

**Publicação Especial NIST 800-181**  
**Revisão 1**

---

**Framework da Força de Trabalho  
para Segurança Cibernética  
(NICE Framework)**

---

Rodney Petersen  
Danielle Santos  
Matthew C. Smith  
Karen A. Wetzel  
Greg Witte

Esta publicação está disponível gratuitamente em:  
<https://doi.org/10.6028/NIST.SP.800-181r1>

**Publicação Especial NIST 800-181**  
**Revisão 1**

# **Framework da Força de Trabalho para Segurança Cibernética (NICE Framework)**

Rodney Petersen (Diretor)

Danielle Santos (Gerente de Comunicações e Operações)

Karen A. Wetzel (Gerente do NICE Framework)

*Iniciativa Nacional para Educação em Segurança Cibernética (NICE)*  
*Divisão de Segurança Cibernética Aplicada*  
*Laboratório de Tecnologia da Informação*

Matthew C. Smith

Greg Witte

*Huntington Ingalls Industries*  
*Annapolis Junction, MD*

Esta publicação está disponível gratuitamente em:  
<https://doi.org/10.6028/NIST.SP.800-181r1>

Novembro de 2020



Departamento de Comércio dos Estados Unidos  
*Wilbur L. Ross, Jr., Secretário*

National Institute of Standards and Technology  
*Walter Copan, Diretor do NIST e Subsecretário de Comércio para Normas e Tecnologia*

## Autoridade

A presente publicação foi desenvolvida pelo NIST de acordo com suas responsabilidades legais nos termos da Lei Federal de Modernização da Segurança da Informação (FISMA) de 2014, 44 U.S.C. § 3551 e seguintes, Direito Público (P.L.) 113-283. O NIST desenvolve normas e diretrizes de segurança da informação, incluindo requisitos mínimos para sistemas de informação federais. Contudo, tais normas e diretrizes não se aplicam aos sistemas de segurança nacional sem a aprovação expressa das autoridades federais responsáveis por tais sistemas. As diretrizes estipuladas neste documento são consistentes com os requisitos da Circular A-130 do Gabinete de Gestão e Orçamento (OMB).

Nenhuma informação na presente publicação deve ser interpretada como contraditória às normas e diretrizes que o Secretário de Comércio, de acordo com sua autoridade prevista em lei, determinou e tornou obrigatórias às agências federais. Tampouco, essas diretrizes devem ser interpretadas como uma alteração ou substituição da autoridade existente do Secretário de Comércio, Diretor do OMB ou qualquer outro funcionário federal. A presente publicação pode ser usada por organizações não governamentais de forma voluntária e não está sujeita a direitos autorais nos Estados Unidos. No entanto, solicitamos que a referência a essa publicação seja feita.

Publicação Especial 800-181 do National Institute of Standards and Technology  
Publ. Esp. Natl. Inst. Stand. Technol. 800-181 Rev. 1, 27 páginas (novembro de 2020)  
CODEN: NSPUE2

Esta publicação está disponível gratuitamente em:  
<https://doi.org/10.6028/NIST.SP.800-181r1>

Certas entidades comerciais, equipamentos ou materiais podem ser citados neste documento para adequadamente descrever um procedimento experimental ou conceito. Tal citação não se configura como recomendação ou endosso do NIST, tampouco sugere que as entidades, materiais ou equipamentos sejam necessariamente os melhores disponíveis para o propósito descrito.

A presente publicação pode conter referências a outras publicações ainda em desenvolvimento pelo NIST de acordo com suas responsabilidades previstas em lei. As informações contidas nessa publicação, incluindo conceitos e metodologias, podem ser utilizadas por agências federais mesmo antes da conclusão de tais publicações complementares. Desta forma, até que cada publicação seja concluída, os requisitos, diretrizes e procedimentos atuais, onde existirem, permanecem vigentes. Para fins de planejamento e transição, as agências federais poderão acompanhar de perto o desenvolvimento dessas novas publicações do NIST.

Recomenda-se que as organizações revisem todas as minutas das publicações durante os períodos estipulados para comentários do público e forneçam *feedback* ao NIST. Inúmeras publicações do NIST sobre segurança cibernética, além das mencionadas acima, estão disponíveis em <https://csrc.nist.gov/publications>.

### Comentários referentes à presente publicação podem ser enviados para:

National Institute of Standards and Technology  
Attn: Applied Cybersecurity Division, Information Technology Laboratory  
[A/c: Divisão de Segurança Cibernética Aplicada, Laboratório de Tecnologia da Informação]  
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000  
E-mail: [NICEFramework@nist.gov](mailto:NICEFramework@nist.gov)

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

## Relatórios sobre Tecnologia de Sistemas Computacionais

O Laboratório de Tecnologia da Informação (ITL) do National Institute of Standards and Technology (NIST) tem o compromisso de fomentar a economia dos Estados Unidos e o bem-estar da população, fornecendo liderança técnica para a infraestrutura de medição e normas do país. O ITL desenvolve testes, métodos de teste, dados de referência, implementações de provas de conceito e análises técnicas para promover o desenvolvimento e uso produtivo da tecnologia da informação. As responsabilidades do ITL incluem o desenvolvimento de normas e diretrizes administrativas, técnicas, físicas e de gestão para a segurança e privacidade, considerado o custo-benefício, de informações em sistemas de informação federais, com exclusão daquelas relacionadas à segurança nacional. A série 800 da Publicação Especial aborda os trabalhos de pesquisa, diretrizes e divulgação do ITL em segurança de sistemas de informação, bem como suas atividades colaborativas com a indústria, o governo e instituições acadêmicas.

### Resumo

A presente publicação da Iniciativa Nacional para Educação em Segurança Cibernética (NICE) descreve o *Framework* da Força de Trabalho para Segurança Cibernética (NICE Framework), uma importante referência para descrever e compartilhar informações sobre o trabalho de segurança cibernética. Esse trabalho é apresentado na forma de declarações de Tarefa e descreve as declarações de Conhecimento e Habilidade que fornecem uma base para aprendizes, incluindo estudantes, pessoas que desejam ingressar no mercado de trabalho e funcionários. O uso dessas declarações ajuda alunos a desenvolverem suas habilidades, ingressantes no mercado de trabalho a demonstrarem suas competências e funcionários a realizarem tarefas. Como um léxico comum e consistente que categoriza e descreve o trabalho de segurança cibernética, o NICE Framework facilita o acesso a informações sobre como identificar, recrutar, desenvolver e reter talentos em segurança cibernética. O NICE Framework é uma fonte de referência que permite a organizações ou setores elaborar publicações ou ferramentas adicionais que atendam às suas necessidades a fim de definir ou fornecer orientações sobre diferentes aspectos da educação, qualificação e desenvolvimento da força de trabalho em segurança cibernética.

### Palavras-chave

Competência; segurança cibernética; espaço cibernético; educação; conhecimento; função; segurança; habilidade; tarefa; equipe; qualificação; força de trabalho; função de trabalho.

## Notificação de divulgação de patente

*NOTIFICAÇÃO: O Laboratório de Tecnologia da Informação (ITL) solicitou que os detentores de reivindicações de patentes, cujo uso possa ser exigido para atendimento às orientações ou requisitos desta publicação, divulguem tais reivindicações de patentes ao ITL. No entanto, os detentores de patentes não são obrigados a responder aos pedidos de patentes do ITL e o ITL não realizou uma pesquisa de patentes para identificar quais patentes, se houver, podem ser aplicáveis à presente publicação.*

*Na data da publicação e no(s) pedido(s) seguinte(s) de identificação de reivindicações de patentes cujo uso pode ser necessário para atendimento às orientações ou requisitos desta publicação, nenhuma reivindicação de patente foi identificada ao ITL.*

*O ITL não declara, de forma explícita ou implícita, que licenças não sejam necessárias para evitar violação de patente no uso desta publicação.*

## Convenções do documento

Os termos “dever” e “não dever” indicam requisitos a serem estritamente cumpridos para atendimento à presente publicação e dos quais nenhum desvio é permitido. Os termos “recomendar” e “não recomendar” indicam que, entre várias possibilidades, uma delas é preferível como especialmente adequada, sem mencionar ou excluir as demais, ou que um determinado curso de ação é tido como melhor, mas não necessariamente exigido, ou que (na forma negativa) uma certa possibilidade ou curso de ação é desencorajado, mas não proibido. Os termos “ser possível” e “não requer” indicam um curso de ação permitido dentro dos limites da publicação. Os termos “poder” e “não poder” indicam uma possibilidade e capacidade, seja material, física ou causal.

Em todo o NICE Framework, os indivíduos que realizam trabalhos de segurança cibernética — incluindo estudantes, candidatos a emprego e funcionários — são denominados Aprendizes. O termo destaca que cada membro da força de trabalho nunca deixa de ser um aprendiz.

## Agradecimentos

O NICE Framework foi desenvolvido por uma Equipe de Autoria Central que inclui representantes de vários departamentos e agências do governo federal dos Estados Unidos. O National Institute of Standards and Technology deseja reconhecer e agradecer os membros dessa equipe, cujos esforços dedicados contribuíram significativamente para a publicação:

William Newhouse, National Institute of Standards and Technology

Pam Frugoli, Departamento do Trabalho

Lisa Dorr, Departamento de Segurança Nacional

Kenneth Vrooman, Agência de Segurança Cibernética e Segurança em Infraestrutura

Bobbie Sanders, Departamento de Defesa

Patrick Johnson, Departamento de Defesa

Matt Isnor, Departamento de Defesa

Stephanie Shively, Departamento de Defesa

Ryan Farr, Departamento de Defesa

Os autores e a Equipe de Autoria Central reconhecem e agradecem as contribuições significativas de indivíduos e organizações nos setores público e privado, cujos comentários atenciosos e construtivos melhoraram a qualidade geral, a eficácia e a utilidade desta publicação. Os autores agradecem especialmente as inúmeras respostas à solicitação de comentários sobre o NICE Framework e à minuta aberta a comentários do público da presente publicação.

Adicionalmente, a equipe agradece e reconhece as contribuições daqueles que compilaram edições anteriores de frameworks nacionais da força de trabalho para segurança cibernética, conforme descrito na página de Histórico do NICE Framework Resource Center. [1]

## Nota aos leitores

Bem-vindos ao Framework da Força de Trabalho para Segurança Cibernética (NICE Framework) da Iniciativa Nacional para Educação em Segurança Cibernética (NICE), Revisão 1. A equipe do Gabinete do Programa NICE recebeu *feedbacks* importantes da comunidade, incluindo diversas respostas a uma solicitação recente de comentários gerais sobre o NICE Framework e também respostas à minuta aberta a comentários do público da presente publicação. Em vista dos *feedbacks* recebidos e do ecossistema acelerado e conectado da segurança cibernética, a equipe de autoria decidiu adotar e promover os atributos de agilidade, flexibilidade, interoperabilidade e modularidade. Esses atributos resultaram em modificações ao NICE Framework que objetivam apresentar uma abordagem simplificada para o desenvolvimento de uma força de trabalho capaz de gerenciar riscos de segurança cibernética. Veja abaixo um resumo das modificações:

- A organização de conceitos na Revisão 1 foi simplificada com a exclusão de Categorias (por exemplo, provisionar, supervisionar e governar com segurança, proteger e defender, analisar, etc.) e de Áreas Especializadas (por exemplo, resposta a incidentes, análise de ameaças, gerenciamento de segurança cibernética, etc.). Para simplificar uma abordagem que oferece agilidade, flexibilidade, interoperabilidade e modularidade às organizações, a Revisão 1 apresenta um conjunto simplificado de “pilares” composto de Tarefas, Conhecimento e Habilidades. As organizações que considerarem úteis as antigas Categorias e Áreas Especializadas podem continuar a usá-las ou criar equipes focadas nesses conceitos e alinhá-las com a presente versão do NICE Framework (consulte a Seção 3.4).
- A Revisão 1 descreve diversos usos de Tarefas, Conhecimento e Habilidades, incluindo métodos de aplicá-los na criação de Funções de Trabalho. Os usuários das Funções de Trabalho descritas no NIST SP 800-181 original podem continuar a usá-las; atualizações a essas funções podem ser publicadas pelo NICE no futuro. [2]

As relações entre Tarefas, Conhecimento, Habilidades e Aptidões mudaram. As declarações de Habilidade e Aptidão da versão anterior foram reformuladas visando a simplicidade, e agrupadas em declarações de Habilidade, que focam na ação do aprendiz. A presente revisão descreve métodos para associar declarações de Conhecimento e Habilidade com declarações de Tarefa para diferentes resultados. As listas de Tarefas, Conhecimento, Habilidades e Funções de Trabalho que estavam disponíveis anteriormente nos Apêndices A e B do Framework de 2017 foram removidas da presente versão para simplificar a manutenção do NICE Framework e facilitar as atualizações dessas listas. As declarações de Tarefa, Conhecimento e Habilidade (TKS), bem como as Competências e Funções de Trabalho correspondentes, serão mantidas como artefatos separados e estarão sujeitas a revisões e atualizações contínuas com um processo de alteração definido e indicação de controle de versões, com o objetivo de gerenciar e comunicar futuras alterações. Até que essas atualizações sejam realizadas, as versões anteriores dessas listas permanecerão disponíveis aos usuários no NICE Framework Resource Center. Para atender a interoperabilidade e a modularidade, as atualizações futuras garantirão que as declarações correspondam às definições finais das declarações TKS ora observadas.

- Para leitores interessados em mapear normas, referências ou recursos em relação ao NICE Framework, a NICE trabalha com o Programa de Referência Informativa On-line

(OLIR) para desenvolver modelos para esses mapeamentos. O Programa OLIR, gerenciado pelo NIST, apresenta um processo para alinhar referências aos documentos do NIST. Ademais, o programa fornece um catálogo dessas referências. [3]



## Resumo executivo

Cada um de nós, individualmente e como parte de uma organização, realiza um trabalho importante, oferecendo uma contribuição para a sociedade. No entanto, à medida que a informação e a tecnologia, incluindo diversos tipos de tecnologia operacional em constante evolução, se tornam cada vez mais complexas e interconectadas, pode ser difícil descrever com clareza o trabalho a ser realizado, ou que desejamos realizar, especialmente nessas áreas. A Iniciativa Nacional para Educação em Segurança Cibernética (NICE) reconhece que os indivíduos que realizam trabalhos de segurança cibernética — incluindo estudantes, candidatos a emprego e funcionários — nunca deixam de ser aprendizes em seus esforços para enfatizar e abordar as implicações da segurança cibernética em diferentes domínios. Esse grupo de pessoas é denominado neste documento como “Aprendizes” e, por vezes, como “força de trabalho em segurança cibernética”, embora o último não signifique que as funções de trabalho e o conteúdo do NICE Framework se apliquem apenas àqueles totalmente incorporados ao domínio da segurança cibernética. As tarefas que esses aprendizes realizam são denominadas “trabalho de segurança cibernética”, e o Framework fornece um meio de descrever esse trabalho com precisão para atender a educação ou a qualificação de aprendizes, bem como o recrutamento, contratação, desenvolvimento e retenção de funcionários. O NICE Framework foi desenvolvido para ajudar a fornecer uma taxonomia de referência, ou seja, uma linguagem comum, do trabalho de segurança cibernética e dos indivíduos que realizam esse trabalho. O NICE Framework atende a missão da NICE de fomentar, promover e coordenar uma comunidade robusta que trabalha em conjunto para promover um ecossistema integrado de educação, qualificação e desenvolvimento da força de trabalho em segurança cibernética. O NICE Framework fornece um conjunto de pilares para descrever as tarefas, o conhecimento e as habilidades necessárias para realização do trabalho de segurança cibernética por indivíduos e equipes. Por meio desses pilares, o NICE Framework permite que as organizações desenvolvam sua força de trabalho para realização do trabalho de segurança cibernética e ajuda os aprendizes a explorar o trabalho de segurança cibernética e participar de atividades de aprendizagem adequadas com o objetivo de promover seus conhecimentos e habilidades. Esse desenvolvimento, por sua vez, beneficia empregadores e funcionários por meio da identificação de planos de carreira que trazem informações sobre como se preparar para o trabalho de segurança cibernética usando os dados das declarações de Tarefa, Conhecimento e Habilidade (TKS) incorporados a Funções de Trabalho e Competências.

O uso de termos e linguagem comuns ajuda a organizar e comunicar o trabalho a ser feito e os atributos daqueles que estão qualificados para executá-lo. Desta forma, o NICE Framework ajuda a simplificar as comunicações e permite foco nas tarefas existentes. Por fim, o uso do NICE Framework melhora a clareza e a consistência em todos os níveis organizacionais, desde um indivíduo a um sistema de tecnologia, programa, organização, setor, estado ou nação.

## Índice

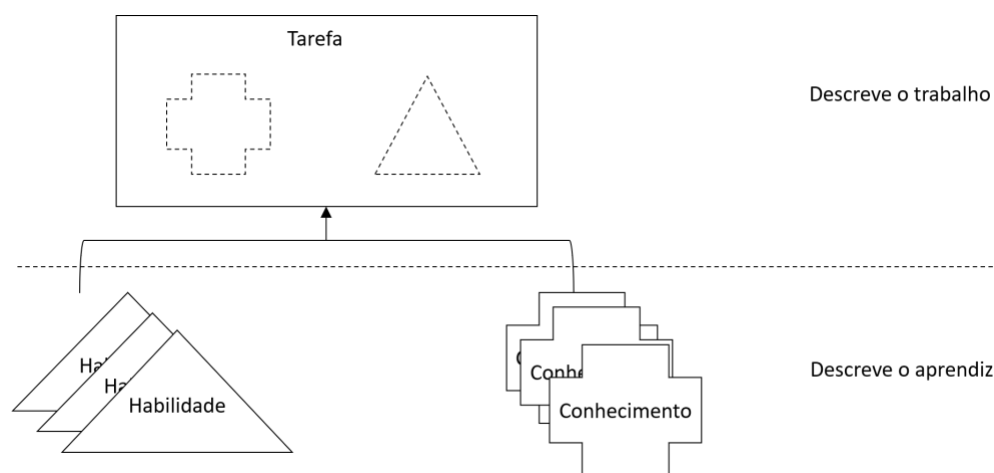
<b>Resumo executivo</b> .....	<b>vii</b>
<b>1 Histórico</b> .....	<b>1</b>
1.1 Atributos do NICE Framework .....	2
1.2 Objetivo e Aplicabilidade .....	3
1.3 Público-alvo .....	3
1.4 Organização desta Publicação .....	3
<b>2 Pilares do NICE Framework</b> .....	<b>5</b>
2.1 Declarações de Tarefa .....	5
2.2 Declarações de Conhecimento .....	6
2.3 Declarações de Habilidade .....	6
<b>3 Utilizando o NICE Framework</b> .....	<b>8</b>
3.1 Utilizando Declarações Existentes de Tarefa, Conhecimento e Habilidade (TKS) .....	8
3.2 Criando Novas Declarações TKS .....	9
3.3 Competências.....	9
3.3.1 Utilizando Competências Existentes.....	11
3.3.2 Criando Novas Competências.....	11
3.4 Funções de Trabalho.....	13
3.4.1 Utilizando Funções de Trabalho Existentes.....	14
3.4.2 Criando uma Nova Função de Trabalho.....	15
3.5 Equipes .....	15
3.5.1 Formando Equipes por meio das Funções de Trabalho .....	15
3.5.2 Formando Equipes por meio das Competências .....	16
<b>4 Conclusão</b> .....	<b>18</b>
<b>Referências</b> .....	<b>19</b>
<b>Appendix A— Acrônimos</b> .....	<b>20</b>
<b>Appendix B— Glossário</b> .....	<b>21</b>

## 1 Histórico

A tecnologia continua a evoluir em um ritmo cada vez maior. Especificamente, a tecnologia que facilita a capacidade de acessar e processar informações com rapidez e eficiência está mudando drasticamente. Trabalhos que exigem projetar, construir, proteger e implementar dados, redes e sistemas aumentam em complexidade. Além disso, descrever esses trabalhos e quem pode executá-los continua sendo um desafio. Somado a isso, as organizações utilizam métodos variados, criados internamente, para tentar superar esse desafio.

A presente publicação da Iniciativa Nacional para Educação em Segurança Cibernética (NICE) apresenta o Framework da Força de Trabalho para Segurança Cibernética (NICE Framework). O NICE Framework ajuda as organizações a superarem os obstáculos na descrição de sua força de trabalho para diversos atores, propondo uma abordagem de pilares. Usando pilares conceituais, o NICE Framework apresenta uma linguagem comum para as organizações utilizarem internamente e entre si. Essa abordagem permite que as organizações adaptem e implementem o NICE Framework de acordo com seu contexto operacional específico. Além disso, ao criar uma linguagem comum, o NICE Framework reduz os obstáculos a organizações que buscam ingressar e operar em conjunto com outras organizações.

A Figura 1, abaixo, apresenta uma visão detalhada do NICE Framework. Os principais pilares do NICE Framework são as declarações de Tarefa, Conhecimento e Habilidade (TKS) (explicadas na Seção 2), descritas juntamente com seus respectivos conceitos. Figura 1 demonstra que existem dois tipos principais de conceitos descritos: “o trabalho” e “o aprendiz”. Notavelmente, aqueles que realizam (ou realizarão) o trabalho (por exemplo, alunos, funcionários ou candidatos a emprego) estão continuamente aprendendo e alcançando objetivos, e podem estar em qualquer etapa do ciclo de vida de aprendizagem. O NICE Framework visa descrever “o trabalho” e “o aprendiz” em termos genéricos que podem ser aplicados a todas as organizações.



**Figura1- Pilares do NICE Framework**

O “trabalho” é o que uma organização precisa para atingir os objetivos de gerenciamento de riscos de segurança cibernética. Cada organização executa tarefas comuns, bem como algumas tarefas específicas ao seu contexto. Por exemplo, toda organização tem alguma forma de tarefa de gerenciamento, ao passo que apenas algumas possuem tarefas para “implantar com segurança

sistemas de energia em massa”. O NICE Framework fornece às organizações uma maneira de descrever seu trabalho por meio de declarações de Tarefa que incorporam declarações auxiliares de Conhecimento e Habilidade.

O “aprendiz” é a pessoa que possui conhecimentos e habilidades. O termo *aprendiz* se aplica a todas as pessoas no escopo deste documento. Um aprendiz pode ser um estudante, um candidato a emprego, um funcionário ou outra pessoa da força de trabalho. Em um contexto organizacional, aprendizes executam tarefas. Em um contexto educacional, aprendizes adquirem novos conhecimentos e habilidades. Todos os indivíduos são considerados aprendizes devido à educação ou qualificação que receberam antes de ingressar na força de trabalho, a processos de qualificação continuada, a processos de autoaprendizado ou a um plano de carreira.

O NICE Framework fornece às organizações uma maneira de descrever a figura dos aprendizes, associando as declarações de Conhecimento e Habilidade a um indivíduo ou grupo. Ao utilizar seu Conhecimento e Habilidades, um aprendiz pode realizar Tarefas para atingir os objetivos da organização. Embora nem todas as organizações usem todos os conceitos relativos a aprendizes, o NICE Framework fornece às organizações um conjunto flexível de pilares que podem ser utilizados conforme a necessidade de seu contexto específico. O reconhecimento do papel que o aprendiz desempenha no desenvolvimento de capacidades para realização do trabalho de segurança cibernética também reforça a aplicabilidade do NICE Framework a provedores de educação e qualificação.

Ao descrever o trabalho e o aprendiz, o NICE Framework fornece às organizações uma linguagem comum para descrever seu trabalho e força de trabalho em segurança cibernética. Partes do NICE Framework descrevem um contexto de trabalho organizacional (Tarefas), outras descrevem um contexto de aprendiz (Conhecimento e Habilidades) e, por fim, a abordagem de pilares do NICE Framework permite que as organizações interliguem os dois contextos.

Ademais, utilizando esses pilares, o NICE Framework fornece um mecanismo para comunicação entre organizações, a qual pode ocorrer seja a nível de colaboradores, setores, estados, ou a nível nacional ou internacional. Essa comunicação pode resultar em soluções inovadoras para desafios comuns, reduzir as barreiras de entrada para novas organizações e indivíduos, bem como facilitar a mobilidade da força de trabalho.

### 1.1 Atributos do NICE Framework

O NICE Framework é uma referência àqueles que procuram descrever o trabalho de segurança cibernética que sua organização realiza, as pessoas que realizarão o trabalho e o aprendizado contínuo necessário para realizar esse trabalho de forma eficaz. A natureza do trabalho e, conseqüentemente, da força de trabalho, pode ser descrita usando os pilares TKS apresentados nas seções a seguir. Esses pilares incorporam os seguintes atributos:

- **Agilidade** — Pessoas, processos e tecnologia amadurecem e devem se adaptar às mudanças. Portanto, o NICE Framework permite que as organizações acompanhem um ecossistema em constante evolução.
- **Flexibilidade** — Embora todas as organizações enfrentem desafios semelhantes, não existe uma solução única para todos os desafios em comum. Portanto, o NICE

Framework permite que as organizações levem em consideração seu contexto operacional específico.

- **Interoperabilidade** — Embora cada solução para um desafio comum seja única, ela deve atender um uso consistente dos termos. Desta forma, o NICE Framework permite que as organizações troquem informações sobre a força de trabalho usando uma linguagem comum.
- **Modularidade** — Embora o risco de segurança cibernética continue sendo a base deste documento, existem outros riscos que as organizações devem gerenciar dentro da empresa. Logo, o NICE Framework permite que as organizações se comuniquem sobre outros tipos de força de trabalho dentro de uma empresa e entre organizações ou setores (por exemplo, privacidade, gestão de risco, engenharia/desenvolvimento de software).

## 1.2 Objetivo e Aplicabilidade

As organizações gerenciam diversas funções de negócios (como operações, finanças, questões jurídicas e recursos humanos) como parte de suas atividades. Cada uma dessas funções de negócios possui riscos associados. Como a tecnologia se tornou um fator facilitador no gerenciamento de uma empresa, os riscos associados à segurança cibernética também foram intensificados. O NICE Framework auxilia as organizações no gerenciamento de riscos de segurança cibernética, fornecendo uma maneira de discutir o trabalho e os aprendizes associados à segurança cibernética. Esses riscos de segurança cibernética constituem uma contribuição importante nas decisões de risco corporativo, conforme descrito no NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. [4]

O presente documento atua como um possível norteador a outras funções de negócios que consideram a criação de frameworks de força de trabalho. As organizações podem aumentar a eficiência usando os mesmos pilares em diversas funções de negócios. Portanto, qualquer organização pode aproveitar este documento.

## 1.3 Público-alvo

A gestão de uma força de trabalho em segurança cibernética envolve diferentes tipos de posições, bem como diferentes tipos de organizações. O público-alvo deste documento inclui agências do setor público, organizações privadas e sem fins lucrativos, provedores de educação e qualificação, desenvolvedores de currículo, provedores de credenciais, profissionais de recursos humanos, gerentes de contratação, gerentes de linha, planejadores da força de trabalho, recrutadores e todos os aprendizes.

## 1.4 Organização desta Publicação

O restante desta Publicação Especial é organizado da seguinte forma:

- Seção 2, Pilares do NICE Framework: Define os componentes dos pilares TKS do NICE Framework

- Seção 3, Utilizando o NICE Framework: Descreve abordagens comuns para uso do NICE Framework
- Seção 4, Conclusão
- Referências: Uma lista de publicações relacionadas citadas neste documento
- Apêndice A, Acrônimos: Uma lista de acrônimos e abreviações utilizados nesta publicação

## 2 Pilares do NICE Framework

O Framework da Força de Trabalho para Segurança Cibernética (NICE Framework) foi desenvolvido com base em um conjunto de pilares que descrevem o trabalho a ser realizado (na forma de Tarefas) e o que é necessário para realizá-lo (por meio de Conhecimento e Habilidades). Esses pilares são conceitos organizacionais que atendem a usabilidade e a implementação do NICE Framework. Eles fornecem um mecanismo que permite às organizações e aos indivíduos compreenderem o escopo e o conteúdo do NICE Framework. Esses pilares não têm como objetivo serem estruturas rígidas, mas sim atuar como diretrizes que podem ser empregadas para facilitar a compreensão.

### 2.1 Declarações de Tarefa

Conforme ilustrado na Figura 1, as declarações de Tarefa descrevem o trabalho, ao passo que as declarações de Conhecimento e Habilidade (K&S) descrevem o aprendiz. Recomenda-se que as declarações de Tarefa foquem na linguagem organizacional e nos padrões de comunicação que agreguem valor à organização. Essas declarações são elaboradas para descrever o trabalho a ser realizado e recomenda-se que estejam alinhadas com o contexto da organização.

As tarefas descrevem o trabalho a ser realizado. Uma tarefa pode ser definida como uma atividade direcionada ao êxito dos objetivos organizacionais, incluindo objetivos de negócios, objetivos de tecnologia ou objetivos de missão. Recomenda-se que as declarações de Tarefa sejam diretas. Embora o trabalho descrito por uma declaração de Tarefa possa ter muitas etapas, como no exemplo abaixo, a declaração em si é fácil de ler e entender.

Uma declaração de Tarefa começa com a atividade a ser executada.

Exemplo: **Solucionar problemas** de hardware e software do sistema.

Uma declaração de Tarefa não declara o objetivo, pois esse pode variar com base nos elementos que motivam a missão e nas necessidades organizacionais.

Exemplo: Conduzir exercícios de treinamento interativos.

No exemplo acima, é possível que o propósito dos exercícios seja criar um ambiente de aprendizagem eficaz, mas esse objetivo não está incluído na própria declaração da Tarefa.

Como demonstra a Figura 1, as Tarefas estão relacionadas às declarações K&S. O aprendiz demonstrará que possui o conhecimento e as habilidades para concluir uma tarefa (ou será desafiado a obter o conhecimento e as habilidades para se preparar para concluir a tarefa). A complexidade da Tarefa é explicada pelas declarações K&S associadas. No exemplo de solução de problemas acima, para solucionar problemas de qualquer parte do software ou hardware, recomenda-se que o aprendiz conheça e compreenda as declarações de Conhecimento relacionadas. O mesmo pode ser dito para as declarações de Habilidade.

#### Tarefa

Uma atividade direcionada para o êxito dos objetivos organizacionais.

#### Declarações de Tarefa

- Fácil de ler e compreender
- Começa com a atividade a ser executada
- Não contém o objetivo da tarefa

## 2.2 Declarações de Conhecimento

As declarações de Conhecimento estão relacionadas às declarações de Tarefa, pois, somente com o entendimento descrito na declaração de Conhecimento, o aprendiz será capaz de concluir a Tarefa. Conhecimento é definido como um conjunto de conceitos que pode ser lembrado. É possível às declarações de Conhecimento descrever conceitos básicos ou específicos. É possível que diversas declarações de Conhecimento sejam necessárias para realizar uma Tarefa. Da mesma forma, é possível que uma única declaração de Conhecimento seja usada para realizar diversas tarefas.

As declarações de Conhecimento podem ser básicas.

Exemplo: Conhecimento das ameaças e vulnerabilidades do espaço cibernético.

As declarações de Conhecimento podem ser específicas.

Exemplo: Conhecimento das fontes de disseminação de informações de vulnerabilidade (por exemplo, alertas de fornecedores, recomendações do governo, erratas da literatura do produto e boletins do setor).

Recomenda-se que as organizações que desenvolvem declarações de Conhecimento considerem os diferentes níveis de conhecimento e experiência dos aprendizes. Um exemplo desses diversos níveis é descrito na Taxonomia de Bloom (revisada), que utiliza uma linguagem que facilita a observação e avaliação do aprendiz. [5]

## 2.3 Declarações de Habilidade

As declarações de Habilidade estão relacionadas às declarações de Tarefa, pois o aprendiz demonstra habilidades na execução de tarefas. Um aprendiz que não consegue demonstrar a habilidade descrita não será capaz de realizar a Tarefa que depende dessa habilidade. Uma Habilidade é definida como a capacidade de realizar uma ação observável. É possível às declarações de Habilidade descrever habilidades simples ou complexas. É possível que diversas declarações de Habilidade sejam necessárias para realizar uma determinada Tarefa. Da mesma forma, é possível que o exercício de uma Habilidade seja usado para realizar mais de uma Tarefa.

As declarações de Habilidade podem ser simples.

Exemplo: Habilidade de reconhecer os alertas de um Sistema de Detecção de Intrusão

As declarações de Habilidade podem ser complexas.

### Conhecimento

Um conjunto de conceitos que pode ser lembrado.

### Declarações de Conhecimento

- Descrever Conhecimentos básicos ou específicos
- É possível que diversas declarações sejam necessárias para realizar uma Tarefa
- É possível que uma única declaração seja usada para realizar diversas Tarefas

### Habilidade

A capacidade de realizar uma ação observável.

### Declarações de Habilidade

- Descreve habilidades simples ou complexas.
- É possível que diversas declarações de Habilidade sejam necessárias para realizar uma Tarefa.
- É possível que uma única declaração de Habilidade seja usada para realizar mais de uma Tarefa.



Exemplo: Habilidade em gerar uma hipótese de como um agente de ameaça evitou o Sistema de Detecção de Intrusão.

Conforme ilustrado na Figura 1, as declarações de Habilidade descrevem o que o aprendiz pode realizar e as declarações de Tarefa descrevem o trabalho a ser realizado. Portanto, é importante separar a linguagem utilizada em declarações de Habilidade e declarações de Tarefa, e usar termos que facilitem a observação e avaliação do aprendiz.

### 3 Utilizando o NICE Framework

Observe-se que, embora o Framework da Força de Trabalho para Segurança Cibernética (NICE Framework) se destine a fornecer pilares comuns úteis a diversas organizações, algumas dessas perceberão a necessidade de adaptar o modelo para que se alinhe melhor ao seu contexto específico. Por exemplo, um fabricante pode ter Tarefas específicas ao setor ou à organização que não estão descritas no NICE Framework. Outras podem considerar as Tarefas aplicáveis, mas precisam ajustar ou desenvolver declarações K&S específicas a fim de aumentar a probabilidade de que as Tarefas sejam concluídas conforme definido por seu contexto específico. Por isso, esses pilares não foram elaborados com a finalidade de serem rígidos, mas sim de fornecer uma linguagem comum para organizações ou setores utilizarem de maneiras que sejam benéficas a um determinado contexto.

Por fim, os exemplos de uso dos pilares do NICE Framework fornecidos abaixo são de natureza hipotética ou conceitual. É possível às organizações utilizar os pilares de diversas maneiras para melhor atender às necessidades locais. Os exemplos apresentados têm o objetivo de ilustrar as possíveis abordagens práticas em relação ao NICE Framework que demonstraram auxiliar o êxito de objetivos organizacionais comuns. Eles fornecem orientações para organizações ou setores que buscam um lugar por onde começar, em vez de uma maneira única de usar o NICE Framework.

#### 3.1 Utilizando Declarações Existentes de Tarefa, Conhecimento e Habilidade (TKS)

Os usuários do NICE Framework fazem referência a uma ou mais declarações de Tarefa, Conhecimento e Habilidade (declarações TKS), conforme especificado na Seção 2, para descrever o trabalho e os aprendizes. As declarações de Tarefa são utilizadas para descrever o trabalho. As declarações de Tarefa possuem declarações K&S associadas. Embora uma declaração de Tarefa possa ter um conjunto recomendado de declarações K&S associadas, é possível aos usuários incluir outras declarações K&S existentes para adaptar as Tarefas ao seu contexto específico. As declarações K&S são utilizadas para descrever os aprendizes e podem ser usadas de diversas maneiras para gerenciar a força de trabalho em segurança cibernética. Elas podem ser utilizadas isoladamente, em conjunto ou não serem utilizadas, dependendo do contexto específico da organização que está implementando-as. Os exemplos de uso hipotético abaixo demonstram áreas onde as declarações TKS podem ser implementadas:

- Programa de acompanhamento da Habilidade do Funcionário para determinar sua qualificação para fins de promoção
- Conhecimento necessário para a conclusão de um curso
- Lista de Tarefas semanais a serem realizadas em uma organização

As declarações e exemplos TKS podem ser encontrados no NICE Framework Resource Center e serão atualizados, conforme necessário, para acompanhar as mudanças resultantes da evolução das missões de negócios, riscos ou tecnologias emergentes. [1]

### 3.2 Criando Novas Declarações TKS

Os usuários são alertados a não modificarem o texto das declarações TKS existentes no NICE Framework. As declarações destinam-se a atender a interoperabilidade. Portanto, alterar seu conteúdo pode resultar em uma subsequente desarmonia no uso de fontes externas. Uma nova declaração pode ser criada caso seja necessário alterar sua redação a fim de atender o contexto específico de um usuário.

Também é possível aos usuários criar declarações de Tarefa, Conhecimento ou Habilidade totalmente novas para personalizar o uso do NICE Framework de acordo com seu contexto específico. Essas declarações adicionais ajudarão a promover discussões internas claras e consistentes sobre os aprendizes e suas atividades de trabalho.

### 3.3 Competências

As competências fornecem um mecanismo para as organizações avaliarem os aprendizes. As competências são definidas por meio de uma abordagem orientada ao empregador que fornece uma visão do contexto específico de uma organização. Além disso, elas permitem que os provedores de educação e qualificação atendam às necessidades do empregador ou do setor, criando experiências de aprendizagem que ajudem os alunos a desenvolverem e demonstrarem suas Competências. As Competências consistem em um nome, sua descrição, método de avaliação e um grupo de declarações TKS associadas.

**Competência**

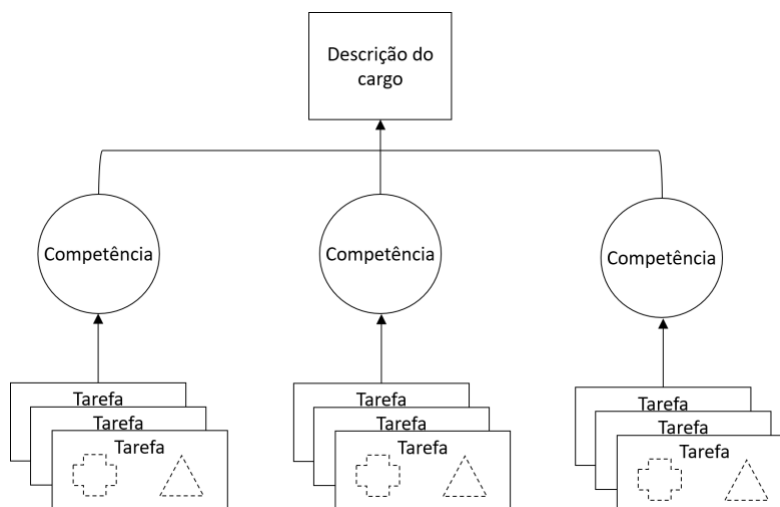
Um mecanismo para as organizações avaliarem os aprendizes.

**Competências são**

- Definidas por meio de uma abordagem orientada ao empregador
- Focadas no aprendiz
- Observáveis e avaliáveis

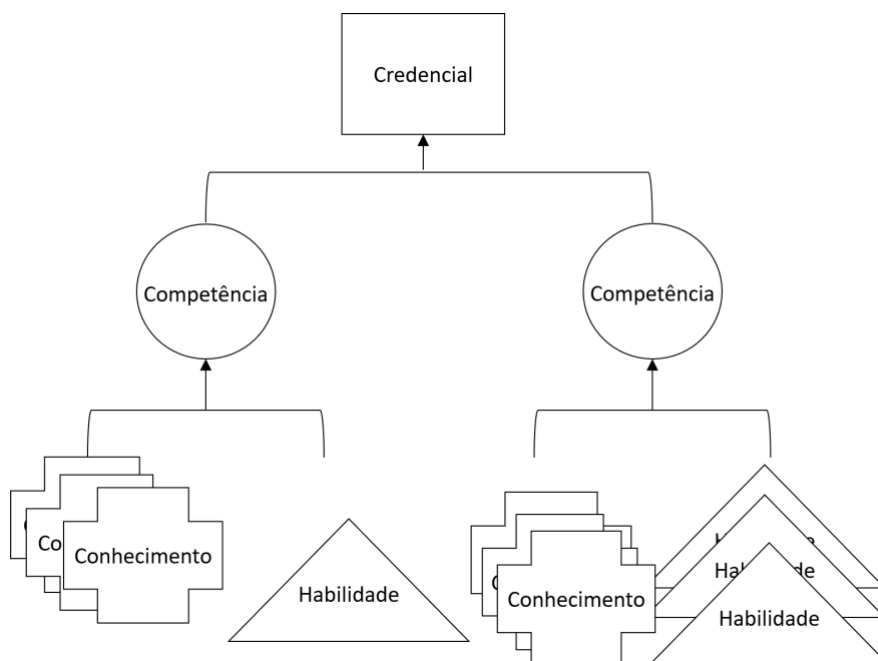
As Competências são flexíveis ao permitir que as organizações incorporem diversas declarações TKS em uma categoria abrangente que define uma necessidade ampla. Embora uma Tarefa e suas declarações de Conhecimento e Habilidade associadas talvez não mudem, a Competência definida de forma mais ampla poderá introduzir novas Tarefas, ou até mesmo Conhecimentos e Habilidades, ou remover os existentes, a fim de atender necessidades diferentes em um ecossistema de segurança cibernética em constante mudança.

As Competências podem ser utilizadas de diversas maneiras. Por exemplo, conforme ilustrado na Figura 2, uma organização pode usar Competências como parte do processo de contratação com a intenção de alcançar objetivos organizacionais específicos. Nesse caso, as Competências podem ser definidas como um grupo de declarações de Tarefas relacionadas. A organização pode então usar essas Competências para avaliar se um candidato pode realizar essas Tarefas. Essa avaliação pode assumir a forma de uma entrevista, teste realizado anteriormente à contratação ou observação de aprendizagem baseada no trabalho.



**Figura2 Utilizando Competências para Avaliar Aprendizes por meio da Descrição de uma Posição**

Outras organizações podem usar Competências para determinar se um aprendiz alcançou um conjunto definido de Habilidades e Conhecimento. Essas organizações podem, conforme ilustrado na Figura 3, escolher utilizar as Competências como grupos de declarações K&S. Essas organizações podem então avaliar os aprendizes quanto a essas declarações K&S. As avaliações podem assumir a forma de testes, demonstrações em laboratório ou avaliações orais.



**Figura 3. Utilizando Competências para Avaliar Aprendizes por meio de uma Credencial**

Os exemplos acima são hipotéticos. Eles podem ser utilizados isoladamente, em conjunto ou não serem utilizados, dependendo do contexto específico da organização que está implementando-os.

### 3.3.1 Utilizando Competências Existentes

As Competências do NICE Framework são uma forma das organizações se alinharem efetivamente ao NICE Framework, sem se aprofundar nos detalhes das declarações TKS. Competências são uma forma de descrever a avaliação de um aprendiz. Ao permitir grupos de declarações TKS definidos pela organização, as Competências permitem que as organizações se comuniquem de forma sucinta e organizem efetivamente seu trabalho de segurança cibernética para fornecer uma visão simplificada da força de trabalho. Outros possíveis usos das Competências incluem:

- Descrever os tipos de Tarefas em uma determinada posição
- Acompanhar as capacidades da força de trabalho
- Descrever os requisitos da equipe
- Demonstrar as capacidades do aprendiz

Embora uma Competência tenha um conjunto recomendado de declarações TKS associadas, os usuários podem adicionar ou remover as declarações existentes para adaptar as Competências ao seu contexto específico. Contudo, os usuários são alertados a não modificarem o título ou a descrição de uma Competência existente do NICE Framework. As Competências destinam-se a atender a interoperabilidade. Portanto, alterar seu conteúdo pode resultar em uma subsequente desarmonia no uso de fontes externas. Uma nova Competência pode ser criada caso seja necessário alterar sua redação a fim de atender o contexto específico de um usuário, conforme descrito abaixo (consulte a Seção 3.3.2).

### 3.3.2 Criando Novas Competências

Algumas organizações podem precisar descrever uma Competência para um contexto específico de seu trabalho de segurança cibernética. O NICE Framework, desenvolvido com o princípio da agilidade, permite que as organizações descrevam uma Competência para atender um ecossistema de segurança cibernética em constante mudança. Isso pode ser feito alterando uma Competência existente para que atenda às necessidades locais ou criando uma Competência nova.

Dois exemplos hipotéticos são fornecidos abaixo para explicar os possíveis processos de uso das Competências. Os dois exemplos abordam a Análise de Dados para mostrar que a mesma Competência pode ser utilizada por meio de abordagens diferentes. Além disso, esses exemplos complementam a Figura 2 e a Figura 3 para auxiliar o leitor em uma possível implementação. Esses exemplos utilizam uma estrutura de tabela para comunicar a Competência. Essa abordagem em tabela é uma entre as diversas que podem ser empregadas por uma organização que busca implementar Competências.

#### Exemplo de Análise de Dados 1

A Tabela 1, abaixo, é informativa e fornece um ponto de partida para a construção de uma Competência. A Competência do Exemplo de Análise de Dados 1 possui um nome e uma descrição que permitem rapidamente à organização identificar uma Competência como aquela que tem valor para sua estrutura e contexto organizacionais. Com o método de avaliação de

“demonstração em laboratório”, a organização está avaliando um aprendiz ao fornecer um ambiente de trabalho simulado para realizar as Tarefas que atendem aos seus objetivos de negócios. (Observe que a Tabela 1 usa Tarefas da versão de 2017 do NICE Framework. [2])

**Tabela 1- Exemplo de criação de uma nova competência de análise de dados com tarefas existentes do NICE Framework 2017**

<b>Nome da Competência:</b> Exemplo de Análise de Dados 1
<b>Descrição da Competência:</b> Coleta, síntese ou análise de informações e dados qualitativos e quantitativos de diferentes fontes para chegar a uma decisão, fazer uma recomendação e/ou compilar relatórios, <i>briefings</i> , resumos executivos e outros documentos.
<b>Método de Avaliação:</b> Demonstração em laboratório
<b>Declarações de Tarefa</b>
T0007   Analisar e definir requisitos e especificações de dados.
T0405   Utilizar linguagem de código aberto, como R, e aplicar técnicas quantitativas (por exemplo, estatísticas descritivas e inferenciais, amostragem, design experimental, testes paramétricos e não paramétricos de diferença, regressão de mínimos quadrados ordinários, linha geral).

No exemplo descrito na Tabela 1, é possível que uma organização dê a um aprendiz um computador com um determinado conjunto de dados e conectado à rede do laboratório. É dado, então, ao aprendiz tempo para que ele demonstre sua capacidade de usar linguagens de código aberto para aplicar técnicas quantitativas aos dados. É possível que uma parte importante desta avaliação seja analisar o conjunto de dados para garantir que os dados atendam a uma determinada especificação antes de concluir a análise. Por meio dessa avaliação, o aprendiz demonstra a Competência do “Exemplo de Análise de Dados 1”, conforme definido pelo empregador.

Uma Competência de Análise de Dados mais detalhada poderia ser muito mais longa. Ao enumerar as declarações de Tarefa dentro da Competência, a organização pode especificar o escopo desejado da Competência. Para facilidade de uso, as Tarefas são apresentadas com as identificações de Tarefas do NICE Framework 2017.

### Exemplo de Análise de Dados 2

A Tabela 2, a seguir, demonstra outro ponto de partida para a criação de uma Competência. O exemplo é informativo. A descrição é a mesma da Tabela 1. No entanto, este exemplo usa declarações de Conhecimento e Habilidade para construir a Competência.

**Tabela 2- Exemplo de criação de uma nova competência de análise de dados com tarefas adicionais**

<b>Nome da Competência:</b> Exemplo de Análise de Dados 2
<b>Descrição da Competência:</b> Coleta, síntese ou análise de informações e dados qualitativos e quantitativos de diferentes fontes para chegar a uma decisão, fazer uma recomendação e/ou compilar

relatórios, <i>briefings</i> , resumos executivos e outros documentos.
<b>Método de Avaliação:</b> Teste
<b>Declarações K&amp;S</b>
S0013   Habilidade em realizar consultas e desenvolver algoritmos para análise de estruturas de dados.
S0021   Habilidade em projetar uma estrutura de análise de dados (ou seja, os tipos de dados que um teste deve gerar e como analisar esses dados).
S0091   Habilidade em analisar dados voláteis.
K0020   Conhecimento de administração de dados e políticas de padronização de dados.
K0338   Conhecimento de técnicas de mineração de dados.

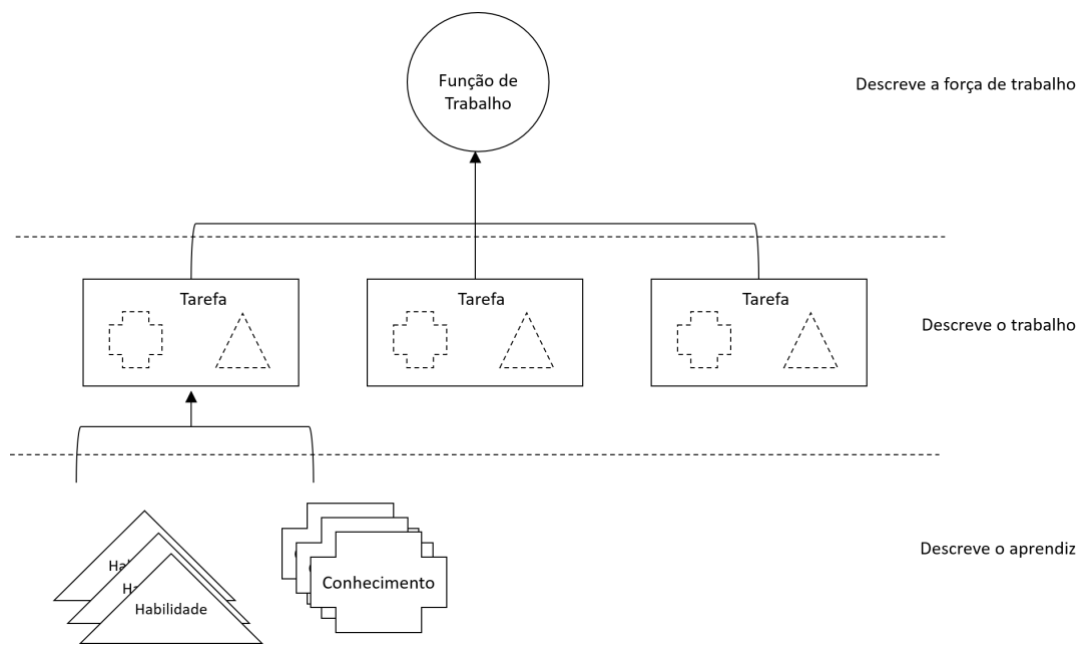
Neste exemplo, a Tabela 2 representa uma Competência de Análise de Dados. Esta Competência pode ser criada por uma instituição certificadora que fornece um teste para avaliar os aprendizes. O teste pode ser administrado em meio físico ou digital. Ao ser aprovado no teste, o aprendiz demonstra a Competência do “Exemplo de Análise de Dados 2”, conforme definido pela instituição certificadora.

(Observe que a Tabela 2 utiliza as declarações K&S da versão de 2017 do NICE Framework. [2])

### 3.4 Funções de Trabalho

As Funções de Trabalho são um caso de uso comum do NICE Framework. Funções de Trabalho são uma forma de descrever um conjunto de trabalho pelo qual alguém é responsável ou deve prestar contas.

Embora os frameworks de força de trabalho anteriores também associassem as Funções de Trabalho às especificações de Conhecimento, Habilidade e Aptidão, o NICE Framework incentiva uma abordagem mais ágil por meio de Tarefas. As Funções de Trabalho são compostas por Tarefas que englobam o trabalho a ser realizado. As Tarefas incluem declarações de Conhecimento e Habilidade associadas que representam o potencial dos aprendizes para realizá-las. Essa abordagem transitiva, ilustrada na Figura 4, promove a flexibilidade e simplifica a comunicação.



**Figura 4 - Relação das Funções de Trabalho com os Pilares**

Os nomes das Funções de Trabalho não são sinônimos de cargos. É possível que algumas Funções de Trabalho coincidam com um cargo, dependendo do uso que uma organização faça desses. Além disso, as Funções de Trabalho não são sinônimos de ocupações.

É possível que uma única Função de Trabalho (por exemplo, Desenvolvedor de Software) seja aplicável a indivíduos com diferentes cargos (por exemplo, engenheiro de software, programador, desenvolvedor de aplicativos). Do mesmo modo, diversas funções podem ser combinadas para criar um cargo específico. Essa abordagem aditiva promove uma melhor modularidade e ilustra o fato de que todos os aprendizes da força de trabalho realizam inúmeras tarefas em várias funções, independentemente de seus cargos. Da mesma forma, o NICE Framework não define níveis de proficiência (por exemplo, Básico, Intermediário, Avançado). Esses atributos, e aqueles relacionados à proficiência com a qual um aprendiz realiza as Tarefas, são abordados em outros modelos ou recursos.

### 3.4.1 Utilizando Funções de Trabalho Existentes

Cada Função de Trabalho se destina a promover o êxito dos objetivos por meio de Tarefas. Embora uma Função de Trabalho possa ter um conjunto predeterminado de Tarefas associadas, é possível aos usuários incluir outras Tarefas existentes para adaptar as Funções de Trabalho ao seu contexto específico. De modo semelhante, um usuário pode desejar remover Funções de Trabalho listadas ou adicionar outras para atender objetivos adicionais. O conjunto atual de componentes do NICE Framework está disponível no NICE Framework Resource Center. [1]

Os usuários são alertados a não modificarem internamente o nome e a descrição de uma Função de Trabalho existente. As Funções de Trabalho destinam-se a atender a interoperabilidade. Portanto, a alteração de seu conteúdo pode resultar em subsequente desarmonia. Uma nova



Função de Trabalho pode ser criada caso seja necessário alterar sua redação, conforme descrito abaixo.

### 3.4.2 Criando uma Nova Função de Trabalho

Também é possível aos usuários criar Funções de Trabalho para ajudar a personalizar o uso do NICE Framework de acordo com seu contexto específico. Essas Funções de Trabalho adicionais ajudarão a promover discussões internas claras e consistentes sobre o trabalho de segurança cibernética.

## 3.5 Equipes

Muitas organizações fazem uso de equipes para enfrentar desafios complexos de forma coletiva, reunindo indivíduos com habilidades e experiências complementares. Ao utilizar diferentes recursos e perspectivas, as equipes permitem que as organizações gerenciem os riscos de forma holística. As equipes aproveitam a especialização de conhecimento e processos de cada membro para distribuir o trabalho de forma eficiente. As equipes podem ser definidas utilizando Funções de Trabalho ou Competências.

### 3.5.1 Formando Equipes por meio das Funções de Trabalho

Uma abordagem centrada na Função de Trabalho para formar equipes permite que as organizações definam quais tipos de Funções de Trabalho são necessários para atingir os objetivos definidos. Como as Funções de Trabalho são compostas por Competências, essa abordagem para formar equipes começa com o trabalho a ser concluído e pode ser considerada uma abordagem “descendente”.

**Tabela 3 - Exemplo de uma equipe de desenvolvimento de software seguro utilizando as Funções de Trabalho do NICE Framework 2017**

Fase do Ciclo de Vida	Função de Trabalho
Design	SP-ARC-002   Arquiteto de segurança
Construção	SP-DEV-001   Desenvolvedor de software
Implementação	OM-NET-001   Especialista em operações de rede
Operação	OM-STS-001   Especialista em suporte técnico
Manutenção	OM-DTA-001   Administrador de banco de dados
Desativação	OV-LGA-001   Consultor jurídico cibernético

A Tabela 3, acima, demonstra uma maneira de criar uma equipe de desenvolvimento de software seguro. As Funções de Trabalho citadas se baseiam nas identificações de Funções de Trabalho da versão de 2017 do NICE Framework. As equipes formadas dessa maneira começam com a identificação do trabalho que precisa ser realizado. Nesse exemplo, a equipe de desenvolvimento de software seguro é organizada por fase do ciclo de vida. A primeira linha demonstra que a equipe levaria em consideração os objetivos da fase de design, incluindo o planejamento, e, portanto, precisaria de um arquiteto de segurança. A Tabela 3 é um exemplo informativo e não inclui todas as Funções de Trabalho que podem estar presentes ou ser necessárias para uma determinada equipe. Para obter mais informações, consulte o *Secure Software Development Framework* do NIST. [6]

**Tabela 4 - Exemplo de criação de uma equipe de segurança cibernética utilizando as Funções de Trabalho do NICE Framework 2017 e Novas Funções de Trabalho**

<b>Função do Framework de Segurança Cibernética</b>	<b>Função de Trabalho</b>
Identificação	Nova Função de Trabalho 1   Gestor de risco
Proteção	SP-RSK-002   Assessor de controle de segurança
Deteção	PR-CDA-001   Analista de defesa cibernética
Atendimento	PR-CIR-001   Responsável pelo atendimento de incidentes de defesa cibernética
Recuperação	Nova Função de Trabalho 2   Especialista em comunicação

A Tabela 4 descreve um exemplo de equipe de segurança cibernética. Semelhante à equipe de desenvolvimento de software seguro, a equipe do exemplo é formada por meio de uma abordagem centrada no trabalho. Ao usar o núcleo do *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*, objetivos de segurança cibernética são selecionados, Tarefas são identificadas para atingir esses objetivos e Funções de Trabalho são selecionadas para definir as funções necessárias para promovê-los. [7]Tabela 4 é um exemplo informativo e não inclui todas as Funções de Trabalho que podem estar presentes ou ser necessárias para uma determinada equipe. Duas novas Funções de Trabalho foram adicionadas para demonstrar uma abordagem mista de uso de Funções de Trabalho existentes (Seção 3.4.1) e criação de novas Funções de Trabalho (Seção 3.4.2). Ao criar Funções de Trabalho, o exemplo demonstra uma abordagem flexível e ágil para personalização do NICE Framework.

### 3.5.2 Formando Equipes por meio das Competências

As equipes também podem ser formadas utilizando Competências. Esta abordagem para formar equipes reconhece que as Tarefas podem ser desconhecidas, mas os tipos de Competências necessárias para resolver o desafio são conhecidos. Essa abordagem pode ser considerada “ascendente”. Portanto, as equipes formadas dessa forma podem ajudar a identificar aprendizes que poderão participar do trabalho da equipe no futuro. Esses aprendizes poderão ou não estar associados a uma Função de Trabalho e simplesmente possuir as Competências necessárias para ajudar a cumprir os objetivos organizacionais.

Por exemplo, é possível que uma equipe de segurança cibernética defensiva que usa suas habilidades para imitar as técnicas de ataque dos adversários (ou seja, uma “Equipe Vermelha”) seja composta pelas seguintes Competências hipotéticas:

- Planejamento de engajamento
- Regras de engajamento
- Teste de invasão (Pen Test)
- Coleta de dados
- Exploração de vulnerabilidade

Ao criar equipes ou outros agrupamentos TKS, cada organização pode personalizar o NICE Framework da maneira que lhe for mais útil para aplicar e comunicar informações sobre os aprendizes (e o trabalho que esses aprendizes irão realizar) a fim de permitir o êxito dos objetivos da missão.

## 4 Conclusão

Por meio da aplicação da abordagem de pilares descrita pelo NICE Framework, os usuários podem se beneficiar de um método consistente para organizar e comunicar o trabalho a ser realizado por meio de declarações de Tarefa e do Conhecimento e Habilidades de cada um dos aprendizes que promove o trabalho. O NICE Framework ajuda a orientar os esforços dos empregadores para descrever o trabalho de segurança cibernética, dos provedores de educação e qualificação para preparar trabalhadores de segurança cibernética e dos aprendizes para demonstrar suas capacidades de realizar o trabalho de segurança cibernética.

A capacidade de descrever Tarefas, Conhecimento e Habilidades é importante para garantir uma compreensão abrangente do trabalho e da força de trabalho. O NICE Framework fornece uma referência que pode ser ampliada, aplicada e utilizada por diferentes organizações ou setores para descrever o trabalho a ser executado em diversas áreas. Os benefícios para essas organizações atendem a missão do NICE de fomentar, promover e coordenar uma comunidade robusta que trabalha em conjunto para promover um ecossistema integrado de educação, qualificação e desenvolvimento da força de trabalho em segurança cibernética.

## Referências

- [1] National Initiative for Cybersecurity Education (2020) *NICE Framework Resource Center*. Disponível no site <https://www.nist.gov/nice/framework>
- [2] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. <https://doi.org/10.6028/NIST.SP.800-181>
- [3] National Institute of Standards and Technology (2020) *National Online Informative References Program*. Disponível no site <https://csrc.nist.gov/projects/olir>
- [4] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. <https://doi.org/10.6028/NIST.IR.8286>
- [5] Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory Into Practice*, 41(4), 212-218. Disponível no site <https://www.depauw.edu/files/resources/krathwohl.pdf>
- [6] Dodson DF, Souppaya MP, Scarfone KA (2020) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. <https://doi.org/10.6028/NIST.CSWP.04232020>
- [7] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>

## Appendix A—Acrônimos

Os acrônimos e abreviações selecionados e utilizados neste documento são definidos a seguir.

ERM	Gestão de Risco Corporativo
FISMA	Lei Federal de Modernização da Segurança da Informação
FOIA	Lei de Liberdade de Informação
ITL	Laboratório de Tecnologia da Informação do NIST
K&S	Declaração(ões) de Conhecimento e Habilidade
NICE	Iniciativa Nacional para Educação em Segurança Cibernética
NIST	National Institute of Standards and Technology
OLIR	Referência Informativa On-line
OMB	Gabinete de Gestão e Orçamento
SSDF	Framework de desenvolvimento de software seguro
TKS	Declarações de Tarefa, Conhecimento e Habilidade

## Appendix B—Glossário

Para obter um glossário completo, acesse <https://csrc.nist.gov/glossary>.

- Competência** Um mecanismo para as organizações avaliarem os aprendizes.
- Conhecimento** Um conjunto de conceitos que pode ser lembrado.
- Habilidade** A capacidade de realizar uma ação observável.
- Tarefa** Uma atividade direcionada ao êxito dos objetivos organizacionais.