Estrutura de Segurança Cibernética (CSF) 2.0 do NIST

National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia)
Esta publicação está disponível gratuitamente no site: https://doi.org/10.6028/NIST.CSWP.29.por

Fevereiro 26, 2024

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Resumo

A Estrutura de Segurança Cibernética (CSF) 2.0 do NIST fornece orientação ao setor, aos órgãos governamentais e a outras organizações para gerenciar os riscos de segurança cibernética. Ela oferece uma taxonomia de resultados de segurança cibernética de alto nível que pode ser usada por qualquer organização - independentemente de seu tamanho, setor ou maturidade - para entender, avaliar, priorizar e comunicar melhor seus esforços de segurança cibernética. A CSF não prescreve como os resultados devem ser alcançados. Em vez disso, ela se vincula a recursos on-line que fornecem orientações adicionais sobre práticas e controles que podem ser usados para alcançar esses resultados. Este documento descreve a CSF 2.0, os seus componentes e algumas das muitas formas como pode ser utilizado.

Palavras-chave

segurança cibernética; estrutura de segurança cibernética (CSF); governança de risco de segurança cibernética; gerenciamento de risco de segurança cibernética; gerenciamento de risco empresarial; perfis; níveis.

Público

Os indivíduos responsáveis por desenvolver e liderar programas de segurança cibernética são o público principal da CSF. A CSF também pode ser usada por outras pessoas envolvidas no gerenciamento de riscos - incluindo executivos, conselhos de administração, profissionais de aquisição, profissionais de tecnologia, gerentes de risco, advogados, especialistas em recursos humanos e auditores de segurança cibernética e gerenciamento de riscos - para orientar suas decisões relacionadas à segurança cibernética. Além disso, a CSF pode ser útil para aqueles que criam e influenciam políticas (por exemplo, associações, organizações profissionais, reguladores) que definem e comunicam prioridades para o gerenciamento de riscos de segurança cibernética.

Conteúdo suplementar

O NIST continuará criando e hospedando recursos adicionais para ajudar as organizações a implementar a CSF, incluindo guias de início rápido e perfis de comunidade. Todos os recursos são disponibilizados publicamente no site do NIST CSF. Sugestões de recursos adicionais para referência no site do NIST CSF sempre podem ser compartilhadas com o NIST em cyberframework@nist.gov.

Nota para os leitores

Salvo indicação em contrário, os documentos citados, referenciados ou extraídos desta publicação não estão totalmente incorporados a ela.

Antes da versão 2.0, a estrutura de segurança cibernética era chamada de "Estrutura para melhorar a segurança cibernética da infraestrutura crítica" Esse título não é usado para a CSF 2.0.

Agradecimentos

A CSF é o resultado de um esforço colaborativo de vários anos entre o setor, o meio acadêmico e o governo dos Estados Unidos e de todo o mundo. O NIST reconhece e agradece a todos aqueles que contribuíram para esta CSF revisada. Informações sobre o processo de desenvolvimento da CSF podem ser encontradas no site do NIST CSF. As lições aprendidas sobre o uso da CSF sempre podem ser compartilhadas com o NIST em cyberframework@nist.gov.

Traduzido por TaikaTranslations LLC sob contrato NIST [133ND23PNB770271]. Tradução oficial do Governo dos EUA.
Translated by TaikaTranslations LLC under contract with NIST [133ND23PNB770271]. Official U.S. Government translation.

A versão oficial em inglês desta publicação está disponível gratuitamente no National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.29.
The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.29.

Índice

Lista de figuras

Prefácio

A Estrutura de Segurança Cibernética (CSF) 2.0 foi projetada para ajudar organizações de todos os tamanhos e setores - incluindo indústria, governo, academia e organizações sem fins lucrativos - a gerenciar e reduzir seus riscos de segurança cibernética. Ela é útil independentemente do nível de maturidade e da sofisticação técnica dos programas de segurança cibernética de uma organização. No entanto, a CSF não adota uma abordagem única para todos os casos. Cada organização tem riscos comuns e exclusivos, bem como apetites e tolerâncias a riscos variados, missões específicas e objetivos para atingir essas missões. Por necessidade, a maneira como as organizações implementam a CSF varia.

Idealmente, a CSF será usada para abordar os riscos de segurança cibernética juntamente com outros riscos da empresa, inclusive os de natureza financeira, de privacidade, da cadeia de suprimentos, de reputação, tecnológicos ou físicos.

A CSF *descreve* os resultados desejados que devem ser compreendidos por um público amplo, incluindo executivos, gerentes e profissionais, independentemente de sua experiência em segurança cibernética. Como esses resultados são neutros em termos de setor, país e tecnologia, eles oferecem à organização a flexibilidade necessária para lidar com seus riscos, tecnologias e considerações de missão exclusivos. Os resultados são mapeados diretamente para uma lista de possíveis controles de segurança a serem considerados imediatamente para reduzir os riscos de segurança cibernética.

Embora não seja prescritiva, a CSF ajuda seus usuários a aprender e selecionar resultados específicos. Sugestões de como resultados específicos podem ser alcançados são fornecidas em um conjunto crescente de recursos on-line que complementam a CSF, incluindo uma série de Quick Start Guides (QSGs). Além disso, várias ferramentas oferecem formatos que podem ser baixados para ajudar as organizações que optam por automatizar alguns de seus processos. Os QSGs sugerem maneiras iniciais de usar a CSF e convidam o leitor a explorar a CSF e os recursos relacionados com mais profundidade. Disponível no site do NIST CSF, a CSF e esses recursos complementares do NIST e de outros devem ser vistos como um "portfólio da CSF" para ajudar a gerenciar e reduzir os riscos. Independentemente de como é aplicado, a CSF solicita que seus usuários considerem sua postura de segurança cibernética no contexto e, em seguida, adaptem a CSF às suas necessidades específicas.

Com base nas versões anteriores, a CSF 2.0 contém novos recursos que destacam a importância da *governança* e das *cadeias de suprimentos*. É dada atenção especial aos QSGs para garantir que a CSF seja relevante e prontamente acessível a organizações menores, bem como a suas contrapartes maiores. O NIST agora fornece *Exemplos de Implementação* e *Referências Informativas*, que estão disponíveis on-line e são atualizados regularmente. A criação de *perfis organizacionais* atuais e de destino ajuda as organizações a comparar onde estão com o que querem ou precisam estar e permite que implementem e avaliem os controles de segurança mais rapidamente.

Os riscos de segurança cibernética estão em constante expansão, e o gerenciamento desses riscos deve ser um processo contínuo. Isso é verdade independentemente de a organização estar apenas começando a enfrentar seus desafios de segurança cibernética ou de estar ativa há muitos anos com uma equipe de segurança cibernética sofisticada e com bons recursos. A CSF foi projetada para ser valiosa para qualquer tipo de organização e espera-se que forneça orientação adequada por um longo período.

1. Visão geral da estrutura de segurança cibernética (CSF)

Este documento é a versão 2.0 da Estrutura de Segurança Cibernética do NIST*(Estrutura* ou *CSF*). Ele inclui os seguintes componentes:

- ***CSF Core***, o núcleo da CSF, que é uma taxonomia de resultados de segurança cibernética de alto nível que pode ajudar qualquer organização a gerenciar seus riscos de segurança cibernética. Os componentes principais da CSF são uma hierarquia de funções, categorias e subcategorias que detalham cada resultado. Esses resultados podem ser compreendidos por um público amplo, incluindo executivos, gerentes e profissionais, independentemente de sua experiência em segurança cibernética. Como os resultados são neutros em termos de setor, país e tecnologia, eles oferecem à organização a flexibilidade necessária para lidar com seus riscos, tecnologias e considerações de missão exclusivos.
- ***Perfis organizacionais da CSF***, que são um mecanismo para descrever a postura de segurança cibernética atual e/ou desejada de uma organização em termos dos resultados da CSF Core.
- ***Níveis da CSF***, que podem ser aplicados aos Perfis Organizacionais da CSF para caracterizar o rigor das práticas de governança e gerenciamento de riscos de segurança cibernética de uma organização. Os níveis também podem fornecer o contexto de como uma organização vê os riscos de segurança cibernética e os processos em vigor para gerenciar esses riscos.

Este documento descreve *que* resultados desejáveis uma organização pode aspirar a alcançar. Ele não *prescreve* resultados nem como eles podem ser alcançados. As descrições de como uma organização pode alcançar esses resultados são fornecidas em um conjunto de recursos on-line que complementam a CSF e estão disponíveis no site do NIST CSF. Esses recursos oferecem orientações adicionais sobre práticas e controles que podem ser usados para atingir os resultados e têm como objetivo ajudar a organização a entender, adotar e usar a CSF. Eles incluem:

- *Referências informativas* que apontam para fontes de orientação sobre cada resultado de padrões, diretrizes, estruturas, regulamentos, políticas globais existentes etc.
- *Exemplos de implementação* que ilustram formas potenciais de alcançar cada resultado
- *Guias de início rápido* que fornecem orientação prática sobre o uso da CSF e seus recursos on-line, incluindo a transição das versões anteriores da CSF para a versão 2.0
- Perfis de comunidade e modelos de perfis organizacionais que ajudam uma organização a colocar a CSF em prática e definir prioridades para gerenciar os riscos de segurança cibernética

Uma organização pode usar a CSF Core, Perfis e Níveis com os recursos suplementares para entender, avaliar, priorizar e comunicar os riscos de segurança cibernética.

- **Compreender e avaliar:** Descrever a postura de segurança cibernética atual ou pretendida de parte ou de toda a organização, determinar as lacunas e avaliar o progresso para solucioná-las.
- **Priorizar:** Identificar, organizar e priorizar ações para gerenciar os riscos de segurança cibernética que se alinham à missão da organização, aos requisitos legais e regulamentares e às expectativas de gerenciamento de riscos e governança.
- **Comunicar:** Fornecer uma linguagem comum para a comunicação dentro e fora da organização sobre riscos, capacidades, necessidades e expectativas de segurança cibernética.

A CSF foi projetada para ser usada por organizações de todos os tamanhos e setores, incluindo indústria, governo, academia e organizações sem fins lucrativos, independentemente do nível de maturidade de seus programas de segurança cibernética. A CSF é um recurso fundamental que pode ser adotado voluntariamente e por meio de políticas e mandatos governamentais. A taxonomia da CSF e os padrões, diretrizes e práticas referenciados não são específicos de cada país, e as versões anteriores da CSF foram aproveitadas com sucesso por muitos governos e outras organizações, dentro e fora dos Estados Unidos.

A CSF deve ser usada em conjunto com outros recursos (por exemplo, estruturas, padrões, diretrizes, práticas líderes) para gerenciar melhor os riscos de segurança cibernética e informar o gerenciamento geral dos riscos de tecnologia da informação e comunicação (ICT) em nível empresarial. A CSF é uma estrutura flexível que se destina a ser adaptada para uso por todas as organizações, independentemente do tamanho. As organizações continuarão a ter riscos exclusivos - incluindo diferentes ameaças e vulnerabilidades - e tolerâncias a riscos, bem como objetivos e requisitos de missão exclusivos. Assim, as abordagens das organizações para gerenciar riscos e suas implementações da CSF variam.

O restante deste documento está estruturado da seguinte forma:

- A seção 2 explica os conceitos básicos da CSF Core: Funções, categorias e subcategorias.
- A seção 3 define os conceitos de Perfis e Níveis de CSF.
- A seção 4 fornece uma visão geral de componentes selecionados do conjunto de recursos on-line da CSF: Referências informativas, exemplos de implementação e guias de início rápido.
- A seção 5 discute como uma organização pode integrar a CSF a outros programas de gerenciamento de riscos.
- Appendix A é a CSF Core.
- Appendix B contém uma ilustração fictícia dos Níveis da CSF.
- Appendix C é um glossário da terminologia da CSF.

2. Introdução à CSF Core

Appendix A é a CSF Core - um conjunto de resultados de segurança cibernética organizados por Função, depois por Categoria e, por fim, por Subcategoria, conforme ilustrado em Fig. 1. Esses resultados não são uma lista de verificação de ações a serem executadas; as ações específicas tomadas para alcançar um resultado variam de acordo com a organização e o caso de uso, assim como o indivíduo responsável por essas ações. Além disso, a ordem e o tamanho das funções, categorias e subcategorias no Core não implicam a seqüência ou a importância de alcançá-las. A estrutura do Core tem o objetivo de ser mais adequada àqueles encarregados de operacionalizar o gerenciamento de riscos em uma organização.

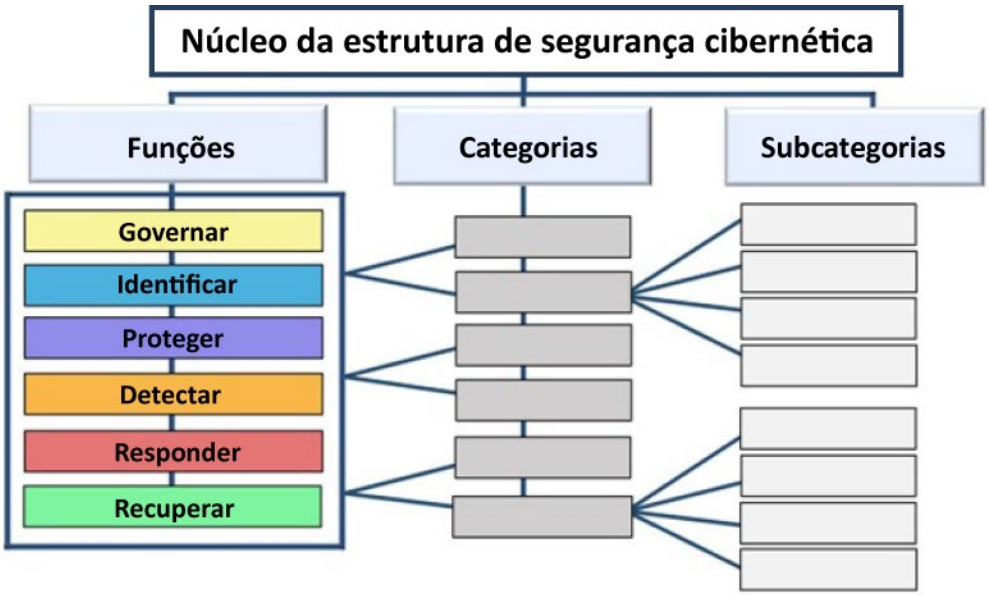

Fig. 1. Estrutura da CSF Core

As funções essenciais da CSF - Governar, Identificar, Proteger, Detectar, Responder e Recuperar - organizam os resultados da segurança cibernética em seu nível mais alto.

- **Govern (GV)** - *A estratégia, as expectativas e a política de gerenciamento de riscos de segurança cibernética da organização são estabelecidas, comunicadas e monitoradas.* A Função de Govern (Governança) fornece resultados para informar o que a organização pode fazer para atingir e priorizar os resultados das outras cinco Funções no contexto de sua missão e das expectativas das partes interessadas. As atividades de governança são essenciais para incorporar a segurança cibernética à estratégia mais ampla de gerenciamento de riscos corporativos (ERM) de uma organização. O Govern aborda a compreensão do contexto organizacional; o estabelecimento da estratégia de segurança cibernética e o gerenciamento de riscos da cadeia de suprimentos de segurança cibernética; funções, responsabilidades e autoridades; políticas; e a supervisão da estratégia de segurança cibernética.
- **Identify (Identificar) (ID)** - *Os riscos atuais de segurança cibernética da organização são compreendidos.* Compreender os ativos da organização (por exemplo, dados, hardware, software, sistemas, instalações, serviços, pessoas), fornecedores e riscos relacionados à

segurança cibernética permite que a organização priorize seus esforços de acordo com sua estratégia de gerenciamento de riscos e as necessidades da missão identificadas na Governança. Essa função também inclui a identificação de oportunidades de melhoria para as políticas, os planos, os processos, os procedimentos e as práticas da organização que apoiam o gerenciamento de riscos de segurança cibernética para informar os esforços de todas as seis funções.

- **Protect (Proteger) (PR)** - *São usadas proteções para gerenciar os riscos de segurança cibernética da organização.* Depois que os ativos e os riscos são identificados e priorizados, o Protect apoia a capacidade de proteger esses ativos para evitar ou reduzir a probabilidade e o impacto de eventos adversos de segurança cibernética, bem como para aumentar a probabilidade e o impacto de aproveitar as oportunidades. Os resultados abrangidos por essa função incluem gerenciamento de identidade, autenticação e controle de acesso; conscientização e treinamento; segurança de dados; segurança de plataforma (ou seja, proteger o hardware, o software e os serviços de plataformas físicas e virtuais); e a resiliência da infraestrutura tecnológica.
- **DETECT (DETECTAR) (DE)** — *Possíveis ataques e comprometimentos de segurança cibernética são encontrados e analisados.* O Detect permite a descoberta e a análise oportunas de anomalias, indicadores de comprometimento e outros eventos potencialmente adversos que podem indicar a ocorrência de ataques e incidentes de segurança cibernética. Essa função oferece suporte a atividades bem-sucedidas de resposta e recuperação de incidentes.
- **RESPOND (RESPONDER) (RS)** — *Ações relacionadas a um incidente de segurança cibernética detectado são tomadas.* Respond apoia a capacidade de conter os efeitos de incidentes de segurança cibernética. Os resultados dessa função abrangem o gerenciamento, a análise, a atenuação, os relatórios e a comunicação de incidentes.
- **RECOVER (RECUPERAR) (RC)** — *Os ativos e as operações afetados por um incidente de segurança cibernética são restaurados*. O Recover apoia a restauração oportuna das operações normais para reduzir os efeitos dos incidentes de segurança cibernética e permitir a comunicação adequada durante os esforços de recuperação.

Embora muitas atividades de gerenciamento de riscos de segurança cibernética se concentrem na prevenção da ocorrência de eventos negativos, elas também podem apoiar o aproveitamento de oportunidades positivas. As ações para reduzir o risco de segurança cibernética podem beneficiar uma organização de outras formas, como o aumento da receita (por exemplo, primeiro oferecendo o espaço excedente das instalações a um provedor de hospedagem comercial para hospedar seus próprios centros de dados e os de outras organizações e, em seguida, transferindo um sistema financeiro importante do centro de dados interno da organização para o provedor de hospedagem para reduzir os riscos de segurança cibernética).

Figure 2 mostra as funções da CSF como uma roda, pois todas as funções estão relacionadas entre si. Por exemplo, uma organização categorizará os ativos em Identificar e tomará medidas para proteger esses ativos em Protect (Proteger). Os investimentos em planejamento e testes nas funções Governar e Identificar darão suporte à detecção oportuna de eventos inesperados na função Detectar, além de possibilitar a resposta a incidentes e ações de recuperação para incidentes de segurança cibernética nas funções Respond (Responder) e Recover (Recuperar). Govern (Governança) está no centro da roda porque informa como a organização implementará as outras cinco funções.

Fig. 2. Funções da CSF

As funções devem ser abordadas ao mesmo tempo. As ações que apoiam Govern (Governar), Identify (Identificar), Protect (Proteger) e Detect (Detectar) devem acontecer continuamente, e as ações que apoiam Respond (Responder) e Recover (Recuperar) devem estar prontas o tempo todo e acontecer quando ocorrerem incidentes de segurança cibernética. Todas as funções têm papéis vitais relacionados a incidentes de segurança cibernética. Os resultados de Govern, Identify e Protect ajudam a prevenir e se preparar para incidentes, enquanto os resultados de Govern, Detect, Respond e Recover ajudam a descobrir e gerenciar incidentes.

Cada função recebe o nome de um verbo que resume seu conteúdo. Cada função é dividida em *Categorias*, que são resultados relacionados à segurança cibernética que compõem coletivamente a função. As *Subcategorias* dividem ainda mais cada categoria em resultados mais específicos das atividades técnicas e de gerenciamento. As subcategorias não são exaustivas, mas descrevem resultados detalhados que apoiam cada categoria.

As funções, categorias e subcategorias se aplicam a todas as TICs usadas por uma organização, incluindo a tecnologia da informação (TI), a Internet das Coisas (IoT) e a tecnologia operacional (TO). Eles também se aplicam a todos os tipos de ambientes tecnológicos, incluindo sistemas de nuvem, móveis e de inteligência artificial. A CSF Core é voltada para o futuro e deve ser aplicada a mudanças futuras em tecnologias e ambientes.

3. Introdução aos perfis e níveis de CSF

Esta seção define os conceitos de Perfis e Níveis de CSF.

3.1. Perfis CSF

Um *perfil organizacional da CSF* descreve a postura de segurança cibernética atual e/ou desejada de uma organização em termos dos resultados do Core. Perfis organizacionais são usados para entender, adaptar, avaliar, priorizar e comunicar os resultados do Core, considerando os objetivos da missão da organização, as expectativas das partes interessadas, o cenário de ameaças e os requisitos. A organização pode, então, priorizar suas ações para alcançar resultados específicos e comunicar essas informações às partes interessadas.

Todo perfil organizacional inclui um ou ambos os itens a seguir:

1. Um *Perfil atual* especifica os resultados principais que uma organização está alcançando (ou tentando alcançar) no momento e caracteriza como ou em que medida cada resultado está sendo alcançado.
2. Um *Perfil alvo* especifica os resultados desejados que uma organização selecionou e priorizou para atingir seus objetivos de gerenciamento de riscos de segurança cibernética. Um Perfil Alvo considera as mudanças previstas na postura de segurança cibernética da organização, como novos requisitos, adoção de novas tecnologias e tendências de inteligência de ameaças.

> Um *Perfil da Comunidade* é uma linha de base dos resultados da CSF que é criada e publicada para tratar de interesses e metas compartilhados entre várias organizações. Um Perfil da Comunidade é normalmente desenvolvido para um determinado setor, subsetor, tecnologia, tipo de ameaça ou outro caso de uso. Uma organização pode usar um Perfil da Comunidade como base para seu próprio Perfil Alvo. Exemplos de perfis de comunidade podem ser encontrados no Site do NIST CSF.

As etapas mostradas em Fig. 3 e resumidas abaixo ilustram uma maneira pela qual uma organização poderia usar um Perfil Organizacional para ajudar a informar a melhoria contínua de sua segurança cibernética.

Fig. 3. Etapas para criar e usar um Perfil Organizacional CSF

1. **Escopo do perfil organizacional.** Documente os fatos e as suposições de alto nível nos quais o perfil se baseará para definir seu escopo. Uma organização pode ter quantos Perfis Organizacionais desejar, cada um com um escopo diferente. Por exemplo, um perfil pode abordar toda a organização ou ter como escopo os sistemas financeiros de uma organização ou o combate a ameaças de ransomware e o tratamento de incidentes de ransomware envolvendo esses sistemas financeiros.
2. **Reúna as informações necessárias para preparar o perfil organizacional.** Exemplos de informações podem incluir políticas organizacionais, prioridades e recursos de gerenciamento de riscos, perfis de riscos corporativos, registros de análise de impacto nos negócios (BIA), requisitos e padrões de segurança cibernética seguidos pela organização, práticas e ferramentas (por exemplo, procedimentos e proteções) e funções de trabalho.
3. **Crie o perfil organizacional.** Determine os tipos de informações que o Perfil deve incluir para os resultados selecionados da CSF e documente as informações necessárias. Considere as implicações de risco do Perfil Atual para informar o planejamento e a priorização do Perfil Alvo. Além disso, considere o uso de um Perfil da Comunidade como base para o Perfil Alvo.
4. **Analise as lacunas entre os perfis atual e desejado e crie um plano de ação.** Realize uma análise de lacunas para identificar e analisar as diferenças entre os perfis atual e desejado e desenvolva um plano de ação priorizado (por exemplo, registro de riscos, relatório detalhado de riscos, plano de ação e marcos [POA&M]) para solucionar essas lacunas.
5. **Implemente o plano de ação e atualize o perfil organizacional.** Siga o plano de ação para solucionar as lacunas e levar a organização a atingir o Perfil Alvo. Um plano de ação pode ter um prazo geral ou ser contínuo.

Dada a importância da melhoria contínua, a organização pode repetir essas etapas sempre que necessário.

Há outros usos para os Perfis organizacionais. Por exemplo, um Perfil atual pode ser usado para documentar e comunicar os recursos de segurança cibernética da organização e as oportunidades conhecidas de melhoria com as partes interessadas externas, como parceiros comerciais ou clientes em potencial. Além disso, um Perfil Alvo pode ajudar a expressar os requisitos e as expectativas de gerenciamento de riscos de segurança cibernética da organização para fornecedores, parceiros e outros terceiros como uma meta a ser atingida por essas partes.

3.2. Níveis da CSF

Uma organização pode optar por usar os Níveis para informar seus Perfis Atual e Alvo. Os Níveis caracterizam o rigor das práticas de governança e gerenciamento de riscos de segurança cibernética de uma organização e fornecem o contexto de como a organização vê os riscos de segurança cibernética e os processos em vigor para gerenciar esses riscos. Os Níveis, conforme mostrado em Fig. 4 e ilustrado em Appendix B, refletem as práticas de uma organização para gerenciar o risco de segurança cibernética como Parcial (Nível 1), Informado sobre o risco (Nível 2), Repetível (Nível 3) e Adaptativo (Nível 4). Os Níveis descrevem uma progressão de respostas informais e ad hoc para abordagens ágeis, informadas sobre os riscos e continuamente aprimoradas. A seleção de Níveis ajuda a definir o tom geral de como uma organização gerenciará seus riscos de segurança cibernética.

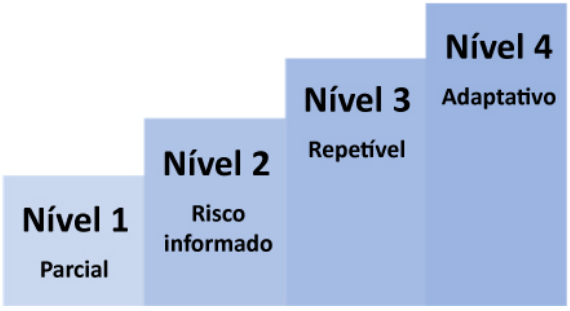

Fig. 4. Níveis da CSF para governança e gerenciamento de riscos de segurança cibernética

Os Níveis devem complementar a metodologia de gerenciamento de riscos de segurança cibernética de uma organização, em vez de substituí-la. Por exemplo, uma organização pode usar os Níveis para se comunicar internamente como referência para uma abordagem de toda a organização[1] para gerenciar os riscos de segurança cibernética. A progressão para Níveis mais altos é incentivada quando os riscos ou mandatos são maiores ou quando uma análise de custo-benefício indica uma redução viável e econômica dos riscos negativos de segurança cibernética.

O site do NIST CSF fornece informações adicionais sobre o uso de Perfis e Níveis. Inclui ponteiros para modelos de Perfis Organizacionais hospedados pelo NIST e um repositório de Perfis Comunitários em uma variedade de formatos legíveis por máquina e utilizáveis por humanos.

[1] Para os fins deste documento, os termos "toda a organização" e "empresa" têm o mesmo significado.

4. Introdução aos recursos on-line que complementam a CSF

O NIST e outras organizações produziram um conjunto de recursos on-line que ajudam as organizações a entender, adotar e usar a CSF. Como estão hospedados on-line, esses recursos adicionais podem ser atualizados com mais frequência do que este documento, que é atualizado com pouca frequência para proporcionar estabilidade aos usuários, e estar disponíveis em formatos legíveis por máquina. Esta seção apresenta uma visão geral de três tipos de recursos on-line: Referências informativas, exemplos de implementação e guias de início rápido.

Referências informativas são mapeamentos que indicam as relações entre o Core e vários padrões, diretrizes, regulamentos e outros conteúdos. As referências informativas ajudam a informar como uma organização pode alcançar os resultados do Core. As referências informativas podem ser específicas do setor ou da tecnologia. Eles podem ser produzidos pelo NIST ou por outra organização. Algumas Referências Informativas têm escopo mais restrito do que uma Subcategoria. Por exemplo, um determinado controle do SP 800-53, Security and Privacy Controls for Information Systems and Organizations (Controles de segurança e privacidade para sistemas de informação e organizações), pode ser uma das muitas referências necessárias para atingir o resultado descrito em uma subcategoria. Outras referências informativas podem ser de nível superior, como um requisito de uma política que aborda parcialmente várias subcategorias. Ao usar a CSF, uma organização pode identificar as Referências Informativas mais relevantes.

Exemplos de implementação fornece exemplos nocionais de etapas concisas e orientadas à ação para ajudar a alcançar os resultados das subcategorias. Os verbos usados para expressar Exemplos incluem compartilhar, documentar, desenvolver, executar, monitorar, analisar, avaliar e exercitar. Os Exemplos não são uma lista abrangente de todas as ações que poderiam ser adotadas por uma organização para atingir um resultado, nem representam uma linha de base das ações necessárias para abordar os riscos de segurança cibernética.

Quick-Start Guides (QSGs) são documentos breves sobre tópicos específicos relacionados à CSF e geralmente são adaptados a públicos específicos. Os QSGs podem ajudar uma organização a implementar a CSF porque destilam partes específicas da CSF em "primeiros passos" acionáveis que uma organização pode considerar no caminho para melhorar sua postura de segurança cibernética e o gerenciamento dos riscos associados. Os guias são revisados em seus próprios prazos, e novos guias são adicionados conforme necessário.

Sugestões de novas referências informativas para a CSF 2.0 sempre podem ser compartilhadas com o NIST em olir@nist.gov. Sugestões de outros recursos para referência no site do NIST CSF, incluindo tópicos adicionais do QSG, devem ser encaminhadas para cyberframework@nist.gov.

5. Melhoria da comunicação e da integração do risco de segurança cibernética

O uso da CSF varia de acordo com a missão e os riscos exclusivos de uma organização. Com o entendimento das expectativas das partes interessadas e do apetite e tolerância a riscos (conforme descrito no Govern), a organização pode priorizar as atividades de segurança cibernética para tomar decisões informadas sobre as despesas e ações de segurança cibernética. Uma organização pode optar por lidar com o risco de uma ou mais maneiras - inclusive mitigando, transferindo, evitando ou aceitando riscos negativos e percebendo, compartilhando, aprimorando ou aceitando riscos positivos - dependendo dos possíveis impactos e probabilidades. É importante ressaltar que uma organização pode usar a CSF tanto internamente para gerenciar seus recursos de segurança cibernética quanto externamente para supervisionar ou se comunicar com terceiros.

Independentemente da utilização da CSF, uma organização pode se beneficiar do uso da CSF como orientação para ajudá-la a entender, avaliar, priorizar e comunicar os riscos de segurança cibernética e as ações que gerenciarão esses riscos. Os resultados selecionados podem ser usados para focar e implementar decisões estratégicas para melhorar as posturas de segurança cibernética e manter a continuidade das funções essenciais da missão, levando em conta as prioridades e os recursos disponíveis.

5.1. Melhoria da comunicação do gerenciamento de riscos

A CSF fornece uma base para melhorar a comunicação em relação às expectativas, ao planejamento e aos recursos de segurança cibernética. A CSF promove o fluxo de informações bidirecional (conforme mostrado na metade superior da Fig. 5) entre os executivos que se concentram nas prioridades e na direção estratégica da organização e os gerentes que gerenciam os riscos específicos de segurança cibernética que podem afetar a realização dessas prioridades. A CSF também apoia um fluxo semelhante (conforme mostrado na metade inferior da Fig. 5) entre os gerentes e os profissionais que implementam e operam as tecnologias. O lado esquerdo da figura indica a importância de os profissionais compartilharem suas atualizações, percepções e preocupações com gerentes e executivos.

Fig. 5. Usando a CSF para melhorar a comunicação do gerenciamento de riscos

A preparação para criar e usar Perfis Organizacionais envolve a coleta de informações sobre as prioridades organizacionais, os recursos e a direção de riscos dos executivos. Em seguida, os gerentes colaboram com os profissionais para comunicar as necessidades comerciais e criar perfis organizacionais informados sobre os riscos. As ações para fechar as lacunas identificadas entre os Perfis Atual e Alvo serão implementadas pelos gerentes e profissionais e fornecerão os principais insumos para os planos em nível de sistema. À medida que o estado-alvo é alcançado em toda a organização, inclusive por meio de controles e monitoramento aplicados no nível do sistema, os resultados atualizados podem ser compartilhados por meio de registros de riscos e relatórios de progresso. Como parte da avaliação contínua, os gerentes obtêm conhecimentos para fazer ajustes que reduzam ainda mais os possíveis danos e aumentem os possíveis benefícios.

A função Govern apoia a comunicação de riscos organizacionais com os executivos. As discussões dos executivos envolvem estratégia, especialmente como as incertezas relacionadas à segurança cibernética podem afetar a realização dos objetivos organizacionais. Essas discussões de governança apoiam o diálogo e o acordo sobre as estratégias de gerenciamento de risco (incluindo o risco da cadeia de suprimentos de segurança cibernética); funções, responsabilidades e autoridades; políticas; e supervisão. À medida que os executivos estabelecem prioridades e objetivos de segurança cibernética com base nessas necessidades, eles comunicam as expectativas sobre o apetite por riscos, a responsabilidade e os recursos. Os executivos também são responsáveis por integrar o gerenciamento de riscos de segurança cibernética aos programas de ERM e aos programas de gerenciamento de riscos de nível inferior (consulte a Seção 5.2). As comunicações refletidas na metade superior da Fig. 5 podem incluir considerações sobre o ERM e os programas de nível inferior e, portanto, informar os gerentes e profissionais.

Os objetivos gerais de segurança cibernética definidos pelos executivos são informados pelos **gerentes** e os transmitem em cascata. Em uma entidade comercial, elas podem se aplicar a uma linha de negócios ou divisão operacional. No caso de entidades governamentais, essas considerações podem ser feitas em nível de divisão ou filial. Ao implementar a CSF, os gerentes se concentrarão em como atingir as metas de risco por meio de serviços, controles e colaboração comuns, conforme expresso no Perfil Alvo e aprimorado por meio das ações rastreadas no plano de ação (por exemplo, registro de risco, relatório detalhado de risco, POA&M).

Os **Profissionais** se concentram na implementação do estado-alvo e na medição das mudanças no risco operacional para ajudar a planejar, executar e monitorar atividades específicas de segurança cibernética. À medida que os controles são implementados para gerenciar o risco em um nível aceitável, os profissionais fornecem aos gerentes e executivos as informações (por exemplo, indicadores-chave de desempenho, indicadores-chave de risco) de que eles precisam para entender a postura de segurança cibernética da organização, tomar decisões informadas e manter ou ajustar a estratégia de risco de acordo. Os Executivos também podem combinar esses dados de risco de segurança cibernética com informações sobre outros tipos de risco de toda a organização. As atualizações das expectativas e prioridades são incluídas nos Perfis Organizacionais atualizados à medida que o ciclo se repete.

5.2. Melhoria da integração com outros programas de gerenciamento de riscos

Toda organização enfrenta vários tipos de risco de TIC (por exemplo, privacidade, cadeia de suprimentos, inteligência artificial) e pode usar estruturas e ferramentas de gerenciamento específicas para cada risco. Algumas organizações integram o ICT e todos os outros esforços de gerenciamento de riscos em um alto nível usando o ERM, enquanto outras mantêm os esforços separados para garantir a atenção adequada a cada um deles. As pequenas organizações, por sua natureza, podem monitorar os riscos em nível empresarial, enquanto as grandes empresas podem manter esforços separados de gerenciamento de riscos integrados ao ERM.

As organizações podem empregar uma abordagem de ERM para equilibrar um *portfólio* de considerações de risco, incluindo a segurança cibernética, e tomar decisões informadas. Os Executivos recebem informações significativas sobre as atividades de risco atuais e planejadas à medida que integram as estratégias de governança e risco com os resultados de usos anteriores da CSF. A CSF ajuda as organizações a traduzir sua terminologia para segurança cibernética e gerenciamento de riscos de segurança cibernética em uma linguagem geral de gerenciamento de riscos que os executivos entenderão.

Os recursos do NIST que descrevem a relação mútua entre o gerenciamento de riscos de segurança cibernética e o ERM incluem:

- *NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick-Start Guide*
- NIST Interagency Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
- IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*

- IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*
- IR 8286C, *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight*
- IR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*
- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

Uma organização também pode considerar a CSF benéfica para a integração do gerenciamento de riscos de segurança cibernética com programas individuais de gerenciamento de riscos de ICT, como, por exemplo:

- **Gerenciamento e avaliação de riscos de segurança cibernética:** A CSF pode ser integrada a programas estabelecidos de gerenciamento e avaliação de riscos de segurança cibernética, tais como SP 800-37, *Risk Management Framework for Information Systems and Organizations*, e SP 800-30, *Guide for Conducting Risk Assessments* da Estrutura de Gerenciamento de Riscos (RMF) do NIST. Para uma organização que usa o RMF do NIST e seu conjunto de publicações, a CSF pode ser usada para complementar a abordagem do RMF para selecionar e priorizar controles de SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.
- **Riscos de privacidade:** Embora a segurança cibernética e a privacidade sejam disciplinas independentes, seus objetivos se sobrepõem em determinadas circunstâncias, conforme ilustrado na Fig. 6.

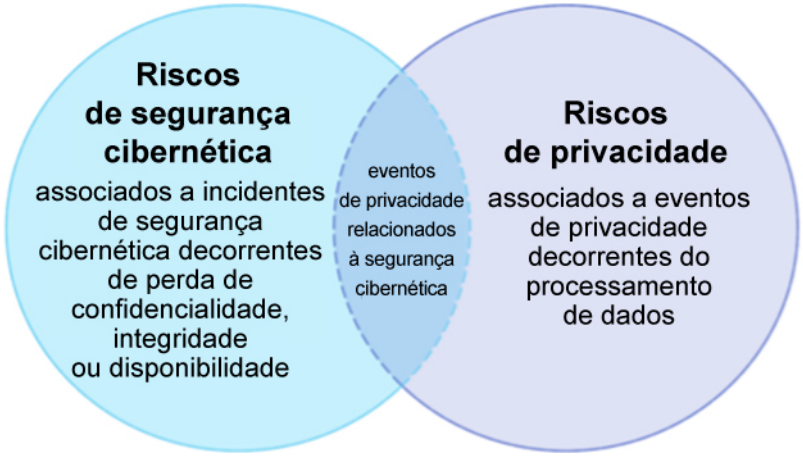

Fig. 6. Relação entre segurança cibernética e risco de privacidade

O gerenciamento de riscos de segurança cibernética é essencial para lidar com os riscos de privacidade relacionados à perda de confidencialidade, integridade e disponibilidade dos dados dos indivíduos. Por exemplo, as violações de dados podem levar ao roubo de

identidade. No entanto, os riscos à privacidade também podem surgir por meios que não estão relacionados a incidentes de segurança cibernética.

Uma organização processa dados para atingir objetivos de missão ou de negócios, o que às vezes pode dar origem a *eventos de privacidade* em que os indivíduos podem ter problemas como resultado do processamento de dados. Esses problemas podem ser expressos de várias maneiras, mas o NIST os descreve como variando de efeitos do tipo dignidade (por exemplo, constrangimento ou estigma) a danos mais tangíveis (por exemplo, discriminação, perda econômica ou danos físicos). A Estrutura de Privacidade e a Estrutura de Segurança Cibernética do NIST podem ser usadas em conjunto para abordar os diferentes aspectos da segurança cibernética e dos riscos à privacidade. Além disso, a Privacy Risk Assessment Methodology (Metodologia de Avaliação de Risco à Privacidade) (PRAM) do NIST tem um catálogo de exemplos de problemas para uso em avaliações de risco à privacidade.

- **Riscos da cadeia de suprimentos:** Uma organização pode usar a CSF para promover a supervisão dos riscos de segurança cibernética e a comunicação com as partes interessadas nas cadeias de suprimentos. Todos os tipos de tecnologia dependem de um ecossistema de cadeia de suprimentos complexo, distribuído globalmente, extenso e interconectado, com rotas geograficamente diversas e vários níveis de terceirização. Esse ecossistema é composto por entidades dos setores público e privado (por exemplo, adquirentes, fornecedores, desenvolvedores, integradores de sistemas, prestadores de serviços de sistemas externos e outros prestadores de serviços relacionados à tecnologia) que interagem para pesquisar, desenvolver, projetar, fabricar, adquirir, entregar, integrar, operar, manter, descartar e, de outra forma, utilizar ou gerenciar produtos e serviços de tecnologia. Essas interações são moldadas e influenciadas por tecnologias, leis, políticas, procedimentos e práticas.

  Devido às relações complexas e interconectadas nesse ecossistema, o gerenciamento de riscos da cadeia de suprimentos (SCRM) é fundamental para as organizações. Cybersecurity SCRM (C-SCRM) é um processo sistemático para gerenciar a exposição ao risco de segurança cibernética em todas as cadeias de suprimentos e desenvolver estratégias, políticas, processos e procedimentos de resposta adequados. As subcategorias da categoria CSF C-SCRM [GV.SC] fornecem uma conexão entre os resultados que se concentram puramente na segurança cibernética e aqueles que se concentram no C-SCRM. SP 800-161r1 (Revisão 1), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, fornece informações detalhadas sobre o C-SCRM.

- **Riscos de tecnologias emergentes:** À medida que novas tecnologias e novos aplicativos de tecnologia se tornam disponíveis, novos riscos se tornam claros. Um exemplo contemporâneo é a inteligência artificial (IA), que apresenta riscos de segurança cibernética e de privacidade, além de muitos outros tipos de risco. A Estrutura de Gerenciamento de Riscos de Inteligência Artificial (AI RMF) do NIST foi desenvolvida para ajudar a lidar com esses riscos. Tratar os riscos de IA juntamente com outros riscos empresariais (por exemplo, financeiros, de segurança cibernética, de reputação e de

privacidade) produzirá um resultado mais integrado e eficiências organizacionais. As considerações e abordagens de gerenciamento de riscos de segurança cibernética e privacidade são aplicáveis ao projeto, desenvolvimento, implantação, avaliação e uso de sistemas de IA. O AI RMF Core usa funções, categorias e subcategorias para descrever os resultados da IA e ajudar a gerenciar os riscos relacionados à IA.

Appendix A. CSF Core

Este apêndice descreve as funções, categorias e subcategorias da CSF Core. Table 1 lista os nomes das funções essenciais e das categorias da CSF 2.0 e os identificadores alfabéticos exclusivos. Cada nome de função na tabela está vinculado à respectiva parte do apêndice. A ordem das funções, categorias e subcategorias do Core não é alfabética; a intenção é que ela tenha maior repercussão entre os encarregados de operacionalizar o gerenciamento de riscos em uma organização. A numeração das subcategorias não é intencionalmente sequencial; as lacunas na numeração indicam as subcategorias da CSF 1.1 que foram realocadas na CSF 2.0.

Tabela 1. Nomes e identificadores de funções essenciais e categorias da CSF 2.0

Função	Categoria	Identificador de categoria
Governar (GV)	Contexto organizacional	GV.OC
	Estratégia de gerenciamento de riscos	GV.RM
	Funções, responsabilidades e autoridades	GV.RR
	Política	GV.PO
	Supervisão	GV.OV
	Segurança cibernética Gerenciamento de riscos da cadeia de suprimentos	GV.SC
Identificar (ID)	Gerenciamento de ativos	ID.AM
	Avaliação de riscos	ID.RA
	Melhoria	ID.IM
Proteger (PR)	Gerenciamento de identidade, autenticação e controle de acesso	PR.AA
	Conscientização e treinamento	PR.AT
	Segurança de dados	PR.DS
	Segurança da plataforma	PR.PS
	Resiliência da infraestrutura tecnológica	PR.IR
Detetar (DE)	Monitoramento contínuo	DE.CM
	Análise de eventos adversos	DE.AE
Responder (RS)	Gerenciamento de incidentes	RS.MA
	Análise de incidentes	RS.AN
	Comunicação e relatórios de resposta a incidentes	RS.CO
	Mitigação de incidentes	RS.MI
Recuperar (RC)	Execução do plano de recuperação de incidentes	RC.RP
	Comunicação de recuperação de incidentes	RC.CO

A CSF Core, as Referências Informativas e os Exemplos de Implementação estão disponíveis no site da CSF 2.0 e por meio da Ferramenta de Referência da CSF 2.0, que permite aos usuários explorá-los e exportá-los em formatos legíveis por humanos e máquinas. A CSF 2.0 Core também está disponível em um formato legado semelhante ao da CSF 1.1.

GOVERNAR (GV): A estratégia, as expectativas e a política de gerenciamento de riscos de segurança cibernética da organização são estabelecidas, comunicadas e monitoradas

- **Contexto organizacional (GV.OC):** As circunstâncias - missão, expectativas das partes interessadas, dependências e requisitos legais, regulamentares e contratuais - que envolvem as decisões de gerenciamento de riscos de segurança cibernética da organização são compreendidas
  - **GV.OC-01:** A missão organizacional é compreendida e informa o gerenciamento de riscos de segurança cibernética
  - **GV.OC-02:** As partes interessadas internas e externas são compreendidas, e suas necessidades e expectativas em relação ao gerenciamento de riscos de segurança cibernética são compreendidas e consideradas
  - **GV.OC-03:** Os requisitos legais, regulamentares e contratuais relativos à segurança cibernética - incluindo obrigações de privacidade e liberdades civis - são compreendidos e gerenciados
  - **GV.OC-04:** Os objetivos, recursos e serviços essenciais dos quais as partes interessadas externas dependem ou esperam da organização são compreendidos e comunicados
  - **GV.OC-05:** Os resultados, os recursos e os serviços dos quais a organização depende são compreendidos e comunicados

- **Estratégia de gerenciamento de riscos (GV.RM):** As prioridades, as restrições, as declarações de tolerância e apetite por riscos e as premissas da organização são estabelecidas, comunicadas e usadas para apoiar as decisões de risco operacional
  - **GV.RM-01:** Os objetivos do gerenciamento de riscos são estabelecidos e acordados pelas partes interessadas da organização
  - **GV.RM-02:** As declarações de apetite e tolerância a riscos são estabelecidas, comunicadas e mantidas
  - **GV.RM-03:** As atividades e os resultados do gerenciamento de riscos de segurança cibernética estão incluídos nos processos de gerenciamento de riscos corporativos
  - **GV.RM-04:** A direção estratégica que descreve as opções adequadas de resposta aos riscos é estabelecida e comunicada
  - **GV.RM-05:** Linhas de comunicação em toda a organização são estabelecidas para riscos de segurança cibernética, incluindo riscos de fornecedores e outros terceiros
  - **GV.RM-06:** Um método padronizado para calcular, documentar, categorizar e priorizar os riscos de segurança cibernética é estabelecido e comunicado
  - **GV.RM-07:** As oportunidades estratégicas (ou seja, riscos positivos) são caracterizadas e incluídas nas discussões sobre os riscos de segurança cibernética da organização

- **Funções, responsabilidades e autoridades (GV.RR):** As funções, responsabilidades e autoridades de segurança cibernética para promover a prestação de contas, a avaliação de desempenho e a melhoria contínua são estabelecidas e comunicadas
  - **GV.RR-01:** A liderança organizacional é responsável pelo risco de segurança cibernética e promove uma cultura consciente dos riscos, ética e de melhoria contínua
  - **GV.RR-02:** As funções, responsabilidades e autoridades relacionadas ao gerenciamento de riscos de segurança cibernética são estabelecidas, comunicadas, compreendidas e aplicadas
  - **GV.RR-03:** Recursos adequados são alocados de acordo com a estratégia de risco de segurança cibernética, funções, responsabilidades e políticas
  - **GV.RR-04:** A segurança cibernética está incluída nas práticas de recursos humanos
- **Política (GV.PO):** A política de segurança cibernética da organização é estabelecida, comunicada e aplicada
  - **GV.PO-01:** A política de gerenciamento de riscos de segurança cibernética é estabelecida com base no contexto organizacional, na estratégia de segurança cibernética e nas prioridades, e é comunicada e aplicada
  - **GV.PO-02:** A política de gerenciamento de riscos de segurança cibernética é revisada, atualizada, comunicada e aplicada para refletir as mudanças nos requisitos, ameaças, tecnologia e missão organizacional
- **Supervisão (GV.OV):** Os resultados das atividades e do desempenho do gerenciamento de riscos de segurança cibernética em toda a organização são usados para informar, melhorar e ajustar a estratégia de gerenciamento de riscos
  - **GV.OV-01:** Os resultados da estratégia de gerenciamento de riscos de segurança cibernética são revisados para informar e ajustar a estratégia e a direção
  - **GV.OV-02:** A estratégia de gerenciamento de riscos de segurança cibernética é revisada e ajustada para garantir a cobertura dos requisitos e riscos organizacionais
  - **GV.OV-03:** O desempenho do gerenciamento de riscos de segurança cibernética da organização é avaliado e revisado para os ajustes necessários
- **Segurança cibernética e gerenciamento de riscos da cadeia de suprimentos (GV.SC):** Os processos de gerenciamento de riscos cibernéticos da cadeia de suprimentos são identificados, estabelecidos, gerenciados, monitorados e aprimorados pelas partes interessadas da organização
  - **GV.SC-01:** Um programa, estratégia, objetivos, políticas e processos de gerenciamento de riscos da cadeia de suprimentos de segurança cibernética são estabelecidos e acordados pelas partes interessadas da organização

- **GV.SC-02:** As funções e responsabilidades de segurança cibernética para fornecedores, clientes e parceiros são estabelecidas, comunicadas e coordenadas interna e externamente
- **GV.SC-03:** O gerenciamento de riscos da cadeia de suprimentos de segurança cibernética é integrado à segurança cibernética e ao gerenciamento de riscos corporativos, à avaliação de riscos e aos processos de melhoria
- **GV.SC-04:** Os fornecedores são conhecidos e priorizados por sua importância
- **GV.SC-05:** Os requisitos para abordar os riscos de segurança cibernética nas cadeias de suprimentos são estabelecidos, priorizados e integrados em contratos e outros tipos de acordos com fornecedores e outros terceiros relevantes
- **GV.SC-06:** O planejamento e a devida diligência são realizados para reduzir os riscos antes de entrar em relacionamentos formais com fornecedores ou outros terceiros
- **GV.SC-07:** Os riscos apresentados por um fornecedor, seus produtos e serviços e outros terceiros são compreendidos, registrados, priorizados, avaliados, respondidos e monitorados no decorrer do relacionamento
- **GV.SC-08:** Fornecedores relevantes e outros terceiros são incluídos nas atividades de planejamento, resposta e recuperação de incidentes
- **GV.SC-09:** As práticas de segurança da cadeia de suprimentos são integradas aos programas de segurança cibernética e de gerenciamento de riscos corporativos, e seu desempenho é monitorado durante todo o ciclo de vida dos produtos e serviços de tecnologia
- **GV.SC-10:** Os planos de gerenciamento de risco da cadeia de suprimentos de segurança cibernética incluem provisões para atividades que ocorrem após a conclusão de uma parceria ou contrato de serviço

IDENTIFICAR (ID): Os riscos atuais de segurança cibernética da organização são compreendidos

- **Gerenciamento de ativos (ID.AM):** Os ativos (por exemplo, dados, hardware, software, sistemas, instalações, serviços, pessoas) que permitem que a organização atinja seus objetivos comerciais são identificados e gerenciados de acordo com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização
  - **ID.AM-01:** Os inventários de hardware gerenciados pela organização são mantidos
  - **ID.AM-02:** Os inventários de software, serviços e sistemas gerenciados pela organização são mantidos
  - **ID.AM-03:** As representações da comunicação de rede autorizada da organização e os fluxos de dados de rede internos e externos são mantidos
  - **ID.AM-04:** Os estoques de serviços prestados pelos fornecedores são mantidos

- **ID.AM-05:** Os ativos são priorizados com base na classificação, criticidade, recursos e impacto na missão
- **ID.AM-07:** São mantidos inventários de dados e metadados correspondentes para os tipos de dados designados
- **ID.AM-08:** Sistemas, hardware, software, serviços e dados são gerenciados ao longo de seus ciclos de vida

- **Avaliação de risco (ID.RA):** O risco de segurança cibernética para a organização, os ativos e os indivíduos são compreendidos pela organização
  - **ID.RA-01:** As vulnerabilidades dos ativos são identificadas, validadas e registradas
  - **ID.RA-02:** A inteligência sobre ameaças cibernéticas é recebida de fóruns e fontes de compartilhamento de informações
  - **ID.RA-03:** As ameaças internas e externas à organização são identificadas e registradas
  - **ID.RA-04:** Os possíveis impactos e as probabilidades de ameaças que exploram vulnerabilidades são identificados e registrados
  - **ID.RA-05:** Ameaças, vulnerabilidades, probabilidades e impactos são usados para entender o risco inerente e informar a priorização da resposta ao risco
  - **ID.RA-06:** As respostas aos riscos são escolhidas, priorizadas, planejadas, monitoradas e comunicadas
  - **ID.RA-07:** As alterações e exceções são gerenciadas, avaliadas quanto ao impacto do risco, registradas e rastreadas
  - **ID.RA-08:** São estabelecidos processos para receber, analisar e responder a divulgações de vulnerabilidades
  - **ID.RA-09:** A autenticidade e a integridade do hardware e do software são avaliadas antes da aquisição e do uso
  - **ID.RA-10:** Os fornecedores críticos são avaliados antes da aquisição

- **Melhoria (ID.IM):** Melhorias nos processos, procedimentos e atividades de gerenciamento de riscos de segurança cibernética da organização são identificadas em todas as funções da CSF
  - **ID.IM-01:** As melhorias são identificadas a partir de avaliações
  - **ID.IM-02:** As melhorias são identificadas a partir de testes e exercícios de segurança, inclusive aqueles realizados em coordenação com fornecedores e terceiros relevantes
  - **ID.IM-03:** As melhorias são identificadas a partir da execução de processos, procedimentos e atividades operacionais
  - **ID.IM-04:** Os planos de resposta a incidentes e outros planos de segurança cibernética que afetam as operações são estabelecidos, comunicados, mantidos e aprimorados

PROTEGER (PR): São usadas proteções para gerenciar os riscos de segurança cibernética da organização

- **Gerenciamento de identidade, autenticação e controle de acesso (PR.AA):** O acesso aos ativos físicos e lógicos é limitado a usuários, serviços e hardware autorizados e gerenciado de acordo com o risco avaliado de acesso não autorizado
  - **PR.AA-01:** As identidades e credenciais de usuários, serviços e hardware autorizados são gerenciadas pela organização
  - **PR.AA-02:** As identidades são comprovadas e vinculadas a credenciais com base no contexto das interações
  - **PR.AA-03:** Usuários, serviços e hardware são autenticados
  - **PR.AA-04:** As afirmações de identidade são protegidas, transmitidas e verificadas
  - **PR.AA-05:** As permissões de acesso, os direitos e as autorizações são definidos em uma política, gerenciados, aplicados e revisados, e incorporam os princípios de privilégio mínimo e separação de tarefas
  - **PR.AA-06:** O acesso físico aos ativos é gerenciado, monitorado e aplicado de acordo com o risco
- **Conscientização e treinamento (PR.AT):** O pessoal da organização recebe treinamento e conscientização sobre segurança cibernética para que possa realizar suas tarefas relacionadas à segurança cibernética
  - **PR.AT-01:** Os funcionários recebem conscientização e treinamento para que tenham o conhecimento e as habilidades para realizar tarefas gerais tendo em mente os riscos de segurança cibernética
  - **PR.AT-02:** Os indivíduos em funções especializadas recebem conscientização e treinamento para que possuam o conhecimento e as habilidades para executar tarefas relevantes, tendo em mente os riscos de segurança cibernética
- **Segurança de dados (PR.DS):** Os dados são gerenciados de acordo com a estratégia de risco da organização para proteger a confidencialidade, a integridade e a disponibilidade das informações
  - **PR.DS-01:** A confidencialidade, a integridade e a disponibilidade dos dados em repouso são protegidas
  - **PR.DS-02:** A confidencialidade, a integridade e a disponibilidade dos dados em trânsito são protegidas
  - **PR.DS-10:** A confidencialidade, a integridade e a disponibilidade dos dados em uso são protegidas
  - **PR.DS-11:** Os backups dos dados são criados, protegidos, mantidos e testados

- **Segurança da plataforma (PR.PS):** O hardware, o software (por exemplo, firmware, sistemas operacionais, aplicativos) e os serviços de plataformas físicas e virtuais são gerenciados de acordo com a estratégia de risco da organização para proteger sua confidencialidade, integridade e disponibilidade
  - **PR.PS-01:** As práticas de gerenciamento de configuração são estabelecidas e aplicadas
  - **PR.PS-02:** O software é mantido, substituído e removido de acordo com o risco
  - **PR.PS-03:** O hardware é mantido, substituído e removido de acordo com o risco
  - **PR.PS-04:** Os registros de log são gerados e disponibilizados para monitoramento contínuo
  - **PR.PS-05:** A instalação e a execução de software não autorizado são evitadas
  - **PR.PS-06:** As práticas de desenvolvimento de software seguro são integradas e seu desempenho é monitorado durante todo o ciclo de vida do desenvolvimento de software
- **Resiliência da infraestrutura tecnológica (PR.IR):** As arquiteturas de segurança são gerenciadas com a estratégia de risco da organização para proteger a confidencialidade, a integridade e a disponibilidade dos ativos e a resiliência organizacional
  - **PR.IR-01:** As redes e os ambientes são protegidos contra acesso lógico e uso não autorizados
  - **PR.IR-02:** Os ativos de tecnologia da organização são protegidos contra ameaças ambientais
  - **PR.IR-03:** Os mecanismos são implementados para atingir os requisitos de resiliência em situações normais e adversas
  - **PR.IR-04:** Capacidade adequada de recursos para garantir a manutenção da disponibilidade

DETETAR (DE): Possíveis ataques e comprometimentos de segurança cibernética são encontrados e analisados

- **Monitoramento contínuo (DE.CM):** Os ativos são monitorados para encontrar anomalias, indicadores de comprometimento e outros eventos potencialmente adversos
  - **DE.CM-01:** As redes e os serviços de rede são monitorados para identificar eventos potencialmente adversos
  - **DE.CM-02:** O ambiente físico é monitorado para encontrar eventos potencialmente adversos
  - **DE.CM-03:** A atividade do pessoal e o uso da tecnologia são monitorados para identificar possíveis eventos adversos

- **DE.CM-06:** As atividades e os serviços dos prestadores de serviços externos são monitorados para identificar eventos potencialmente adversos
- **DE.CM-09:** O hardware e o software de computação, os ambientes de tempo de execução e seus dados são monitorados para encontrar eventos potencialmente adversos

- **Análise de eventos adversos (DE.AE):** Anomalias, indicadores de comprometimento e outros eventos potencialmente adversos são analisados para caracterizar os eventos e detectar incidentes de segurança cibernética
  - **DE.AE-02:** Os eventos potencialmente adversos são analisados para entender melhor as atividades associadas
  - **DE.AE-03:** As informações são correlacionadas a partir de várias fontes
  - **DE.AE-04:** O impacto estimado e o escopo dos eventos adversos são compreendidos
  - **DE.AE-06:** As informações sobre eventos adversos são fornecidas à equipe e às ferramentas autorizadas
  - **DE.AE-07:** A inteligência sobre ameaças cibernéticas e outras informações contextuais são integradas à análise
  - **DE.AE-08:** Os incidentes são declarados quando os eventos adversos atendem aos critérios de incidentes definidos

RESPONDER (RS): São tomadas ações relacionadas a um incidente de segurança cibernética detectado

- **Gerenciamento de incidentes (RS.MA):** As respostas aos incidentes de segurança cibernética detectados são gerenciadas
  - **RS.MA-01:** O plano de resposta a incidentes é executado em coordenação com terceiros relevantes assim que um incidente é declarado
  - **RS.MA-02:** Os relatórios de incidentes são triados e validados
  - **RS.MA-03:** Os incidentes são categorizados e priorizados
  - **RS.MA-04:** Os incidentes são escalonados ou elevados conforme necessário
  - **RS.MA-05:** Os critérios para iniciar a recuperação de incidentes são aplicados
- **Análise de incidentes (RS.AN):** As investigações são conduzidas para garantir uma resposta eficaz e apoiar as atividades forenses e de recuperação
  - **RS.AN-03:** A análise é realizada para estabelecer o que ocorreu durante um incidente e a causa raiz do incidente
  - **RS.AN-06:** As ações realizadas durante uma investigação são registradas, e a integridade e a procedência dos registros são preservadas

- **RS.AN-07:** Os dados e metadados de incidentes são coletados e sua integridade e procedência são preservadas
- **RS.AN-08:** A magnitude de um incidente é estimada e validada

- **Comunicação e relatórios de resposta a incidentes (RS.CO):** As atividades de resposta são coordenadas com as partes interessadas internas e externas, conforme exigido por leis, regulamentos ou políticas
  - **RS.CO-02:** As partes interessadas internas e externas são notificadas sobre incidentes
  - **RS.CO-03:** As informações são compartilhadas com as partes interessadas internas e externas designadas

- **Mitigação de incidentes (RS.MI):** São realizadas atividades para evitar a expansão de um evento e mitigar seus efeitos
  - **RS.MI-01:** Os incidentes são contidos
  - **RS.MI-02:** Os incidentes são erradicados

RECUPERAR (RC): Os ativos e as operações afetados por um incidente de segurança cibernética são restaurados

- **Execução do plano de recuperação de incidentes (RC.RP):** As atividades de restauração são realizadas para garantir a disponibilidade operacional dos sistemas e serviços afetados por incidentes de segurança cibernética
  - **RC.RP-01:** A parte de recuperação do plano de resposta a incidentes é executada após o início do processo de resposta a incidentes
  - **RC.RP-02:** As ações de recuperação são selecionadas, definidas no escopo, priorizadas e executadas
  - **RC.RP-03:** A integridade dos backups e de outros ativos de restauração é verificada antes de usá-los para a restauração
  - **RC.RP-04:** As funções de missão crítica e o gerenciamento de riscos de segurança cibernética são considerados para estabelecer normas operacionais pós-incidente
  - **RC.RP-05:** A integridade dos ativos restaurados é verificada, os sistemas e serviços são restaurados e o status operacional normal é confirmado
  - **RC.RP-06:** O fim da recuperação do incidente é declarado com base em critérios e a documentação relacionada ao incidente é concluída

- **Comunicação de recuperação de incidentes (RC.CO):** As atividades de restauração são coordenadas com partes internas e externas
  - **RC.CO-03:** As atividades de recuperação e o progresso na restauração das capacidades operacionais são comunicados às partes interessadas internas e externas designadas

- **RC.CO-04:** As atualizações públicas sobre a recuperação de incidentes são compartilhadas usando métodos e mensagens aprovados

Appendix B. Níveisda CSF

Table 2 contém uma ilustração fictícia dos Níveis da CSF discutidos na Seção 3. Os Níveis caracterizam o rigor das práticas de governança de riscos de segurança cibernética de uma organização ("Govern") e das práticas de gerenciamento de riscos de segurança cibernética (IDENTIFY, PROTECT, DETECT, RESPOND, e RECOVER).

Tabela 2. Ilustração fictícia dos níveis da CSF

Nível	Governança de riscos de segurança cibernética	Gerenciamento de riscos de segurança cibernética
Nível 1: Parcial	A aplicação da estratégia de risco de segurança cibernética organizacional é gerenciada de forma ad hoc. A priorização é ad hoc e não se baseia formalmente em objetivos ou no ambiente de ameaças.	A conscientização dos riscos de segurança cibernética é limitada em nível organizacional. A organização implementa o gerenciamento de riscos de segurança cibernética de forma irregular, caso a caso. A organização pode não ter processos que permitam que as informações de segurança cibernética sejam compartilhadas dentro da organização. Em geral, a organização não tem conhecimento dos riscos de segurança cibernética associados aos seus fornecedores e aos produtos e serviços que adquire e utiliza.
Nível 2: Risco informado	As práticas de gerenciamento de riscos são aprovadas pela gerência, mas podem não ser estabelecidas como política para toda a organização. A priorização das atividades de segurança cibernética e das necessidades de proteção é diretamente informada pelos objetivos de risco organizacional, pelo ambiente de ameaças ou pelos requisitos de negócios/missão.	Há uma conscientização dos riscos de segurança cibernética em nível organizacional, mas não foi estabelecida uma abordagem em toda a organização para gerenciar os riscos de segurança cibernética. A consideração da segurança cibernética nos objetivos e programas organizacionais pode ocorrer em alguns níveis da organização, mas não em todos. A avaliação do risco cibernético dos ativos organizacionais e externos ocorre, mas normalmente não é repetível ou recorrente. As informações de segurança cibernética são compartilhadas na organização de maneira informal. A organização está ciente dos riscos de segurança cibernética associados aos seus fornecedores e aos produtos e serviços que adquire e utiliza, mas não age de forma consistente ou formal em resposta a esses riscos.
Nível 3: Repetível	As práticas de gerenciamento de riscos da organização são formalmente aprovadas e expressas como política. As políticas, os processos e os procedimentos de risco informado são definidos, implementados conforme pretendido e revisados.	Existe uma abordagem em toda a organização para gerenciar os riscos de segurança cibernética. As informações sobre segurança cibernética são compartilhadas rotineiramente por toda a organização. Existem métodos consistentes para responder com eficácia às mudanças nos riscos. Os funcionários possuem o conhecimento e as habilidades para

Nível	Governança de riscos de segurança cibernética	Gerenciamento de riscos de segurança cibernética
	As práticas de segurança cibernética da organização são atualizadas regularmente com base na aplicação dos processos de gerenciamento de riscos às mudanças nos requisitos de negócios/missão, ameaças e cenário tecnológico.	desempenhar suas funções e responsabilidades designadas. A organização monitora de forma consistente e precisa os riscos de segurança cibernética dos ativos. Os executivos seniores de segurança cibernética e não cibernéticos se comunicam regularmente sobre os riscos de segurança cibernética. Os executivos garantem que a segurança cibernética seja considerada em todas as linhas de operação da organização. A estratégia de risco da organização é informada pelos riscos de segurança cibernética associados aos seus fornecedores e aos produtos e serviços que ela adquire e utiliza. Os funcionários agem formalmente sobre esses riscos por meio de mecanismos como acordos escritos para comunicar os requisitos básicos, estruturas de governança (por exemplo, conselhos de risco) e implementação e monitoramento de políticas. Essas ações são implementadas de forma consistente e conforme o planejado e são continuamente monitoradas e revisadas.
Nível 4: Adaptativo	Há uma abordagem em toda a organização para gerenciar os riscos de segurança cibernética que usa políticas, processos e procedimentos informados sobre riscos para lidar com possíveis eventos de segurança cibernética. A relação entre os riscos de segurança cibernética e os objetivos organizacionais é claramente compreendida e considerada na tomada de decisões. Os executivos monitoram os riscos de segurança cibernética no mesmo contexto dos riscos financeiros e de outros riscos organizacionais. O orçamento organizacional baseia-se em um entendimento do ambiente de risco atual e previsto e da tolerância ao risco. As unidades de negócios implementam a visão executiva e analisam os riscos em nível de sistema no contexto das tolerâncias de riscos organizacionais. O gerenciamento de riscos de segurança cibernética faz parte da cultura organizacional. Ele evolui a partir de uma conscientização das atividades anteriores e da conscientização contínua das	A organização adapta suas práticas de segurança cibernética com base em atividades anteriores e atuais de segurança cibernética, incluindo lições aprendidas e indicadores preditivos. Por meio de um processo de melhoria contínua que incorpora tecnologias e práticas avançadas de segurança cibernética, a organização se adapta ativamente a um cenário tecnológico em constante mudança e responde de maneira oportuna e eficaz a ameaças sofisticadas e em evolução. A organização usa informações em tempo real ou quase em tempo real para entender e agir de forma consistente sobre os riscos de segurança cibernética associados a seus fornecedores e aos produtos e serviços que adquire e utiliza. As informações de segurança cibernética são constantemente compartilhadas por toda a organização e com terceiros autorizados.

Nível	Governança de riscos de segurança cibernética	Gerenciamento de riscos de segurança cibernética
	atividades nos sistemas e redes organizacionais. A organização pode considerar de forma rápida e eficiente as mudanças nos objetivos do negócio/missão na forma como o risco é abordado e comunicado.	

Appendix C. Glossário

Categoria da CSF
Um grupo de resultados relacionados à segurança cibernética que, coletivamente, compõem uma Função CSF.

Perfil da comunidade CSF
Uma linha de base dos resultados da CSF que é criada e publicada para tratar de interesses e objetivos compartilhados entre várias organizações. Um Perfil da Comunidade é normalmente desenvolvido para um determinado setor, subsetor, tecnologia, tipo de ameaça ou outro caso de uso. Uma organização pode usar um Perfil da Comunidade como base para seu próprio Perfil Alvo.

CSF Core
Uma taxonomia de resultados de segurança cibernética de alto nível que pode ajudar qualquer organização a gerenciar seus riscos de segurança cibernética. Seus componentes são uma hierarquia de funções, categorias e subcategorias que detalham cada resultado.

Perfil atual da CSF
Parte de um Perfil Organizacional que especifica os resultados essenciais que uma organização está alcançando (ou tentando alcançar) no momento e caracteriza como ou até que ponto cada resultado está sendo alcançado.

Função da CSF
O mais alto nível de organização para resultados de segurança cibernética. Há seis funções CSF: *Govern, Identify, Protect, Detect, Respond*, e *Recover* (Governar, Identificar, Proteger, Detectar, Responder e Recuperar).

Exemplo de implementação da CSF
Uma ilustração concisa, orientada para a ação e nocional de uma maneira de ajudar a alcançar um resultado do CSF Core.

Referência informativa da CSF
Um mapeamento que indica uma relação entre um resultado da CSF Core e um padrão, diretriz, regulamento ou outro conteúdo existente.

Perfil organizacional da CSF
Um mecanismo para descrever a postura de segurança cibernética atual e/ou desejada de uma organização em termos dos resultados da CSF Core.

Guia de início rápido da CSF
Um recurso suplementar que fornece orientações breves e práticas sobre tópicos específicos relacionados à CSF.

Subcategoria da CSF
Um grupo de resultados mais específicos de atividades técnicas e gerenciais de segurança cibernética que compõem uma categoria da CSF.

Perfil alvo da CSF
Uma parte de um Perfil Organizacional que especifica os resultados principais desejados que uma organização selecionou e priorizou para atingir seus objetivos de gerenciamento de riscos de segurança cibernética.

Nível da CSF
Uma caracterização do rigor das práticas de governança e gerenciamento de riscos de segurança cibernética de uma organização. Há quatro Níveis: Parcial (Nível 1), Informado sobre riscos (Nível 2), Repetível (Nível 3) e Adaptativo (Nível 4).

Determinados equipamentos, instrumentos, software ou materiais comerciais ou não comerciais são identificados neste documento para especificar adequadamente o procedimento experimental. Tal identificação não implica recomendação ou endosso de qualquer produto ou serviço pelo NIST, nem implica que os materiais ou equipamentos identificados sejam necessariamente os melhores disponíveis para a finalidade.

Políticas da série técnica do NIST
Declarações de direitos autorais, uso e licenciamento
Sintaxe do identificador de publicação da série técnica do NIST

Como citar esta publicação da série técnica do NIST:
Instituto Nacional de Padrões e Tecnologia (2024) Estrutura de Segurança Cibernética (CSF) 2.0 do NIST (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 por. https://doi.org/10.6028/NIST.CSWP.29.por

Informações de contato
cyberframework@nist.gov

National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia)
Attn: Divisão de Segurança Cibernética Aplicada, Laboratório de Tecnologia da Informação
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Todos os comentários estão sujeitos à liberação de acordo com a Lei de Liberdade de Informação (FOIA).