Uso do Framework NIST CSF e Community Profiles na Proteção Setorial das Infraestruturas Críticas

Ernesto Marcos Silveira[1], **Éder Souza Gualberto**[1]

[1]Programa de Pós-Graduação em engenharia Elétrica – Universidade de Brasília (UNB)

ernesto.silveira@aluno.unb.br, eder.gualberto@redes.unb.br

Abstract. *Sectoral protection of Critical Infrastructure against cyberattacks is a major concern for the Brazilian government. The current regulatory framework assigns numerous responsibilities to those responsible for these sectors, but few tools are available for effective cyber risk management at the sectoral level. This article addresses this issue, proposing the use of the NIST Cybersecurity Framework (NIST CSF) and its Community Profiles to establish criteria and monitor security in entities responsible for Critical Infrastructure.*

Resumo. *A proteção setorial das Infraestruturas Críticas contra ataques cibernéticos é uma grande preocupação do Estado brasileiro. O arcabouço normativo atual estabelece muitas responsabilidades a aqueles responsáveis por estes setores, porém poucas são as ferramentas disponíveis para o gerenciamento eficaz dos riscos cibernéticos no nível setorial. Este artigo aborda essa questão, propondo o uso do NIST Cybersecurity Framework (NIST CSF) e seus Community Profiles para estabelecer critérios e monitorar a segurança das entidades responsáveis pelas Infraestruturas Críticas.*

1. Introdução

A preocupação com a segurança das infraestruturas críticas ganhou maior relevância no cenário internacional após os atentados terroristas de setembro de 2001, nos Estados Unidos. Na ocasião, aeronaves sequestradas foram utilizadas como armas contra alvos estratégicos, resultando em milhares de mortes e expressivos prejuízos econômicos e sociais [Estados Unidos 2001]. O episódio revelou a vulnerabilidade das infraestruturas estratégicas e impulsionou uma agenda global voltada à sua proteção.

No Brasil, esse debate começou a ganhar forma em 2006, quando uma facção criminosa coordenou ataques a estruturas públicas em retaliàção transferência de presos para unidades de segurança máxima. O episódio evidenciou fragilidades no aparato nacional e reforçou a necessidade de políticas voltadas à proteção de ativos e serviços essenciais [BRASIL 2020a].

Em 2008, o tema consolidou-se com a criação do Grupo de Trabalho de Segurança das Infraestruturas Críticas (GT-SIC), instituído pela Portaria nº 2/2008 do Gabinete de Segurança Institucional. Nesse momento, foram reconhecidos como setores críticos os de energia, águas, telecomunicações, transportes e finanças [BRASIL 2008], posteriormente ampliados para incluir os setores de Defesa, Biossegurança e Governo Digital.

O marco normativo mais significativo ocorreu em 2018, com a promulgação do Decreto nº 9.573, que instituiu a Política Nacional de Segurança das Infraestruturas

Críticas (PNSIC) [BRASIL 2018]. Nos anos seguintes, novos normativos reforçaram a importância da proteção desses ativos: em 2020, foram aprovadas a Estratégia Nacional de Segurança das Infraestruturas Críticas [BRASIL 2020b] e a Estratégia Nacional de Cibersegurança [BRASIL 2020a], que estabeleceram diretrizes e ações específicas para a segurança digital. Como desdobramento da publicação dessas estratégias, em 2021, foi editado o Decreto nº 10.748, que criou a Rede Federal de Gestão de Incidentes Cibernéticos (REGIC) e atribuiu responsabilidades setoriais de segurança cibernética às Agências Reguladoras, ao Banco Central e à Comissão de Valores Mobiliários - CVM [BRASIL 2021].

Mais recentemente, em 2025, a Estratégia Nacional de Cibersegurança foi atualizada pelo Decreto nº 12.573, ampliando a ênfase na proteção cibernética das infraestruturas críticas. A atualização reforçou a necessidade de uma abordagem setorial e introduziu de forma explícita a gestão de riscos cibernéticos por setor, consolidando a perspectiva de governança integrada entre setores estratégicos [BRASIL 2025].

No plano internacional, uma das principais iniciativas nesse campo foi o desenvolvimento do NIST Cybersecurity Framework (NIST CSF) pelo National Institute of Standards and Technology (NIST), a pedido do governo norte-americano. Publicado em sua versão 1.0 em 2014, o documento ofereceu aos operadores de infraestruturas críticas uma estrutura de apoio para a gestão de riscos cibernéticos, com foco essencialmente operacional [NIST 2014] Posteriormente, em 2024, foi lançada a versão 2.0, que ampliou a aplicabilidade do framework para além das infraestruturas críticas e incorporou aspectos de governança [NIST 2024].

Nesse contexto, caracterizado pela crescente interdependência entre setores e pela necessidade de fortalecimento da segurança cibernética, o objetivo geral deste artigo é analisar a aplicação do NIST Cybersecurity Framework (NIST CSF) — em especial de seus Community Profiles — como instrumento para a estruturação e o monitoramento setorial da segurança cibernética em setores críticos, por meio da adaptação do NIST CSF às necessidades de proteção cibernética dos setores de infraestruturas críticas, considerando as características do contexto brasileiro.

Para o alcance desse objetivo geral, estabelecem-se os seguintes objetivos específicos:

1. Revisar alguns conceitos fundamentais sobre infraestruturas críticas, com vistas a compreender o que são os ativos críticos, suas características e os riscos associados à sua operação;
2. Descrever a estrutura e os componentes do NIST CSF, examinando sua aplicabilidade à segurança cibernética das infraestruturas críticas;
3. Analisar o contexto setorial da segurança cibernética no Brasil, considerando o papel dos reguladores e coordenadores setoriais;
4. Propor uma adaptação do ciclo de implantação do NIST CSF, visando sua adequação ao contexto dos setores de infraestruturas críticas, incorporando atividades relacionadas a supervisão, coordenação e ao monitoramento setorial da segurança cibernética.

O restante deste artigo está organizado nas seguintes seções: a próxima seção apresenta uma discussão conceitual sobre infraestruturas críticas, com ênfase na identificação

de serviços essenciais, ativos críticos e na análise de riscos. Em seguida, descreve-se a estrutura do NIST CSF, com considerações sobre sua aplicabilidade à segurança cibernética das infraestruturas críticas. Por fim, discute-se o contexto setorial da segurança cibernética nas infraestruturas críticas brasileiras, no qual se propõe um ciclo de implantação e avaliação de segurança cibernética fundamentado no NIST CSF e caracterizado pelas atividades conjuntas dos operadores de infraestruturas críticas e dos responsáveis setoriais, como reguladores ou coordenadores.

2. As Infraestruturas Críticas

Definir o que é uma infraestrutura crítica pode parecer simples em um primeiro momento, mas trata-se de um conceito complexo e dependente do contexto de cada país, sua cultura e prioridades nacionais. De modo geral, o termo refere-se a estruturas, serviços e ativos que sustentam o funcionamento essencial da sociedade.

Na União Europeia, infraestruturas críticas são definidas como ativos necessários para a provisão de serviços fundamentais, como saúde pública, economia, segurança e meio ambiente [UNIÃO EUROPÉIA 2022]. No Reino Unido, a ênfase recai sobre ativos cuja perda ou comprometimento pode afetar serviços essenciais, resultando em perdas de vidas humanas, danos econômicos e sociais, ou ainda comprometer a segurança nacional [NPSA 2025]. Já no Brasil, conforme a Política Nacional de Segurança das Infraestruturas Críticas (PNSIC), são aquelas cuja interrupção ou destruição causa grave impacto social, econômico, ambiental, político, internacional e de segurança do Estado e da sociedade [BRASIL 2018].

Apesar das variações, essas definições compartilham elementos comuns, dos quais emergem algumas características centrais das Infraestruturas Críticas:

- **Essencialidade**: são indispensáveis para o funcionamento da sociedade.
- **Potencial Impacto**: sua falha gera consequências significativas.
- **Necessidade de Resiliência**: devem suportar falhas e ataques, mantendo continuidade da operação.
- **Dificuldade de Substituição**: não podem ser facilmente substituídas ou replicadas.
- **Vulnerabilidade**: apresentam pontos frágeis que precisam ser protegidos.
- **Interdependência**: funcionam em rede, onde falhas em um setor podem desencadear efeitos em outros.

Essa última característica é particularmente enfatizada em pesquisas recentes, [Kure and Islam 2019] destacam como vulnerabilidades podem se propagar em efeito cascata entre setores interligados, ampliando os riscos, [Papamichael et al. 2024] cita que as Infraestruturas Críticas são sistemas complexos e interdependentes, onde uma potencial falha que se propaga entre as infraestruturas pode afetar toda a rede.

2.1. Serviços essenciais e ativos críticos

As infraestruturas não são críticas por si mesmas, mas pela função que desempenham ao fornecer serviços essenciais à sociedade. Portanto, a identificação de ativos críticos passa, primeiramente, pela definição desses serviços e de seu grau de importância. Um ativo será considerado crítico na medida em que sua indisponibilidade comprometer a manutenção de tais serviços [Federal Ministry of the Interior (Germany) 2009].

Essa identificação de ativos é uma etapa essencial que precede a identificação dos riscos, pois proporciona a priorização dos ativos com base em sua criticidade [da Silva et al. 2025].

Devemos considerar que a maior parte das infraestruturas críticas são monitoradas e controladas por sistemas de TIC com suas vulnerabilidades inerentes [Luiijf et al. 2003]. Estes ativos subjacentes devem ser considerados na avaliação de riscos dos ativos críticos. É fundamental, também, considerar a dependência de fornecedores e as dependências de estruturas de parceiros setoriais ou intersetoriais.

Os principais passos para a identificação de infraestruturas críticas são os seguintes:

1. **Definição de facilidades e serviços essenciais** – deve ser realizada em nível nacional ou setorial, considerando prioridades estratégicas.
2. **Identificação de ativos críticos** - listagem dos ativos que sustentam esses serviços e facilidades essenciais, avaliando sua relevância para a continuidade operacional.
3. **Identificação de ativos subjacentes** – recursos tecnológicos e de apoio que, embora indiretos, são indispensáveis.
4. **Análise na cadeia de suprimentos** – avaliação da dependência de fornecedores e impactos de possíveis interrupções.
5. **Dependências setoriais** – análise dos vínculos entre operadores de um mesmo setor.
6. **Dependências intersetoriais** - análise de setores-base, como energia e comunicações, que sustentam múltiplos outros setores.

Essa abordagem baseada em interdependências amplia a noção de criticidade, revelando vulnerabilidades que poderiam ser subestimadas em análises isoladas.

2.2. Análise de riscos

A análise de riscos em infraestruturas críticas tem como ponto de partida a identificação e priorização dos ativos críticos e suas interdependências. A partir dessa base, aplicam-se metodologias de gestão de riscos, que tradicionalmente envolvem as etapas de identificação, análise, avaliação, tratamento e monitoramento dos riscos.

A etapa de identificação de riscos consiste no mapeamento de vulnerabilidades e ameaças (naturais, acidentais, tecnológicas ou intencionais), levando em conta tanto os impactos diretos quanto os efeitos em cascata resultantes de interdependências entre setores.

A análise envolve a mensuração da probabilidade e do impacto de incidentes, considerando critérios como segurança humana, continuidade de serviços e danos econômicos. Modelos quantitativos e qualitativos podem ser empregados, incluindo matrizes de risco, simulações de cenários e análises de rede para estudar a propagação de falhas. [Kure and Islam 2019] ressaltam a relevância de métodos baseados em modelagem de sistemas interdependentes, que permitem prever como falhas em um ativo podem comprometer outros.

O tratamento de riscos envolve a implementação de medidas de mitigação, tais como o fortalecimento dos controles de segurança, a capacitação contínua de colabo-

radores e a gestão da segurança ao longo da cadeia de suprimentos. Em certos contextos, pode-se recorrer à transferência de riscos, por meio de mecanismos como seguros especializados. Contudo, no caso das infraestruturas críticas, essa estratégia apresenta limitações, pois os impactos decorrentes de incidentes podem transcender os limites organizacionais, afetando toda a sociedade e a própria segurança nacional [Johansmeyer 2024].

O monitoramento é essencial para assegurar a eficácia e a atualização contínua do processo de gestão de riscos. Envolve o acompanhamento sistemático de indicadores de desempenho dos controles de segurança, auditorias, testes de resiliência e exercícios de simulação de crises. O monitoramento também deve incluir a análise de eventos passados, de forma a alimentar o processo de melhoria contínua. A gestão de riscos deve ser dinâmica, iterativa e adaptável, especialmente em setores críticos sujeitos a ameaças emergentes [NIST 2024],

3. NIST CSF

Reconhecendo a crescente ameaça cibernética às Infraestruturas Críticas e os desafios associados à segurança nacional, o governo dos Estados Unidos da América publicou a Ordem Executiva nº 13.636 – "Improving Critical Infrastructure Cybersecurity", na qual destacou a necessidade de fortalecer a cibersegurança desses setores estratégicos e determinou a elaboração de um framework voltado à mitigação de riscos cibernéticos. [ESTADOS UNIDOS 2013].

O desenvolvimento do Framework foi atribuído ao National Institute of Standards and Technology (NIST), que deveria conduzir o processo em parceria com a indústria e a academia. O documento deveria ser de adoção voluntária, baseado em padrões e melhores práticas já consolidadas, e assegurar a preservação da privacidade e das liberdades civis [NIST 2014].

O framework foi criado seguindo as orientações da Ordem Executiva e com ampla participação da sociedade. Os seguintes objetivos oientaram sua criação: [NIST 2018a]

1. **Melhorar a segurança e a resiliência das infraestruturas críticas**, reconhecendo que o funcionamento confiável dessas infraestruturas é vital para a segurança nacional, para a economia e para o bem-estar público.
2. **Promover um ambiente cibernético que estimule eficiência, inovação e prosperidade econômica**, além de garantir segurança, privacidade, confidencialidade dos negócios e liberdades civis. Isto é, o Framework não deve tolher a inovação nem os direitos civis, mas incorporá-los como parte da política.
3. **Estabelecer uma estrutura voluntária** que possa ser adotada pelos proprietários e operadores de infraestruturas críticas de forma flexível, sem imposição regulatória direta, para que haja adesão maior e adaptação ao contexto específico de cada entidade.
4. **Alinhar política, negócios e tecnologia**: o Framework deveria servir como ponto de convergência entre decisões de gestão (governança), requisitos de negócio, operações de TI e técnicas de segurança, para que as medidas de cibersegurança sejam coerentes com os objetivos estratégicos das organizações.
5. **Facilitar comunicação e criar um entendimento comum sobre risco cibernético** entre entidades públicas, privadas, operadoras de infraestrutura

crítica, reguladores e fornecedores, estabelecendo uma linguagem compartilhada que favoreça melhores decisões, colaboração e o compartilhamento de informações sobre ameaças.

6. **fornecer orientação prática**: o Framework deveria incluir formatos ou mecanismos (categorias, subcategorias, perfis, níveis) que auxiliassem organizações a mapear sua situação atual, definir metas, priorizar ações, acompanhar progresso. Isto também inclui guias, referências informativas e exemplos ou práticas correntes.

A primeira versão do Framework foi publicada em 2014, sendo estruturada em três componentes principais: Core (Núcleo), Implementation Tiers (Níveis de Implementação) e Profiles (Perfis). O Núcleo estabelece cinco funções essenciais da segurança cibernética — Identificar, Proteger, Detectar, Responder e recuperar —, subdivididas em categorias e subcategorias. Os Níveis de Implementação fornecem um mecanismo de caracterização da postura organizacional frente aos riscos, permitindo avaliar a maturidade em cibersegurança, enquanto os Perfis possibilitam a adaptação do Framework às particularidades de cada organização [NIST 2014].

O objetivo inicial do Framework foi oferecer uma estrutura voltada à segurança operacional das infraestruturas críticas. Entretanto, com o lançamento da versão 2.0, em 2024, ampliou-se a aplicabilidade do modelo, tornando-o adequado a organizações de qualquer setor, porte ou nível de maturidade. [NIST 2024] Uma inovação relevante dessa versão foi a introdução de uma sexta função — a Governança, que reforça a integração da cibersegurança com a gestão estratégica das organizações.

3.1. Funções, Categorias e Subcategorias

O Núcleo (Core) do NIST Cybersecurity Framework (CSF) consiste em um conjunto de resultados de cibersegurança que podem ser utilizados pelas organizações para apoiar a gestão de riscos cibernéticos. Esses resultados estão organizados em três níveis hierárquicos: Funções, Categorias e Subcategorias. Essa estrutura não deve ser entendida como uma sequência prescritiva de ações, mas como um modelo de referência que orienta a definição de prioridades, o planejamento de medidas de segurança e a adaptação das práticas conforme o contexto específico de cada organização [NIST 2024].

No nível mais abrangente, encontram-se as Funções, que fornecem uma visão estruturada e de alto nível da postura organizacional em relação ao risco cibernético. Elas abrangem desde aspectos estratégicos — como a formulação de políticas, definição de responsabilidades e a implementação de mecanismos de supervisão — até aspectos operacionais, como a detecção, a resposta e a recuperação diante de incidentes de segurança [Bernardo et al. 2025].

Com a publicação da versão 2.0, em 2024, o Framework passou a contar com seis Funções: Governança, Identificar, Proteger, Detectar, Responder e Recuperar. A inclusão da função Governança representou um avanço significativo, pois ampliou a aplicabilidade do Framework ao integrar a cibersegurança à gestão estratégica e corporativa, vinculando-a à missão, aos objetivos de negócio, aos requisitos legais e setoriais e à gestão de riscos da cadeia de suprimentos. Dessa forma, o Framework deixou de ser apenas um guia de controles técnicos e operacionais, consolidando-se como um instrumento de governança, alinhamento estratégico e suporte à tomada de decisão em segurança cibernética [NIST 2024].

Essa evolução reforçou o papel do NIST CSF como uma referência flexível e adaptável para diferentes setores e portes organizacionais [Toussaint et al. 2024]. Esse aspecto é particularmente relevante para a proteção de infraestruturas críticas, nas quais a integração entre governança e operações de segurança é essencial. Além disso, essa integração será igualmente importante para alinhar a gestão de riscos cibernéticos com as exigências regulatórias e setoriais.

3.1.1. Função Governança

A função Governança busca estabelecer a cibersegurança como uma responsabilidade essencial da governança corporativa, devendo ser integrada à estratégia organizacional, à cultura institucional e aos processos de tomada de decisão [Edwards 2024].

Sua atuação compreende o estabelecimento, a comunicação e o monitoramento da estratégia de gestão de riscos cibernéticos, políticas, papéis e responsabilidades, além da supervisão do contexto organizacional e de relação com terceiros. Assegurando também a conformidade com o arcabouço legal e regulatório, bem como o suporte do nível executivo da organização, de modo a garantir que as decisões sejam tomadas no mais alto nível estratégico. Por seu caráter estruturante, trata-se de uma função central que orienta e direciona a implementação das demais funções de cibersegurança.

Essa função tem um papel fundamental na proteção setorial das infraestruturas críticas, pois facilita o alinhamento dos objetivos organizacionais com o contexto e as exigências de segurança.

A função Governança tem um papel fundamental na boa condução da proteção cibernética das Infraestruturas Críticas, pois facilita a adequação entre os objetivos organizacionais e as exigências de segurança setoriais, exigindo que a alta direção da entidade trabalhe não apenas com uma visão interna de risco, mas também com consciência das interdependências externas, das obrigações regulatórias e do impacto social dos serviços prestados.

Categoria: Contexto Organizacional

Esta categoria define a direção a ser seguida pela organização na segurança cibernética, envolve compreender a missão, os objetivos, as partes interessadas, as dependências e o ambiente legal e regulatório em que a organização opera.

O contexto setorial em que a organização opera deve ser considerado, pois o ambiente das infraestruturas críticas é, muitas vezes, fortemente regulado, com partes interessadas muito preocupadas com a segurança [Markopoulou and Papakonstantinou 2021]. O Governo e os órgãos de controle setorial realizam monitoramento constante para garantir a continuidade da operação das infraestruturas críticas. As Organizações que possuem estruturas dependentes também demonstrarão preocupação.

Categoria: Estratégia de Gestão de Riscos

A categoria Gestão Estratégica de Riscos orienta a definição dos objetivos de gerenciamento de riscos, bem como das declarações de apetite e tolerância a riscos. Inclui a incorporação dos resultados da gestão de riscos cibernéticos aos processos cor-

porativos de decisão, assegurando coerência entre as estratégias organizacionais e operacionais. Também prevê o estabelecimento de métodos padronizados de identificação, categorização e priorização de riscos.

A gestão de riscos organizacional deve seguir orientações e critérios de risco estabelecidos setorialmente, evitando suportar, nas infraestruturas críticas, riscos superiores aos determinados pelas normas e regulamentos.

Determinados níveis de risco podem ser aceitáveis para a organização, no entanto, por questões de interdependências com estruturas de outras organizações do setor ou de outros setores [Korkali et al. 2017], o apetite de risco pode ter que ser moderado.

Categoria: Papéis, Responsabilidades e Autoridades

As funções de governança em segurança cibernética devem estar formalmente definidas, comunicadas e compreendidas por toda a organização. A alta gestão deve ser responsável pelos riscos cibernéticos, assegurando adequada alocação de recursos e integração das práticas de segurança ao ciclo de atividades da organização.

Nos setores de infraestruturas críticas, deve-se ter clareza das responsabilidades em segurança, pois, em casos de incidentes ou auditorias, são esses os profissionais com os quais os órgãos governamentais ou regulatórios buscarão informações.

Categoria: Política

Uma política de segurança cibernética deve ser formalmente estabelecida e mantida. Esta precisa estar alinhada com o contexto do negócio, com a estratégia de riscos e prioridades da organização.

A política de segurança cibernética da organização deve seguir as diretrizes setoriais para a proteção das infraestruturas críticas, implantando as medidas definidas e mantendo-se em conformidade com os limites estabelecidos. Garantias de continuidade da operação devem ser previstas quando as infraestruturas críticas estiverem envolvidas.

Categoria: Supervisão

A organização monitora, supervisiona e revisa a estratégia de cibersegurança, as políticas e as práticas para garantir sua eficácia contínua.

Deve haver uma supervisão interna da eficácia das medidas de segurança cibernética aplicadas às infraestruturas críticas, mantendo indicadores de desempenho em conformidade com requisitos estabelecidos setorialmente.

A supervisão interna garantirá a conformidade quando a supervisão setorial realizar auditorias ou requisitar relatórios.

Categoria: Gestão de Riscos da Cadeia de Suprimentos

Um programa de gestão de riscos de segurança cibernética na cadeia de suprimentos, que Identifica, avalia e gerencia os riscos de segurança relacionados a terceiros, parceiros e fornecedores deve ser implantado. Este programa deve ser abrangente e adaptado à complexa rede de cadeias de suprimento modernas [Edwards 2024].

A cadeia de suprimentos é um importante vetor de ameaças à segurança das infraestruturas críticas [Aarland and Gjøsæter 2022], a organização deve considerar os

riscos e vulnerabilidades possivelmente associados aos seus parceiros e fornecedores [Miranda Zottmann et al. 2023], e que possam comprometer a segurança das infraestruturas críticas sob sua responsabilidade.

3.1.2. Função Identificar

A função Identificar tem como finalidade desenvolver uma compreensão organizacional que permita gerenciar o risco cibernético para sistemas, pessoas, ativos, dados e capacidades. Antes de decidir o que proteger e como proteger, a organização precisa saber o que possui, onde isso está, quais são as suas dependências e exigências de negócio, e quais riscos e vulnerabilidades afetam esses elementos.

As Infraestruturas Críticas devem receber uma atenção especial, pois não são ativos comuns. Questões de essencialidade, interdependência e criticidade devem ser consideradas, com base nas normas e procedimentos definidos legalmente para o setor.

Categoria: Gerenciamento de Ativos

Os ativos organizacionais — incluindo hardware, software, dados, estruturas físicas, serviços e pessoal — devem ser identificados, catalogados e continuamente gerenciados. Para isso, a organização deve manter um inventário atualizado e detalhado dos ativos sob sua responsabilidade, com destaque para aqueles que compõem as infraestruturas críticas.

Esse inventário é essencial para a atribuição clara de responsabilidades quanto à proteção dos ativos e para o atendimento À conformidade com os normativos legais e regulatórios aplicáveis a tais estruturas [NIST 2018b].

Os ativos críticos devem ser priorizados conforme sua relevância para a continuidade dos serviços essenciais e o impacto potencial decorrente de sua indisponibilidade ou comprometimento [Kure and Islam 2019].

A etapa de gerenciamento de ativos deve ainda incluir a identificação e análise das interdependências entre os diversos componentes do sistema, uma vez que vulnerabilidades em um ativo podem repercutir sobre outros de forma direta ou indireta [Kure and Islam 2019]. Essa análise deve considerar também dependências externas, abrangendo relações intra e intersetoriais.

Categoria: Avaliação de Riscos

A categoria Avaliação de Riscos é responsável por identificar, analisar e avaliar riscos cibernéticos que podem impactar a organização. Isso envolve compreender as ameaças mais prováveis, as vulnerabilidades existentes nos ativos e processos, e o impacto potencial desses eventos sobre a missão, as operações, a reputação e a segurança da organização.

Essa categoria fornece a base para decisões de priorização — ou seja, ajuda a definir onde investir recursos de segurança, quais controles adotar e como alinhar os esforços de proteção ao apetite e à tolerância ao risco do negócio.

Operadores de infraestruturas críticas precisam conhecer o provável impacto que interrupções em seus ativos podem causar, assim como, o impacto que interrupções em

estruturas de terceiros podem causar em suas estruturas, para que possam desenvolver medidas corretas de mitigação [Bloomfield et al. 2017].

Categoria: Melhoria

O objetivo central dessa categoria é garantir que a organização não fique estagnada em sua postura de risco cibernético, mas que continuamente busque avaliar seus processos, testar suas defesas, aprender com falhas, incidentes, exercícios e experiências do cotidiano, para implementar melhorias que reforcem sua resiliência.

As ameaças cibernéticas estão cada vez mais sofisticadas; portanto, a melhoria contínua é essencial para fortalecer a resiliência e garantir a sobrevivência da organização [Edwards 2024].

A melhoria da segurança nas infraestruturas críticas deve ser planejada em conjunto com as partes interessadas, considerando as interdependências intra e inter-setoriais. Exercícios setoriais simulados de cibersegurança são uma excelente forma de testar a efetividade de controles frente às necessidades impostas pela dependência de outros atores.

3.1.3. Função Proteger

A organização deve implementar controles apropriados para mitigar os riscos identificados, de modo a garantir a continuidade das operações e a entrega ininterrupta de serviços essenciais. As medidas devem combinar controles técnicos, administrativos e físicos, sendo priorizadas segundo a avaliação de risco organizacional e setorial [NIST 2024].

Os ativos críticos — identificados e priorizados — devem receber atenção especial na seleção e na intensidade dos controles; a proteção deve ser proporcional à criticidade operacional do ativo, ao impacto potencial de sua indisponibilidade e ao seu papel nas dependências intra e intersetoriais [Rinaldi et al. 2001].

É imprescindível estabelecer salvaguardas específicas para a cadeia de suprimentos e para as dependências externas. Controles contratuais, requisitos de segurança para fornecedores, verificação de integridade de componentes, avaliação contínua de fornecedores e mecanismos conjuntos de monitoração e resposta são práticas recomendadas para reduzir o risco introduzido por terceiros [Moreira et al. 2021].

Categoria: Gerenciamento de Identidade, Autenticação e Controle de Acesso

Uma gestão de identidades e credenciais deve estar estabelecida, para salvaguardar ativos e usuários e proteger contra acesso não autorizado.

Para os ativos críticos, devem ser mantidas regras de acesso mais rigorosas. Técnicas modernas, como autenticação multifatorial e políticas de privilégio mínimo, podem proporcionar melhores resultados.

Categoria: Conscientização e Treinamento

O fator humano é fundamental para a eficácia da segurança da informação, uma vez que grande parte dos incidentes ocorre por falhas humanas [Safianu et al. 2016]. Questões de segurança relacionadas ao fator humano devem ser tratadas por meio de um robusto programa de treinamento e conscientização.

Colaboradores que atuam diretamente com infraestruturas críticas devem ter os conhecimentos e habilidades necessárias para garantir a operação segura destes ativos, bem como, para mitigar impactos diante da ocorrência de incidentes.

Categoria: Segurança de dados

Os dados mantidos pela organização devem ser protegidos por políticas e controles que preservem a confidencialidade, a integridade e a disponibilidade ao longo de todo o seu ciclo de vida [NIST 2024]. Essa proteção requer a implementação de: classificação e inventário de dados, políticas de retenção e descarte, controles de acesso e autenticação robustos, mecanismos de detecção de alteração e planos de continuidade e recuperação que garantam disponibilidade mesmo sob ataque ou falha operacional.

Dados relacionados a infraestruturas críticas devem receber tratamento prioritário: sua identificação, classificação e aplicação de controles devem ser orientadas pela criticidade do dado para a continuidade dos serviços essenciais e pelo potencial impacto social ou de segurança nacional em caso de comprometimento.

Categoria: Segurança de Plataforma

A organização deve estabelecer um gerenciamento de configuração, que englobe hardware, software e estruturas de terceiros (p.ex computação em nuvem), garantindo que todos os ativos da infraestrutura de tecnologia da informação estejam gerenciados e protegidos.

Ativos de tecnologia da informação que são subjacentes às infraestruturas críticas, quando não sejam eles mesmos infraestruturas críticas, devem ter prioridade na proteção, de acordo com sua importância para o desenvolvimento dos serviços essenciais.

Categoria: Resiliência da Infraestrutura Tecnológica

Um plano que garanta a resiliência da infraestrutura tecnológica da organização deve ser implementado, para garantir a continuidade da operação mesmo diante de ameaças e falhas. Deve haver um planejamento estratégico que contenha aspectos como infraestrutura escalável, balanceamento de carga entre estruturas e mecanismos de redundância.

A continuidade da operação das infraestruturas críticas deve ser o ponto central do plano de resiliência, garantindo o menor impacto possível na prestação dos serviços essenciais.

3.1.4. Função Detectar

A função Detectar busca identificar prontamente eventos cibernéticos adversos. Nenhuma proteção é totalmente infalível, portanto, deve-se manter um monitoramento contínuo da segurança, para que se possam detectar anomalias, indicadores de comprometimento e comportamentos fora do normal, permitindo a análise e a adoção de medidas de proteção ou remediação.

O monitoramento das infraestruturas críticas deve ser pautado pelo grau de criticidade dos ativos e pelo potencial impacto da falha desses elementos nos serviços essenciais que deles dependem.

Categoria: Monitoramento Contínuo

O cenário da segurança digital é vasto e complexo, assim, o monitoramento meticuloso de redes, ambientes, recursos e pessoal constitui um pilar fundamental da defesa [Edwards 2024]. É crucial implementar sistemas de detecção de intrusão em tempo real, técnicas de detecção de anomalias em tráfego de dados e análise comportamental.

Os ataques cibernéticos, em muitos casos, objetivam prioritariamente invadir ativos críticos, pois estes são mais importantes e sua falha ou indisponibilidade causa impactos maiores. O monitoramento desses ativos torna-se, portanto, ainda mais essencial.

Categoria: Análise de eventos Adversos

A organização deve aprimorar sua postura de segurança por meio da análise dos incidentes ocorridos, aplicando as lições aprendidas para a melhoria dos procedimentos de segurança.

O compartilhamento de informações nos setores de infraestruturas críticas sobre eventos adversos pode trazer benefícios significativos aos operadores de infraestruturas críticas que possuem interdependências, fortalecendo a postura de segurança global do setor.

3.1.5. Função Responder

Um plano de resposta a incidentes deve ser implantado. A organização deve manter uma abordagem estruturada e planejada capaz de conter impactos de incidentes, erradicar as ameaças e recuperar a normalidade das operações.

Infraestruturas críticas envolvidas em incidentes devem ter prioridade na recuperação. Um plano de comunicação com partes interessadas que operem infraestruturas críticas dependentes deve ser acionado, e as autoridades devem ser notificadas quando necessário.

Categoria: Gerenciamento de Incidentes

O tratamento de incidentes deve ser executado de acordo com um plano de resposta a incidentes previamente definido, com procedimentos e responsabilidades claramente estabelecidos.

Em um contexto setorial de infraestruturas críticas, o plano de resposta a incidentes pode precisar ser executado em colaboração com terceiros interessados, que possuam infraestruturas críticas interligadas, com autoridades setoriais e, eventualmente, com fornecedores de ativos dos quais as infraestruturas críticas sejam dependentes.

Categoria: Análise de incidentes

A análise de incidentes deve buscar identificar a causa-raiz dos eventos e compreender os fatores subjacentes que contribuíram para sua ocorrência. Entre seus principais objetivos estão fornecer subsídios para a correção de falhas, aprimorar processos internos e fortalecer a postura de segurança da organização, prevenindo recorrências.

No contexto de infraestruturas críticas, a análise de incidentes assume papel ainda mais relevante. Incidentes cibernéticos ou operacionais nesses ambientes podem impactar diretamente a continuidade de serviços essenciais, ocasionando prejuízos significativos a terceiros e à sociedade. Por isso, a análise deve ser abrangente e detalhada, de modo a identificar não apenas as causas imediatas, mas também os impactos na cadeia de partes envolvidas, incluindo fornecedores, operadores e usuários finais.

Além disso, a condução da análise deve considerar o atendimento a obrigações regulatórias e normativas, que frequentemente exigem a divulgação de informações precisas e tempestivas sobre a natureza e as consequências dos incidentes. As informações obtidas também podem subsidiar comunicados públicos e orientar decisões estratégicas durante a resposta e recuperação.

Uma análise de incidentes bem estruturada contribui para uma recuperação mais rápida e eficaz dos serviços afetados, reforçando a resiliência operacional das Infraestruturas Críticas.

Categoria: Comunicação e relatórios de respostas a incidentes

A comunicação de incidentes para partes interessadas — como detentores de estruturas interligadas, autoridades competentes, fornecedores e parceiros — deve ser clara, precisa e tempestiva. A divulgação rápida de informações sobre incidentes pode reduzir impactos adversos em organizações que mantêm dependências com a infraestrutura afetada, bem como mitigar a propagação de ameaças para entidades com arquiteturas ou sistemas similares.

Nos setores de infraestruturas críticas, as obrigações legais e regulatórias relativas à comunicação e ao reporte de incidentes são geralmente robustas e exigem observância rigorosa. Isso inclui não apenas notificações obrigatórias a reguladores, mas também relatórios formais com conteúdo mínimo exigido por lei, prazos bem definidos e documentação transparente do incidente, dos impactos e das ações corretivas adotadas.

Categoria: Mitigação de incidentes

Incidentes devem ser contidos e erradicados de forma célere, de modo que se minimize a existência de vetores de propagação ou comprometimento adicional. É imperativo que sejam definidas estratégias robustas para limitar a disseminação dos incidentes, tanto internamente quanto para sistemas externos ou entidades dependentes.

Em infraestruturas críticas, essas estratégias de mitigação devem abranger ações destinadas a isolar componentes, dispositivos ou redes afetadas, evitando que o incidente comprometa outros setores ou estruturas operacionais interligadas.

Deve-se realizar avaliação das vulnerabilidades descobertas durante o incidente, com mitigação imediata sempre que possível. ou documentação formal como risco aceitável quando a mitigação total não for viável no curto prazo.

A mitigação deve sustentar a resiliência operacional das infraestruturas críticas, assegurar o cumprimento de exigências regulatórias e reduzir o risco de propagação para terceiros.

3.1.6. Função Recuperar

A função Recuperar concentra-se no desenvolvimento e implementação de atividades de resiliência operacional, destinadas a reestabelecer capacidades ou serviços prejudicados por incidentes cibernéticos, garantindo o retorno às operações normais com o menor impacto possível. Essa função abrange o planejamento de recuperação, a melhoria contínua baseada em lições aprendidas, e a comunicação eficaz, tanto interna quanto externa, de modo que todos os envolvidos compreendam o progresso e o estado das ações de recuperação.

No contexto das Infraestruturas Críticas, a função Recuperar possui caráter estratégico. A interrupção de serviços essenciais — como energia elétrica, telecomunicações, abastecimento de água, transporte ou saúde — pode produzir efeitos diretos sobre a segurança pública e o bem-estar social. Dessa forma, os ativos críticos devem ser priorizados nos planos de recuperação, garantindo que as atividades vitais sejam restabelecidas com a maior brevidade possível. Os procedimentos de recuperação devem ser formalmente definidos, testados periodicamente e atualizados em consonância com as mudanças tecnológicas, operacionais e regulatórias.

Categoria: Execução do plano de recuperação de incidentes

A execução do plano de recuperação de incidentes requer a aplicação criteriosa das ações previamente definidas para restabelecer as operações impactadas por um incidente cibernético, restaurando não apenas sistemas técnicos, mas também assegurando a integridade, a confidencialidade e a disponibilidade dos ativos afetados. Deve-se assegurar que todas as ações de recuperação sejam conduzidas de acordo com os critérios previamente estabelecidos no plano. Isso inclui verificar a integridade dos backups e dos ativos de restauração antes de sua utilização, restaurar sistemas somente após confirmar que os dados e componentes envolvidos estão livres de comprometimentos, e confirmar que as operações retomadas satisfazem os níveis operacionais normais e seguros.

Nas infraestruturas críticas, o plano de recuperação deve contemplar todos os elementos indispensáveis à retomada dos serviços essenciais, minimizando o tempo de indisponibilidade e evitando interrupções prolongadas.

Adicionalmente, a execução do plano de recuperação em ambientes com interdependências setoriais requer coordenação entre organizações afetadas e seus parceiros operacionais. Devem existir mecanismos formais de comunicação e sincronização que viabilizem a recuperação conjunta e harmonizada, prevenindo efeitos em cascata decorrentes de falhas interconectadas.

Categoria: Comunicação de recuperação de incidentes

A comunicação do processo de recuperação é elemento fundamental para o restabelecimento da confiança institucional e da transparência operacional. As informações devem ser transmitidas de forma clara, precisa e tempestiva, refletindo o progresso real das atividades, as etapas concluídas, os obstáculos enfrentados e as ações corretivas em curso.

No caso das infraestruturas críticas, é imprescindível que a comunicação da recuperação seja dirigida também às autoridades competentes, bem como às entidades

interdependentes — como fornecedores, operadores e parceiros com infraestruturas interligadas. Tais comunicações permitem que as partes interessadas avaliem o estado de normalização dos serviços e ajustem suas próprias operações ou medidas de contingência.

Sempre que aplicável, e conforme exigências legais ou regulatórias, deve haver comunicação pública estruturada sobre o restabelecimento das operações. Essa transparência contribui para a proteção da reputação institucional, evidencia o comprometimento com a conformidade regulatória e reforça a confiança dos usuários e do público na capacidade da organização de se recuperar e manter a continuidade da prestação dos serviços essenciais.

3.1.7. Subcategorias

As subcategorias representam o nível mais refinado do núcleo do NIST CSF. Cada subcategoria expressa um resultado específico, que contribui diretamente para o fortalecimento da postura de risco da organização. Elas funcionam como metas de resultado, que podem ser traduzidas em ações concretas e mensuráveis, possibilitando que a organização avalie seu estado atual e defina um plano de melhoria contínua.

No NIST CSF 2.0, o framework compõe-se de 106 subcategorias, distribuídas nas 23 categorias apresentadas anteriormente. Essas subcategorias são orientadas a resultados, mas não prescrevem exatamente como as organizações devem alcançá-las, cabendo à organização escolher ou adaptar controles, processos e ferramentas que façam sentido em seu contexto.

Para operacionalizar as subcategorias, pode-se recorrer às referências informativas (Informative References) que o NIST vincula a cada subcategoria. Essas referências apontam, por exemplo, para controles do ISO/IEC 27001, NIST SP 800-53, CIS Controls ou outras bibliotecas de controles reconhecidas. Desse modo, uma subcategoria pode ser materializada por meio de um ou mais controles desses padrões, Além disso, pode-se fazer uso de outros conjuntos de controles, que sejam compatíveis com o NIST CSF.

3.2. Níveis de Implementação

O NIST CSF adota uma abordagem estruturada para avaliar e aprimorar a gestão de riscos cibernéticos nas organizações, utilizando os Níveis de Implementação (Implementation Tiers). Esses níveis refletem a maturidade e são uma ferramenta para entender o grau de sofisticação e integração das práticas de governança e gestão de riscos cibernéticos dentro da organização [Edwards 2024].. Eles auxiliam a contextualizar como a organização percebe os riscos cibernéticos e os processos estabelecidos para gerenciá-los.

Os quatro níveis de implementação do NIST CSF são:

- **Nível 1 – Parcial (Partial)**: Neste nível, as práticas de gestão de riscos cibernéticos são reativas e ad hoc, com pouca ou nenhuma coordenação entre as partes da organização. A organização possui uma compreensão limitada dos riscos cibernéticos e as respostas a incidentes são improvisadas.
- **Nível 2 – Informado por Risco (Risk Informed)**: As práticas de gestão de riscos são mais estruturadas, com alguma documentação e procedimentos definidos. A organização começa a integrar a gestão de riscos cibernéticos em seus processos, embora de forma ainda limitada.

- **Nível 3 – Repetível (Repeatable)**: As práticas de gestão de riscos são bem definidas, documentadas e implementadas de forma consistente em toda a organização. Há uma abordagem proativa para a gestão de riscos, com processos estabelecidos para identificar, avaliar e mitigar riscos cibernéticos.
- **Nível 4 – Adaptativo (Adaptive)**: A organização possui uma abordagem ágil e resiliente para a gestão de riscos cibernéticos, adaptando-se continuamente às mudanças no ambiente de ameaças. As práticas são continuamente avaliadas e aprimoradas, com uma forte integração entre a gestão de riscos cibernéticos e os objetivos estratégicos da organização.

Esses níveis de implementação fornecem um contexto para como as decisões de risco cibernético são tomadas e implementadas dentro da organização, refletindo o grau de formalização, integração e adaptação das práticas de gestão de riscos cibernéticos. Eles ajudam a organização a avaliar sua posição atual em relação à gestão de riscos cibernéticos e a identificar áreas para melhoria contínua [NIST 2024].

Ao aplicar os níveis de implementação do NIST CSF, uma organização pode mapear seu perfil de risco atual e desejado, alinhando suas práticas de gestão de riscos cibernéticos com seus objetivos estratégicos e requisitos regulatórios. Isso facilita a comunicação interna e externa sobre a postura de segurança cibernética da organização e apoia o desenvolvimento de um plano de ação para aprimorar continuamente suas práticas de gestão de riscos cibernéticos.

3.3. Perfis

Os Perfis (Profiles) no NIST CSF ajudam a dar visibilidade a postura de segurança cibernética de uma organização. Eles refletem os resultados previstos no Núcleo do NIST CSF, bem como o nível de implementação correspondente, e permitem que a organização faça uma avaliação concreta de onde está (AS IS) e para onde quer ir (TO BE).

O Perfil Atual (ou organizacional) reflete os resultados de segurança cibernética que a organização já alcançou. Envolve uma análise dos controles, das práticas e das capacidades existentes, confrontando o que o Núcleo do CSF define como meta com aquilo que realmente está implantado. O Perfil Alvo (Target Profile) define o patamar desejado de segurança cibernética, levando em conta fatores como os objetivos em segurança da organização, as exigências regulatórias e legais e o ambiente de ameaças.

A comparação entre o Perfil Atual e o Perfil Alvo possibilita identificar lacunas de segurança, definir priorizações com base em risco e impacto, e estabelecer um plano de ação. Essa abordagem promove um ciclo de melhoria contínua, no qual avaliações periódicas permitem ajustar o Perfil Alvo ou reformular o plano de ação à medida que recursos, ameaças e requisitos mudam.

Em contextos de infraestruturas críticas, os Perfis permitem que se identifique quais ativos críticos devem estar seguros com maior urgência, quais práticas ou subcategorias requerem melhorias de implementação para atender a exigências regulatórias ou operacionais, e como articular ações com parceiros que possuam estruturas interdependentes ou com autoridades. Além disso, ao tornar explícitas as posturas de segurança atual e desejada, os Perfis permitem a comunicação eficiente sobre a segurança cibernética da organização.

3.3.1. Perfis da Comunidade (Community Profiles)

O conceito de Perfil da Comunidade foi introduzido na versão 2.0 do NIST CSF com o objetivo de estabelecer uma base comum de resultados e práticas de segurança cibernética voltadas a grupos de organizações que compartilham objetivos, riscos ou obrigações semelhantes. Uma de suas aplicações é o contexto setorial de infraestruturas críticas [Pascoe et al. 2024b]. Esses Perfis são elaborados para contextos específicos, refletindo as necessidades relativas a legislações, regulamentações setoriais e padrões técnicos comuns.

No contexto das infraestruturas críticas, a aplicação desses Perfis pode trazer vantagens estratégicas. Tais infraestruturas ultrapassam os interesses da entidade que as controla, sendo elementos estratégicos para o bom funcionamento da sociedade, da economia e da segurança nacional. Dessa forma, os limites aceitáveis de risco e as medidas de proteção necessárias não devem ser definidos exclusivamente pelos interesses da organização operadora, mas também devem refletir um conjunto de exigências legais e regulatórias.

Um Perfil da Comunidade pode ser desenvolvido para refletir essas necessidades legais e regulamentares, servindo como uma base de referência em segurança cibernética que oriente as organizações do setor.. A partir desse perfil, cada entidade pode desenvolver o seu Perfil-Alvo, ajustando os controles e capacidades de acordo com suas particularidades operacionais e nível de exposição ao risco desejado, alinhando sua estratégia de segurança às expectativas legais e regulatórias.

Além de orientar as organizações na definição de seus objetivos de segurança, os perfis da comunidade também podem ser utilizados por responsáveis setoriais para avaliar de forma comparativa a postura de risco das organizações sob sua tutela. Isso possibilita uma análise mais consistente das lacunas existentes, apoia auditorias e incentiva melhorias contínuas baseadas em parâmetros comuns, promovendo, assim, uma elevação setorial do nível de resiliência cibernética.

3.3.2. Ciclo de implementação dos Perfis do NIST CSF

O NIST CSF estabelece um processo para a implementação e uso dos perfis organizacionais, estruturado em cinco fases distintas: definição de escopo, coleta de informações, construção do perfil atual, análise de lacunas e elaboração do plano de ação e, por fim a implementação do plano de ação com a atualização do perfil organizacional [NIST 2024].

Na fase inicial, define-se o escopo de aplicação, identificando os ativos, processos, sistemas, interfaces e dependências que serão objeto de análise. Essa delimitação permite ajustar os recursos, estabelecer limites operacionais e fundamentar a integração das exigências normativas com os objetivos de negócio. Em seguida, procede-se à coleta de informações relevantes, tais como arquitetura de sistemas, fluxos de dados críticos, avaliações de risco, responsabilidades organizacionais e contexto externo de ameaças, com o objetivo de compreender o contexto operacional da organização e a sua exposição aos riscos de cibersegurança.

A terceira fase consiste na construção do Perfil Atual (Current Profile), que de-

screve os resultados de segurança cibernética que a organização já alcançou, em termos das funções, categorias e subcategorias do Núcleo do NIST CSF. A partir desse diagnóstico, na quarta fase, é realizada a Análise de Lacunas (gap analysis) entre o perfil atual e o perfil-alvo desejado (Target Profile). Com base nessa comparação, a organização estabelece um plano de ação, que define medidas para fechar as lacunas identificadas.

Na quinta e última fase do ciclo, ocorre a implementação do plano de ação por meio de controles gerenciais e técnicos, em que o perfil organizacional atua como uma baliza para rastrear o status da implementação. Os controles e riscos podem , então, ser monitorados por meio de indicadores de desempenho ou indicadores de risco [Pascoe et al. 2024a].

4. Proteção setorial das Infraestruturas Críticas

O Brasil possui um sólido arcabouço normativo voltado à proteção das Infraestruturas Críticas, estruturado a partir de três instrumentos centrais: a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC) e o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC).

A PNSIC, instituída pelo Decreto nº 9.573/2018, estabelece os princípios, conceitos e diretrizes gerais que orientam a atuação do Estado brasileiro na proteção das Infraestruturas críticas e dos serviços essenciais. Entre seus fundamentos, destacam-se a abordagem integrada de riscos, a cooperação entre entes públicos e privados, e o reconhecimento das interdependências entre setores críticos.

Complementando esse marco normativo, a ENSIC define os objetivos estratégicos e eixos estruturantes da política nacional. A Estratégia atua como um guia de médio e longo prazo para a implementação das ações de segurança, priorizando a prevenção de ameaças, o fortalecimento da resiliência, a resposta coordenada a incidentes e a rápida recuperação dos serviços essenciais. Também enfatiza a importância da governança multissetorial e da padronização de práticas.

Por sua vez, o PLANSIC detalha iniciativas estratégicas e metas específicas, além de atribuir responsabilidades setoriais a ministérios e órgãos federais, cabendo a cada setor de Infraestrutura Crítica (energia, comunicações, transportes, finanças, defesa etc.) a elaboração de planos setoriais de segurança. Entre suas diretrizes, o PLANSIC prevê o desenvolvimento de metodologias padronizadas para a identificação e classificação de infraestruturas críticas, a realização de análises de risco integradas, o compartilhamento de informações e a promoção de estudos sobre as interdependências entre infraestruturas.

Alguns setores também estabeleceram seus próprios normativos. No setor de telecomunicações, a Agência Nacional de Telecomunicações (Anatel) institui o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber). Esse regulamento exige das prestadoras políticas de segurança formalizadas, gestão de riscos, inventário de ativos críticos, planos de resposta a incidentes e avaliações de vulnerabilidade. De modo semelhante, no setor elétrico, a Resolução Normativa ANEEL nº 964/2021 obriga os agentes do setor a elaborar políticas de segurança cibernética, notificar incidentes de maior impacto e compartilhar informações.

Os normativos federais e setoriais incentivam a adoção de normas e padrões na-

cionais ou internacionais de boas práticas, porém sem impor ou sugerir um padrão específico. Os operadores de infraestruturas têm liberdade para implementar o padrão que melhor se adeque à sua realidade, desde que observem as diretrizes definidas pelos normativos.

No entanto, a adoção de um padrão de referência, como o NIST CSF, pode trazer inúmeros benefícios para a segurança cibernética setorial, tais como:

- **Estabelece uma linguagem comum** entre reguladores, operadores e órgãos governamentais, facilitando a comunicação e a cooperação intersetorial;
- **Define expectativas claras** quanto à postura de segurança e aos níveis de controle esperados;
- **Favorece a coordenação de segurança** e o alinhamento de prioridades entre organizações ou setores interdependentes;
- **Permite avaliação de maturidade** e melhor planejamento na evolução da segurança;
- **Fornece uma base para indicadores de desempenho**, fortalecendo a governança em segurança.

A integração entre o arcabouço normativo nacional e o NIST CSF pode trazer um avanço na postura de segurança cibernética dos setores de infraestruturas críticas, proporcionando maior previsibilidade regulatória, padronização e melhor capacidade de resposta coordenada a riscos e ameaças ao bom funcionamento dos serviços essenciais, garantindo maior segurança à sociedade.

4.1. Ciclo de proteção e avaliação setorial de segurança cibernéticas baseado no NIST CSF

Um dos objetivos do NIST CSF é auxiliar os operadores de infraestruturas críticas na identificação e desenvolvimento de diretrizes de risco de segurança cibernética [Moreira et al. 2021]. Ainda assim, a aplicação do ciclo de implementação do NIST CSF nos setores críticos requer adaptações. Para as organizações operadoras de infraestruturas críticas, é necessária a inclusão de uma fase preliminar de identificação, classificação e priorização dos ativos críticos, conforme discutido na seção 2. Essa etapa deve anteceder a fase de definição de escopo prevista pelo NIST CSF, servindo como base para direcionar os esforços de avaliação e implementação de controles de segurança cibernética.

Além do ciclo organizacional de implementação, deve existir um ciclo setorial de governança, conduzido por um responsável setorial (órgão regulador, autoridade competente ou entidade coordenadora). Esse responsável deve estabelecer diretrizes normativas e técnicas que orientem as organizações na implementação de seus controles de segurança, bem como definir mecanismos de avaliação e monitoramento dos resultados alcançados por essas entidades.

O ciclo setorial inicia-se com a definição do contexto setorial de segurança cibernética, que deve incluir políticas, legislações, regulamentações específicas e padrões técnicos aplicáveis. Esse contexto deve especificar os serviços essenciais do setor, classificados conforme sua criticidade e interdependências, permitindo que as organizações identifiquem as infraestruturas críticas sob sua responsabilidade e avaliem fatores relevantes de exposição aos riscos.

A partir desse contexto, o responsável setorial deve desenvolver um perfil setorial de segurança cibernética, que traduza a visão estratégica do setor em relação à segurança e resiliência, e estabelecer Perfis Comunitários (Community Profiles) que orientem as organizações na criação de seus perfis-alvo. Esses perfis devem refletir os níveis aceitáveis de risco, controle e mensuração esperados para o setor, conforme diretrizes regulatórias e políticas governamentais voltadas às Infraestruturas Críticas.

A Figura 1 apresenta o modelo proposto de implementação e avaliação setorial de segurança cibernética em operadores de infraestruturas críticas. O modelo é composto por dois ciclos interconectados — um conduzido pelo responsável setorial e outro pelas organizações operadoras — baseados no NIST CSF.

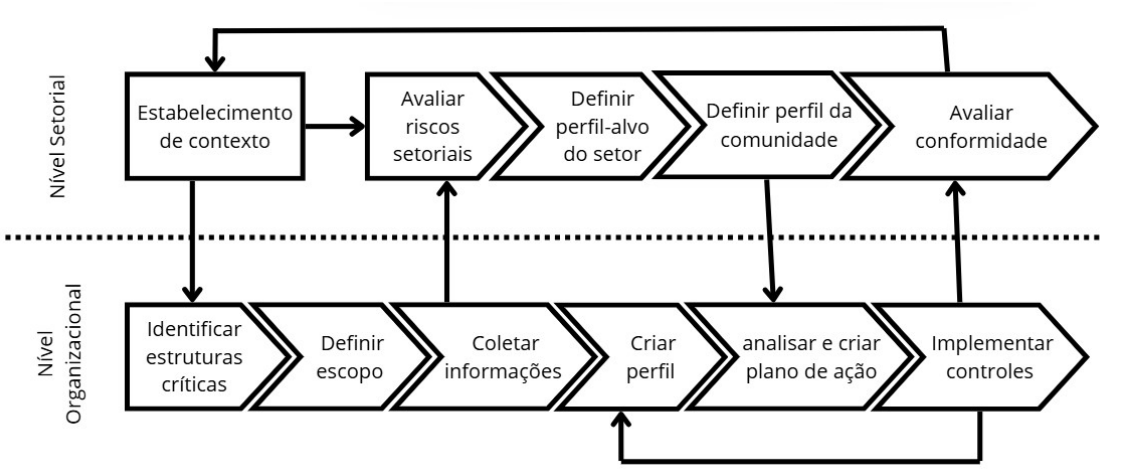

Figure 1. Ciclo de proteção e avaliação de Infraestruturas críticas

O contexto setorial estabelece as expectativas e parâmetros de segurança cibernética, definindo o apetite de risco setorial, que orienta a gestão de riscos das organizações na proteção das Infraestruturas Críticas. Em seguida, cada entidade realiza a identificação de seus ativos críticos e ativos subjacentes, conduzindo uma análise de sua postura de segurança e construindo seu perfil organizacional (Current Profile).

Paralelamente, ocorre a avaliação de riscos organizacional, complementada por uma avaliação de riscos setorial, conduzida pelo responsável setorial. Essa avaliação integrada analisa as interdependências intra e intersetoriais e identifica riscos combinados que possam afetar múltiplas organizações simultaneamente, construindo uma visão sistêmica do risco cibernético setorial.

Com base nos resultados dessas avaliações, é possível elaborar um perfil de segurança setorial e perfis comunitários de referência, alinhados ao apetite de risco definido para o setor. As organizações, então, utilizam esses perfis como guia para definir seus perfis-alvo (Target Profiles) e planejar ações de melhoria, reduzindo as lacunas entre o estado atual e o desejado de segurança.

Ao final do ciclo, o responsável setorial, em conjunto com as organizações do setor, deve conduzir uma avaliação consolidada da postura de segurança cibernética, verificando o grau de alinhamento às diretrizes setoriais e aos perfis comunitários. Os resultados desse processo devem retroalimentar o ciclo, ajustando o contexto setorial e pro-

movendo a melhoria contínua e coordenada da resiliência cibernética em todo o setor.

4.2. Considerações sobre o modelo

A aplicação do modelo proposto pode gerar benefícios significativos para os diversos interessados na proteção das infraestruturas críticas. Os operadores passam a ter uma visão mais clara sobre o que se espera deles em matéria de segurança cibernética, podendo, assim, alinhar de forma eficiente suas estratégias internas de segurança com as exigências setoriais. Os reguladores e coordenadores setoriais, por sua vez, passam a desempenhar de maneira mais eficaz o papel de garantir a segurança cibernética das infraestruturas críticas sob sua tutela. Os governos obtêm maior visibilidade sobre os resultados da implementação de suas políticas públicas relacionadas à segurança cibernética. Por fim, a sociedade ganha confiança de que os serviços essenciais continuarão sendo prestados de forma contínua e segura, mesmo diante de ameaças cibernéticas.

A adoção do NIST CSF como base para o modelo acrescenta um importante grau de robustez, visto que diversos estudos comprovam que sua aplicação reduz de forma significativa a ocorrência de incidentes cibernéticos, especialmente em setores de infraestrutura crítica, resultando em avanços consistentes na maturidade da segurança cibernética das organizações em que foi implementado [Salas-Riega et al. 2025].

O maior desafio para a implantação desse modelo reside nas etapas iniciais, notadamente na definição de contexto e na identificação de ativos críticos, que demandam o desenvolvimento de metodologias ajustadas às especificidades dos diferentes setores de infraestrutura crítica. Já existem estudos relevantes sobre esses temas. Por exemplo, [Fekete 2011] propõe critérios gerais para a avaliação de infraestruturas críticas; [Rinaldi et al. 2001] aborda a identificação e a análise das múltiplas formas de interdependência entre infraestruturas críticas; e [Šarūnienė et al. 2024] e [Theocharidou and Giannopoulos 2015] apresentam metodologias de avaliação de riscos aplicáveis às infraestruturas críticas, enfatizando a importância de uma clara definição do contexto e da identificação precisa dos ativos críticos.

Apesar da existência de diversos estudos sobre a identificação de infraestruturas críticas, ainda é necessária uma metodologia que considere as particularidades operacionais e regulatórias.

5. Conclusão

A proteção cibernética de infraestruturas críticas representa um dos maiores desafios na gestão da segurança nacional e setorial. Trata-se de um ambiente complexo, com grande interdependência operacional e multiplicidade de atores. Nesse cenário, o framework NIST CSF oferece uma base consistente, que pode ser adaptada para que organizações atinjam um nível adequado de segurança cibernética e cumpram exigências regulatórias aplicadas às infraestruturas críticas.

O estabelecimento de um contexto setorial é o ponto de partida para atingir esse objetivo. Ele define as regras de identificação das infraestruturas críticas, os níveis aceitáveis de risco e os padrões de segurança esperados. A partir dessas diretrizes, as organizações podem estruturar seus próprios ciclos de gestão cibernética — identificando ativos críticos, avaliando riscos, definindo perfis-alvo e implementando controles — de modo coerente com as expectativas setoriais.

A abordagem aqui apresentada, baseada em dois ciclos interconectados — setorial e organizacional — cria um mecanismo dinâmico de retroalimentação, em que as avaliações de risco das organizações subsidiam as análises setoriais, e os perfis comunitários definidos pelo setor orientam as estratégias individuais de segurança e conformidade. Com isso, promove-se não apenas a proteção isolada de cada infraestrutura, mas também a resiliência sistêmica do setor como um todo.

References

Aarland, M. and Gjøsæter, T. (2022). Digital supply chain vulnerabilities in critical infrastructure: A systematic literature review on cybersecurity in the energy sector. In *Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP*, pages 326–333. INSTICC, SciTePress.

Bernardo, L., Malta, S., and Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the nist csf. *Electronics*, 14(7).

Bloomfield, R. E., Popov, P., Salako, K., Stankovic, V., and Wright, D. (2017). Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering & System Safety*, 167:198–217.

BRASIL (2008). Portaria nº 2, de 08 de fevereiro de 2008 - institui grupos técnicos de segurança de infra-estruturas críticas (gtsic) e dá outras providências. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=11/02/2008. Acesso em: 25 ago. 2025.

BRASIL (2018). Política nacional de segurança de infraestruturas críticas (pnsic). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 25 ago. 2025.

BRASIL (2020a). Estratégia nacional de segurança cibernética - e-ciber. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 25 ago. 2025.

BRASIL (2020b). Estratégia nacional de segurança das infraestruturas críticas. Disponível em: https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm. Acesso em: 25 ago. 2025.

BRASIL (2021). Decreto nº 10.748, de 16 de junho de 2021. institui a rede federal de gestão de incidentes cibernéticos – regic. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10748.htm. Acesso em: 25 ago. 2025.

BRASIL (2025). Decreto nº 12.573, de 4 de agosto de 2025. atualiza a estratégia nacional de cibersegurança. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 25 ago. 2025.

da Silva, E. G., Georg, M. A. C., Júnior, L. A. R., Ferreira, L. R., de Melo, L. P., and Nunes, R. R. (2025). International perspectives on critical infrastructure: Evaluation criteria and definitions. *International Journal of Critical Infrastructure Protection*, 49:100761.

Edwards, J. (2024). *A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice*. Wiley (Wiley-Blackwell), Hoboken, NJ, 1 edition.

Estados Unidos (2001). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Government Printing Office, Washington, DC.

ESTADOS UNIDOS (2013). Executive order 13636: Improving critical infrastructure cybersecurity. Disponível em:`https://www.govinfo.gov/app/details/DCPD-201300091`. Acesso em: 02 set. 2025.

Federal Ministry of the Interior (Germany) (2009). National strategy for critical infrastructure protection (cip strategy). Disponível em: `https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/civil-protection/kritis_englisch.pdf?__blob=publicationFile\&v=5`. Acesso em: 27 de setembro de 2025.

Fekete, A. (2011). Common criteria for the assessment of critical infrastructures. *International Journal of Disaster Risk Science*, 2(1):15–24.

Johansmeyer, T. (2024). If cyber is uninsurable, the united states has a major strategy problem. *The Journal of Risk Management and Insurance*, 28(2):1–19.

Korkali, M., Veneman, J. G., Tivnan, B. F., Bagrow, J. P., and Hines, P. D. H. (2017). Reducing cascading failure risk by increasing infrastructure network interdependence. *Scientific Reports*, 7.

Kure, H. I. and Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems*, 4(4):332–340.

Luiijf, E. A. M., Burger, H. H., and Klaver, M. H. A. (2003). Critical (information) infrastructure protection in the netherlands. In *GI Jahrestagung (Schwerpunkt "Sicherheit – Schutz und Zuverlässigkeit")*, pages 9–19. Disponível em: subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf.

Markopoulou, D. and Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law Security Review*, 41:105502.

Miranda Zottmann, C. E., Stuckert do Amaral, T. M., Nunes, R. R., and Costa Gondim, J. J. (2023). Comparing software supply chain protection approaches. In *2023 Workshop on Communication Networks and Power Systems (WCNPS)*, pages 1–7.

Moreira, F. R., da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T., and Nunes, R. R. (2021). Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. *IEEE Access*, 9:129605–129618.

NIST (2014). Framework for improving critical infrastructure cybersecurity: Version 1.0. Technical report, National Institute of Standards and Technology, Gaithersburg, MD.

NIST (2018a). History and creation of the csf 1.1. Disponível em: https://www.nist.gov/cyberframework/history-and-creation-framework. Acesso em: 11 set. 2025.

NIST (2018b). It asset management: How-to guide (nist special publication 1800-5). Technical Report NIST SP 1800-5, National Cybersecurity Center of Excellence (NCCoE). Provides practical guidance for implementing asset inventory and management aligned with the NIST Cybersecurity Framework.

NIST (2024). The nist cybersecurity framework 2.0. Nist cybersecurity white paper (cswp) nist cswp 29 ipd, National Institute of Standards and Technology, Gaithersburg, MD.

NPSA (2025). Critical national infrastructure. Disponível em: https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure. Acesso em: 11 set. 2025.

Papamichael, M., Dimopoulos, C., and Boustras, G. (2024). Performing risk assessment for critical infrastructure protection: an investigation of transnational challenges and human decision-making considerations. *Sustainable and Resilient Infrastructure*, 9(4):367–385.

Pascoe, C., Quinn, S., and Scarfone, K. (2024a). Nist cybersecurity framework 2.0: Quick-start guide for creating and using organizational profiles. Special Publication NIST SP 1301 SP 1301, National Institute of Standards and Technology, Gaithersburg, MD.

Pascoe, C., Snyder, J. N., and Scarfone, K. A. (2024b). Nist cybersecurity framework 2.0: A guide to creating community profiles. Nist cybersecurity white paper (cswp) nist cswp 32 ipd, National Institute of Standards and Technology, Gaithersburg, MD.

Rinaldi, S., Peerenboom, J., and Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6):11–25.

Safianu, O., Twum, F., and Hayfron-Acquah, J. B. (2016). Information system security threats and vulnerabilities: Evaluating the human factor in data protection. *International Journal of Computer Applications*, 143(5):8–14.

Salas-Riega, J. L., Riega-Virú, Y., Ninaquispe-Soto, M., and Salas-Riega, J. M. (2025). Cybersecurity and the nist framework: A systematic review of its implementation and effectiveness against cyber threats. *International Journal of Advanced Computer Science and Applications*, 16(6).

Theocharidou, M. and Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. part ii: A new approach. Technical Report LB-NA-27332-EN-N, Luxembourg (Luxembourg).

Toussaint, M., Krima, S., and Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, 39:100604.

UNIÃO EUROPÉIA (2022). Directive (eu) 2022/2557 on the resilience of critical entities. Disponível em: https://eur-lex.europa.eu/eli/dir/2022/2557/oj. Acesso em: 11 set. 2025.

Šarūnienė, I., Martišauskas, L., Krikštolaitis, R., Augutis, J., and Setola, R. (2024). Risk assessment of critical infrastructures: A methodology based on criticality of infrastructure elements. *Reliability Engineering & System Safety*, 243:109797.