei nº 15.184, de 4 de agosto de 2025.

Nº 1.053, de 4 de agosto de 2025. Restituição ao Congresso Nacional de autógrafo do projeto de lei que, sancionado, se transforma na Lei nº 15.185, de 4 de agosto de 2025.

Nº 1.054, de 4 de agosto de 2025. Restituição ao Congresso Nacional de autógrafo do projeto de lei que, sancionado, se transforma na Lei nº 15.186, de 4 de agosto de 2025.

Nº 1.055, de 4 de agosto de 2025. Restituição ao Congresso Nacional de autógrafo do projeto de lei que, sancionado, se transforma na Lei nº 15.187, de 4 de agosto de 2025.

CÂMARA DE COMÉRCIO EXTERIOR

CONSELHO ESTRATÉGICO

RESOLUÇÃO CEC Nº 11, DE 4 DE AGOSTO DE 2025

Autoriza o Ministério das Relações Exteriores a acionar o mecanismo de solução de controvérsias da Organização Mundial do Comércio acerca de medidas tarifárias impostas pelos Estados Unidos da América a produtos brasileiros.

O CONSELHO ESTRATÉGICO DA CÂMARA DE COMÉRCIO EXTERIOR, no uso da atribuição que lhe confere o art. 3º, inciso III, do Decreto nº 11.428, de 02 de março de 2023, tendo em vista a Ata Final que Incorpora os Resultados da Rodada Uruguai de Negociações Comerciais Multilaterais do GATT, assinada em Marraqueche, em 12 de abril de 1994, aprovada pelo Decreto Legislativo nº 30, de 15 de dezembro de 1994, promulgada pelo Decreto nº 1.355, de 30 de dezembro de 1994, e considerando Consulta Eletrônica CEC nº 02/2025, conforme previsto no o Art. 4º, X, do Anexo II da Resolução Gecex nº 480, de 10 de maio de 2023, alterada pela Resolução Gecex nº 510, de 16 de agosto de 2023, resolve:

Art. 1º Autoriza o Ministério das Relações Exteriores a acionar o mecanismo de solução de controvérsias da Organização Mundial do Comércio acerca de medidas tarifárias impostas pelos Estados Unidos da América a produtos brasileiros.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

GERALDO JOSÉ RODRIGUES ALCKMIN FILHO
Presidente do Conselho

CONSELHO DE GOVERNO

CÂMARA DE REGULAÇÃO DO MERCADO DE MEDICAMENTOS SECRETARIA EXECUTIVA

PORTARIA CMED Nº 3, DE 4 DE AGOSTO DE 2025.

Divulga a lista de apresentações de medicamentos que serão inativadas no SAMMED por não apresentarem dados de comercialização nos últimos 5 (cinco) semestres reportados à CMED.

A SECRETÁRIA-EXECUTIVA DA CÂMARA DE REGULAÇÃO DO MERCADO DE MEDICAMENTOS, no uso das competências que lhe conferem o art. 6º, inciso XII, da Lei nº 10.742, de 6 de outubro de 2003, c/c art. 7º, parágrafo único, inciso III, do Decreto nº 4.766, de 26 de julho de 2003, c/c art. 11, incisos IX e XI, do Anexo da Resolução CM-CMED nº 02, de 3 de junho de 2025 (Regimento Interno da CMED), c/c art. 1º da Resolução CMED nº 2, de 23 de fevereiro de 2015, em obediência ao disposto no art. 9º, inciso II, do Decreto nº 12.002, de 22 de abril de 2022, de acordo com deliberação do Comitê Técnico-Executivo da CMED na ocasião da 7ª Reunião Ordinária de 2025, realizada nos dias 31 de julho e 1º de agosto de 2025, e

Considerando que o Sistema de Acompanhamento de Mercado de Medicamentos (Sammed) tem por objetivo viabilizar a adoção, implementação e coordenação de atividades relativas à regulação econômica do mercado de medicamentos, voltadas a promover a assistência farmacêutica à população, por meio de mecanismos que estimulem a oferta de medicamentos e a competitividade do setor; e

Considerando que muitos medicamentos que constam atualmente na lista de preços da Câmara de Regulação do Mercado de Medicamentos (CMED) não apresentaram dados de comercialização nos últimos relatórios enviados, causando falsa impressão de concorrência no mercado e podendo dificultar os processos de compras públicas; resolve:

Art. 1º Fica divulgada, no sítio eletrônico da CMED, no Portal da ANVISA: https://www.gov.br/anvisa/pt-br/assuntos/medicamentos/cmed/legislacao/portarias, a lista de apresentações de medicamentos que serão inativadas no Sammed por não apresentarem dados de comercialização nos últimos 5 (cinco) semestres reportados à Secretaria-Executiva da CMED (2º semestre/2022, 2023 e 2024).

Art. 2º Para manter os preços de suas apresentações divulgados na Lista de Preços de Medicamentos da CMED, a empresa deverá comprovar comercialização durante o período ou apresentar justificava para a manutenção, em até 30 (trinta) dias a partir da vigência desta Portaria, por meio do Sistema de Acompanhamento do Mercado de Medicamentos (Sammed), através da opção "Solicitar alteração de empresa".

Art. 3º Uma vez inativada a apresentação no Sammed, a empresa que pretender voltar a comercializá-la deverá apresentar o competente Documento Informativo de Preço à CMED, nos termos da Resolução CMED nº 2, de 5 de março de 2004.

Art. 4º Esta Portaria entra em vigor no dia 1º de setembro de 2025.

DANIELA MARRECO CERQUEIRA