ANEXO

PLANO NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

1. INTRODUÇÃO

Para implementar a atividade de Segurança de Infraestruturas Críticas no País, foi aprovada a Política Nacional de Segurança de Infraestruturas Críticas por meio do Decreto nº 9.573, de 22 de novembro de 2018. Essa Política tem como finalidade garantir a segurança e a resiliência das Infraestruturas Críticas e a continuidade da prestação de seus serviços.

Nesse sentido, foi aprovada a Estratégia Nacional de Segurança de Infraestruturas Críticas por meio do Decreto nº 10.569, de 9 de dezembro de 2020, como documento orientador, que organiza os objetivos e iniciativas estratégicas em eixos estruturantes, retrata o foco estratégico para direcionar os esforços e sinaliza os resultados a serem alcançados. Todas essas informações serviram de orientação estratégica e de referência para a formulação de outro instrumento da Política Nacional de Segurança de Infraestruturas Críticas, o Plano Nacional de Segurança de Infraestruturas Críticas, conforme estabelecido no art. 7º do Anexo ao Decreto nº 9.573, de 2018.

Vale ressaltar que a gestão de riscos é componente fundamental para a atividade de Segurança de Infraestruturas Críticas, incluída a fixação de método lógico e sistemático para estabelecer os contextos e identificar, avaliar e tratar os riscos, a fim de atender a critérios e requisitos necessários à continuidade das operações.

A abordagem deve ser a mais abrangente possível e levar em consideração falhas em geral e ameaças de toda ordem, provenientes de ação humana, de catástrofes ou de desastres naturais. Dessa forma, garante-se que a sinergia entre as medidas de proteção seja explorada ao máximo. Já a avaliação das vulnerabilidades permite sugerir opções para eliminar ou reduzir as fraquezas das Infraestruturas Críticas e torná-las mais resistentes às ameaças.

Por outro lado, os esforços despendidos na proteção das Infraestruturas Críticas não podem ser vistos como garantia de segurança plena. Instalações, bens, serviços ou sistemas podem ser acometidos por situação de crise, momento em que entrarão em cena as medidas de mitigação e contingência, com vistas a incrementar a resiliência da infraestrutura e assegurar o seu retorno à normalidade dentro de padrões de tempo adequados à respectiva criticidade.

A correta equação entre as duas situações é a chave para o êxito da atividade de Segurança de Infraestruturas Críticas e proporcionará valiosos subsídios para o emprego judicioso dos recursos existentes.

2. SISTEMA INTEGRADO DE DADOS DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

A gestão de riscos voltada para a Segurança de Infraestruturas Críticas requer organização e coordenação efetiva das lideranças. O emprego de solução automatizada na gestão de riscos e de continuidade dos negócios é primordial para esse desafio, haja vista a quantidade de informações que é produzida, a necessidade de monitoramento constante sobre o nível de ameaça e de vulnerabilidade identificados nas diversas infraestruturas e, em

situação de crise, o acompanhamento tempestivo que possibilite à autoridade adotar a decisão mais adequada para aquele momento.

Assim, o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas será a estrutura operacional que irá subsidiar o acompanhamento e monitoramento permanente da Segurança das Infraestruturas Críticas do País, identificadas nos diversos setores. Como órgão articulador da atividade de Segurança de Infraestruturas Críticas, o Gabinete de Segurança Institucional da Presidência da República orientará o desenvolvimento e a implantação desse Sistema, que incluirá, entre outras, as seguintes ferramentas:

I - metodologias para identificar as Infraestruturas Críticas;

II - iniciativas para compartilhar informações e fornecer dados sobre alertas de riscos; e

III - análise de riscos e da interdependência das Infraestruturas Críticas.

Informações provenientes de proprietários ou operadores das Infraestruturas Críticas monitoradas serão inseridas nesse Sistema, que repercutirá sobre um repertório de dados já cadastrados, relacionados às ameaças e vulnerabilidades daquelas infraestruturas.

O modelo de parceria e os mecanismos de compartilhamento de informações do Sistema Integrado de Dados de Segurança de Infraestruturas Críticas serão estruturados de forma a dar suporte à cooperação e colaboração entre os setores público e privado. Nesse sentido, haverá a necessidade de proteção das informações sensíveis e do estabelecimento de protocolos seguros de compartilhamento de informações, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação, no Decreto nº 9.637, de 26 de dezembro de 2018, e em legislações decorrentes.

3. INTERDEPENDÊNCIA

O trabalho de identificação das Infraestruturas Críticas e a análise de riscos fornecem insumos para o estudo da relação de dependência ou interferência de uma infraestrutura crítica em outra, ou de uma área prioritária de Infraestruturas Críticas em outra. A interrupção total ou parcial de uma infraestrutura crítica, além de comprometer o funcionamento do setor a que pertence, pode acarretar impactos em cascata às Infraestruturas Críticas de outros setores.

O estudo da interdependência e o levantamento dos possíveis efeitos em cascata no caso de falhas são fundamentais para o planejamento da atividade de Segurança de Infraestruturas Críticas. Identificar, entender e analisar a interdependência constitui etapa essencial para o tratamento dessa questão, proporcional à amplitude e à diversidade das Infraestruturas Críticas do País.

O intercâmbio de informações entre Infraestruturas Críticas de uma mesma área prioritária e de áreas diferentes é fundamental para o estudo da interdependência. Isso facilitará o entendimento mútuo e levará a uma análise mais precisa na busca da redução de riscos e de solução das questões ligadas à temática.

Serão procuradas soluções inovadoras, redundâncias e planos alternativos para aprimorar a resiliência das Infraestruturas Críticas, com vistas à redução da dependência entre elas. Dessa forma, Infraestruturas Críticas que dependam, por exemplo, do fornecimento de energia elétrica, contarão com alternativas que lhes permitirão funcionar caso seu fornecedor principal deixe de operar.

Para a análise das interdependências, o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas será o instrumento que viabilizará a geração, a medição e a quantificação do conhecimento, que possibilitará a recomendação de ações e criará um banco de dados e um mapeamento da interdependência entre as Infraestruturas Críticas do País.

4. ATRIBUIÇÃO DE RESPONSABILIDADES

A ocorrência de incidentes que envolvam Infraestruturas Críticas, com as consequências que eles acarretam, como, por exemplo, a interrupção do fornecimento de água e energia elétrica, serviços básicos para a população, é assunto que cada vez mais se destaca dentro do Governo e da sociedade. É consciência comum a necessidade do desenvolvimento de ações na área de Segurança de Infraestruturas Críticas, implementadas de forma integrada e participativa.

Para a governança das atividades de Segurança de Infraestruturas Críticas no âmbito da administração pública federal e com vistas a atender ao objetivo estratégico da Estratégia Nacional de Segurança de Infraestruturas Críticas de estabelecer uma estrutura de governança, será criado o Comitê Gestor de Segurança de Infraestruturas Críticas. Esse Comitê Gestor será composto por um conjunto de órgãos responsáveis por articular, orientar, propor e gerir a implementação de ações relacionadas à Segurança das Infraestruturas Críticas, o qual buscará, inclusive, assegurar o cumprimento das metas estabelecidas neste Plano. Assim, o planejamento integrado, a ação conjunta e a execução continuada de providências que visem a atender a segurança e resiliência das Infraestruturas Críticas brasileiras farão parte de suas atividades.

Entre as responsabilidades a serem atribuídas ao referido Comitê Gestor, está a de estabelecer uma rede de comunicação e difusão de informações relacionadas à temática, o que será normatizado no decreto de sua criação. Essa rede será integrada por representantes designados como pontos focais pelas instituições convidadas, para a facilitação no atingimento dos objetivos propostos na legislação referente à Segurança das Infraestruturas Críticas, principalmente daqueles voltados à conscientização sobre a relevância do tema.

Ressalta-se que, entre os pressupostos identificados para a implementação da Segurança das Infraestruturas Críticas, destacam-se a obediência à Constituição e ao ordenamento jurídico pátrio e a caracterização da atividade como um esforço conjunto do Estado, da sociedade e do cidadão. A partir dessa base, para a execução dessa tarefa, ficam definidas as seguintes atribuições:

I - Gabinete de Segurança Institucional da Presidência da República:

a) realizar o acompanhamento de assuntos pertinentes às Infraestruturas Críticas, com prioridade aos que se refiram à avaliação de riscos;

b) implementar e gerir o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas;

c) promover a cooperação com órgãos e entidades nacionais e internacionais nas atividades voltadas para a Segurança das Infraestruturas Críticas;

d) articular e cooperar com os órgãos e entidades públicos e privados no levantamento das Infraestruturas Críticas;

e) coordenar os grupos técnicos de segurança de Infraestruturas Críticas;

f) realizar visitas técnicas para acompanhar a atividade de Segurança das Infraestruturas Críticas; e

g) integrar grupo de gerenciamento de crise para tratamento de eventos relevantes ocorridos com Infraestruturas Críticas;

II - Ministérios responsáveis pelas áreas prioritárias:

a) elaborar, em cooperação com órgãos e entidades dos setores público e privado, os planos setoriais de segurança de infraestruturas críticas, conforme a tabela a seguir; e

b) implementar as ações estratégicas de sua responsabilidade, elencadas neste Plano, sob pena de responsabilização junto aos órgãos de fiscalização e controle, internos e externos;

sobre o nível de criticidade e de vulnerabilidade identificadas nas diversas infraestruturas e, em

DISTRIBUIÇÃO DAS RESPONSABILIDADES ENTRE OS MINISTÉRIOS PARA A ELABORAÇÃO DOS PLANOS SETORIAIS DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

ÁREA PRIORITÁRIA	SETOR	MINISTÉRIO RESPONSÁVEL*
Águas	Barragens	Ministério do Desenvolvimento Regional
	Abastecimento Urbano de Águas	
Energia	Energia Elétrica	Ministério de Minas e Energia
	Peganbio**	
Transporte	Terrestre	Ministério da Infraestrutura
	Aéreo	
	Aquaviário	
Comunicações	Telecomunicações	Ministério das Comunicações
	Radiodifusão	
	Serviços Postais	
Finanças	Finanças	Ministério da Economia
Biossegurança e Bioproteção	Biossegurança e Bioproteção	Ministério da Saúde
Defesa	Defesa	Ministério da Defesa

* Considerada a existência de Infraestruturas Críticas aderentes a outros Ministérios, senão os definidos como responsáveis pelas respectivas áreas prioritárias, o Ministério responsável ficará encarregado pela articulação necessária ao cumprimento do previsto neste Plano, em coordenação com o Comitê Gestor de Segurança de Infraestruturas Críticas.

** Petróleo, Gás Natural e Biocombustíveis.

III - Agência Brasileira de Inteligência:

a) cooperar na proteção de Infraestruturas Críticas nacionais; e

b) monitorar e realizar o enfrentamento eficaz de ações adversas contra interesses nacionais, conforme estabelecido pela Política Nacional de Inteligência e pela Estratégia Nacional de Inteligência; e

IV - demais órgãos e entidades do setor público federal:

a) participar dos trabalhos desenvolvidos nas três esferas de governo; e

b) cooperar no planejamento e execução da atividade de Segurança de Infraestruturas Críticas.

Ademais, será buscada a colaboração dos Governos estaduais, distrital e municipais no que diz respeito à cooperação com os órgãos da administração pública federal no planejamento e na execução da atividade de Segurança de Infraestruturas Críticas, no desenvolvimento e implementação de programas voltados para a Segurança de Infraestruturas Críticas nas respectivas áreas de atuação, além da elaboração de planos correspondentes.

Incentivará, também, o envolvimento de entidades do setor privado em trabalhos desenvolvidos nas três esferas de governo, e cooperará no planejamento e na execução da atividade de Segurança de Infraestruturas Críticas.

O meio universitário e os centros de pesquisa poderão contribuir para o aprimoramento da Segurança de Infraestruturas Críticas do País, especialmente por meio de iniciativas que priorizem a pesquisa e o desenvolvimento de novos métodos de controle, da avaliação do nível de segurança alcançado em cada setor, da realização de análises independentes que permitam subsidiar a atualização dos planejamentos governamentais e da implementação de programas de capacitação de recursos humanos.

As federações, confederações, conselhos, associações, entidades congêneres e os cidadãos poderão apoiar a atividade de Segurança de Infraestruturas Críticas, apresentar sugestões e recomendações e disponibilizar às três esferas de governo a sua experiência no tema.

Ressalta-se que algumas Infraestruturas Críticas, como oleodutos, gasodutos e cabos submarinos, extrapolam as fronteiras dos países. Esse fato reforça a importância da cooperação internacional para a gestão de segurança, que deve contemplar o estabelecimento de parcerias permanentes e dinâmicas entre proprietários e operadores de Infraestruturas Críticas e Governos dos países envolvidos.

5. PLANOS SETORIAIS

Observadas as diretrizes constantes da Estratégia Nacional de Segurança de Infraestruturas Críticas, os planos setoriais serão elaborados e desenvolvidos sob coordenação dos Ministérios diretamente relacionados com as áreas prioritárias e respectivos setores, em colaboração com órgãos e entidades públicos e privados, incluídos os parceiros estaduais, distritais e municipais detentores de conhecimento na proteção de Infraestruturas Críticas.

Tanto a implementação do Plansic quanto a dos planos setoriais contarão com o apoio do Ministério da Defesa, na forma estabelecida pela Estratégia Nacional de Defesa, que relaciona, entre as ações estratégicas que visam a contribuir para o incremento do nível de segurança nacional, as medidas para a Segurança de Infraestruturas Críticas.

Os planos setoriais serão documentos complementares ao Plansic e tratarão especificamente das ações de Segurança de Infraestruturas Críticas relativas a cada setor, de acordo com suas especificidades, e orientarão sobre os níveis desejáveis de proteção, sobre as atividades de segurança a serem executadas e sobre a priorização na alocação de recursos. Os planos setoriais deverão, no mínimo:

I - estabelecer objetivos e metas para que sejam atingidos níveis de proteção adequados para o setor;

II - definir os parceiros do setor, as autoridades envolvidas, a legislação que ampara o plano setorial e as atribuições e responsabilidades dos diversos atores;

III - estabelecer ou relacionar procedimentos para a interação setorial, compartilhamento de informações, coordenação de esforços e parcerias;

IV - identificar a abordagem ou metodologia setorial específica utilizada pelo Ministério, em coordenação com o Gabinete de Segurança Institucional da Presidência da República e outros parceiros, para conduzir as atividades de Segurança de Infraestruturas Críticas;

V - estabelecer a criação, por parte das agências reguladoras, de planos específicos de coordenação e cooperação nas medidas relacionadas às Infraestruturas Críticas, incluída a resposta a incidentes;

VI - prever a capacitação de servidores em gestão de riscos, de crises e de continuidade de negócios, de gestão e de serviços; e

VII - estar alinhados com o disposto na Estratégia Nacional de Segurança Cibernética, no Decreto nº 10.748, de 16 de julho de 2021, e nas legislações correlatas.

6. PLANOS ESTADUAIS, DO DISTRITO FEDERAL E MUNICIPAIS

Será incentivada a elaboração de estratégias e planos de Segurança de Infraestruturas Críticas pelos Governos estaduais, distrital e municipais, os quais poderão abordar a proteção das Infraestruturas Críticas nas respectivas áreas de atuação, com ênfase na conjugação dos esforços desenvolvidos por órgãos e entidades regionais dos setores público e privado. A implementação será feita de forma coordenada e integrada com a ação do Governo federal, sobretudo para facilitar o gerenciamento de riscos no âmbito do Plansic.

Orienta-se que planos estaduais, distrital e municipais incluam ações que são básicas da atividade de Segurança de Infraestruturas Críticas, como:

I - estabelecer metas e objetivos;

II - identificar instalações físicas, serviços, bens, sistemas e redes críticos;

III - avaliar riscos;

IV - estabelecer prioridades;

V - implementar programas de segurança e estratégias de resiliência;

VI - mensurar a eficácia dos esforços de gerenciamento de riscos; e

VII - compartilhar informações entre os parceiros dos setores público e privado.

A atuação integrada das três esferas de governo é essencial para a implementação do Plansic e dos planos setoriais e contribuirá decisivamente para a segurança das Infraestruturas Críticas do País. É importante que os Estados, o Distrito Federal e os Municípios elaborem seus planos de Segurança de Infraestruturas Críticas de forma a adotar estrutura similar à do Plansic, com diretrizes gerais e planos específicos correspondentes às áreas de energia, transportes, comunicações, águas, finanças e biossegurança e bioproteção.

7. OUTROS PLANOS OU PROGRAMAS RELACIONADOS À SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

Os proprietários e operadores de Infraestruturas Críticas do setor privado, por iniciativa própria ou em decorrência de regulamentações, desenvolvem e mantêm planos de gerenciamento de risco empresarial que incluem a proteção regular das instalações, a continuidade de negócios e planos emergenciais de gerenciamento. As ações levadas a efeito no âmbito dos negócios são relevantes para a efetiva implementação do Plansic.

Os parceiros do setor privado são convidados a participar do esforço conjunto do Estado e da sociedade, o que contribui para tornar seguras as Infraestruturas Críticas do País. A revisão de planos e programas buscará o alinhamento com o trabalho de Segurança de Infraestruturas Críticas desenvolvido pelos parceiros governamentais de todas as três esferas de governo.

8. GERENCIAMENTO DA SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DO PAÍS

O monitoramento sobre o funcionamento regular das Infraestruturas Críticas, os relatórios expedidos pelo Sistema Integrado de Dados de Segurança de Infraestruturas Críticas e o acompanhamento sistêmico de atos e fatos da vida nacional são instrumentos que constituem o elo entre as operações regulares de gerenciamento de riscos da Segurança de Infraestruturas Críticas e as atividades de gerenciamento de crises ou de incidentes. A análise pormenorizada do ambiente de ameaça, em face das ações de proteção estabelecidas nos planejamentos de Segurança de Infraestruturas Críticas, pode fornecer indicadores que recomendem a transição de um processo regular de segurança para um processo de gerenciamento de crise.

Os processos de integração e transição entre as atividades de Segurança de Infraestruturas Críticas e o gerenciamento de crises requererão, entre outras, as seguintes ações dos órgãos e entidades que atuam na Segurança de Infraestruturas Críticas:

I - acompanhar e avaliar continuamente a situação das Infraestruturas Críticas;

II - implementar, quando for necessário, medidas de proteção;

III - intercambiar informações que auxiliem no gerenciamento de crises;

IV - manter canais de comunicação permanentes com os parceiros; e

V - expedir alertas oportunos.

Independentemente do grau da ameaça, propõe-se que os responsáveis pelas Infraestruturas Críticas se mantenham vigilantes, preparados e prontos para deter, eliminar ou reduzir riscos que se materializem. Para tanto, são necessárias análises do grau de ameaça em intervalos regulares, a fim de verificar a necessidade de ajustes na proteção. O desenvolvimento das medidas de segurança e de planos de contingência e continuidade de negócios é de responsabilidade dos proprietários e operadores das Infraestruturas Críticas.

O monitoramento constante das ameaças, por meio de ações da Inteligência de Estado, pode indicar eventuais necessidades de ajustes nos sistemas de proteção das Infraestruturas Críticas nacionais. Para tanto, o Gabinete de Segurança Institucional da Presidência da República possui em sua estrutura a Agência Brasileira de Inteligência, criada pela Lei nº 9.883, de 7 de dezembro de 1999. De acordo com o disposto no inciso III do caput do art. 4º da referida Lei, uma das competências da referida Agência é "avaliar as ameaças, internas e externas, à ordem constitucional", o que inclui ameaças à segurança das Infraestruturas Críticas nacionais, muitas delas elencadas na Política Nacional de Inteligência, nos termos do disposto no Decreto nº 8.793, de 29 de junho de 2016.

O estabelecimento de um processo de avaliação das medidas implementadas pelos órgãos e entidades responsáveis tem a finalidade de instituir mecanismos que possibilitem a mensuração do nível de segurança das Infraestruturas Críticas do País. Por sua vez, os mecanismos de acompanhamento dessas medidas visam a possibilitar que a Segurança de Infraestruturas Críticas efetivamente funcione conforme planejado, assegurada a prestação de serviços indispensáveis ao Estado e à sociedade brasileira.

A adoção de sistemas de avaliação e de acompanhamento, com ênfase para o caráter preventivo das medidas de segurança, considerará o aumento da capacidade de resiliência das respectivas Infraestruturas Críticas e contribuirá para o pronto restabelecimento dos serviços quando afetados. Esses sistemas, consideradas as peculiaridades de cada setor, poderão incluir mecanismos de aplicação simples e imediata, como listas de verificação, questionários, planilhas, relatórios, comunicados e mensagens.

Nesse contexto, convém registrar que o ambiente cibernético é palco de ameaças que ganham gradativamente mais relevância nas organizações. A intersecção entre essa temática e a de Segurança das Infraestruturas Críticas torna importante o gerenciamento integrado da aplicação das legislações referentes aos dois temas.

Assim, propõe-se que cada setor estabeleça critérios específicos, em razão das peculiaridades inerentes às respectivas Infraestruturas Críticas. Entretanto, sugere-se a adoção de algumas diretrizes gerais para a avaliação e o acompanhamento das medidas de Segurança de Infraestruturas Críticas:

8.1. Avaliação

Os processos de avaliação estarão voltados para aperfeiçoar as medidas adotadas e aumentar o nível de segurança, com prioridade para a prevenção. A avaliação poderá estabelecer recomendações, especialmente as relacionadas aos aspectos que podem resultar em impactos sociais, ambientais, econômicos, políticos, internacionais ou à segurança do Estado e da sociedade brasileira.

Como parte integrante da avaliação, poderão ser realizadas atividades de treinamento, exercícios e simulações, com vistas a contribuir para a capacitação de recursos humanos e para o permanente aprimoramento das atividades de Segurança de Infraestruturas Críticas. Essas ações poderão ser conjugadas com programas educacionais a serem contemplados nos planos setoriais. Cada setor poderá planejar e executar um programa anual de treinamento, com o propósito de avaliar os procedimentos específicos.

A interdependência é aspecto de suma importância a ser examinado, diante da relevância da relação de dependência ou interferência de uma infraestrutura crítica em outra, ou de sua área em outra.

8.2. Acompanhamento

As revisões sistemáticas destinam-se a atualizar o planejamento das atividades de Segurança de Infraestruturas Críticas, como parte do esforço conjunto do Estado, sociedade e cidadão e serão realizadas a cada dois anos, com base no relatório de acompanhamento de metas deste Plano, produzido pelo Comitê Gestor de Segurança de Infraestruturas Críticas.

A realização de visitas às Infraestruturas Críticas, por parte do Gabinete de Segurança Institucional da Presidência da República ou dos Ministérios das áreas prioritárias, é um instrumento valioso e eficaz para o acompanhamento da correta aplicação das medidas de segurança, uma vez que viabiliza melhor intercâmbio de informações e cooperação entre as diversas instituições envolvidas. No planejamento das visitas técnicas, poderá, por meio de prévio ajuste entre as partes, ser requerido o preenchimento de listas de verificação ou questionários, com a finalidade de orientar as ações de acompanhamento.

A ausência de um sistema automatizado de monitoramento não constitui motivo para que não haja o acompanhamento das Infraestruturas Críticas. Respeitadas as características de cada setor e consideradas as especificidades de cada negócio, o acompanhamento das Infraestruturas Críticas pode ser realizado por consulta direta a responsáveis previamente designados em uma lista de contatos, por elaboração de comunicados pontuais, por remessa de relatórios periódicos ou eventuais, por intermédio de aplicativos de mensagens ou por meio de outras ações e medidas de efetivo resultado prático.

8.3. Resposta a incidentes

A implementação continuada da estrutura de gerenciamento de risco, das parcerias e das redes de compartilhamento de informações do Plansic oferece mecanismos de rápida avaliação de impacto de incidentes nas Infraestruturas Críticas, de auxílio no estabelecimento de prioridades para a restauração de seus serviços e de compartilhamento de informações sobre incidentes. Possibilita que os planos de resposta a incidentes contenham uma abordagem de perigos múltiplos, que incorpore as melhores práticas de áreas como defesa civil, resgate, serviços médicos emergenciais e de profissionais como bombeiros e policiais.

Os órgãos e as entidades do Sistema Nacional de Proteção e Defesa Civil são parceiros importantes, com experiência prática na gestão de uma série de desastres naturais, ameaças humanas e outras emergências que podem afetar as Infraestruturas Críticas. Suas estruturas de coordenação de operações e seus recursos foram elaborados para auxiliar a tomada de decisão durante a resposta a uma ameaça específica ou incidente. Servem para unificar e ampliar as capacidades de gerenciamento de incidentes e recursos de agências individuais e de organizações isoladas.

A Política Nacional de Proteção e Defesa Civil, instituída pela Lei nº 12.608, de 10 de abril de 2012, orienta os processos de coordenação entre órgãos federais, agências reguladoras, Governos estaduais e do Distrito Federal, Governos municipais e parceiros do setor privado, tanto para preparação pré-incidente quanto para resposta e recuperação pós-incidente. Também especifica atribuições e responsabilidades no gerenciamento de incidentes, incluídas as funções de apoio emergencial destinado a acelerar o fluxo de recursos e programas de apoio à área do incidente.

9. AÇÕES ESTRATÉGICAS

A seguir, apresenta-se a proposta de um conjunto de ações estratégicas, com respectivas metas e prazos, elaboradas com o objetivo de estabelecer e organizar responsabilidades na implementação da Política Nacional de Segurança de Infraestruturas Críticas. Todos os prazos estabelecidos serão contados a partir da data da publicação deste Plano.

Nessa primeira fase do Plansic, as ações estratégicas foram construídas com foco no estabelecimento de uma estrutura de governança, nas iniciativas de capacitação e conscientização dos atores envolvidos e no estabelecimento de uma ferramenta de armazenamento, gestão e integração dos dados e informações. Assim, espera-se criar um ambiente propício para o desenvolvimento, em fase futura, de ações mais direcionadas às Infraestruturas Críticas do País, com o estabelecimento de cooperações baseadas nas interdependências, com a integração de iniciativas, com vistas à redução de custos, com a realização de ações coordenadas de proteção, a fim de resultar em maior eficiência, entre outros.

Eixo estruturante: articulação institucional Objetivo estratégico 1.1. da Estratégia Nacional de Segurança de Infraestruturas Críticas - estabelecer estrutura de governança compatível com a atividade de Segurança de Infraestruturas Críticas.			
AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
1.1.1. Propor a criação do Comitê Gestor de Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Seis meses	Decreto que dispõe sobre o Comitê Gestor de Segurança de Infraestruturas Críticas encaminhado pelo Gabinete de Segurança Institucional da Presidência da República.
1.1.2. Estimular a interlocução de órgãos envolvidos com Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Rede de comunicação entre os órgãos envolvidos com Segurança de Infraestruturas Críticas estabelecida.
1.1.3. Informar ao Gabinete de Segurança Institucional da Presidência da República, via ofício, as unidades, secretarias, departamento ou afins, dos órgãos que ficarão responsáveis pelo tratamento e prestação de contas acerca da implementação das ações previstas neste Plano.	Ministério da Justiça e Segurança Pública Ministério da Defesa Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional	Trinta dias	Recebimento, pelo Gabinete de Segurança Institucional da Presidência da República, de cem por cento das indicações.

Eixo estruturante: articulação institucional Objetivo estratégico 1.2. da Estratégia Nacional de Segurança de Infraestruturas Críticas - estabelecer a Política Nacional de Segurança de Infraestruturas Críticas como política de Estado.			
AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
1.2.1. Apresentar proposta de Projeto de Lei sobre a Política Nacional de Segurança de Infraestruturas Críticas à Câmara de Relações Exteriores e de Defesa Nacional do Conselho de Governo.	Gabinete de Segurança Institucional da Presidência da República	Dois anos	Proposta de Projeto de Lei sobre a Política Nacional de Segurança de Infraestruturas Críticas encaminhada para deliberação da Câmara de Relações Exteriores e de Defesa Nacional do Conselho de Governo.

Eixo estruturante: articulação institucional Objetivo estratégico 1.3. da Estratégia Nacional de Segurança de Infraestruturas Críticas - promover a integração e a articulação entre os diversos setores da administração pública e do setor privado envolvidos na temática de Segurança de Infraestruturas Críticas, com vistas à troca de informações e à realização de ações conjuntas de interesse recíproco.			
AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
1.3.1. Estabelecer protocolo para intercâmbio de informações entre os órgãos envolvidos com Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Dezoito meses	Protocolo definido com orientações gerais de intercâmbio de informações de Segurança de Infraestruturas Críticas.
1.3.2. Estabelecer normativos que internalizem o protocolo de intercâmbio de informações, definido pelo Gabinete de Segurança Institucional da Presidência da República, sobre as Infraestruturas Críticas.	Ministério da Defesa Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional	Trinta meses	Protocolo de intercâmbio de informações sobre as Infraestruturas Críticas, definido pelo Gabinete de Segurança Institucional da Presidência da República, internalizado pelos Ministérios das áreas prioritárias.
1.3.3. Estabelecer canal de comunicação para o fornecimento de informações provenientes do programa Vigidesastres, quando referentes a ocorrências com Infraestruturas Críticas, para o Comitê Gestor de Segurança de Infraestruturas Críticas.	Ministério da Saúde	Seis meses	Canal de comunicação estabelecido para o fornecimento de informações provenientes do Vigidesastres ou similar ao Comitê Gestor de Segurança de Infraestruturas Críticas.
1.3.4. Estabelecer canal de comunicação para o fornecimento de informações provenientes do Centro Nacional de Gerenciamento de Riscos e Desastres, quando referentes a ocorrências com Infraestruturas Críticas, para o Comitê Gestor de Segurança de Infraestruturas Críticas.	Ministério do Desenvolvimento Regional	Seis meses	Canal de comunicação estabelecido para o fornecimento de informações provenientes do Centro Nacional de Gerenciamento de Riscos e Desastres ou similar ao Comitê Gestor de Segurança de Infraestruturas Críticas.

Eixo estruturante: conscientização e capacitação Objetivo estratégico 2.1. da Estratégia Nacional de Segurança de Infraestruturas Críticas - fortalecer a cultura de prevenção e de resposta coordenada na elaboração de políticas públicas de Segurança de Infraestruturas Críticas.			
AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
2.1.1. Propor a órgãos e entidades públicas, das respectivas áreas prioritárias, a abordagem da temática de Segurança de Infraestruturas Críticas nos seus processos de desenvolvimento de políticas públicas.	Gabinete de Segurança Institucional da Presidência da República Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional	Quatro anos	Abordagem da temática de Segurança de Infraestruturas Críticas proposta em políticas públicas aderentes.
2.1.2. Realizar seminário nacional de Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Um seminário nacional de Segurança de Infraestruturas Críticas realizado a cada dois anos.

Eixo estruturante: conscientização e capacitação
Objetivo estratégico 2.2. da Estratégia Nacional de Segurança de Infraestruturas Críticas - fomentar a capacitação e a educação em Segurança de Infraestruturas Críticas.

AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
2.2.1. Realizar capacitação em Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Um evento de capacitação realizado por ano, a partir do segundo ano de vigência do Plano Nacional de Segurança de Infraestruturas Críticas - Plansic.
2.2.2. Encaminhar ao Gabinete de Segurança Institucional da Presidência da República lista de cursos nacionais e internacionais considerados relevantes à temática de defesa e de Segurança de Infraestruturas Críticas.	Ministério da Justiça e Segurança Pública Ministério da Defesa Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional	Quatro anos	Lista de cursos encaminhada ao Gabinete de Segurança Institucional da Presidência da República, semestralmente.
2.2.3. Divulgar aos órgãos, às entidades e às instituições de interesse cursos nacionais e internacionais sobre temas afetos à defesa e segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Lista atualizada de cursos divulgada, semestralmente.
2.2.4. Realizar exercício ou simulação conjunta de incidentes que envolva diferentes setores de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Exercício ou simulação realizada, que envolva dois ou mais setores de Infraestruturas Críticas.
2.2.5. Envolver, nos exercícios de Guardião Cibernético, setores abordados em Segurança de Infraestruturas Críticas.	Ministério da Defesa	Quatro anos	Dois ou mais setores de Infraestruturas Críticas envolvidos na realização dos exercícios de Guardião Cibernético.

Eixo estruturante: conscientização e capacitação
Objetivo estratégico 2.3. da Estratégia Nacional de Segurança de Infraestruturas Críticas - implementar ações de divulgação e fóruns setoriais de debate acerca da temática de Segurança de Infraestruturas Críticas.

AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
2.3.1. Realizar fóruns de discussão conjunta de temas relevantes para diferentes setores de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Um fórum de discussão conjunta realizado a cada dois anos.
2.3.2. Disponibilizar levantamento atualizado e consolidado de normativos relativos à Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Cem por cento dos normativos identificados como relativos à Segurança de Infraestruturas Críticas disponibilizados na página institucional do Gabinete de Segurança Institucional da Presidência da República.

Eixo estruturante: conscientização e capacitação
Objetivo estratégico 2.4. da Estratégia Nacional de Segurança de Infraestruturas Críticas - disseminar a temática de Segurança de Infraestruturas Críticas e conscientizar a administração pública e o setor privado acerca da sua relevância para a defesa e segurança nacional.

AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
2.4.1. Divulgar periódicos eletrônicos de forma a demonstrar a correlação entre defesa e segurança nacional e a temática Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Periódicos divulgados semestralmente.
2.4.2. Considerar, no desenvolvimento de suas políticas públicas, o endereçamento dos interesses da defesa e da segurança nacional na proteção, conservação ou expansão das Infraestruturas Críticas.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Quatro anos	Endereçamento, no desenvolvimento de políticas públicas, dos interesses da defesa e da segurança nacional na proteção, conservação ou expansão das Infraestruturas Críticas.

Eixo estruturante: fomento às ações
Objetivo estratégico 3.1. da Estratégia Nacional de Segurança de Infraestruturas Críticas - estimular a adoção de ações e a priorização de projetos relacionados à prevenção e à resposta coordenada.

AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
3.1.1. Encaminhar, ao Comitê Gestor de Segurança de Infraestruturas Críticas, relatório que contenha oportunidades de parcerias interinstitucionais para implementação de ações de Segurança de Infraestruturas Críticas, no âmbito de suas competências.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Quatro anos	Encaminhamento ao Comitê Gestor de Segurança de Infraestruturas Críticas de relatório anual que contenha oportunidades de parcerias interinstitucionais para implementação de ações de Segurança de Infraestruturas Críticas.

Eixo estruturante: fomento às ações
Objetivo estratégico 3.2. da Estratégia Nacional de Segurança de Infraestruturas Críticas - viabilizar fontes de recursos para as ações de prevenção e de resposta coordenada, inclusive com agilidade na sua disponibilização.

AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
3.2.1. Incluir, em seus planejamentos, ações coordenadas que concorram para a Segurança das Infraestruturas Críticas, no âmbito de suas competências.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Dois anos	Ações coordenadas que concorram para a Segurança das Infraestruturas Críticas incluídas nos planejamentos de cada órgão.
3.2.2. Propor às agências reguladoras e outras entidades públicas, vinculadas às respectivas áreas prioritárias, a internalização de ações ligadas a este Plano e aos planos setoriais.	Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Dois anos	Propostas de internalização de ações ligadas a este Plano e aos planos setoriais encaminhadas às agências reguladoras e outras entidades públicas.

Eixo estruturante: fomento às ações
Objetivo estratégico 3.3. da Estratégia Nacional de Segurança de Infraestruturas Críticas - incentivar a adoção de proteções básicas e de boas práticas (normas e recomendações).

AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
3.3.1. Elaborar guia de boas práticas em Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Um ano	Guia de boas práticas em Segurança de Infraestruturas Críticas disponibilizado.
3.3.2. Elaborar guia complementar de boas práticas em Segurança de Infraestruturas Críticas para os setores das suas respectivas áreas prioritárias.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Dois anos	Guia complementar de boas práticas de todos os setores de Infraestruturas Críticas disponibilizado.
3.3.3. Disseminar, pelos meios de comunicação públicos disponíveis (documentos, sítios eletrônicos, e-mails e outros), aos órgãos e às entidades, subordinados e vinculados às respectivas áreas prioritárias, conteúdo de Segurança de Infraestruturas Críticas originário de experiências das instituições nacionais e internacionais.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Quatro anos	Cem por cento das experiências nacionais e internacionais, identificadas como relevantes, disseminadas oportunamente.

Eixo estruturante: fomento às ações
Objetivo estratégico 3.4. da Estratégia Nacional de Segurança de Infraestruturas Críticas - desenvolver e disseminar recomendações de Segurança de Infraestruturas Críticas no âmbito de cada setor.

AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
3.4.1. Elaborar planos setoriais de Segurança de Infraestruturas Críticas das respectivas áreas prioritárias, conforme distribuição na tabela do item 4 deste Plano.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Dezoito meses	Propostas de planos setoriais encaminhados ao Comitê Gestor de Segurança de Infraestruturas Críticas.
3.4.2. Estabelecer canal de comunicação interno para o compartilhamento de informações e recomendações de Segurança de Infraestruturas Críticas relacionadas ao setor, entre os órgãos e as entidades subordinados ou vinculados às respectivas áreas prioritárias.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Dois anos	Canal de comunicação estabelecido entre os Ministérios das áreas prioritárias e as entidades dos setores sob sua responsabilidade.
3.4.3. Disponibilizar, no sítio eletrônico do órgão, uma página eletrônica sobre Segurança de Infraestruturas Críticas (internet e intranet).	Gabinete de Segurança Institucional da Presidência da República Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Um ano	Página eletrônica com informações de Segurança de Infraestruturas Críticas disponibilizada.

Eixo estruturante: gestão de dados e informações
Objetivo estratégico 4.1. da Estratégia Nacional de Segurança de Infraestruturas Críticas - promover, no âmbito da administração pública e do setor privado, a geração, a disponibilização e a atualização periódica de dados íntegros, consistentes e padronizados sobre Infraestruturas Críticas e ameaças.

AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
4.1.1. Estabelecer protocolo de cooperação com as entidades reguladoras ou, na inexistência dessas, com os operadores das Infraestruturas Críticas, para o fornecimento de informações de dados sobre as Infraestruturas Críticas e eventuais ameaças.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Três anos	Protocolo de cooperação estabelecido entre os Ministérios e entidades reguladoras ou operadores de Infraestruturas Críticas.
4.1.2. Encaminhar, ao Gabinete de Segurança Institucional da Presidência da República, relatório anual de monitoramento das metas estabelecidas neste Plano.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa	Quatro anos	Relatório anual encaminhado ao Gabinete de Segurança Institucional da Presidência da República.
4.1.3. Encaminhar, ao Gabinete de Segurança Institucional da Presidência da República, relatório anual de monitoramento das metas estabelecidas nos planos setoriais.	Ministério da Economia Ministério da Infraestrutura Ministério da Saúde	Quatro anos	Relatório anual setorial encaminhado ao Gabinete de Segurança Institucional da Presidência da República, a partir da publicação do respectivo plano setorial.

	Ministério de Minas e Energia Ministério das Comunicações Ministério do Desenvolvimento Regional Ministério da Defesa		

Eixo estruturante: gestão de dados e informações Objetivo estratégico 4.2. da Estratégia Nacional de Segurança de Infraestruturas Críticas - desenvolver um sistema dedicado à gestão de informações relacionadas à Segurança de Infraestruturas Críticas.			
AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
4.2.1. Implementar o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Dois anos	Sistema Integrado de Dados de Segurança de Infraestruturas Críticas alimentado com informações das áreas prioritárias e respectivos setores previstos neste Plano, conforme previsto na tabela do item 4.
4.2.2. Publicar normativo específico com diretrizes para a gestão do Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, incluído o compartilhamento de informações relevantes de Segurança de Infraestruturas Críticas.	Gabinete de Segurança Institucional da Presidência da República	Dois anos	Normativo publicado.

Eixo estruturante: gestão de dados e informações Objetivo estratégico 4.3. da Estratégia Nacional de Segurança de Infraestruturas Críticas - incentivar a adoção de recursos e de procedimentos voltados para a segurança cibernética nas Infraestruturas Críticas.			
AÇÃO ESTRATÉGICA	ÓRGÃO RESPONSÁVEL	PRAZO	META
4.3.1. Realizar ações de conscientização sobre a importância do investimento em prevenção, com o objetivo de minimizar os custos decorrentes de ataques cibernéticos.	Gabinete de Segurança Institucional da Presidência da República	Quatro anos	Uma ação anual realizada por meio de inserção da temática em palestras, simpósios, apresentações e outros.
4.3.2. Estabelecer um protocolo de integração entre o Sistema Integrado de Segurança de Infraestruturas Críticas e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov.	Gabinete de Segurança Institucional da Presidência da República	Dois anos	Protocolo de integração entre o Sistema Integrado de Segurança de Infraestruturas Críticas e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov estabelecido.