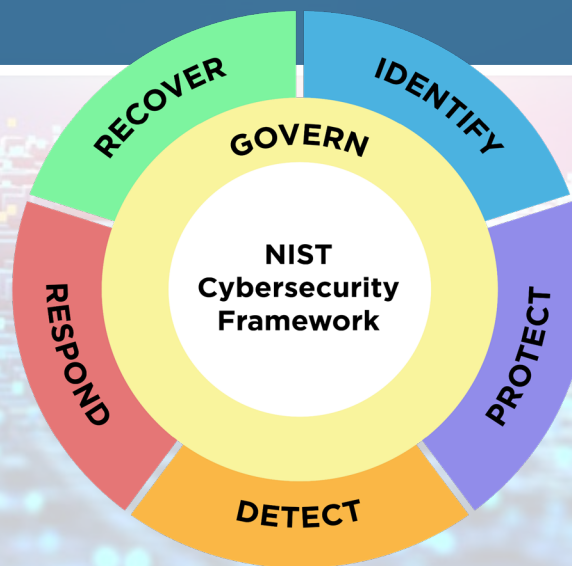




NIST Cybersecurity Framework 2.0:

Guia de início rápido para pequenas empresas



U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Publicação especial da NIST
NIST SP 1300 por
<https://doi.org/10.6028/NIST.SP.1300.por>
Fevereiro de 2024

NIST Cybersecurity Framework 2.0:

Guia de início rápido para pequenas empresas

Finalidade

Este guia fornece às pequenas e médias empresas (PMEs), especificamente àquelas que têm planos de segurança cibernética modestos ou inexistentes, considerações para dar início à sua estratégia de gerenciamento de riscos de segurança cibernética usando a Estrutura de Segurança Cibernética (CSF) 2.0 da NIST. O guia também pode ajudar outras organizações relativamente pequenas, como organizações sem fins lucrativos, órgãos governamentais e escolas. É um complemento à NIST CSF e não tem a intenção de substituí-la.

O que é a estrutura de segurança cibernética da NIST?

A Estrutura de Segurança Cibernética da NIST é uma orientação voluntária que ajuda as organizações - independentemente do tamanho, setor ou maturidade - a **compreender melhor, avaliar, priorizar e comunicar** seus esforços de segurança cibernética. A Estrutura não é uma abordagem única para todos para gerenciar os riscos de segurança cibernética. Este suplemento e a CSF 2.0 completa podem ajudar organizações a considerar e registrar suas próprias tolerâncias a riscos, prioridades, ameaças vulnerabilidades, requisitos, etc.

Primeiros passos com a estrutura de segurança cibernética

A CSF organiza os resultados da segurança cibernética em seis funções de alto nível: *Govern, Identify, Protect, Detect, Respond, e Recover* (Governar, Identificar, Proteger, Detectar, Responder e Recuperar). Essas funções, quando consideradas em conjunto, fornecem uma visão abrangente do gerenciamento do risco de segurança cibernética. As atividades listadas para cada função neste guia podem oferecer um bom ponto de partida para sua empresa. Para obter exemplos específicos e orientados para a ação de como realizar as atividades listadas, consulte os [Exemplos de Implementação da CSF 2.0](#). Se houver atividades contidas neste guia que você não entenda ou não se sinta à vontade para abordar por conta própria, este guia pode servir como um prompt de discussão com quem você escolheu para ajudá-lo a reduzir seus riscos de segurança cibernética, como um provedor de serviços de segurança gerenciada (MSSP).



EXPLORE MAIS RECURSOS DA CSF 2.0

nist.gov/cyberframework

Encontre rapidamente o que você precisa, incluindo:

- ✓ Um conjunto de NOVOS Guias de início rápido
 - ✓ Exemplos de implementação
 - ✓ Ferramentas de pesquisa
- ✓ Perguntas frequentes
 - ✓ E muito mais!

GOVERNAR



A função Governar ajuda a estabelecer e monitorar a estratégia, as expectativas e a política de gerenciamento de riscos de segurança cibernética da sua empresa.

Ações a serem consideradas

Entender

- Entenda como os riscos de segurança cibernética podem atrapalhar o cumprimento da missão da sua empresa. (GV.OC-01)
- Entenda seus requisitos legais, regulamentares e contratuais de segurança cibernética. (GV.OC-03)
- Entenda quem, em sua empresa, será responsável por desenvolver e executar a estratégia de segurança cibernética. (GV.RR-02)

Avaliar

- Avalie o impacto potencial de uma perda total ou parcial de ativos e operações comerciais essenciais. (GV.OC-04)
- Avalie se o seguro de segurança cibernética é adequado para sua empresa. (GV.RM-04)
- Avalie os riscos de segurança cibernética apresentados por fornecedores e outros terceiros antes de estabelecer relacionamentos formais. (GV.SC-06)

Priorizar

- Priorize o gerenciamento dos riscos de segurança cibernética juntamente com outros riscos comerciais. (GV.RM-03)

Comunicar

- Comunique o apoio da liderança a uma cultura consciente dos riscos, ética e de melhoria contínua. (GV.RR-01)
- Comunique, aplique e mantenha políticas para gerenciar os riscos de segurança cibernética. (GV.PO-01)

Introdução à governança de segurança cibernética

Você pode usar essas tabelas para começar a pensar na sua estratégia de governança de segurança cibernética.

Defina o contexto organizacional		Documentação dos requisitos de segurança cibernética	
Nossa declaração de missão comercial:		Liste seus requisitos legais:	
Quais riscos de segurança cibernética podem nos impedir de cumprir essa missão?		Liste seus requisitos regulatórios:	
		Liste seus requisitos contratuais:	

Mergulho técnico profundo: [Preparação dos riscos de segurança cibernética para o gerenciamento de riscos corporativos e a supervisão da governança](#)

Perguntas a serem consideradas

- À medida que nossa empresa cresce, com que frequência estamos revisando nossa estratégia de segurança cibernética?
- Precisamos aprimorar as habilidades de nossa equipe atual, contratar talentos ou contratar um parceiro externo para nos ajudar a estabelecer e gerenciar nosso plano de segurança cibernética?
- Temos políticas de uso aceitável em vigor para a empresa e para os dispositivos de propriedade dos funcionários que acessam os recursos da empresa? Os funcionários foram instruídos sobre essas políticas?

Recursos relacionados

- [Manual de recursos para a segurança de cadeias de suprimentos de pequeno e médio porte](#)
- [Escolher um fornecedor/prestador de serviços](#)

[Veja todos os recursos da NIST CSF 2.0 aqui](#)

IDENTIFICAR



A função Identify ajuda a determinar o risco atual de segurança cibernética para a empresa.

Ações a serem consideradas

Entender

- Entenda de quais ativos sua empresa depende, criando e mantendo um inventário de hardware, software, sistemas e serviços. *(ID.AM -01/ 02/04)*

Avaliar

- Avalie seus ativos (físicos e de TI) quanto a possíveis vulnerabilidades. *(ID.RA-01)*
- Avalie a eficácia do programa de segurança cibernética da empresa para identificar as áreas que precisam ser melhoradas. *(ID.IM-01)*

Priorizar

- Priorize o inventário e a classificação de seus dados comerciais. *(ID.AM-07)*
- Priorize a documentação das ameaças internas e externas à segurança cibernética e as respostas associadas usando um registro de riscos. *(ID.RA)*

Comunicar

- Comunique planos, políticas e práticas recomendadas de segurança cibernética a toda a equipe e a terceiros relevantes. *(ID.IM-04)*
- Comunique à equipe a importância de identificar as melhorias necessárias nos processos, procedimentos e atividades de gerenciamento de riscos de segurança cibernética. *(ID.IM)*

Introdução à identificação do risco atual de segurança cibernética para sua empresa

Antes de proteger seus ativos, é necessário identificá-los. Em seguida, você pode determinar o nível adequado de proteção para cada ativo com base em sua sensibilidade e criticidade para a missão de seus negócios. Você pode usar esta tabela de exemplo para começar a fazer seu inventário de ativos de tecnologia da informação (TI). À medida que sua empresa amadurece, você pode considerar o uso de uma solução automatizada de inventário de ativos ou de um provedor de serviços gerenciados de segurança para ajudá-lo a gerenciar todos os seus ativos comerciais.

Software/ hardware/ sistema/ serviço	Uso oficial do ativo:	Administrador ou proprietário do ativo:	Identifique os dados confidenciais aos quais o ativo tem acesso:	A autenticação multifatorial é necessária para acessar esse ativo?	Risco para os negócios se perdermos o acesso a esse ativo

Mergulho técnico profundo: [Integração da segurança cibernética e do gerenciamento de riscos corporativos](#)

Perguntas a serem consideradas

- Quais são os nossos ativos comerciais mais importantes (dados, hardware, software, sistemas, instalações, serviços, pessoas etc.) que precisamos proteger?
- Quais são os riscos de segurança cibernética e de privacidade associados a cada ativo?
- Quais tecnologias ou serviços a equipe está usando para realizar seu trabalho? Esses serviços ou tecnologias são seguros e aprovados para uso?

Recursos relacionados

- [Modelo de registro de risco da NIST](#)
- [Faça um balanço. Saiba quais informações confidenciais você possui](#)
- [Avaliando sua resiliência operacional e práticas de segurança cibernética](#)

[Veja todos os recursos da NIST CSF 2.0 aqui](#)

PROTEGER



A função Protect oferece suporte à sua capacidade de usar proteções para evitar ou reduzir os riscos de segurança cibernética.

Ações a serem consideradas

Entender

- Entenda a quais informações os funcionários devem ou têm acesso. Restrinja o acesso a informações confidenciais apenas aos funcionários que precisam delas para realizar seu trabalho. (PR.AA-05)

Avaliar

- Avalie a pontualidade, a qualidade e a frequência do treinamento de segurança cibernética da sua empresa para os funcionários. (PR.AT-01/02)

Priorizar

- Priorize a exigência de autenticação multi-fator em todas as contas que a oferecem e considerar o uso de gerenciadores de senhas para ajudar você e sua equipe a gerar e proteger senhas fortes. (PR.AA-03)
- Priorize a alteração das senhas padrão do fabricante. (PR.AA-01)
- Priorize a atualização regular e a aplicação de patches em softwares e sistemas operacionais. Ative as atualizações automáticas para ajudá-lo a se lembrar. (PR.PS-02)
- Priorize o backup regular de seus dados e o teste de seus backups. (PR.DS-11)
- Priorize a configuração de seus tablets e laptops para ativar a criptografia de disco completo para proteger os dados. (PR.DS-01)

Comunicar

- Comunique à sua equipe como reconhecer ataques comuns, relatar ataques ou atividades suspeitas e realizar tarefas básicas de higiene cibernética. (PR.AT-01/02)

Introdução à proteção de sua empresa

A ativação da autenticação multifator (MFA) é uma das maneiras mais rápidas e econômicas de proteger seus dados. Começar com as contas que podem acessar as informações mais confidenciais. Usar esta lista de verificação para dar um começo, mas lembre-se de que sua própria lista será maior do que isso:

Conta	MFA ativado (S/N)
Conta(s) bancária(s)	
Conta(s) contábil(eis) e fiscal(is)	
Conta(s) de comerciante	
Conta(s) de ID do Google, Microsoft e/ou Apple	
Conta(s) de e-mail	
Gerenciador(es) de senhas	
Conta(s) do website	

Mergulho técnico profundo: [Diretrizes de identidade digital da NIST](#)

Perguntas a serem consideradas

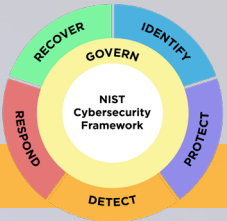
- Estamos restringindo o acesso e os privilégios apenas àqueles que precisam deles? Estamos removendo o acesso quando eles não precisam mais dele?
- Como estamos higienizando e destruindo com segurança os dados e os dispositivos de armazenamento de dados quando eles não são mais necessários?
- Os funcionários possuem o conhecimento e as habilidades necessárias para desempenhar suas funções com a segurança em mente?

Recursos relacionados

- [Recursos de treinamento em segurança cibernética](#)
- [Autenticação multifatorial](#)
- [Protegendo sua empresa contra phishing](#)

[Veja todos os recursos da NIST CSF 2.0 aqui](#)

DETECTAR



A função Detect fornece resultados que o ajudam a encontrar e analisar possíveis ataques e comprometimentos de segurança cibernética.

Ações a serem consideradas

Entender

- Entenda como identificar indicadores comuns de um incidente de segurança cibernética. *(DE.CM)*

Avaliar

- Avalie suas tecnologias de computação e serviços externos quanto a desvios do comportamento esperado ou típico. *(DE.CM-06/09)*
- Avalie seu ambiente físico quanto a sinais de adulteração ou atividade suspeita. *(DE.CM-02)*

Priorizar

- Priorize a instalação e a manutenção de software antivírus e anti-malware em todos os dispositivos da empresa - incluindo servidores, desktops e laptops. *(DE.CM-09)*
- Priorize a contratação de um provedor de serviços para monitorar computadores e redes em busca de atividades suspeitas se você não tiver os recursos para fazer isso internamente. *(DE.CM)*

Comunicar

- Comunique com o responsável autorizado pelo incidente, como um MSSP, sobre os detalhes relevantes do incidente para ajudá-lo a analisá-lo e atenuá-lo. *(DE.AE-06/07)*

Primeiros passos na detecção de incidentes

Alguns indicadores comuns de um incidente de segurança cibernética são:



- Perda do acesso habitual a dados, aplicativos ou serviços
- Rede com lentidão incomum
- O software antivírus alerta quando detecta que um host está infectado com malware
- Várias tentativas de login com falha
- Um administrador de e-mail vê muitos e-mails devolvidos com conteúdo suspeito
- Um administrador de rede percebe um desvio incomum dos fluxos de tráfego de rede típicos

Mergulho técnico profundo: [Guia de tratamento de incidentes de segurança de computadores da NIST](#)

Perguntas a serem consideradas

- Os dispositivos usados em nossa empresa, sejam eles de propriedade da empresa ou dos funcionários, têm software antivírus instalado?
- Os funcionários sabem como detectar possíveis ataques à segurança cibernética e como denunciá-los?
- Como nossa empresa está monitorando seus registros e alertas para detectar possíveis incidentes cibernéticos?

Recursos relacionados

- [Proteção e resposta a ransomware](#)
- [Detecção de uma possível intrusão](#)
- [Recursos de treinamento em segurança cibernética](#)

[Veja todos os recursos da NIST CSF 2.0 aqui](#)

RESPONDER



A função Respond apoia sua capacidade de tomar medidas em relação a um incidente de segurança cibernética detectado.

Ações a serem consideradas

Entender

- Entenda qual é o seu plano de resposta a incidentes e quem tem autoridade e responsabilidade pela implementação de vários aspectos do plano. *(RS.MA-01)*

Avaliar

- Avalie sua capacidade de responder a um incidente de segurança cibernética. *(RS.MA-01)*
- Avalie o incidente para determinar sua gravidade, o que aconteceu e sua causa principal. *(RS.AN-03, RS.MA-03)*

Priorizar

- Priorize a adoção de medidas para conter e erradicar o incidente para evitar mais danos. *(RS.MI)*

Comunicar

- Comunique um incidente de segurança cibernética confirmado a todas as partes interessadas internas e externas (por exemplo, clientes, parceiros de negócios, agências de aplicação da lei, órgãos reguladores), conforme exigido por leis, regulamentos, contratos ou políticas. *(RS.CO-02/03)*

Primeiros passos com um plano de resposta a incidentes

Antes da ocorrência de um incidente, você deve estar preparado(a) com um plano de resposta básico. Isso será personalizado de acordo com a empresa, mas deve incluir:

- ✓ **Um defensor de negócios:** Alguém que seja responsável por desenvolver e manter seu plano de resposta a incidentes.
- ✓ **Para quem ligar:** Liste todos os indivíduos que podem fazer parte de seus esforços de resposta a incidentes. Inclua suas informações de contato, responsabilidades e autoridade.
- ✓ **O que/quando/como reportar:** Liste as responsabilidades de comunicação/relatórios de sua empresa, conforme exigido por leis, regulamentos, contratos ou políticas.

Mergulho técnico profundo: [Guia de tratamento de incidentes de segurança de computadores da NIST](#)

Perguntas a serem consideradas

- Temos um plano de resposta a incidentes de segurança cibernética? Em caso afirmativo, já o praticamos para ver se é viável?
- Sabemos quem são as principais partes interessadas internas e externas e os tomadores de decisão que ajudarão se tivermos um incidente de segurança cibernética confirmado?

Recursos relacionados

- [Noções básicas do plano de resposta a incidentes](#)
- [Centro de Reclamações sobre Crimes na Internet do FBI](#)
- [Resposta a violações de dados: Um guia para empresas](#)
- [Boas práticas recomendadas para a resposta às vítimas e a denúncia de incidentes cibernéticos](#)

Contato	Telef one
Líder empresarial:	
Contato técnico:	
Polícia Estadual:	
Legal:	
Banco:	
Seguro:	

[Veja todos os recursos da NIST CSF 2.0 aqui](#)

RECUPERAR



A função Recover envolve atividades para restaurar ativos e operações que foram afetados por um incidente de segurança cibernética.

Ações a serem consideradas

Entender

- Entenda quem, dentro e fora de sua empresa, tem responsabilidades de recuperação. *(RC.RP-01)*

Avaliar

- Avalie o que aconteceu preparando um relatório pós-ação - por conta própria ou em consulta com um fornecedor/parceiro - que documente o incidente, as ações de resposta e recuperação tomadas e as lições aprendidas. *(RC.RP-06)*
- Avalie a integridade de seus dados e ativos de backup antes de usá-los para restauração. *(RC.RP-03)*

Priorizar

- Priorize suas ações de recuperação com base nas necessidades organizacionais, nos recursos e nos ativos afetados. *(RC.RP-02)*

Comunicar

- Comunique regularmente e de forma segura com as partes interessadas internas e externas. *RC.CO*
- Comunique e documente a conclusão do incidente e a retomada das atividades normais. *(RC.RP-06)*

Começando com um manual de recuperação

Um manual normalmente inclui os seguintes elementos essenciais:

- ✓ Um conjunto de processos formais de recuperação
- ✓ Documentação da criticidade dos recursos organizacionais (por exemplo, pessoas, instalações, componentes técnicos, serviços externos)
- ✓ Documentação de sistemas que processam e armazenam informações organizacionais, especialmente ativos importantes. Isso ajudará a informar a ordem de prioridade da restauração
- ✓ Uma lista do pessoal que será responsável pela definição e implementação dos planos de recuperação
- ✓ Um plano abrangente de comunicações de recuperação

Mergulho técnico profundo: [Guia da NIST para recuperação de eventos de segurança cibernética](#)

Perguntas a serem consideradas

- Quais são nossas lições aprendidas? Como podemos minimizar as chances de ocorrer um incidente de segurança cibernética no futuro?
- Quais são as nossas obrigações legais, regulamentares e contratuais de comunicação com as partes interessadas internas e externas sobre um incidente de segurança cibernética?
- Como podemos garantir que as medidas de recuperação que estamos adotando não estão introduzindo novas vulnerabilidades em nossos negócios?

Recursos relacionados

- [Recursos de treinamento em segurança cibernética](#)
- [Criação de um plano de recuperação de desastres de TI](#)
- [Backup e recuperação de recursos](#)

[Veja todos os recursos da NIST CSF 2.0 aqui](#)

Perfis e recursos adicionais



Uso de perfis organizacionais para implementar a estrutura de segurança cibernética

Um perfil organizacional da CSF descreve a postura de segurança cibernética atual e/ou desejada de uma organização em termos dos resultados de segurança cibernética do Núcleo da CSF. 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.
 - Além disso, considere o uso de um **Perfil da Comunidade** como base para o Perfil Alvo. Um Perfil da Comunidade é normalmente desenvolvido para um determinado setor, subsetor, tecnologia, tipo de ameaça ou outro caso de uso.
 - Você também pode optar por usar a **CSF Tiers** para informar a criação do seu Perfil. Os níveis caracterizam o rigor atual ou pretendido das práticas de uma organização por função ou categoria do CSF. Consulte o [Quick-Start Guide for Using the CSF Tiers](#) ([Guia de início rápido para usar as camadas da CSF](#)) para obter mais informações sobre as camadas e seu uso.

Veja o [Quick-Start Guide for Creating and Using Organizational Profiles](#) ([Guia de início rápido para criar e usar perfis organizacionais](#)) para obter informações mais detalhadas sobre como começar a criar perfis atuais e de destino para sua organização.

Recursos adicionais

A [NIST Cybersecurity Framework Reference Tool](#) ([Ferramenta de referência da estrutura de segurança cibernética da NIST](#)) permite que os usuários explorem a CSF 2.0 Core completo em versões legíveis por humanos e máquinas (em JSON e Excel), além de manter recursos com informações para ajudá-lo a alcançar os resultados desejados, como:

- [Mapeamento](#): Referências informativas são mapeamentos que indicam as relações entre a CSF 2.0 e vários padrões, diretrizes, regulamentos e outros conteúdos. Ajudam a informar como uma organização pode alcançar os resultados do Núcleo.
- Os [exemplos de implementação](#) fornecem ilustrações de etapas concisas e orientadas para a ação para guiar as organizações na obtenção dos resultados da CSF. Os exemplos não são uma lista abrangente de todas as ações que poderiam ser adotadas por uma organização, nem uma linha de base das ações necessárias; são um conjunto de exemplos úteis para fazer com que as organizações pensem em medidas concretas.

A [NIST Cybersecurity and Privacy Reference Tool](#) ([CPRT - Ferramenta de Referência de Segurança Cibernética e Privacidade da NIST](#)) oferece uma maneira simples de acessar dados de referência de vários padrões, diretrizes e estruturas de segurança cibernética e privacidade da NIST, que podem ser baixados em formatos comuns (XLSX e JSON).

O [NIST SP 800-53](#) fornece um catálogo de controles de segurança e privacidade que você pode escolher. Os controles são flexíveis, personalizáveis e implementados como parte de um processo que abrange toda a organização para gerenciar riscos. [Visualize e exporte](#) a partir da Cybersecurity and Privacy Reference Tool (CPRT - Ferramenta de Referência de Segurança Cibernética e Privacidade).

O [The Workforce Framework for Cybersecurity](#) ([Estrutura da Força de Trabalho para Segurança Cibernética \(NICE Framework\)](#)) ajuda os empregadores a alcançar os resultados da CSF 2.0, auxiliando-os a identificar lacunas críticas na equipe e nos recursos de segurança cibernética; determinar e comunicar as responsabilidades e descrições de cargos; e fornecer treinamento de pessoal e planos de carreira.