Diário Oficial
Imprensa Nacional

REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF

Nº 134 - DOU de 19/07/21 - Seção 1 - p. 2

DECRETO Nº 10.748, DE 16 DE JULHO DE 2021

Institui a Rede Federal de Gestão de Incidentes Cibernéticos.

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 :

CAPÍTULO I

DA REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

Art. 1º Fica instituída a Rede Federal de Gestão de Incidentes Cibernéticos, nos termos do disposto no inciso VII do **caput** do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018.

§ 1º A participação dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional na Rede Federal de Gestão de Incidentes Cibernéticos será obrigatória.

§ 2º A participação das empresas públicas e das sociedades de economia mista federais e das suas subsidiárias na Rede Federal de Gestão de Incidentes Cibernéticos será voluntária e ocorrerá por meio de adesão.

§ 3º A Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia participará da Rede Federal de Gestão de Incidentes Cibernéticos na condição de órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp do Poder Executivo federal.

Art. 2º A Rede Federal de Gestão de Incidentes Cibernéticos tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação.

Art. 3º São objetivos da Rede Federal de Gestão de Incidentes Cibernéticos:

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

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;

III - divulgar informações sobre ataques cibernéticos;

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

V - promover a celeridade na resposta a incidentes cibernéticos.

Art. 4º Para fins do disposto neste Decreto, considera-se:

I - equipe de prevenção, tratamento e resposta a incidentes cibernéticos - grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração

pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade;

II - equipe de coordenação setorial - equipe de prevenção, tratamento e resposta a incidentes cibernéticos das agências reguladoras, do Banco Central do Brasil ou da Comissão Nacional de Energia Nuclear ou das suas entidades reguladas responsáveis por coordenar as atividades de segurança cibernética e de centralizar as notificações de incidentes das demais equipes do setor regulado;

III - equipes principais - equipes de prevenção, tratamento e resposta a incidentes cibernéticos de entidades, públicas ou privadas, responsáveis por ativos de informação, em especial aqueles relativos a serviços essenciais, cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade, nos termos do disposto no inciso I do parágrafo único do art. 1º do Anexo ao Decreto nº 9.573, de 22 de novembro de 2018;

IV - áreas prioritárias - áreas definidas no Plano Nacional de Segurança de Infraestruturas Críticas para a aplicação da Política Nacional de Segurança de Infraestruturas Críticas, nos termos do disposto no inciso I do **caput** do art. 9º do Anexo ao Decreto nº 9.573, de 2018;

V - incidente cibernético - ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso;

VI - plano de gestão de incidentes cibernéticos para a administração pública federal - plano que orienta as equipes dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, exceto das agências reguladoras, do Banco Central do Brasil e da Comissão Nacional de Energia Nuclear, sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos; e

VII - planos setoriais de gestão de incidentes cibernéticos - planos que orientam as equipes nas agências reguladoras, no Banco Central do Brasil, na Comissão Nacional de Energia Nuclear ou nas suas entidades reguladas sobre a coordenação de atividades referentes à prevenção, ao tratamento e à resposta a incidentes cibernéticos inerentes ao setor específico.

CAPÍTULO II

DA COMPOSIÇÃO

Art. 5º A Rede Federal de Gestão de Incidentes Cibernéticos será composta pelo Gabinete de Segurança Institucional da Presidência da República, pelos órgãos e pelas entidades da administração pública federal direta, autárquica e fundacional e, observado o disposto nos § 2º do art. 1º, pelas empresas públicas e sociedades de economia mista e pelas suas subsidiárias que aderirem à Rede.

§ 1º O Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República coordenará a Rede Federal de Gestão de Incidentes Cibernéticos por meio do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

§ 2º Os órgãos e as entidades da administração pública federal direta, autárquica e fundacional atuarão na Rede Federal de Gestão de Incidentes Cibernéticos por meio das suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, nos termos do disposto nos inciso I a III do **caput** do art. 4º.

§ 3º Observado o interesse do Estado em relação à segurança cibernética nacional, outras entidades públicas ou privadas poderão ser convidadas pelo Gabinete de Segurança Institucional da Presidência da República para integrar a Rede Federal de Gestão de Incidentes Cibernéticos, por meio de ofício, desde que cumpridos os requisitos de que trata o art. 7º.

Art. 6º No âmbito do Ministério da Defesa e das Forças Singulares, a articulação com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo será feita prioritariamente por meio da equipe de coordenação setorial, operada pelo Comando de Defesa Cibernética, na condição de órgão central do Sistema Militar de Defesa Cibernética.

§ 1º Excepcionalmente, as equipes de prevenção, tratamento e resposta a incidentes cibernéticos do Ministério da Defesa e das Forças Singulares poderão articular-se diretamente com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, hipótese em que deverão informar a equipe de coordenação setorial do Ministério da Defesa.

§ 2º As informações compartilhadas pelas equipes de prevenção, tratamento e resposta a incidentes cibernéticos de que trata o § 1º com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo observarão as restrições legais de acesso a dados em razão das necessidades de segurança do Estado.

Art. 7º A adesão das entidades de que trata o § 2º do art. 1º será formalizada por ato do dirigente máximo do órgão da administração pública federal direta ao qual estejam vinculadas ou subordinadas.

§ 1º Quando da elaboração do ato de que trata o **caput**, o órgão da administração pública federal direta avaliará se há necessidade de dispor sobre requisitos adicionais às normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República em decorrência das atividades desenvolvidas pelas entidades de que trata o § 2º do art. 1º, principalmente quando essas atividades estiverem relacionadas com infraestrutura crítica.

§ 2º As entidades de que trata o § 2º do art. 1º que solicitarem a adesão à Rede Federal de Gestão de Incidentes Cibernéticos deverão cumprir os seguintes requisitos para serem aprovadas pelo Gabinete de Segurança Institucional da Presidência da República:

I - possuir equipe de prevenção, tratamento e resposta a incidentes cibernéticos implementada de acordo com as normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República; e

II - encaminhar ao Gabinete de Segurança Institucional da Presidência da República, por meio de sua equipe de prevenção, tratamento e resposta a incidentes cibernéticos ou de sua equipe de coordenação setorial, termo de adesão à Rede Federal de Gestão de Incidentes Cibernéticos assinado pelo dirigente máximo ou representante legal.

§ 3º A adesão à Rede Federal de Gestão de Incidentes Cibernéticos dependerá da aprovação formal pelo Gabinete de Segurança Institucional da Presidência da República, que poderá recusá-la motivadamente, mesmo que tenham sido cumpridos os requisitos estabelecidos neste artigo.

§ 4º O disposto neste artigo se aplica, no que couber, a outras pessoas jurídicas de direito privado e às pessoas jurídicas de direito público interno de outros Poderes e entes federativos que forem convidadas pelo Gabinete de Segurança Institucional da Presidência da República para integrar a Rede Federal de Gestão de Incidentes Cibernéticos.

§ 5º A colaboração espontânea, caso a caso, das entidades de que trata o § 2º do art. 1º com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo ou com quaisquer de seus integrantes independerá da adesão à Rede Federal de Gestão de Incidentes Cibernéticos.

Art. 8º As pessoas jurídicas que não pertencerem à administração pública federal direta, autárquica e fundacional e que tiverem firmado termo de adesão com o Gabinete de Segurança Institucional da Presidência da República para integrar a Rede Federal de Gestão de Incidentes Cibernéticos deverão reportar-se à equipe de coordenação setorial à qual estiverem vinculadas ou, na sua inexistência, diretamente ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, nas hipóteses de:

I - incidente cibernético que extrapole a sua capacidade de saná-lo; e

II - vulnerabilidade em ativos de informação que a sua equipe de prevenção, tratamento e resposta a incidentes cibernéticos julgue que possa causar incidente cibernético, tanto em sua rede computacional quanto na de outras entidades.

Art. 9º A saída da pessoa jurídica de que trata o § 4º do art. 7º da Rede Federal de Gestão de Incidentes Cibernéticos ocorrerá:

I - a pedido de seu dirigente máximo; ou

II - por decisão do Gabinete de Segurança Institucional da Presidência da República, na hipótese de:

a) descumprimento dos requisitos de que trata o art. 7º;

b) descumprimento do disposto no plano setorial de gestão de incidentes cibernéticos; ou

c) conveniência administrativa.

CAPÍTULO III

DAS COMPETÊNCIAS

Art. 10. Compete ao Gabinete de Segurança Institucional da Presidência da República:

I - coordenar a Rede Federal de Gestão de Incidentes Cibernéticos; e

II - convocar reunião da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo para deliberar sobre ocorrência de incidente cibernético grave ou quando identificar risco cibernético elevado, nos termos do disposto no Decreto nº 9.819, de 3 de junho de 2019.

Art. 11. Compete ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, por meio do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo:

I - coordenar as atividades das equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos integrantes da Rede Federal de Gestão de Incidentes Cibernéticos relativas à prevenção, ao tratamento e à resposta aos incidentes cibernéticos;

II - articular-se, por meio de plataforma computacional dedicada, com as equipes de prevenção, tratamento e resposta a incidentes cibernéticos de que trata o inciso I, para coordená-las;

III - elaborar, atualizar e divulgar o plano de gestão de incidentes cibernéticos para os órgãos e as entidades da administração pública federal direta, autárquica e fundacional;

IV - articular-se com órgãos ou unidades correlatos de outros países;

V - buscar a cooperação internacional, com ênfase no compartilhamento de informações sobre ameaças, vulnerabilidade e incidentes cibernéticos;

VI - difundir alertas, recomendações e estatísticas sobre incidentes cibernéticos para os integrantes da Rede Federal de Gestão de Incidentes Cibernéticos; e

VII - manter atualizado o sítio eletrônico do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo com alertas, recomendações e estatísticas sobre incidentes cibernéticos, ressalvado o disposto no art. 15.

Art. 12. Compete aos órgãos e às entidades da administração pública federal direta, autárquica e fundacional:

I - instituir e implementar as suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, nos termos do disposto no inciso VII do **caput** do art. 15 do Decreto nº 9.637, de 2018, e nas normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República;

II - apoiar as atividades de suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos e as ações de segurança da informação, nos termos do disposto no art. 15 do Decreto nº 9.637, de 2018;

III - identificar as equipes principais das áreas prioritárias sob a sua responsabilidade, nos termos do disposto nos incisos III e IV do **caput** do art. 4º;

IV - comunicar imediatamente o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, por meio de suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, sobre a existência de

vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados, nos termos do disposto no art. 17 do Decreto nº 9.637, de 2018;

V - requerer diretamente às equipes principais identificadas, ou por meio da equipe de coordenação setorial, quando instituída, as notificações sobre os incidentes cibernéticos de maior impacto;

VI - notificar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, diretamente ou por meio da equipe de coordenação setorial, quando instituída, quanto aos incidentes cibernéticos de maior impacto, com base nas informações obtidas das equipes de prevenção, tratamento e resposta a incidentes cibernéticos das entidades sob a sua gestão;

VII - promover ações de capacitação e profissionalização de suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, nos termos do disposto no art. 15 do Decreto nº 9.637, de 2018;

VIII - manter atualizada a infraestrutura utilizada por suas equipes de prevenção, de tratamento e de resposta a incidentes cibernéticos; e

IX - sanar, com urgência, as vulnerabilidades cibernéticas, em especial aquelas identificadas nos alertas e nas recomendações expedidos pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

§ 1º Os incidentes cibernéticos de maior impacto a que se referem os incisos V e VI do **caput** serão estabelecidos com base na classificação de severidade que consta do processo de gestão de riscos de segurança da informação do órgão ou da entidade.

§ 2º O disposto neste artigo também se aplica às agências reguladoras, ao Banco Central do Brasil e à Comissão Nacional de Energia Nuclear.

Art. 13. Compete às agências reguladoras, ao Banco Central do Brasil e à Comissão Nacional de Energia Nuclear:

I - instituir ou designar equipe de coordenação setorial, nos termos do disposto no inciso II do **caput** do art. 4º;

II - apoiar as atividades de suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos, nos termos do disposto no Decreto nº 9.637, de 2018;

III - identificar as equipes principais das áreas prioritárias sob a sua regulação, nos termos do disposto no inciso III e IV do **caput** do art. 4º;

IV - requerer às equipes principais identificadas, por meio da equipe de coordenação setorial, as notificações sobre os incidentes cibernéticos de maior impacto;

V - notificar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, por meio da equipe de coordenação setorial, quanto aos incidentes cibernéticos de maior impacto, com base nas informações obtidas das equipes de prevenção, tratamento e resposta a incidentes cibernéticos das entidades sob a sua regulação;

VI - analisar os riscos cibernéticos que deverão constar do plano setorial de gestão de incidentes cibernéticos específico;

VII - estabelecer a sua forma de articulação com a equipe de coordenação setorial;

VIII - identificar outras entidades, públicas ou privadas, relevantes para a segurança cibernética em sua área prioritária;

IX - fornecer informações relativas às equipes de prevenção, tratamento e resposta a incidentes cibernéticos das entidades de que trata o inciso VIII, que deverão constar do plano setorial de gestão de incidentes cibernéticos; e

X - identificar as infraestruturas críticas de suas áreas prioritárias que requeiram atenção em termos de segurança cibernética nacional.

§ 1º Os incidentes cibernéticos de maior impacto a que se referem os incisos IV e V do **caput** serão estabelecidos com base na classificação de severidade que consta do processo de gestão de riscos de segurança da informação do órgão ou da entidade.

§ 2º O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo divulgará os elementos básicos e a periodicidade de atualização do plano setorial de gestão de incidentes cibernéticos a que se referem os incisos VI e IX do **caput** em seu sítio eletrônico.

§ 3º O disposto neste artigo aplica-se também a outros órgãos e entidades da administração pública federal direta, autárquica e fundacional com competência de regulação em área prioritária que venha a ser estabelecida no Plano Nacional de Segurança de Infraestruturas Críticas, no prazo de até dezoito meses, contado da data de notificação pelo Gabinete de Segurança Institucional da Presidência da República, para que o órgão ou a entidade implemente as ações necessárias.

Art. 14. Compete às equipes de coordenação setorial:

I - elaborar o plano setorial de gestão de incidentes cibernéticos de que trata o inciso VI do **caput** do art. 13; e

II - coordenar as atividades e centralizar as notificações de incidentes recebidas das demais equipes de prevenção, tratamento e resposta a incidentes cibernéticos das entidades sob a sua coordenação.

Parágrafo único. Compete, ainda, às equipes de coordenação setorial obedecer ao disposto nas normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República que dispõem sobre equipes de prevenção, tratamento e resposta a incidentes cibernéticos.

CAPÍTULO IV

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 15. As informações específicas sobre os incidentes cibernéticos e sobre as configurações e características técnicas de ativos de informação de cada órgão ou entidade da administração pública federal direta, autárquica e fundacional são consideradas imprescindíveis à segurança da sociedade e do Estado.

§ 1º As informações de que trata o **caput** somente poderão ser acessadas por profissionais autorizados pelas autoridades responsáveis pelos ativos de informação dos órgãos ou das entidades da administração pública federal direta, autárquica e fundacional.

§ 2º O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo divulgará em seu sítio eletrônico estatísticas gerais de interesse público relacionadas aos incidentes cibernéticos ocorridos nos órgãos e nas entidades da administração pública federal direta, autárquica e fundacional.

Art. 16. As ações previstas para o funcionamento da Rede Federal de Gestão de Incidentes Cibernéticos a cargo dos órgãos e das entidades de que trata o art. 13 que incluam a instituição ou a designação das equipes de coordenação setorial deverão ser implementadas no prazo de dezoito meses, contado da data de publicação deste Decreto.

Art. 17. Os órgãos e as entidades da administração pública federal direta, autárquica e fundacional de que trata o § 1º do art. 1º deverão implementar as ações previstas para o funcionamento da Rede Federal de Gestão de Incidentes Cibernéticos no prazo de um ano, contado da data de publicação deste Decreto.

Art. 18. Este Decreto entra em vigor na data de sua publicação.

Brasília, 16 de julho de 2021; 200º da Independência e 133º da República.

JAIR MESSIAS BOLSONARO

Augusto Heleno Ribeiro Pereira