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

NIST Cybersecurity Framework 2.0: Guia de Início Rápido para Criar e Usar Perfis

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

NIST Publicação Especial
NIST SP 1301 por
https://doi.org/10.6028/NIST.SP.1301.por
Fevereiro de 2024

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

UM GUIA DE INÍCIO RÁPIDO

INTRODUÇÃO

Impulsionando o Progresso ao Longo do Tempo com Perfis Organizacionais

Um ***Perfil Organizacional*** descreve a postura atual e/ou alvo de cibersegurança de uma organização em termos de resultados de cibersegurança do Núcleo da Estrutura de Cibersegurança (CSF). Os Perfis Organizacionais são usados para entender, personalizar, avaliar e priorizar resultados de cibersegurança com base nos objetivos da missão da organização, nas expectativas das partes interessadas, no cenário de ameaças e nos requisitos. A organização pode então agir estrategicamente para alcançar esses resultados. Esses Perfis também podem ser usados para avaliar o progresso em direção aos resultados almejados e para comunicar informações pertinentes às partes interessadas.

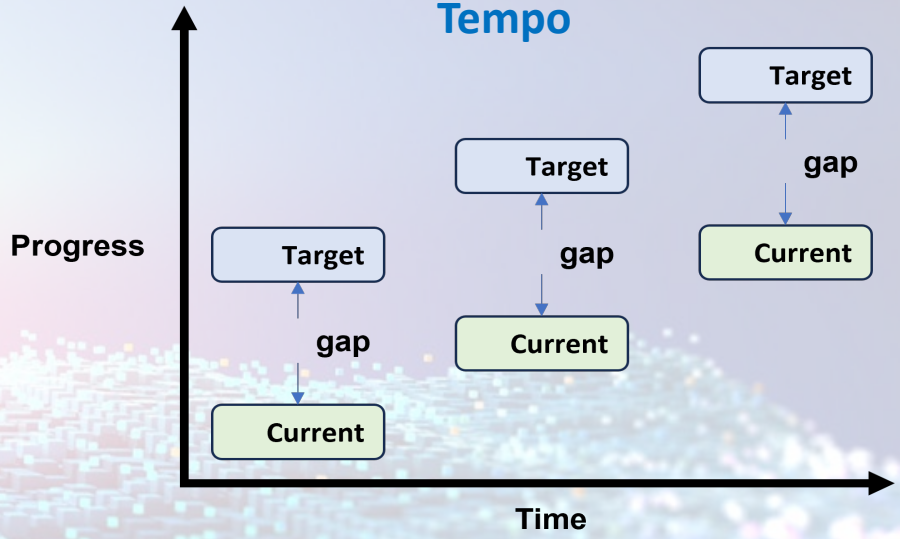
Os Perfis Organizacionais podem ser categorizados como:

- Um ***Perfil Atual*** que especifica os resultados da CSF que uma organização está atualmente alcançando e caracteriza como ou em que medida cada resultado está sendo alcançado.
- Um ***Perfil Alvo*** que especifica os resultados desejados da CSF que uma organização selecionou e priorizou para alcançar seus objetivos de gerenciamento de risco de cibersegurança. Um Perfil Alvo considera mudanças antecipadas na postura de cibersegurança da organização, como novos requisitos, adoção de novas tecnologias e tendências na inteligência de ameaças.

Criar e Usar Perfis Organizacionais com o Processo de Cinco Etapas da CSF

O CSF 2.0 descreve um processo de cinco etapas para criar e usar Perfis Organizacionais. Especificamente, o processo compara um Perfil Alvo aspiracional com um Perfil Atual avaliado. Então, é realizada uma análise de lacunas e um plano de ação é desenvolvido e implementado. Esse processo naturalmente leva a refinamentos no Perfil Alvo a serem usados durante a próxima avaliação.

Progresso ao Longo do Tempo



Criar e Usar Perfis Organizacionais

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

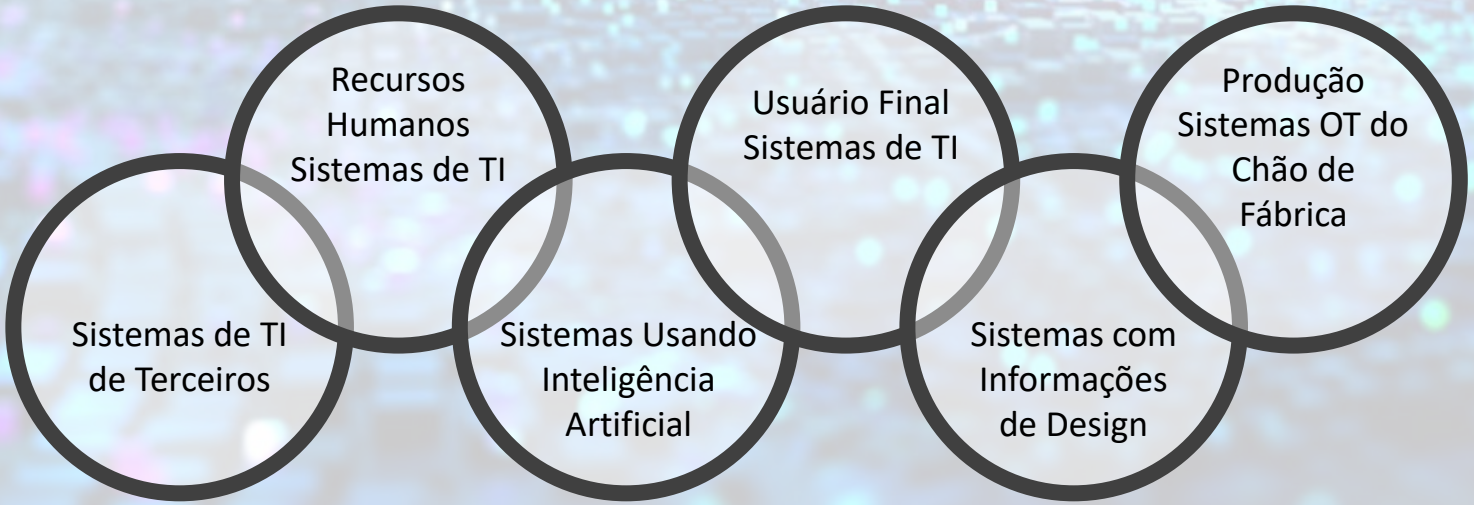
UM GUIA DE INÍCIO RÁPIDO

DEFINIR O ESCOPO DO PERFIL ORGANIZACIONAL

O escopo define os fatos e suposições de alto nível nos quais os Perfis serão baseados. Você pode ter quantos Perfis Organizacionais desejar, cada um com um escopo diferente.

Perguntas a serem respondidas ao definir o escopo do seu Perfil incluem:

- Qual é o motivo para criar o Perfil Organizacional?
- O Perfil cobrirá toda a organização? Se não, quais divisões da organização, ativos de dados, ativos de tecnologia, produtos e serviços e/ou parceiros e fornecedores serão incluídos?
- O Perfil abordará todos os tipos de ameaças, vulnerabilidades, ataques e defesas de cibersegurança? Se não, quais tipos serão incluídos?
- Quais indivíduos ou equipes serão responsáveis por desenvolver, revisar e operacionalizar o Perfil?
- Quem será responsável por definir as expectativas para ações para alcançar os resultados almejados?



Fatos sobre o Perfil Organizacional

Maneiras de Pensar sobre Perfis

Uma determinada organização pode desejar usar vários Perfis.

Cada Perfil pode ter um escopo distinto com base em fatores como:

- categoria de tecnologia (TI, OT)
- tipos de dados (PII, PHI, PCI)
- usuários (funcionários, terceiros)

O escopo de um Perfil determina a aplicabilidade de um determinado resultado da CSF.

Pode ser útil combinar dois ou mais Perfis quando os escopos se sobrepõem.

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

UM GUIA DE INÍCIO RÁPIDO

COLETAR AS INFORMAÇÕES NECESSÁRIAS

Exemplos de informações podem incluir políticas organizacionais, prioridades e recursos de gerenciamento de riscos, requisitos e normas de cibersegurança... As fontes de informação necessárias dependerão do caso de uso, dos elementos que os Perfis capturarão e do nível de detalhe desejado. Fontes comuns de informação incluem:

1. Perfis Comunitários

Um ***Perfil Comunitário*** é uma base de resultados da CSF criada e publicada para abordar *interesses e objetivos compartilhados entre várias organizações.*. Um Perfil Comunitário é geralmente destinado a um setor ou subsetor específico, tecnologia, tipo de ameaça ou outro caso de uso.

Uma organização pode usar um Perfil Comunitário como base para seu próprio Perfil Alvo copiando o Perfil Comunitário para um Perfil Organizacional. Um Perfil Comunitário pode ser adaptado por:

- Ajustar as prioridades de resultados específicos da CSF
- Adicionar Subcategorias, Referências Informativas ou orientações de implementação específicas da organização

Veja *Um Guia para Criar Perfis Comunitários da CSF 2.0* para mais informações sobre como criar e usar Perfis Comunitários.

2. Modelo de Perfil Organizacional do NIST

O NIST fornece um **modelo de Perfil Organizacional da CSF** como uma planilha do Microsoft Excel. Você pode baixá-lo e preenchê-lo para criar Perfis Atuais e Alvos para sua organização. O modelo facilita a comparação lado a lado dos Perfis Atuais e Alvos para identificar e analisar lacunas. Você pode encontrar o modelo no site do CSF 2.0.

Prioritização

A Principal Característica de um Perfil

A noção central de um Perfil Alvo é determinar prioridades diferentes para os resultados aplicáveis da CSF. As prioridades ajudam a determinar quais partes do seu programa de cibersegurança devem receber mais, ou menos, recursos. As prioridades de cibersegurança são impulsionadas por objetivos estratégicos, leis, regulamentos e respostas a riscos. Para saber mais, consulte a SP 800-37 sobre tarefas de gerenciamento de riscos em toda a organização na *Etapa de Preparação.* O IR 8286B oferece informações sobre como o Núcleo da CSF apoia as decisões de resposta ao risco.

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

UM GUIA DE INÍCIO RÁPIDO

CRIAR O PERFIL ORGANIZACIONAL – PARTE 1

Determinar que tipos de informações de apoio cada Perfil deve incluir para os resultados do FCS selecionados... As etapas para criar um Perfil Organizacional são:

3a: Baixe a planilha de modelo de Perfil Organizacional CSF mais recente e personalize conforme desejado.

3b: Inclua resultados de segurança cibernética que se apliquem ao seu caso de uso e documente as justificativas conforme necessário.

3c: Documente as **Práticas atuais de** segurança cibernética nas colunas Perfil Atual. Entradas mais detalhadas podem fornecer melhores insights para etapas posteriores.

3d: Documente as **Metas** de cibersegurança e os planos para alcançá-las nas colunas Perfil Alvo. As inscrições podem ser baseadas em Referências Informativas da CSF, novos requisitos de segurança cibernética, novas tecnologias e tendências em inteligência de ameaças cibernéticas.

3e: Observe a importância de cada meta usando o campo **Prioridade**.

Resultados da CSF		Perfil Atual			Perfil Alvo	
Identificador	**Descrição**	**Práticas**	**Status**	**Avaliação**	**Prioridade**	**Metas**
Os identificadores e descrições do Núcleo da CSF – Funções, Categorias, Subcategorias. Você também pode adicionar seus próprios resultados para lidar com os riscos e requisitos exclusivos de sua organização.		Políticas, processos, procedimentos e outras atividades relacionadas a um resultado. Pode incluir artefatos que contenham evidências de alcançar um resultado.	O estado ou condição atual de um resultado, como se está sendo alcançado e em que grau.	Uma avaliação das práticas atuais utilizando escalas como: • alta/média/baixa • 1-5 • 0-100%, • vermelho/amarelo/verde	A importância relativa de um resultado utilizando escalas como: • Baixa/Média/Alta • 1/2/3/4/5 • rankings (1, 2, 3…)	Tais como: • Políticas, Processos e Procedimentos • Funções e Responsabilidades Selecionadas de: • Referências Informativas - padrões, orientações e melhores práticas

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

UM GUIA DE INÍCIO RÁPIDO

CRIAR O PERFIL ORGANIZACIONAL – PARTE 2

A tabela abaixo mostra um exemplo hipotético de uma única linha de um Perfil Organizacional Isso é apenas para fins ilustrativos. Aqui estão algumas dicas tiradas do exemplo:

- Adicione e remova colunas do modelo de Perfil Organizacional para atender às suas necessidades. A CSF incentiva os usuários a registrar qualquer informação que seja significativa e a usar o formato que preferirem.
- As colunas não precisam ser as mesmas para o Perfil Atual e o Perfil Alvo.
- Inclua Referências Informativas para entender as diferenças entre Práticas e Metas. Este exemplo mostra os controles SP 800-53 entre colchetes.

Resultados da CSF		Perfil Atual			Perfil Alvo	
Identificador	**Descrição**	**Práticas**	**Status**	**Avaliação**	**Prioridade**	**Metas**
PR.PS-01	As práticas de gestão de configuração são estabelecidas e aplicadas.	Política: Versão 1.4 da política de Gestão de Configuração , última atualização em 14/10/22. Define a política de controle de alteração de configuração [**CM-1**]. Procedimentos: Os proprietários do sistema e os gerentes de tecnologia implementam informalmente as práticas de gerenciamento de configuração. Os processos de controle de mudanças não são seguidos de forma consistente. O CIO especifica as linhas de base de configuração [**CM-2**] para as plataformas e aplicativos de TI mais amplamente utilizados dentro da organização, mas o uso da linha de base não é monitorado ou aplicado de forma consistente em toda a organização.	A gestão de configuração é parcialmente implementada dentro da organização. Alguns sistemas não seguem as linhas de base disponíveis e outros sistemas não possuem linhas de base, portanto, podem ter configurações fracas que os tornam mais suscetíveis ao uso indevido e comprometimento. Alterações não autorizadas podem passar despercebidas. Algumas alterações não são testadas ou rastreadas.	3 *de 5*	Alta	Política: A política de Gerenciamento de Configuração exige que as linhas de base de configuração sejam especificadas, usadas, aplicadas e mantidas para todas as tecnologias de commodities usadas pela organização. A política exige que os processos de controle de mudanças sejam seguidos para todas as tecnologias dentro da organização [**CM-1**]. Procedimentos: Cada divisão da organização tem um plano de gerenciamento de configuração [**CM-9**], bem como mantém, implementa e impõe linhas de base de configuração [**CM-2**] e configurações [**CM-6**] para seus sistemas. As linhas de base são aplicadas a todos os sistemas antes da liberação da produção. Todos os sistemas são monitorados continuamente quanto a alterações inesperadas de configuração, e os tickets são gerados automaticamente quando ocorrem desvios das linhas de base. As partes designadas analisam as solicitações de mudança e as análises de impacto correspondentes [**CM-4**] e aprovam ou negam cada [**CM-3**].

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

UM GUIA DE INÍCIO RÁPIDO

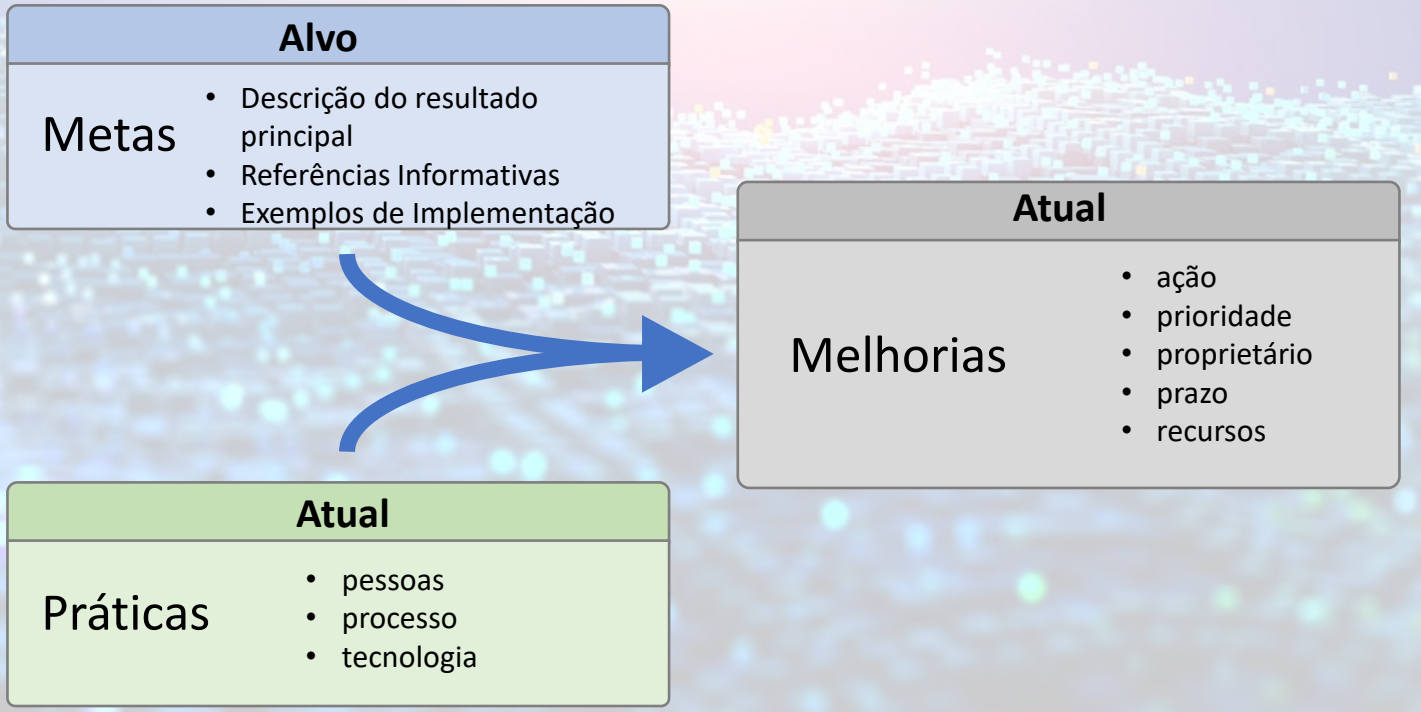
ANALISAR LACUNAS E CRIAR UM PLANO DE AÇÃO – PARTE 1

Identificar e analisar as diferenças entre os Perfis Atual e Alvo permite que uma organização encontre lacunas e desenvolva um plano de ação priorizado para lidar com essas lacunas. Usar Perfis dessa maneira ajuda sua organização a tomar decisões mais bem informadas sobre como melhorar o gerenciamento de riscos de segurança cibernética de maneira priorizada e econômica.

Etapa 4a

Como Analisar Lacunas

Compare e contraste suas **práticas** atuais, entre pessoas, processos e tecnologias, com as melhores práticas descritas nas descrições de resultados da CSF, Referências Informativas e Exemplos de Implementação. Com esses **objetivos** em mente, faça observações sobre as diferenças e documente esses itens como possíveis melhorias.



Etapa 4b

Como Criar Planos de Ação

O plano de ação é uma lista de **melhorias** pendentes para o seu programa de segurança cibernética. Além da análise de lacunas do Perfil Organizacional, o plano de ação deve considerar os impulsionadores da missão, benefícios, riscos e recursos necessários (por exemplo, pessoal, financiamento). Os planos de ação devem ter todos os itens essenciais no gráfico (à esquerda).

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

UM GUIA DE INÍCIO RÁPIDO

ANALISAR LACUNAS E CRIAR UM PLANO DE AÇÃO – PARTE 2

Identificar e analisar as diferenças entre os Perfis Atual e Alvo permite que uma organização encontre lacunas e desenvolva um plano de ação priorizado para lidar com essas lacunas. A CSF fornece links para ferramentas, controles e recursos de implementação que lhe ajudarão a analisar lacunas [**Etapa 4a**] e criar planos de ação [**Etapa 4b**]. Uma abordagem recomendada para o desenvolvimento de planos de ação é usar a Ferramenta de Referência NIST CSF 2.0 para seguir as referências das Subcategorias pertinentes do seu Perfil Alvo aos controles NIST SP 800-53 associados.

Quais as Melhores Práticas a Usar

Referências Informativas: relações entre o Núcleo e várias melhores práticas, incluindo padrões, diretrizes, regulamentos e outros recursos. As referências ajudam a informar como uma organização pode alcançar os resultados do FCS. Eles também ajudam a conectar os resultados desejados a outros documentos comuns de segurança cibernética, como ISO/IEC 27001 e SP 800-53, que fornece um catálogo de controles de segurança e privacidade.

Como Implementar as Melhores Práticas

Exemplos de Implementação: descrições nocionais de maneiras pelas quais os resultados do FCS podem ser cumpridos. Os exemplos não são uma lista abrangente de *todas as* ações que poderiam ser tomadas por uma organização, nem são uma *linha de base* de ações necessárias; são ideias úteis para fazer as organizações pensarem em medidas concretas. A Ferramenta de Referência NIST CSF 2.0 permite que os usuários explorem o núcleo da CSF 2.0 completo e façam o download nos formatos Excel e JSON.

Exemplo de Implementação

Um Trecho da Ferramenta de Referência NIST CSF 2.0

Subcategory

PR.PS-01: As práticas de gestão de configuração são aplicadas (anteriormente PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03).

Exemplos de Implementação

Ex1: Estabelecer, testar, implantar e manter linhas de base reforçadas que apliquem as políticas de segurança cibernética da organização e forneçam apenas recursos essenciais (ou seja, princípio da menor funcionalidade)

Ex2: Revise todas as definições de configuração padrão que podem afetar potencialmente a segurança cibernética ao instalar ou atualizar o software

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

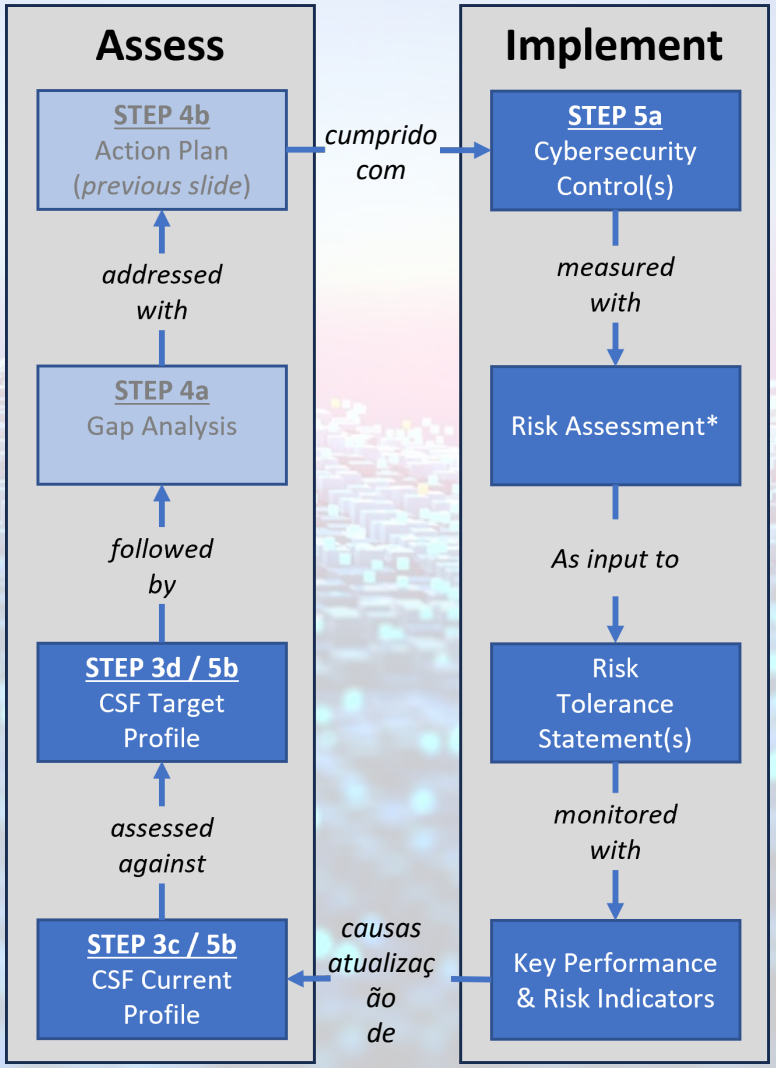
UM GUIA DE INÍCIO RÁPIDO

IMPLEMENTAR PLANO DE AÇÃO E ATUALIZAR PERFIL

Etapa 5a

Implementação de Planos de Ação

O Plano de Ação é cumprido através de qualquer combinação de controles gerenciais, programáticos e técnicos. À medida que esses controles são implementados, o Perfil Organizacional pode ser usado para rastrear o status da implementação. Posteriormente, os controles e riscos associados podem ser monitorados por meio de Indicadores-Chave de Desempenho (KPI) e Indicadores-Chave de Risco (KRI). Os riscos cibernéticos que estão além da tolerância ao risco são observados por meio de avaliações de risco. Riscos além da Tolerância ao Risco podem solicitar atualizações no Plano de Ação, Perfil Organizacional e/ou declarações de Tolerância ao Risco. A Análise de Lacunas também pode resultar na criação de POA&M para lacunas que levarão a um cronograma de remediação mais longo. Mais informações sobre KPI, KRI, Tolerância ao Risco e POA&Ms podem ser descobertas no IR 8286B e SP 800-37.



Etapa 5b

Atualizando Seu Perfil

Implementar atividades que sigam seu Plano de Ação faz parte de um programa contínuo de gerenciamento de riscos cibernéticos (ciclos de feedback e linhas de comunicação mais sutis do que as mostradas). As Avaliações de Risco, conforme descrito na SP 800-30, podem alavancar as declarações de Tolerância ao Risco ao identificar riscos, bem como determinar a probabilidade e o impacto desses riscos. A mudança na probabilidade e no impacto é uma medida da eficácia do Plano de Ação e dos controles discretos. O monitoramento de risco também é realizado usando KPI e KRI. Mudanças nos riscos, probabilidades e/ou impactos podem resultar em atualizações no Perfil Organizacional.

* A Avaliação de Risco pode ocorrer a qualquer momento e pode informar qualquer etapa

NIST CSF 2.0: CRIANDO E USANDO PERFIS ORGANIZACIONAIS

UM GUIA DE INÍCIO RÁPIDO

PRÓXIMAS ETAPAS

O Que Aprendemos. Este QSG explicou os seguintes termos:

Perfil Organizacional – Resultados principais da CSF relevantes para uma organização específica

Perfil da Comunidade – Resultados principais da CSF que se aplicam a várias organizações

Perfil Atual – os resultados de segurança cibernética que uma organização está alcançando atualmente

Perfil Alvo – os resultados desejados que uma organização deseja alcançar

Análise de Lacunas – determinar as diferenças entre os Perfis Atual e Alvo

Referências Informativas – melhores práticas que implementam vários resultados principais da CSF

Exemplos de Implementação – maneiras nocionais pelas quais as organizações podem alcançar as Subcategorias CSF

Plano de Ação – abordar lacunas e avançar em direção ao Perfil Alvo

O Que Vem a Seguir. Aqui está uma lista de coisas que você pode fazer para colocar este QSG em prática:

- Familiarize-se com o modelo de Perfil Organizacional NIST CSF
- Veja se há um Perfil da Comunidade relevante para você no site Perfis da Comunidade NIST
- Determine quantos Perfis Organizacionais CSF você precisa [**Etapa 1**]
- Faça um inventário dos seus requisitos de segurança cibernética
- Priorize os resultados do FCS em seus Perfis Organizacionais [**Etapa 2**]
- Avalie seu perfil atual [**Etapa 3**]
- Leia mais sobre Referências Informativas
- Melhore o seu programa de segurança cibernética ao longo do tempo [**Etapas 4 e 5**]

Aprendendo Mais

Leitura

IR 8286B NIST IR 8286B, *Priorizando o Risco de Segurança Cibernética para o Gerenciamento de Riscos Corporativos*

SP 800-37 NIST SP 800-37 Revisão 2, *Estrutura de Gerenciamento de Riscos para Sistemas de Informação e Organizações*

SP 800-53 NIST SP 800-53 Revisão 5, *Controles de Segurança e Privacidade para Sistemas de Informação e Organizações*

SP 800-30 NIST SP 800-30 Revisão 1, *Guia para Realização de Avaliações de Risco*

Recursos

Modelo de Perfil Organizacional 2.0

Ferramenta de Referência NIST CSF

Referências Informativas

Exemplos de Implementação

Um Guia Para Criar Perfis da Comunidade CSF 2.0

Guia de Início Rápido para Usar os Níveis da CSF