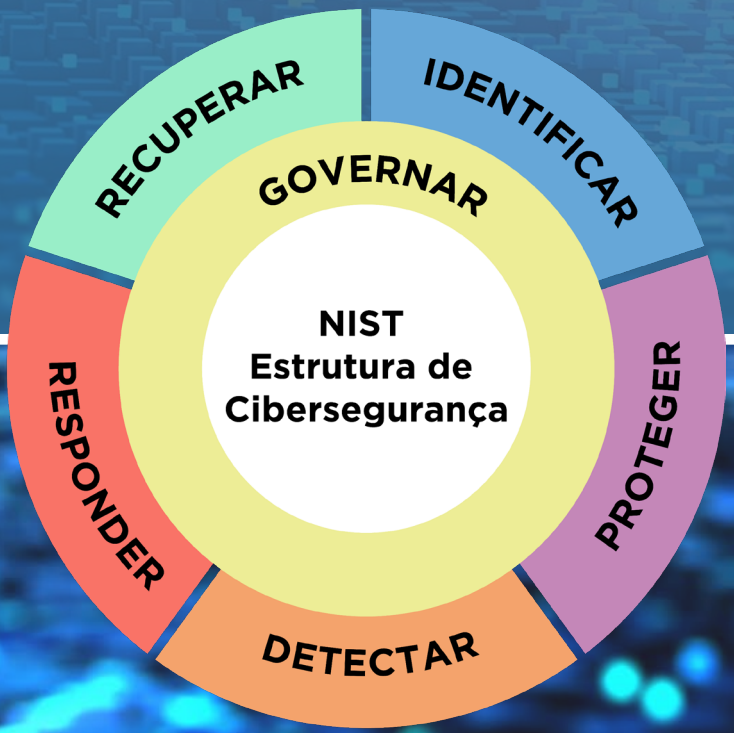
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0:

GUIA DE RECURSOS E VISÃO GERAL



NIST Publicação Especial
NIST SP 1299 por

https://doi.org/10.6028/NIST.SP.1299.por
Fevereiro de 2024

NIST CSF 2.0:
GUIA DE RECURSOS E VISÃO GERAL

O QUE É A CSF 2.0... E FORMAS POPULARES DE USÁ-LA?

A Estrutura de Cibersegurança do NIST (CSF) 2.0 pode ajudar as organizações a gerenciar e reduzir seus riscos de segurança cibernética à medida que iniciam ou melhoram seu programa de segurança cibernética. A CSF descreve os resultados específicos que as organizações podem alcançar para lidar com o risco. Outros recursos do NIST ajudam a explicar ações específicas que podem ser tomadas para alcançar cada resultado. *Este guia é um suplemento ao NIST CSF e não se destina a substituí-lo.*

A CSF 2.0, juntamente com os recursos suplementares do NIST, pode ser usada pelas organizações para entender, avaliar, priorizar e comunicar os riscos de segurança cibernética; é particularmente útil para promover a comunicação interna e externa entre as equipes — bem como a integração com estratégias mais amplas de gerenciamento de riscos.

A CSF 2.0 é organizada em seis Funções — **Governar, Identificar, Proteger, Detectar, Responder** e **Recuperar.** Juntas, essas funções fornecem uma visão abrangente para gerenciar o risco de segurança cibernética. Este *Guia de Recursos e Visão Geral* oferece detalhes sobre cada Função para servir como potenciais pontos de partida.

A CSF 2.0 é composta por:

- **Núcleo da CSF** - Uma taxonomia de resultados de segurança cibernética de alto nível que pode ajudar qualquer organização a gerenciar seus riscos de segurança cibernética.
- **Perfis Organizacionais da CSF** - Um mecanismo para descrever a postura de segurança cibernética atual e/ou alvo de uma organização em termos dos resultados do Núcleo da CSF.
- **Camadas CSF** - Podem ser aplicadas aos Perfis Organizacionais CSF para caracterizar o rigor das práticas de governança e gestão de riscos de segurança cibernética de uma organização.

NIST CSF 2.0:
GUIA DE RECURSOS E VISÃO GERAL

EXPLORAR MAIS RECURSOS CSF 2.0

Referências Informativas	**Visualize e crie mapeamentos entre a CSF 2.0 e outros documentos.** Você quer enviar seus mapeamentos para documentos do NIST e exibi-los em nosso site? Por favor, clique no link à esquerda ou envie um e-mail para olir@nist.gov se tiver alguma dúvida.
Ferramenta de Referência de Segurança Cibernética e Privacidade (CPRT)	**Navegue e baixe o Núcleo da CSF 2.0 & conteúdo mapeado**. A CPRT fornece um mecanismo centralizado, padronizado e modernizado para gerenciar conjuntos de dados de referência (e oferece um formato consistente para acessar dados de referência de vários padrões, diretrizes e estruturas de segurança cibernética e privacidade do NIST).
Exemplos de Implementação	Visualize e baixe exemplos nocionais de etapas concisas e orientadas para a ação para ajudar a alcançar os resultados das Subcategorias do FCS 2.0, além das orientações fornecidas nas Referências Informativas.
Ferramenta de Referência CSF 2.0	Acesse versões legíveis por humanos e máquinas do Núcleo (em JSON e Excel). Você também pode visualizar e exportar partes dos principais termos de pesquisa.

Recursos Adicionais Incluem:

Perfis da comunidade e modelos de perfil (ajude as organizações a colocar a CSF em prática)

Ferramentas de pesquisa (simplifique e agilize à medida que procura informações específicas)

Documentos conceituais (saiba mais sobre vários tópicos da CSF)

Perguntas frequentes (veja o que os outros estão perguntando e obtenha respostas para as principais perguntas)

Explore o conjunto de recursos da CSF 2.0 do NIST

NIST CSF 2.0:
GUIA DE RECURSOS E VISÃO GERAL

NAVEGANDO PELOS GUIAS DE INÍCIO RÁPIDO (QSG) CSF 2.0 do NIST

Tipo QSG	Descrição	Explorar
Pequenas Empresas (PMEs)	Fornece às PMEs, especificamente aquelas que têm planos modestos ou inexistentes de segurança cibernética, considerações para iniciar sua estratégia de gerenciamento de riscos de segurança cibernética.	Veja o QSG
Criando e Usando Perfis Organizacionais	Fornece a todas as organizações considerações para criar e usar Perfis Atuais e/ou Alvo para implementar a CSF 2.0.	Veja o QSG
Usando as Camadas da CSF	Explica como qualquer organização pode aplicar as Camadas CSF aos Perfis Organizacionais para caracterizar o rigor de suas práticas de governança e gestão de riscos de segurança cibernética.	Veja o QSG
Rascunho do Gerenciamento de Riscos da Cadeia de Suprimentos de Segurança Cibernética (C-SCRM)	Ajuda todas as organizações a se tornarem adquirentes e fornecedores inteligentes de produtos e serviços de tecnologia, melhorando seus processos de C-SCRM.	Veja o QSG
Rascunho de Profissionais de Gerenciamento de Riscos Corporativos (ERM)	Detalhes de como os profissionais de Gerenciamento de Riscos Corporativos podem utilizar os resultados fornecidos no CSF 2.0 para melhorar o gerenciamento de riscos de segurança cibernética organizacional.	Veja o QSG

...e muito mais a seguir no futuro.

Ver o repositório QSG on-line atual

NIST CSF 2.0: GUIA DE RECURSOS E VISÃO GERAL

GOVERNAR

A estratégia, as expectativas e a política de gerenciamento de risco cibernético da organização são estabelecidas, comunicadas e monitoradas

Compreender e avaliar necessidades específicas de segurança cibernética. Determinar os riscos e as necessidades exclusivas de sua organização. Discutir o ambiente de risco atual e previsto e a quantidade de risco que sua organização está disposta a aceitar. Buscar informações e ideias de toda a organização. Entender o que funcionou ou não funcionou bem no passado e discutir abertamente.

Desenvolver uma estratégia de risco de segurança cibernética personalizada. Isso deve ser baseado nos objetivos específicos de segurança cibernética de sua organização, no ambiente de risco e nas lições aprendidas com o passado — e com os outros. Gerenciar, atualizar e discutir a estratégia em intervalos regulares. As funções e responsabilidades devem ser claras.

Estabelecer políticas de gerenciamento de riscos definidas. As políticas devem ser aprovadas pela administração e devem ser organizacionais, repetíveis e recorrentes, e devem estar alinhadas com o ambiente atual de ameaças à segurança cibernética, riscos (que mudarão ao longo do tempo) e objetivos da missão. Incorporar políticas na cultura da empresa para ajudar a impulsionar e inspirar a capacidade de tomar decisões informadas. Responsabilizar-se por obrigações legais, regulatórias e contratuais.

Desenvolver e comunicar práticas organizacionais de segurança cibernética. Elas devem ser diretas e comunicadas regularmente. Eles devem refletir a aplicação do gerenciamento de riscos a mudanças na missão ou requisitos de negócios, ameaças e cenário técnico geral. Documentar as práticas e compartilhá-las com espaço para feedback e agilidade para mudar de curso.

Estabelecer e monitorar o gerenciamento de riscos da cadeia de suprimentos de segurança cibernética. Estabelecer estratégia, política, funções e responsabilidades — inclusive para supervisionar fornecedores, clientes e parceiros. Incorporar requisitos nos contratos. Envolver parceiros e fornecedores no planejamento, resposta e recuperação.

Implementar supervisão e pontos de verificação contínuos. Analisar os riscos em intervalos regulares e monitorá-los continuamente (assim como faria com os riscos financeiros).

IDENTIFICAR

Os riscos de cibersegurança atuais da organização são compreendidos.

Identificar processos e ativos críticos de negócios. Considerar quais das atividades de sua organização absolutamente devem continuar a ser viáveis. Por exemplo, isso pode incluir manter um site para receber pagamentos, proteger com segurança as informações de clientes/pacientes ou garantir que as informações críticas para sua organização permaneçam acessíveis e precisas.

Manter inventários de hardware, software, serviços e sistemas. Saiba quais computadores e softwares sua organização utiliza — incluindo serviços fornecidos por fornecedores —, pois esses são frequentemente os pontos de entrada de agentes mal-intencionados. Esse inventário pode ser tão simples quanto uma planilha. Considere incluir dispositivos e aplicativos próprios, alugados e pessoais dos funcionários.

Fluxos de informações do documento. Considere que tipo de informação sua organização coleta e usa (e onde os dados estão localizados e como eles são usados), especialmente quando contratos e parceiros externos estão envolvidos.

Identifique ameaças, vulnerabilidades e riscos aos ativos. Informados pelo conhecimento de ameaças internas e externas, os riscos devem ser identificados, avaliados e documentados. Exemplos de maneiras de documentá-los incluem registros de risco – repositórios de informações de risco, incluindo dados sobre riscos ao longo do tempo. Garantir que as respostas aos riscos sejam identificadas, priorizadas e executadas, e que os resultados sejam monitorados.

As lições aprendidas são usadas para identificar melhorias. Ao conduzir as operações comerciais do dia-a-dia, é importante identificar maneiras de refinar ou melhorar ainda mais o desempenho, incluindo oportunidades para gerenciar e reduzir melhor os riscos de segurança cibernética. Isso requer um esforço intencional de sua organização em todos os níveis. Se houver um incidente, avalie o que aconteceu. Prepare um relatório pós-ação que documente o incidente, a resposta, as ações de recuperação tomadas e as lições aprendidas.

NIST CSF 2.0: GUIA DE RECURSOS E VISÃO GERAL

PROTEGER

Salvaguardas para gerenciar o riscos de segurança cibernética da organização são usadas.

Gerenciar acesso. Crie contas exclusivas para os funcionários e garanta que os usuários tenham acesso apenas aos recursos necessários. Autentique os usuários antes que eles tenham acesso a informações, computadores e aplicativos. Gerenciar e rastrear o acesso físico às instalações/dispositivos.

Treinar os usuários. Treine regularmente os funcionários para garantir que estejam cientes das políticas e procedimentos de segurança cibernética e que tenham conhecimento e habilidades para executar tarefas gerais e específicas; explique como reconhecer ataques comuns e relate atividades suspeitas. Certas funções podem exigir treinamento extra.

Proteger e monitorar seus dispositivos. Considere o uso de produtos de segurança de endpoint. Aplique configurações uniformes aos dispositivos e controle as alterações nas configurações do dispositivo. Desative serviços ou recursos que não suportam funções de missão. Configure sistemas e serviços para gerar registros de log. Certifique-se de que os dispositivos sejam descartados com segurança.

Proteger dados confidenciais. Certifique-se de que os dados confidenciais armazenados ou transmitidos sejam protegidos por criptografia. Considere utilizar a verificação de integridade para que apenas alterações aprovadas sejam feitas nos dados. Exclua e/ou destrua dados com segurança quando não forem mais necessários.

Gerenciar e manter o software. Atualize regularmente sistemas operacionais e aplicativos; habilitar atualizações automáticas. Substitua o software em fim de vida por versões suportadas. Considere o uso de ferramentas de software para verificar se há vulnerabilidades adicionais nos dispositivos e corrigi-las.

Realizar backups regulares. Faça backup de dados em horários acordados ou use recursos de backup integrados; soluções de software e nuvem podem automatizar esse processo. Mantenha pelo menos um conjunto de dados com backups frequentes offline para protegê-los contra ransomware. Teste para garantir que os dados de backup possam ser restaurados com sucesso nos sistemas.

DETECTAR

Possíveis ataques e comprometimentos de segurança cibernética são encontrados e analisados.

Monitorar redes, sistemas e instalações continuamente para encontrar eventos potencialmente adversos. Desenvolva e tese processos e procedimentos para detecção de indicadores de um incidente de segurança cibernética na rede e no ambiente físico. Coletar informações de registro de várias fontes organizacionais para ajudar na detecção de atividades não autorizadas.

Determinar e analisar o impacto estimado e o escopo dos eventos adversos. Se um evento de segurança cibernética for detectado, sua organização deve trabalhar de forma rápida e completa para entender o impacto do incidente. Compreenda detalhes sobre quaisquer incidentes de segurança cibernética ajudará a informar a resposta.

Fornecer informações sobre eventos adversos a funcionários e ferramentas autorizados. Quando eventos adversos são detectados, forneça informações sobre o evento internamente ao pessoal autorizado para garantir que as ações apropriadas de resposta a incidentes sejam tomadas.

NIST CSF 2.0: GUIA DE RECURSOS E VISÃO GERAL

RESPONDER

Ações em relação a um incidente de segurança cibernética são tomadas.

Executar um plano de resposta a incidentes assim que um incidente for declarado, em coordenação com terceiros relevantes.
Para executar adequadamente um plano de resposta a incidentes, certifique-se de que todos conheçam suas responsabilidades; isso inclui entender quaisquer requisitos (por exemplo, regulatórios, relatórios legais e compartilhamento de informações).

Categorizar e priorizar os incidentes e encaminhar ou elevar conforme necessário. Analise o que está ocorrendo, determine a causa raiz do incidente e priorize quais incidentes exigem atenção primeiro de sua organização. Comunique essa priorização à sua equipe e garanta que todos entendam a quem as informações devem ser comunicadas em relação a um incidente priorizado quando ele ocorrer.

Coletar dados de incidentes e preservar sua integridade e procedência. Colete informações de maneira segura ajudará na resposta de sua organização a um incidente. Garanta que os dados ainda estejam seguros após o incidente para manter a reputação e a confiança de sua organização das partes interessadas. Armazene essas informações de maneira segura também pode ajudar a informar planos de resposta atualizados e futuros para serem ainda mais eficazes.

Notificar as partes interessadas internas e externas sobre quaisquer incidentes e compartilhe informações sobre incidentes com elas — seguindo as políticas definidas por sua organização. Compartilhar com segurança informações consistentes com planos de resposta e acordos de compartilhamento de informações. Notificar parceiros de negócios e clientes sobre incidentes de acordo com os requisitos contratuais.

Conter e erradicar incidentes. A execução de um plano de resposta desenvolvido e testado ajudará sua organização a conter os efeitos de um incidente e erradicá-lo. Uma coordenação e comunicação significativas com as partes interessadas podem resultar em uma resposta e mitigação mais eficazes do incidente.

RECUPERAR

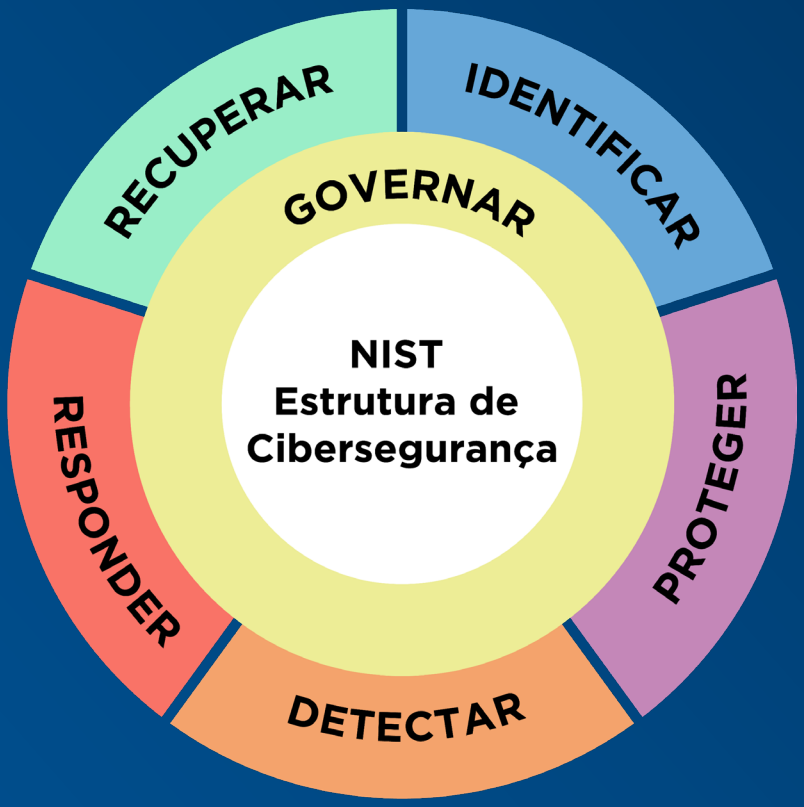
Ativos e operações afetados por um incidente de segurança cibernética são restaurados.

Compreender funções e responsabilidades. Compreenda quem, dentro e fora do seu negócio, tem responsabilidades de recuperação. Saiba quem tem acesso e autoridade para tomar decisões para realizar seus esforços de resposta em nome do negócio.

Executar seu plano de recuperação. Garanta a disponibilidade operacional dos sistemas e serviços afetados; e priorize e execute tarefas de recuperação.

Verificar novamente o seu trabalho. É importante garantir a integridade dos backups e outros ativos de recuperação antes de usá-los para retomar as operações comerciais regulares.

Comunicar-se com as partes interessadas internas e externas. Explique cuidadosamente o que, como e quando as informações serão compartilhadas com várias partes interessadas, para que todas as partes interessadas recebam as informações de que precisam, mas nenhuma informação inadequada seja compartilhada. Comunique à sua equipe quaisquer lições aprendidas e revisões de processos, procedimentos e tecnologias (seguindo as políticas já definidas pela organização). Este é um bom momento para treinar ou retreinar a equipe sobre as melhores práticas de segurança cibernética.



Departamento de Comércio dos EUA
Gina M. Raimondo, Secretária

Instituto Nacional de Padrões e Tecnologia
Laurie E. Locascio, Diretora do NIST e Subsecretária de Comércio para Padrões e Tecnologia