ANEXO

ESTRATÉGIA NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

1. INTRODUÇÃO

As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente.

De maneira geral, os países buscam se preparar para possíveis imprevistos que possam afetar tais infraestruturas, identificando ações e procedimentos que permitam garantir o seu funcionamento, ainda que com algum tipo de restrição.

Nesse quadro, torna-se imperativa a atividade denominada segurança de infraestruturas críticas, cuja implementação necessita do esforço conjunto do Estado e da sociedade.

A segurança de infraestruturas críticas passou a ser uma tendência mundial logo após os atentados terroristas ocorridos nos Estados Unidos da América, em 11 de setembro de 2001. O governo americano, à época, publicou uma série de diretrizes de segurança interna, entre as quais havia a elaboração de um plano nacional abrangente para garantir a segurança de infraestruturas críticas, por meio de cooperação das autoridades e das agências federais, regionais e locais, além do setor privado e de outras entidades.

Da mesma forma, a União Europeia desenvolveu seu programa de proteção, visando assegurar níveis de proteção adequados e uniformes das infraestruturas críticas, reduzir ao mínimo suas falhas e facultar meios de recuperação rápida de seus serviços. Como consequência, em 2006, a Comissão Europeia publicou uma diretiva determinando a seus Estados-membros adotar os componentes de tal programa em seus estatutos nacionais.

Igualmente, o Conselho de Segurança da Organização das Nações Unidas, em recorrentes resoluções, tem encorajado seus Estados-membros a realizarem esforços coordenados, inclusive por meio de cooperação internacional, no desenvolvimento ou na melhora de suas estratégias para reduzir os riscos às infraestruturas críticas, com foco na ameaça de ataques terroristas, incluindo a adoção de medidas de preparação e promoção da interoperabilidade na segurança.

No Brasil, o tema teve impulso a partir de 2006, após os ataques perpetrados por uma organização criminosa a várias instalações sediadas no Estado de São Paulo. Esses eventos levaram o Governo brasileiro a tomar a iniciativa de identificar quais infraestruturas do País deveriam ser prioritariamente protegidas, no caso de novas ocorrências daquela natureza.

Desse modo, a atividade de segurança de infraestruturas críticas foi inserida no rol de competências da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, conforme o Decreto nº 9.819, de 3 de junho de 2019. A iniciativa buscou estudar e propor a implementação de medidas e de ações relacionadas à segurança de infraestruturas críticas, tendo como foco o aspecto da prevenção. Observou-se que se tratava de assunto com necessidade de acompanhamento permanente e estudo aprofundado em âmbito institucional.

Nesse quesito, cabe citar a Estratégia Nacional de Defesa, aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, que relacionou as medidas para a segurança das áreas de infraestruturas críticas, como ações estratégicas que visam contribuir para o incremento do nível de segurança nacional, em especial no que se refere a energia, transportes, águas, finanças e comunicações. Naquele documento, definiu-se que a coordenação, a avaliação, o monitoramento e a redução de riscos seriam de competência do Gabinete de Segurança Institucional da Presidência da República.

No âmbito das atividades de inteligência, cuja coordenação na administração pública federal também compete ao Gabinete de Segurança Institucional da Presidência da República, a Política Nacional de Inteligência, aprovada pelo Decreto nº 8.793, de 29 de junho de 2016, e a Estratégia Nacional de Inteligência, aprovada pelo Decreto de 15 de dezembro de 2017, preveem a cooperação na proteção das infraestruturas críticas nacionais, por meio do monitoramento de ameaças relativas a atos de sabotagem que atentem contra o funcionamento dessas infraestruturas.

Ademais, nos termos da Lei nº 13.844, de 18 de junho de 2019, cabe ao Gabinete de Segurança Institucional da Presidência da República o acompanhamento de assuntos pertinentes às infraestruturas críticas, com prioridade aos assuntos que se referem à avaliação de riscos, em parceria com diversos órgãos públicos ou entes privados, sendo uma atividade essencialmente preventiva e voltada a antecipar soluções para situações que possam ocorrer nas áreas das infraestruturas críticas do País.

Nesse contexto, o Gabinete de Segurança Institucional da Presidência da República desenvolve o trabalho de identificação e análise de riscos das infraestruturas críticas do País, tendo iniciado com as áreas de comunicações, energia, transportes, finanças e águas, em parceria com órgãos públicos e entes privados. Foi no âmbito desse trabalho que, em 2008, surgiu pela primeira vez no País a definição de infraestruturas críticas, sendo consideradas aquelas instalações, serviços e bens cuja interrupção ou destruição provocará sério impacto social, econômico, político, internacional ou à segurança nacional.

Trata-se, portanto, de infraestruturas que necessitam de medidas de segurança capazes de garantir sua integridade e seu funcionamento, o que significa dizer que a segurança física e operacional precisa ser conhecida e acompanhada, a fim de assegurar a prestação desses serviços essenciais. A segurança efetiva se inicia com a compreensão clara de todos os tipos e níveis de risco que uma organização enfrenta.

1.1. ATIVIDADE DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

A segurança de infraestruturas críticas é atividade fundamental no reforço da segurança e da resiliência dos setores estratégicos vitais para o funcionamento dos Estados, individualmente ou em blocos, configurando-se tema de grande projeção internacional.

Dessa maneira, em consonância com as atribuições previstas no Anexo I ao Decreto nº 9.668, de 2 de janeiro de 2019, o Gabinete de Segurança Institucional da Presidência da República instituiu, no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo e sob sua coordenação, Grupos Técnicos de Segurança de Infraestruturas Críticas nas áreas de energia, transporte, águas, comunicações e finanças.

Os Grupos Técnicos de Segurança de Infraestruturas Críticas são compostos por representantes de órgãos e de entidades correspondentes às áreas prioritárias e especialistas podem ser convidados. As atribuições de cada Grupo Técnico são:

- manter em contínuo aperfeiçoamento a identificação e a classificação das infraestruturas críticas;

- identificar as possíveis ameaças e vulnerabilidades dessas infraestruturas críticas; e

- propor medidas de controle para redução dos riscos às infraestruturas críticas correspondentes à área prioritária considerada.

Em uma visão mais ampla, a atividade de segurança de infraestruturas críticas tem por finalidade articular, em diversos níveis e esferas do Poder Público, bem como no setor privado, o desenvolvimento de um processo de segurança preventiva de recursos humanos, de equipamentos, de instalações, de serviços, de sistemas, de informações e de outros recursos que, de alguma forma, assegurem a resiliência e o funcionamento dos serviços e das atividades indispensáveis ao Estado e à sociedade.

Portanto, para obtenção dos melhores resultados, a colaboração no fornecimento de dados precisos sobre as infraestruturas e suas respectivas operações é de suma importância. Com essa troca de informações, o trabalho alcançará seu objetivo de promover a prevenção e a redução de riscos e custos, especialmente aqueles relativos à segurança e à defesa da sociedade e do Estado brasileiros.

Cabe ressaltar que, considerando o caráter sensível da segurança de infraestruturas críticas, os resultados advindos da análise de risco de cada infraestrutura crítica serão divulgados apenas aos seus respectivos operadores, cabendo a eles a definição das ações de mitigação necessárias.

1.2. POLÍTICA NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

Com a intenção de definir as orientações indispensáveis ao esforço conjunto a ser desenvolvido pelos órgãos e entidades dos setores público e privado no que diz respeito à atividade de segurança de infraestruturas críticas, foi aprovada a Política Nacional de Segurança de Infraestruturas Críticas - PNSIC, por meio do Decreto nº 9.573, de 22 de novembro de 2018.

A PNSIC tem como finalidade principal garantir a segurança e a resiliência das infraestruturas críticas e a continuidade da prestação de seus serviços. Além disso, passou a caracterizar a segurança de infraestruturas críticas como uma atividade de Estado, sinalizando à sociedade brasileira a prioridade que o Governo brasileiro atribui ao tema no âmbito da segurança institucional.

Como princípios da PNSIC, destacam-se o uso da análise de riscos como base para prevenção e resiliência e a integração entre as diferentes esferas do Poder Público, do setor empresarial e dos demais segmentos da sociedade.

Suas diretrizes são pautadas no aprimoramento e na efetividade das ações de segurança de infraestruturas críticas nacionais, por meio de exemplos de políticas semelhantes adotadas por outros países, além da cooperação entre órgãos, entidades e entes federativos ou mesmo entre os setores público e privado, sejam eles de participação nacional ou estrangeira.

No que se refere aos objetivos, a PNSIC estabelece o caminho (diretrizes e instrumentos) para adoção de uma consciência preventiva no planejamento da segurança de infraestruturas críticas (prevenção) e, no caso de haver falhas, na superação dos impactos (resiliência), tendo por base a integração do conhecimento (dados) e das ações (interdependência) e o interesse pelo bem-estar comum (defesa e segurança nacional).

Para a consecução desses objetivos, a PNSIC cita como instrumentos necessários: a Estratégia Nacional de Segurança de Infraestruturas Críticas - Ensic, como documento orientador e principal; o Plano Nacional de Segurança de Infraestruturas Críticas; e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, que reunirá todas as informações produzidas e será empregado no apoio às decisões.

2. PRINCÍPIOS

Os prestadores de serviços, seus usuários e o Estado brasileiro compartilham interesses de que as infraestruturas críticas funcionem de maneira regular e segura.

Nesse contexto, os prestadores buscam a rentabilidade sustentável de seus negócios; os usuários buscam serviços que atendam às suas necessidades e melhorem a sua qualidade de vida; e o Estado atua como agente regulador.

Em consonância com esse interesse comum, a atividade de segurança de infraestruturas críticas e, consequentemente, a implementação da PNSIC devem seguir alguns princípios.

2.1. ANÁLISE DE RISCOS CONTINUADA

Alguns fatores podem afetar a continuidade dos serviços provenientes das infraestruturas críticas de um país, tais como as ameaças provenientes da ação humana ou de desastres naturais e a ocorrência de falhas de toda ordem. Adicionalmente, as vulnerabilidades relacionadas à estrutura física, aos sistemas de proteção pessoal (física ou técnica), aos processos, às operações ou a outras áreas que possam ser alvos de eventos adversos, se exploradas, também podem vir a prejudicar ou interromper a prestação dos serviços.

Todas as atividades de um ativo ou de um sistema envolvem riscos, os quais devem ser identificados, caracterizados e, em seguida, analisados quanto à necessidade e viabilidade de aplicação de controles, de maneira a reduzir a probabilidade de ocorrência dos eventos relacionados a tais riscos. Os riscos absolutos não são admissíveis. Após tratamento adequado, devem permanecer apenas os riscos residuais, que são aqueles aceitos ou que não podem ser tratados. A correta equação entre as duas situações é a chave para o êxito da atividade de segurança de infraestruturas críticas, proporcionando valiosos subsídios para o emprego judicioso dos recursos existentes.

A atividade de segurança de infraestruturas críticas engloba o conjunto de medidas de caráter preventivo e reativo destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas. Essas informações são obtidas por meio da aplicação de metodologia de gestão de riscos, a qual fornece um diagnóstico das condições de segurança das infraestruturas e, consequentemente, possibilita a identificação das medidas necessárias para a redução dos riscos (prevenção) e para a mitigação das consequências (reação).

2.1.1. Ameaças, vulnerabilidades, consequências e medidas de controle

Para a análise de riscos de uma infraestrutura crítica são necessários dois levantamentos: o levantamento das ameaças reais ou potenciais, com base em vários fatores, inclusive no potencial de periculosidade ou capacidade danosa do perigo; e o levantamento das vulnerabilidades, relacionadas a sistemas de proteção pessoal (física ou técnica), estrutura física, processos, operações ou de outras áreas que possam ser alvos de eventos adversos.

Assim, é possível avaliar como as ameaças podem explorar as vulnerabilidades e, com isso, determinar o nível do risco, sua probabilidade ou frequência de ocorrência e os possíveis impactos ou consequências. Essa abordagem é a mais abrangente possível e leva em consideração falhas em geral e ameaças de toda ordem, provenientes de ação humana ou de desastres naturais. Dessa forma, garante-se que a sinergia entre as medidas de controle seja explorada ao máximo. Já a avaliação das vulnerabilidades permite sugerir ações para eliminar ou reduzir as fraquezas das infraestruturas críticas, tornando-as mais resistentes às ameaças.

Diversas organizações e entidades responsáveis pela gestão da segurança de suas infraestruturas críticas desenvolvem sistemas para o gerenciamento, monitoramento e controle permanente de múltiplas atividades. Criam as chamadas ilhas de informação, com tecnologias e metodologias potencialmente diferentes, que visam satisfazer os requisitos específicos da área considerada. Esse contexto evidencia a necessidade de um sistema centralizado de gestão da informação, de nível estratégico, robusto e eficaz, que permita às autoridades decidirem, em tempo hábil e com base em uma visão integrada dos diversos cenários, pela implementação das ações necessárias e de forma acertada.

2.2. ATUAÇÃO INTEGRADA

Destaca-se que parte cada vez mais significativa das infraestruturas críticas do País são de propriedade ou operadas pelo setor privado. Como consequência, é reconhecida a necessidade da construção de uma parceria entre o Governo federal e o setor privado de forma a unir esforços na garantia da segurança e resiliência das infraestruturas críticas. Essas parcerias dependem do compartilhamento de informações entre esses atores, respeitando a privacidade, a liberdade e a necessidade de sua salvaguarda.

A análise conjunta das informações relacionadas às infraestruturas críticas, dentro de uma mesma área prioritária ou entre áreas distintas, gera conhecimento e proporciona melhor compreensão da complexidade dos possíveis cenários de segurança. As respostas aos eventos adversos, incluindo a continuidade das atividades essenciais durante e depois do ocorrido, ganham em eficiência e efetividade quando há o conhecimento prévio pelas partes envolvidas sobre as medidas de reforço da segurança a serem adotadas.

O compartilhamento de informações serve de base para a formulação de políticas em questões relativas à segurança e ao treinamento de atores importantes e imprescindíveis. Assim, será possível manter acompanhamento das condições físicas e operacionais das infraestruturas críticas indispensáveis à população.

Os diversos atores relacionados com o tema devem conduzir uma análise sobre modelos de parceria público-privada existentes, considerando opções para agilizar os processos de colaboração e troca de informações e minimizar a duplicação de esforços. Além disso, a análise deve considerar como o modelo pode ser flexível e adaptável para atender às necessidades específicas de diferentes setores.

2.3. REDUÇÃO DE CUSTOS PARA A SOCIEDADE

Uma vez que os investimentos em infraestruturas constituem uma prioridade essencial para fomentar o desenvolvimento econômico e social dos países, torna-se fundamental que a prevenção e a resiliência sejam consideradas em investimentos atuais e futuros. Se não forem construídas e gerenciadas adequadamente, as infraestruturas críticas, tais como aquelas dos setores de energia, de transportes, de águas e saneamento, de finanças e comunicações, podem atuar como vetores na propagação de impactos negativos de desastres. Danos a sistemas críticos podem gerar dificuldades sociais significativas ao interromperem o acesso a serviços essenciais, bem como impactos econômico-financeiros decorrentes da interrupção do funcionamento de empresas por prazo superior à duração do evento.

As infraestruturas críticas sustentam economias, governos e sociedades. Sua segurança e sua resiliência não só determinam o grau em que os países podem ser afetados por desastres naturais, acidentes e ataques intencionais, mas também revelam sua capacidade para responder e se recuperar diante de tais eventos.

No entanto, quando não são capazes de suportar os impactos de um choque, as infraestruturas críticas podem atuar como multiplicadores de riscos, aumentando a gravidade da situação, uma vez que os efeitos-cascata, entre setores distintos, acrescentam camadas adicionais de complexidade e frequentemente dificultam - ou impedem - a implementação de ações de resposta.

Portanto, investir em segurança de infraestruturas críticas, de forma preventiva e reativa, visando preservar ou restabelecer a prestação dos serviços relacionados a tais infraestruturas, auxilia sobremaneira a redução de custos financeiros, sociais, políticos e outros.

No mesmo sentido, no caso da ocorrência de um desastre, a reparação de uma determinada infraestrutura crítica pode envolver montantes significativos de recursos públicos. Assim, cabe à administração pública desempenhar um papel crucial na promoção da resiliência das infraestruturas críticas, estimulando, por exemplo, a adoção de medidas de redução de riscos pelos proprietários ou operadores dessas infraestruturas, assim como o financiamento de atividades que busquem elevar a conscientização dos proprietários e operadores em relação a riscos e a medidas de resiliência.

2.4. DEFESA E SEGURANÇA NACIONAL

A preservação da soberania política e a defesa da integridade territorial constituem os elementos fundamentais para a definição dos objetivos de segurança nacional, o que inclui a proteção da população, das infraestruturas críticas e das funções essenciais do Estado.

Neste contexto, merece especial consideração a proteção das infraestruturas críticas, desenvolvida e consolidada preventivamente, uma vez que as referidas infraestruturas são elementos fundamentais para o desenvolvimento econômico do País.

A amplitude territorial do Brasil, a grande extensão de fronteiras, o notório crescimento dos índices de adensamento urbano nas grandes cidades - e a posição econômica de tais cidades no cenário global - tornam a segurança de infraestruturas críticas uma atividade de relevante valor estratégico para a defesa e a segurança do País.

As vulnerabilidades encontradas nas imensas extensões territoriais da nossa fronteira implicam na necessidade de reforço dos dispositivos atuais de defesa e segurança, buscando mitigar a ocorrência de ameaças intencionais às nossas infraestruturas críticas. Neste aspecto, além da preocupação com a segurança das fronteiras, é necessário estabelecer prioridades no emprego dos mecanismos de defesa, de modo a proteger e conservar as próprias infraestruturas críticas.

3. DESAFIOS

Tendo como base as orientações da PNSIC, estabelecidas em seus princípios, objetivos e diretrizes, surgem desafios de caráter estratégico e de grande relevância para que a atividade de segurança de infraestruturas críticas atue com eficácia em prol dos interesses do Estado e da sociedade brasileira.

Os desafios relacionados a seguir reúnem os elementos considerados essenciais para que os objetivos da PNSIC sejam alcançados:

a) reconhecimento da PNSIC como política de Estado;

b) comprometimento da administração pública e do setor privado, no nível decisório, fomentando um ambiente institucional e normativo favorável à adoção de ações preventivas e de divulgação a respeito da segurança das infraestruturas críticas;

c) consolidação da cultura de segurança junto aos órgãos da administração pública, ao setor privado e à sociedade;

d) elaboração de políticas públicas que fomentem a conscientização, a capacitação e a educação dos atores envolvidos com a atividade de segurança de infraestruturas críticas;

e) institucionalização da gestão de riscos na administração pública e em entidades privadas;

f) criação de normas que contemplem estrutura de governança visando à prevenção, à proteção, à mitigação, à resposta e à recuperação;

g) ampliação do treinamento e da capacitação das partes interessadas e relacionadas a cada infraestrutura crítica, tendo como base a PNSIC;

h) responsabilização no cumprimento dos objetivos estabelecidos para a segurança de infraestruturas críticas;

i) superação dos entraves institucionais de forma articulada;

j) integração das estruturas de comando e controle dos setores público e privado;

k) obtenção da sinergia entre os diversos setores, inclusive com aqueles não relacionados diretamente às infraestruturas críticas, em prol da segurança;

l) priorização orçamentária para execução de ações relacionadas à prevenção e à reação;

m) estruturação e compartilhamento dos dados qualificados a serem integrados e armazenados entre os entes envolvidos com a atividade de segurança de infraestruturas críticas;

n) implementação de tecnologias e dispositivos voltados para a segurança da informação, com o objetivo de permitir o compartilhamento seguro de dados sobre infraestruturas críticas;

o) estabelecimento de canais de comunicação que garantam a capilaridade na troca de informações entre a administração pública e as entidades privadas; e

p) Criação de um ambiente que proporcione confiança e colaboração entre as empresas, suas representações e os órgãos governamentais.

4. EIXOS ESTRUTURANTES

A identificação dos eixos estruturantes é resultado da análise dos desafios reconhecidos para a implementação da PNSIC.

Dessa avaliação foram extraídos quatro grandes eixos, que constituem os principais pilares para a efetividade da atividade de segurança de infraestruturas críticas. Os eixos organizam os desafios de modo a criar uma Estratégia organicamente coerente e coesa, que deve impulsionar o funcionamento da atividade de segurança de infraestruturas críticas.

São eixos estruturantes da Ensic:

1. articulação institucional - para implementação da PNSIC se deve fortalecer a articulação entre órgãos e entidades dos setores público e privado envolvidos direta e indiretamente com a segurança das infraestruturas críticas e, adicionalmente, é necessário estabelecer uma governança capaz de reunir e orientar todos os envolvidos de modo a alcançar a integração em todos os níveis;

2. conscientização e capacitação - a divulgação de informações sobre o tema de segurança das infraestruturas críticas, incluindo sua importância para a defesa e segurança nacional, auxilia o desenvolvimento de uma cultura de prevenção e resposta, além disso, é necessário capacitar os órgãos e entidades envolvidos, públicos e privados, para a maior compreensão sobre suas responsabilidades e competências diante do tema;

3. fomento às ações - recomendar e estimular a adoção de ações coordenadas para fortalecer a atividade de segurança de infraestruturas críticas, viabilizando os recursos necessários, sejam técnicos ou financeiros; os investimentos em segurança de infraestruturas críticas auxiliam o País a prevenir incidentes de grande impacto e, quando não for possível impedi-los, a responder de modo tempestivo e eficaz; e

4. gestão de dados e informações - para auxiliar na articulação institucional em prol da atividade de segurança de infraestruturas críticas, faz-se necessária a seleção, organização e qualificação dos dados e informações gerados, disponibilizando-os aos responsáveis pelas decisões estratégicas no momento pertinente.

5. OBJETIVOS E INICIATIVAS ESTRATÉGICAS

A Ensic é o documento orientador e de referência para a elaboração do Plano Nacional de Segurança de Infraestruturas Críticas. Os objetivos estratégicos a seguir apresentados, sem ordem de prioridade e organizados por eixos estruturantes, retratam o foco estratégico para direcionar os esforços na implementação da PNSIC, além de sinalizar os resultados a serem alcançados. Já o desdobramento dos objetivos estratégicos em iniciativas estratégicas fornece a direção para o emprego efetivo desses esforços, indicando o contexto e o tipo de medidas a serem executadas por todos os envolvidos e que comporão o referido Plano Nacional.

Para a estruturação do Plano Nacional de Segurança de Infraestruturas Críticas, cada iniciativa será executada por meio de uma ou mais ações, sob responsabilidade de um ou mais órgãos ou entidades, cada qual com a sua contribuição. Assim, deverá ser elaborada uma matriz de responsabilidades que contemple o conjunto de iniciativas estipuladas para o cumprimento dos objetivos estratégicos. Além disso, o Plano Nacional deverá contar com mecanismos de acompanhamento da execução das ações e do atingimento de metas.

EIXOS ESTRUTURANTES	OBJETIVOS ESTRATÉGICOS	INICIATIVAS ESTRATÉGICAS
1. Articulação institucional	1.1. Estabelecer estrutura de governança compatível com a atividade de segurança das infraestruturas críticas.	1.1.1. Criar entidade responsável pela coordenação (núcleo duro) do trabalho de implementação da PNSIC, composta preferencialmente por representantes dos Ministérios competentes. 1.1.2. Instituir o Sistema de Governança de Segurança de Infraestruturas Críticas, composto por todos os órgãos e entidades dos setores público e privado com pertinência na integridade física e no funcionamento das infraestruturas críticas, estabelecendo objetivos e atribuições. 1.1.3. Elaborar o Plano Nacional de Segurança de Infraestruturas Críticas como documento orientador para a implementação da PNSIC nas áreas definidas como prioritárias e nos respectivos setores sobre a integridade e funcionamento das infraestruturas críticas.
	1.2. Estabelecer a PNSIC como política de Estado.	1.2.1. Propor projeto de lei estabelecendo a PNSIC como política de Estado, assegurando o posicionamento técnico dos trabalhos desenvolvidos.
	1.3. 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.	1.3.1 Propiciar, no âmbito do Sistema de Governança de Segurança de Infraestruturas Críticas, o intercâmbio de informações relacionadas à segurança de infraestruturas críticas, visando inclusive a orientar o planejamento de ações conjuntas.
2. Conscientização e capacitação	2.1. Fortalecer a cultura de prevenção e de resposta coordenada na elaboração de políticas públicas de segurança de infraestruturas críticas.	2.1.1. Integrar a PNSIC com outras políticas de Estado. 2.1.2. Promover ciclos de debates e conscientização a respeito da importância das infraestruturas críticas para a defesa e segurança nacional.
	2.2. Fomentar a capacitação e a educação em segurança de infraestruturas críticas.	2.2.1. Fomentar as ações de capacitação existentes em defesa e segurança de infraestruturas críticas. 2.2.2. Estimular o interesse no tema de segurança de infraestruturas críticas por meio de reconhecimento de mérito. 2.2.3. Estimular o desenvolvimento de habilidade nos órgãos e entidades da administração pública e em entidades do setor privado envolvidos com a segurança de infraestruturas críticas, em atividades de planejamento e execução de gestão de riscos, de crises e de continuidade de negócios.
	2.3. Implementar ações de divulgação e fóruns setoriais de debate acerca do tema de segurança de infraestruturas críticas.	2.3.1. Internalizar, em políticas públicas, diretrizes de divulgação acerca do tema de segurança de infraestruturas críticas (resoluções, portarias etc.). 2.3.2. Divulgar o conhecimento sobre a segurança de infraestruturas críticas e sua importância para a administração pública e para o setor privado.
	2.4. Disseminar o tema de segurança de infraestruturas críticas e conscientizar a administração pública e o setor privado acerca da sua relevância para a defesa e segurança nacional.	2.4.1. Conscientizar a administração pública e o setor privado da importância da relação entre o interesse da defesa e da segurança nacional com a segurança de infraestruturas críticas. 2.4.2. Fortalecer o arcabouço normativo que defina a prevalência do interesse da defesa e da segurança nacional na proteção, conservação e expansão das infraestruturas críticas sobre outros interesses.

3. Fomento às ações	3.1. Estimular a adoção de ações e a priorização de projetos relacionados à prevenção e à resposta coordenada.	3.1.1. Estimular a cooperação entre órgãos e entidades federais, estaduais, distritais, municipais e do setor privado nas ações necessárias à proteção das infraestruturas críticas e à manutenção do seu funcionamento. 3.1.2. Estimular a elaboração de planos de prevenção e resposta coordenadas das infraestruturas críticas.
	3.2. Viabilizar fontes de recursos para as ações de prevenção e de resposta coordenada, inclusive com agilidade na sua disponibilização.	3.2.1. Estabelecer, no planejamento orçamentário e financeiro, a priorização de recursos para a implementação de ações necessárias à proteção das infraestruturas críticas e à continuidade de seu funcionamento. 3.2.2. Promover a adoção de medidas para mitigar o contingenciamento de recursos alocados.
	3.3. Incentivar a adoção de proteções básicas e de boas práticas (normas e recomendações).	3.3.1. Estabelecer diretrizes gerais de proteção básica e de boas práticas em segurança de infraestruturas críticas. 3.3.2. Aprimorar as atividades de segurança das infraestruturas críticas, inclusive com base em experiências internacionais e em instruções de órgãos de controle. 3.3.3. Estabelecer no Plano Nacional de Segurança de Infraestruturas Críticas a obrigatoriedade de adoção de medidas para sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança.
	3.4. Desenvolver e disseminar recomendações de segurança de infraestruturas críticas no âmbito de cada setor.	3.4.1. Estabelecer no Plano Nacional de Segurança de Infraestruturas Críticas a previsão de elaboração de Planos Setoriais de segurança de infraestruturas críticas, sob responsabilidade dos órgãos e das entidades envolvidos com cada setor. 3.4.2. Estabelecer mecanismos de disseminação (sistemas, periódicos ou informativos) das recomendações de segurança de infraestruturas críticas.
4. Gestão de dados e informações	4.1. 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.	4.1.1. Orientar a organização, a tempestividade na atualização, na transmissão e no armazenamento dos dados sobre infraestruturas críticas e ameaças. 4.1.2. Acompanhar a evolução da segurança das infraestruturas críticas, com base em métricas e periodicidade pré-definidas no Plano Nacional de Segurança de Infraestruturas Críticas e nos planos setoriais (relatórios, indicadores e ferramentas, entre outros).
	4.2. Desenvolver um sistema dedicado à gestão de informações relacionadas à segurança de infraestruturas críticas.	4.2.1. Dispor de um sistema dedicado (central) para a captação, a integração, o armazenamento e o compartilhamento de informações relacionadas à segurança das infraestruturas críticas. 4.2.2. Promover o compartilhamento de informações relevantes para a segurança de infraestruturas críticas, considerando regras de segurança da informação e a legislação específica.
	4.3. Incentivar a adoção de recursos e de procedimentos voltados para a segurança cibernética nas infraestruturas críticas.	4.3.1. Estimular os responsáveis pelas infraestruturas críticas a ampliarem seus investimentos em recursos cada vez mais avançados de segurança cibernética. 4.3.2. Orientar as infraestruturas críticas a observarem a Estratégia Nacional de Segurança Cibernética, principalmente o disposto no item 2.3.5 do Anexo ao Decreto nº 10.222, de 2020.

6. DISPOSIÇÕES FINAIS

Elemento central para a implementação da PNSIC, a Ensic define quais são as principais ações a serem adotadas no sentido de assegurar a integridade da prestação de serviços indispensáveis ao Estado e à sociedade brasileira.

Para tanto, estabelece os princípios para a atividade de segurança de infraestruturas críticas e identifica os desafios a serem enfrentados, os eixos estruturantes para a efetividade da atividade e os objetivos e iniciativas estratégicas que orientarão a elaboração do Plano Nacional de Segurança de Infraestruturas Críticas, a fase executiva da implementação da Política.

A partir desse núcleo de prioridades, ficam evidenciados o percurso a ser seguido e as dificuldades que poderão ser encontradas na efetivação das ações a serem adotadas.

Assim, para dar cumprimento aos objetivos estratégicos estabelecidos pela Ensic, diversos entes envolvidos com a segurança de infraestruturas críticas deverão formular ações que serão consolidadas no Plano Nacional de Segurança de Infraestruturas Críticas.