

# Publicação retirada da série técnica do NIST

## Aviso

A publicação anexa foi retirada(arquivada) mas sua tradução para o português está disponível. A publicação original em inglês foi absorvida por outra publicação (listada abaixo).

### Publicação retirada (arquivada)

<b>Série / Número</b>	NIST Special Publication (SP) 800-181
<b>Título</b>	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
<b>Data de publicação</b>	Agosto de 2017
<b>Data de retirada</b>	16 de novembro de 2020
<b>Nota de retirada</b>	SP 800-181 está sendo inteiramente substituída pela publicação SP 800-181 Revision 1.

### Publicação(ões) absorvida(s)

A publicação anexa foi **substituída** pela(s) seguinte(s) publicação(ões):

<b>Série / Número</b>	NIST Special Publication (SP) 800-181 Revision 1
<b>Título</b>	Workforce Framework for Cybersecurity (NICE Framework)
<b>Autores</b>	Rodney Petersen; Danielle Santos; Karen A. Wetzel; Matthew C. Smith; Greg Witte
<b>Data de publicação</b>	Novembro de 2020
<b>URL/DOI</b>	<a href="https://doi.org/10.6028/NIST.SP.800-181r1">https://doi.org/10.6028/NIST.SP.800-181r1</a>

### Informações adicionais

<b>Contato</b>	NICE Framework: NICEframework@nist.gov
<b>Última revisão da publicação anexa</b>	
<b>Outras informações</b>	National Initiative for Cybersecurity Education (NICE): <a href="https://nist.gov/nice">https://nist.gov/nice</a> <a href="https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final">https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final</a>
<b>Link do anúncio de retirada</b>	

**Publicação Especial do NIST 800-181**

---

**Iniciativa Nacional para Educação em  
Cibersegurança (NICE)  
Estrutura da Força de Trabalho em  
Segurança Cibernética**

---

William Newhouse  
Stephanie Keith  
Benjamin Scribner  
Greg Witte

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

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

**Publicação Especial do NIST 800-181**

# **Iniciativa Nacional para Educação em Cibersegurança (NICE) Estrutura da Força de Trabalho em Cibersegurança**

**William Newhouse**

*Divisão de Segurança Cibernética Aplicada  
Laboratório de Tecnologia da Informação*

**Stephanie Keith**

*Cyber Workforce Strategy & Policy Division (Divisão da força de trabalho de estratégia e  
política cibernética)  
Escritório do Vice-Chefe de Informação do DoD*

**Benjamin Scribner**

*Ramo de educação e conscientização cibernética  
Diretoria Nacional de Proteção e Programas do DHS*

**Greg Witte**

*G2, Inc.  
Annapolis Junction, MD*

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

Agosto 2017



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

National Institute of Standards and Technology (Instituto Nacional de Normas e Tecnologia)  
*Kent Rochford, Diretor em Exercício do NIST e Subsecretário de Comércio para Normas e Tecnologia*

## Autoridade

Esta publicação foi desenvolvida pelo NIST de acordo com suas responsabilidades legais nos termos da Federal Information Security Modernization Act (FISMA) [Lei Federal de Modernização da Segurança da Informação] de 2014, 44 U.S.C. § 3551 *et seq.*, Lei Pública (P.L.) 113-283. O NIST (Instituto Nacional de Normas e Tecnologia) é responsável por desenvolver normas e diretrizes de segurança da informação, incluindo requisitos mínimos para sistemas de informação federais, porém, tais normas e diretrizes não se aplicam aos sistemas de segurança nacional sem a aprovação expressa das devidas autoridades federais que exercem autoridade normativa sobre tais sistemas. Esta diretriz é consistente com os requisitos da Circular A-130 do Office of Management and Budget (OMB) (Escritório de Gestão e Orçamento).

Nenhuma informação nesta publicação deve ser interpretada como contraditória às normas e diretrizes obrigatórias e vinculativas para as agências federais pelo Secretário de Comércio nos termos da sua autoridade legal. Como também, essas diretrizes não devem ser interpretadas como tendo o intuito de alterar ou substituir os poderes existentes do Secretário de Comércio, Diretor do OMB ou qualquer outra autoridade federal. Esta publicação pode ser usada por organizações não governamentais voluntariamente, e não está sujeita a direitos autorais nos Estados Unidos. No entanto, uma atribuição seria apreciada pelo NIST.

Publicação especial do Instituto Nacional de Normas e Tecnologia 800-181  
Natl. Inst. Stand. Technol. Spec. Publ. 800-181, 144 páginas (August 2017)  
CODEN: NSPUE2

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

Certas entidades comerciais, equipamentos ou materiais podem ser identificados neste documento para descrever adequadamente determinado procedimento ou conceito experimental. Esta identificação não tem a intenção de sugerir recomendação ou endosso do NIST, nem tem a intenção de sugerir que as entidades, materiais ou equipamentos são necessariamente os melhores disponíveis para tal propósito.

Esta publicação pode conter referências a outras publicações atualmente sendo produzidas pelo NIST de acordo com suas responsabilidades estatutárias a ele atribuídas. As informações nesta publicação, incluindo conceitos e metodologias, podem ser usadas por agências federais mesmo antes da conclusão de tais publicações complementares. Assim sendo, até que cada publicação seja concluída, os requisitos, diretrizes e procedimentos atuais, onde existam, permanecem operacionais. Para fins de planejamento e transição, as agências federais podem desejar acompanhar de perto o desenvolvimento dessas novas publicações produzidas pelo NIST.

As organizações são incentivadas a revisar todos os esboços preliminares das publicações durante os períodos de comentários públicos e fornecer feedback ao NIST. Muitas publicações do NIST sobre segurança cibernética, além das mencionadas acima, estão disponíveis em <http://csrc.nist.gov/publications>.

## Comentários a esta publicação podem ser enviados para:

National Institute of Standards and Technology (Instituto Nacional de Normas e Tecnologia)  
A/C: NICE, Divisão de Segurança Cibernética Aplicada, Laboratório de Tecnologia da Informação  
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000  
Email: [niceframework@nist.gov](mailto:niceframework@nist.gov)

Todos os comentários estão sujeitos a divulgação no âmbito da Lei de Liberdade de Informação (FOIA).

## Relatórios sobre Tecnologia de Sistemas Informáticos

O Laboratório de Tecnologia da Informação (ITL) do NIST promove a economia e o bem-estar público dos EUA, fornecendo liderança técnica para a infraestrutura de medições e normas da Nação. O ITL desenvolve testes, métodos de testes, dados de referência, implementações de prova de conceito e análises técnicas para promover o desenvolvimento e o uso produtivo da tecnologia da informação. As responsabilidades do ITL incluem o desenvolvimento de normas e diretrizes gerenciais, administrativas, técnicas e físicas para a segurança a custo razoável e a privacidade de outras informações, além das relacionadas à segurança nacional em sistemas federais de informação. A Publicação Especial da série 800 relata a pesquisa, diretrizes e os esforços de divulgação do ITL no tocante à segurança do sistema de informação e suas atividades colaborativas com a indústria, governo e organizações acadêmicas.

### Resumo

Esta publicação descreve a Cybersecurity Workforce Framework [Estrutura da Força de Trabalho em Cibersegurança] (NICE Framework) da National Initiative for Cybersecurity Education [Iniciativa Nacional para Educação em Cibersegurança] (NICE). Ela serve como um recurso de referência fundamental para descrever e compartilhar informações sobre o trabalho de segurança cibernética e os conhecimentos, habilidades e aptidões (KSAs) necessárias para concluir tarefas que possam reforçar a postura de cibersegurança em uma organização. Usando uma terminologia comum e consistente que categoriza e descreve o trabalho de segurança cibernética, o NICE Framework facilita a comunicação sobre como identificar, recrutar, desenvolver e reter talentos em cibersegurança. O NICE Framework é uma fonte de referência através da qual organizações ou setores podem desenvolver publicações ou ferramentas adicionais que atendam às suas necessidades para definir ou fornecer orientação sobre diferentes aspectos do desenvolvimento, planejamento, treinamento e educação da força de trabalho em cibersegurança.

### Palavras-chave

Habilidade; cibersegurança; ciberespaço; educação; conhecimento; função; habilidade; área de especialidade; tarefa; treinamento; função de trabalho.

### Revisões

Visite o website de revisões do NICE Framework [\[1\]](#) para verificar se houve alguma atualização.

### Conteúdo suplementar

Uma planilha de referência para o NICE Framework está disponível em <https://www.nist.gov/file/372581>.

## Reconhecimentos

Os autores reconhecem com gratidão e expressam seu apreço pelas importantes contribuições de indivíduos e organizações nos setores público e privado, cujos comentários ponderados e construtivos melhoraram a qualidade geral, a eficácia e a utilidade desta publicação.

Agradecemos a liderança e o trabalho de Rodney Petersen, Diretor da Iniciativa Nacional para Educação em Segurança Cibernética (NICE) do NIST. Queremos também agradecer aos seguintes indivíduos: Tanya Brewer, Dean Bushmiller, Lynne Clarke, Jerri Damavandy, Lisa Dorr, Ryan Farr, Jim Foti, Jodi Guss, Keith Hall, Chris Kelsall, Elizabeth Lennon, Jeff Marron, Joshua Musicante, Stephen Olechnowicz, Lori Pfannenstein, Chuck Romine, Kevin Sanchez-Cherry, Danielle Santos, Stephanie Shively, Matthew Smith, Kevin Stine, Bluma Sussman, Caroline Tan, Baris Yakin, e Clarence Williams por suas contribuições individuais para esta publicação.

O primeiro NICE Framework foi postado para comentários públicos em setembro de 2012, e publicado como trabalho final em abril de 2013, sendo intitulado National Cybersecurity Workforce Framework [Estrutura da força de trabalho em segurança cibernética] versão 1.0 [2].

Os autores reconhecem a Dra. Jane Homeyer, Anne Quigley, Rex Min, Noel Kyle, Maya Yankelevich e Peggy Maxson por liderarem o desenvolvimento deste trabalho, como também Montana Williams e Roy Burgess por sua liderança no desenvolvimento do National Cybersecurity Workforce Framework versão 2.0, que foi publicado em abril de 2014 [3].

Finalmente, os autores reconhecem respeitosamente o trabalho fundamental em segurança informática que data da década de 1960. A visão, as percepções e os esforços dedicados dos primeiros pioneiros em segurança informática servem como base filosófica e técnica para as tarefas, conhecimentos, competências e habilidades presentes nesta publicação.

### Informações sobre marcas registradas

Todas as marcas registradas e marcas comerciais pertencem às suas respectivas organizações.

## Síntese

A Iniciativa Nacional para Educação em Cibersegurança (NICE), liderada pelo Instituto Nacional de Normas e Tecnologia (NIST) do Departamento de Comércio dos EUA, é uma parceria entre o governo, o mundo acadêmico e o setor privado, trabalhando conjuntamente para energizar e promover uma rede robusta e um ecossistema de educação, treinamento e desenvolvimento da força de trabalho em segurança cibernética.

O NICE cumpre essa missão trabalhando coordenadamente com parceiros governamentais, acadêmicos e da indústria para trazer evoluções aos programas de sucesso existentes, facilitar mudanças e inovações, e proporcionar liderança e visão para aumentar o número de profissionais do setor de cibersegurança qualificados, ajudando a manter a segurança da nossa nação.

O NICE está empenhado em cultivar uma força de trabalho integrada de segurança cibernética que seja globalmente competitiva, desde a contratação até a aposentadoria, e preparada para proteger nossa nação dos desafios existentes e emergentes de segurança cibernética. O NICE promove, por todo o país, iniciativas que aumentam o número de pessoas com conhecimentos, habilidades e aptidões para realizar as tarefas necessárias para o trabalho em cibersegurança.

Conforme as ameaças que exploram vulnerabilidades em nossa infraestrutura cibernética crescem e evoluem, uma força de trabalho de segurança cibernética integrada deve estar apta a criar o design, desenvolver, implementar e manter estratégias cibernéticas defensivas e ofensivas. Uma força de trabalho integrada na área de cibersegurança inclui funções técnicas e não técnicas que contam com o trabalho de pessoas conhecedoras e experientes. Uma força de trabalho de segurança cibernética integrada pode enfrentar os desafios de cibersegurança inerentes ao processo de preparação de organizações, para que assim possam implementar com sucesso aspectos de suas missões e processos de negócios conectados ao ciberespaço.

Esta publicação oferece referências fundamentais no apoio a uma força de trabalho apta a atender às necessidades de cibersegurança de uma organização, usando um léxico comum e consistente para descrever o trabalho de segurança cibernética por categoria, área de especialidade e função de trabalho. Ela fornece um superconjunto de conhecimentos, habilidades e aptidões (KSAs) (do inglês *knowledge, skills and abilities*) e tarefas de segurança cibernética para cada função de trabalho. O NICE Framework oferece suporte à comunicação organizacional e setorial de maneira consistente, nas áreas de educação, treinamento e desenvolvimento da força de trabalho em cibersegurança.

Um usuário do NICE Framework usará este recurso como referência em diferentes aspectos do desenvolvimento da força de trabalho, educação e/ou treinamento, sendo que, quando o material for usado em níveis organizacionais, o usuário deverá personalizar o material extraído do NICE Framework, adaptando-o a normas, regulamentos, necessidades e missão da organização. O NICE Framework é um ponto de partida, usado como referência para o conteúdo de orientação e diretrizes sobre planos de carreira, educação, capacitação e programas de credenciamento.

O NICE Framework é um recurso que fortalecerá a capacidade de comunicação clara e consistente de uma organização sobre o trabalho de segurança cibernética e os colaboradores que integram a área de cibersegurança. Organizações ou setores podem desenvolver publicações ou ferramentas adicionais que atendam às suas necessidades para definir ou fornecer orientação sobre diferentes aspectos do desenvolvimento, planejamento, treinamento e educação da força de trabalho.

Uma ferramenta de planilha de referência online [\[4\]](#) está disponível no site do NICE Framework [\[5\]](#).

## Tabela de Conteúdo

<b>Executive Summary .....</b>	<b>1</b>
<b>1 Introduction .....</b>	<b>4</b>
1.1 NICE Framework Background .....	5
1.2 Purpose and Applicability.....	5
1.3 Audience/Users.....	6
1.3.1 Employers .....	6
1.3.2 Current and Future Cybersecurity Workers .....	7
1.3.3 Educators/Trainers .....	7
1.3.4 Technology Providers.....	7
1.4 Organization of this Special Publication.....	8
<b>2 NICE Framework Components and Relationships .....</b>	<b>9</b>
2.1 Components of the NICE Framework .....	9
2.1.1 Categories .....	9
2.1.2 Specialty Areas .....	9
2.1.3 Work Roles .....	9
2.1.4 Knowledge, Skills, and Abilities (KSAs).....	9
2.1.5 Tasks.....	10
2.2 NICE Framework Component Relationships .....	10
<b>3 Using the NICE Framework .....</b>	<b>12</b>
3.1 Identification of Cybersecurity Workforce Needs .....	12
3.2 Recruitment and Hiring of Highly Skilled Cybersecurity Talent .....	13
3.3 Education and Training of Cybersecurity Workforce Members .....	13
3.4 Retention and Development of Highly Skilled Cybersecurity Talent .....	14

**4 Extensions ..... 15**

4.1 Competencies ..... 15

4.2 Job Titles ..... 15

4.3 Cybersecurity Guidance and Guideline documents ..... 15

**Lista de Apêndices**

**Appendix A – Listing of NICE Framework Components ..... 16**

A.1 NICE Framework Workforce Categories ..... 16

A.2 NICE Framework Specialty Areas ..... 17

A.3 NICE Framework Work Roles ..... 20

A.4 NICE Framework Tasks ..... 30

A.5 NICE Framework Knowledge Descriptions ..... 69

A.6 NICE Framework Skills Descriptions ..... 89

A.7 NICE Framework Ability Descriptions ..... 102

**Appendix B – Work Role Detail Listing ..... 110**

B.1 Securely Provision (SP) ..... 110

B.2 Operate and Maintain (OM) ..... 117

B.3 Oversee and Govern (OV) ..... 121

B.4 Protect and Defend (PR) ..... 128

B.5 Analyze (AN) ..... 130

B.6 Collect and Operate (CO) ..... 135

B.7 Investigate (IN) ..... 141

**Appendix C – Workforce Development Tools ..... 143**

C.1 DHS Cybersecurity Workforce Development Toolkit ..... 143

    C.1.1 Proficiency Levels and Career Paths ..... 143

C.2 Baldrige Cybersecurity Excellence Builder Tool ..... 144

C.3 Position Description Drafting Tool ..... 144

**Appendix D – Cross Reference to Guidance and Guideline Documents ..... 145**

D.1 Cybersecurity Framework ..... 145

    D.1.2 Example Integration of Cybersecurity Framework with NICE Framework ..... 147

D.2 Systems Security Engineering ..... 149

D.3 U.S. Office of Personnel Management Federal Cybersecurity Codes ..... 150

<b>Appendix E – Acronyms .....</b>	<b>152</b>
<b>Appendix F – References .....</b>	<b>154</b>

### Lista de Tabelas

Table 1 - NICE Framework Workforce Categories .....	16
Table 2 - NICE Framework Specialty Areas .....	17
Table 3 - NICE Framework Work Roles .....	21
Table 4 - NICE Framework Tasks .....	30
Table 5 - NICE Framework Knowledge Descriptions .....	69
Table 6 - NICE Framework Skills Descriptions .....	89
Table 7 - NICE Framework Ability Descriptions .....	102
Table 8 - Crosswalk of NICE Framework Workforce Categories to Cybersecurity Framework Functions .....	147
Table 9 – Crosswalk of Work Role IDs to OPM Cybersecurity Codes .....	151

## 1 Introdução

A National Initiative for Cybersecurity Education (NICE) [A Iniciativa Nacional para Educação em Cibersegurança], liderada pelo National Institute of Standards and Technology (NIST) [Instituto Nacional de Normas e Tecnologia] do Departamento de Comércio dos EUA, é uma parceria entre o governo, o mundo acadêmico e o setor privado, que busca energizar e promover uma rede robusta e um ecossistema de educação, treinamento e desenvolvimento da força de trabalho em cibersegurança. O NICE cumpre essa missão trabalhando de forma colaborativa com parceiros governamentais, mundo acadêmico e setor industrial, com o intuito de otimizar programas de sucesso existentes, facilitar a mudança e inovação, promovendo a liderança e a visão para aumentar o número de profissionais de segurança cibernética qualificados, ajudando a manter a nossa nação segura e economicamente competitiva.

O NICE está empenhado em cultivar uma força de trabalho integrada de segurança cibernética que seja globalmente competitiva, desde a contratação até a aposentadoria, estando preparada para proteger nossa nação dos desafios de cibersegurança existentes e emergentes.

Ao longo deste documento, o termo "força de trabalho em cibersegurança" significa uma força de trabalho com funções que causam impacto na capacidade de uma organização de proteger seus dados, sistemas e operações. Estão incluídas novas funções de trabalho tradicionalmente conhecidas como funções de segurança de tecnologia da informação (TI). Tais funções foram acrescentadas a esta estrutura de força de trabalho para destacar sua importância para a postura geral de uma organização em relação à cibersegurança. Além disso, algumas funções de trabalho descritas neste documento mencionam o termo mais curto '*cibernética*' (*cyber*) para incluir setores onde o ciberespaço se tornou a norma de conversação.

A força de trabalho em cibersegurança inclui não apenas uma equipe focada na área técnica, mas também aqueles que aplicam o conhecimento de segurança cibernética ao preparar a organização para implementar com sucesso a sua missão. Uma força de trabalho em cibersegurança experiente e qualificada é vital para lidar com os riscos de segurança cibernética dentro do processo geral de gestão de risco de uma organização.

## 1.1 Contexto do NICE Framework

O conceito do NICE Framework começou antes da sua implantação em 2010, e se desenvolveu por reconhecer-se que a força de trabalho em cibersegurança não havia ainda sido definida e avaliada. Em 2008, para enfrentar esse desafio, o Conselho de Diretores Federais da Tecnologia da Informação (CIO) assumiu a tarefa de fornecer uma estrutura padrão para compreender as funções de cibersegurança dentro do governo federal. As contribuições de grupos de enfoque, compostos por especialistas na área oriundos de várias agências federais, ajudaram o Conselho Federal de CIOs a produzir um relatório de pesquisa que fazia referência a outros esforços de desenvolvimento profissional em tecnologia da informação que já estavam em andamento. Como resultado, treze funções específicas foram identificadas como necessárias pelas agências para conduzir o trabalho em cibersegurança.

Com base nessa exploração inerentemente multidisciplinar no "campo" da cibersegurança, a Iniciativa Nacional Ampla em Segurança Cibernética, com enfoque na força de trabalho, incumbiu várias agências de trabalharem juntas, visando a desenvolver uma estrutura de força de trabalho em segurança cibernética. O trabalho preliminar foi aberto para receber comentários públicos em setembro de 2011. Os comentários foram incorporados à versão 1.0 [2].

Posteriormente, uma ampla revisão de todo o governo dos EUA indicou áreas específicas a serem examinadas e refinadas. O Departamento de Segurança Interna (DHS) recebeu contribuições e validou as recomendações finais por meio de grupos de enfoque com especialistas de todo o país, do governo, da indústria e da academia, o que resultou em uma segunda versão do NICE Framework, versão 2.0 [3], que foi divulgada publicamente em 2014.

O Gabinete do Secretário de Defesa (OSD) expandiu a versão 2.0 por meio de compromissos internos com componentes de serviço, e compromissos externos com o setor privado. Os coautores do DHS e do NIST trabalharam com o OSD para refinar a expansão proposta, o que resultou nesta publicação, tendo como objetivo enfatizar sua aplicabilidade no setor privado e reforçar a visão de que o NICE Framework é um recurso de referência para os setores público e privado.

## 1.2 Objetivo e aplicabilidade

Esta publicação serve como recurso de referência fundamental para apoiar uma força de trabalho apta a atender às necessidades de segurança cibernética de uma organização. Ela fornece às organizações um léxico comum e consistente que categoriza e descreve o trabalho de segurança cibernética.

Usar o NICE Framework como uma referência fundamental, resultará em melhorias na comunicação, o que é necessário para identificar, recrutar e desenvolver talentos em segurança cibernética. O NICE Framework permitirá que os empregadores usem uma linguagem focada e

consistente em programas de desenvolvimento profissional, no uso de certificações do setor e credenciais acadêmicas, e na seleção de oportunidades de treinamento relevantes para a sua força de trabalho.

O NICE Framework facilita o uso de uma abordagem mais consistente, comparável e repetível para selecionar e especificar funções de cibersegurança para cargos dentro das organizações. Ele também fornece um léxico comum que as instituições acadêmicas podem usar para desenvolver currículos de segurança cibernética que melhor preparem os alunos para as necessidades atuais e futuras da força de trabalho em cibersegurança.

A aplicação do NICE Framework oferece a possibilidade de descrever todo o trabalho de segurança cibernética. Um objetivo de aplicabilidade do NICE Framework é que qualquer trabalho ou cargo no âmbito de segurança cibernética possa ser descrito, identificando o material relevante de um ou mais componentes do NICE Framework. Para cada trabalho ou posição, o contexto da missão ou processos e prioridades de negócios indicarão qual o material que deve ser selecionado utilizando o NICE Framework.

Organizações ou setores podem usar o NICE Framework para desenvolver publicações ou ferramentas adicionais que atendam às suas necessidades para definir ou fornecer orientação sobre diferentes aspectos do desenvolvimento, planejamento, treinamento e educação da força de trabalho.

### **1.3 Audiência/Usuários**

O NICE Framework pode ser visto como um dicionário não prescritivo da força de trabalho em cibersegurança. Os usuários do NICE Framework que o usam como referência, devem implementá-lo localmente para diferentes fins de desenvolvimento, instrução ou treinamento da força de trabalho.

#### **1.3.1 Empregadores**

O uso de uma terminologia comum do NICE Framework permite que os empregadores possam inventariar e desenvolver a sua força de trabalho em cibersegurança. O NICE Framework pode ser usado por empregadores e a liderança organizacional para:

- Inventariar e rastrear a sua força de trabalho em cibersegurança para maior compreensão dos pontos fortes e das falhas em Conhecimentos, Habilidades e Aptidões, além das tarefas realizadas;
- Identificar os requisitos de treinamento e qualificação para desenvolver conhecimentos, habilidades e aptidões essenciais para desempenhar tarefas em cibersegurança;
- Melhorar as descrições de cargos e anúncios de vagas de emprego selecionando KSAs (conhecimentos, habilidades e aptidões) e tarefas relevantes, uma vez que as funções e tarefas de trabalho são identificadas;
- Identificar as funções de trabalho mais relevantes e desenvolver planos de carreira para orientar os funcionários na aquisição das habilidades necessárias para tais funções; e

- Estabelecer uma terminologia compartilhada entre os gerentes de contratação e a equipe de recursos humanos (RH) para o recrutamento, retenção e treinamento de uma força de trabalho altamente especializada.

### 1.3.2 Trabalhadores atuais e futuros em cibersegurança

O NICE Framework oferece suporte aos que atuam na área de cibersegurança e aos que desejam atuar nesta área, para explorar tarefas dentro das categorias de segurança cibernética e funções de trabalho. Ele também auxilia as pessoas que servem de apoio aos trabalhadores, como especialistas em contratação de pessoal e orientadores profissionais, para que possam ajudar os candidatos e alunos a entenderem melhor as funções de trabalho em cibersegurança e os conhecimentos, habilidades e aptidões inerentes aos cargos e valorizados pelos empregadores para cargos e posições em demanda na área de cibersegurança.

Esses funcionários recebem suporte adicional quando anúncios de vagas e descrições de cargos em aberto usam a terminologia comum do NICE Framework para fornecer descrições claras e consistentes sobre as tarefas e o treinamento necessário em cibersegurança para que possam ocupar tais cargos.

Quando os provedores de treinamento e certificação da indústria usam a terminologia comum do NICE Framework, os que trabalham, ou que desejam trabalhar no campo de cibersegurança, podem encontrar esses provedores de treinamento e/ou certificação, aptos a ensinar as tarefas necessárias para assegurar um cargo em cibersegurança ou uma promoção a um cargo mais elevado. O uso de um vocabulário comum ajuda alunos e profissionais a obter KSAs que normalmente são demonstrados por uma pessoa cuja posição em cibersegurança inclui uma determinada função de trabalho. Esse entendimento os ajuda a encontrar programas acadêmicos que incluam aprendizados e unidades de conhecimento que se encaixam nos KSAs e nas tarefas valorizadas pelos empregadores.

### 1.3.3 Educadores/Treinadores

O NICE Framework serve de referência para educadores desenvolverem currículo, certificado ou programas de graduação, programas de treinamento, cursos, seminários e exercícios ou desafios que incluem os KSAs e as tarefas descritas no NICE Framework.

Especialistas de RH na área de colocação de pessoal e orientadores profissionais podem usar o NICE Framework como um recurso para explorar carreiras.

### 1.3.4 Provedores de tecnologia

O NICE Framework permite que um provedor de tecnologia identifique as funções de trabalho de segurança cibernética, os KSAs e tarefas associados aos produtos e serviços de hardware e software que eles fornecem. Um provedor de tecnologia pode então criar materiais de suporte adequados para ajudar os integrantes da força de trabalho em cibersegurança na configuração e gerenciamento correto para seus produtos.

## 1.4 Organização desta Publicação Especial

O restante desta publicação especial foi organizado da seguinte maneira:

- O capítulo 2 define os componentes do NICE Framework: (i) Categorias; (ii) Áreas de especialidade; (iii) Funções de trabalho; (iv) Superconjuntos associados de conhecimentos, habilidades e aptidões; e (v) Tarefas para cada função de trabalho.
- O capítulo 3 descreve o uso do NICE Framework
- O capítulo 4 menciona áreas onde outras publicações, diretrizes, orientações e ferramentas podem expandir o impacto do NICE Framework.
- 4.3 Appendix A descreve a lista do NICE Framework de categorias, áreas de especialidade, funções de trabalho, KSAs e tarefas.
- Appendix B traz uma lista detalhada de cada função de trabalho, incluindo os KSAs e tarefas associadas.
- Appendix C traz alguns exemplos de ferramentas de desenvolvimento da força de trabalho
- Appendix D traz alguns exemplos de orientações ou diretrizes que fazem uma referência cruzada entre o conteúdo desses documentos e os componentes do NICE Framework
- Appendix E apresenta siglas e abreviações selecionadas usadas neste documento.
- Appendix F fornece referências citadas neste documento.

## 2 Componentes e Relacionamentos do NICE Framework

### 2.1 Componentes do NICE Framework

O NICE Framework organiza a segurança cibernética e trabalhos relacionados. Esta seção apresenta e define os componentes principais do NICE Framework em apoio a essas áreas.

#### 2.1.1 Categorias

As categorias integram a estrutura organizacional abrangente do NICE Framework. Existem sete categorias e todas são compostas por áreas especializadas e funções de trabalho. Essa estrutura organizacional é baseada em extensas análises de cargos, que agrupam trabalho e trabalhadores com funções principais típicas, independentemente dos títulos dos cargos ou outros termos ocupacionais.

#### 2.1.2 Áreas de especialidade

As categorias contêm agrupamentos de trabalho em cibersegurança, que são chamados de Áreas de Especialidade. A Estrutura da Força de Trabalho em Segurança Cibernética Nacional versão 1.0 contém 31 especialidades [2] e a Estrutura da Força de Trabalho em Segurança Cibernética Nacional versão 2.0 [3] contém 32 especialidades. Cada área de especialidade representa uma área de trabalho concentrado, ou função, dentro da cibersegurança e trabalhos relacionados. Nas versões anteriores do NICE Framework, as tarefas e KSAs eram associados a cada área de especialidade. Os KSAs e tarefas agora estão associados às funções de trabalho.

#### 2.1.3 Funções de trabalho

As funções de trabalho são os agrupamentos mais detalhados de segurança cibernética e trabalhos relacionados, que incluem uma lista de atributos necessários para desempenhar determinada função, na forma de conhecimentos, habilidades e aptidões (KSAs) e tarefas executadas naquela função.

O trabalho realizado em um cargo ou posição é descrito pela seleção de uma ou mais funções de trabalho do NICE Framework relevantes para aquele cargo ou posição, em apoio à missão e aos processos de negócios.

Para ajudar na organização e comunicação sobre as responsabilidades relativas à segurança cibernética, as funções de trabalho são agrupadas em classes específicas de categorias e áreas de especialidade, conforme demonstrado no Appendix A.

#### 2.1.4 Conhecimentos, Habilidades e Aptidões (KSAs)

Conhecimentos, habilidades e aptidões (KSAs) são os atributos necessários para desempenhar funções de trabalho e geralmente são demonstrados por meio de experiência, educação ou treinamento relevante.

**Conhecimento** é o conjunto de informações aplicadas diretamente ao desempenho de uma função.

**Habilidade** costuma ser definida como uma competência observável para realizar uma ação psicomotora aprendida. Habilidades no domínio psicomotor descrevem a capacidade de manipular fisicamente uma ferramenta ou instrumento, por exemplo, usando a mão ou um martelo. As habilidades necessárias para cibersegurança dependem menos da manipulação física de ferramentas e instrumentos e mais da aplicação de ferramentas, estruturas, processos e controles que têm impacto na atitude de uma organização ou indivíduo em relação à cibersegurança.

**Aptidão** é a competência de realizar um comportamento observável ou um comportamento que resulta em um produto observável.

### 2.1.5 Tarefas

Uma Tarefa é um trabalho definido e específico que, combinado com outras tarefas identificadas, compõe o trabalho em uma área de especialidade ou função de trabalho específica.

## 2.2 Relacionamentos dos componentes do NICE Framework

Os componentes do NICE Framework descrevem o trabalho de segurança cibernética. Conforme ilustrado na [Figura 1](#), cada categoria é composta por áreas de especialidade, e cada uma delas é composta por uma ou mais funções de trabalho. Cada função de trabalho, por sua vez, inclui KSAs e Tarefas.

Quando o agrupamento de componentes é feito desta maneira, ele simplifica a comunicação sobre tópicos referentes à força de trabalho em cibersegurança e ajuda no alinhamento com outras estruturas. Associações específicas de funções de trabalho para KSAs e tarefas são mostradas no Apêndice B e em uma planilha de referência [\[4\]](#) postada no website do NICE Framework [\[5\]](#).

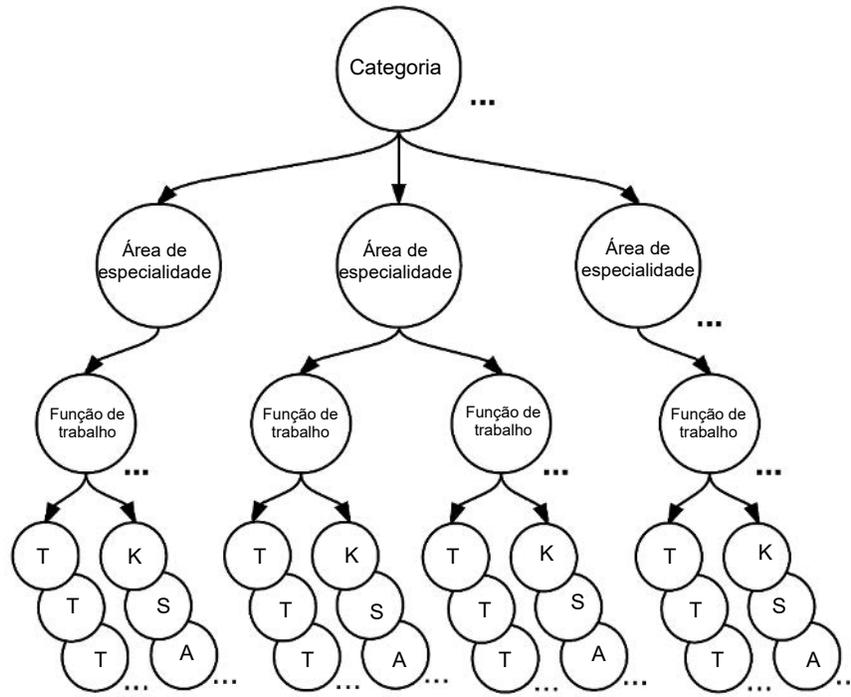


Figura 1 - Relações entre os componentes do NICE Framework

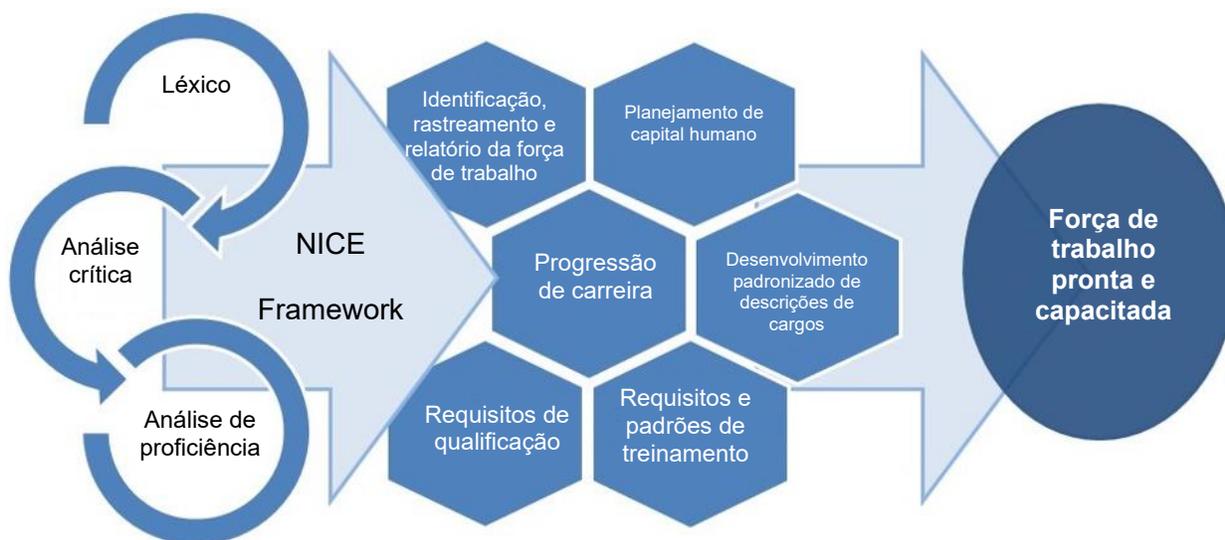
### 3 Usando o NICE Framework

Usar o NICE Framework para entender as necessidades organizacionais e avaliar até que ponto essas necessidades são atendidas pode ajudar uma organização a planejar, implementar e monitorar um programa de segurança cibernética bem-sucedido.

#### 3.1 Identificação das necessidades da força de trabalho em cibersegurança

A cibersegurança é um campo em rápida mudança e expansão. Essa expansão requer um quadro de trabalhadores qualificados para ajudar as organizações a executar as funções de cibersegurança. À medida que as organizações identificam o que é necessário para gerenciar adequadamente os riscos de segurança cibernética atuais e futuros, os líderes precisam considerar os recursos necessários e a capacidade da força de trabalho em cibersegurança.

**Error! Reference source not found.** ilustra como o NICE Framework é uma referência central para ajudar os empregadores a construir uma força de trabalho de segurança cibernética pronta e capaz.



**Figura 2 - Componentes essenciais para uma força de trabalho em cibersegurança pronta e capaz**

As setas circulares no lado esquerdo da [Figura 2](#) são atividades que provavelmente terão um impacto na capacidade de uma organização de desenvolver uma força de trabalho pronta e capaz:

- A terminologia de fácil entendimento do NICE Framework esclarece a comunicação entre educadores de segurança cibernética, instrutores/certificadores, empregadores e funcionários.
- A realização da análise de criticidade identificará os KSAs e tarefas que são essenciais para um desempenho bem-sucedido de uma determinada função de trabalho e aqueles que são essenciais para várias funções de trabalho.

- A execução de uma análise de proficiência informará a expectativa de uma organização referente ao nível necessário para os cargos (ex.: nível básico, especialista), que compreendem muitas vezes mais de uma função de trabalho. A análise de proficiência deve permitir o refinamento da seleção das tarefas relevantes e KSAs necessários para as funções de trabalho inerentes a determinado cargo.

Appendix C identifica algumas ferramentas para o desenvolvimento da força de trabalho que apoiam a identificação das necessidades de força de trabalho em cibersegurança.

### **3.2 Recrutamento e contratação de talentos altamente qualificados em cibersegurança**

Usar o NICE Framework como referência, ajudará as organizações a realizar o planejamento estratégico da força de trabalho e a contratação. O material do NICE Framework, quando usado durante a criação ou revisão das descrições de cargos em anúncios de vagas e de empregos, ajudará os candidatos a procurar cargos específicos pelos quais estão interessados, sabendo que são capazes e qualificados. As tarefas usadas para descrever os deveres e responsabilidades de um cargo e os KSAs usados para descrever as habilidades e qualificações necessárias para o cargo permitem que os candidatos e gerentes de contratação se comuniquem de forma mais eficaz. Descrições de cargos e anúncios de vagas usando a terminologia do NICE Framework dão suporte a critérios de avaliação mais consistentes para examinar e aprovar candidatos.

Para organizações que estão preocupadas com lacunas na força de trabalho, uma revisão da lista de tarefas do NICE Framework pode determinar tarefas específicas que não estão sendo realizadas pela organização. Essas tarefas permitem que a organização identifique funções de trabalho e áreas de especialidade que apresentam lacunas. A organização fica mais capacitada a se envolver com a comunidade de fornecedores de educação, treinamento, credenciamento e certificação que orientam o que têm a oferecer usando o NICE Framework. A organização pode identificar o treinamento que permitirá que atuais membros da equipe resolvam o problema das lacunas. Os gerentes de contratação da organização, usando dados extraídos do NICE Framework, poderão identificar os candidatos que possuam KSAs para realizar as tarefas de cibersegurança.

### **3.3 Educação e treinamento dos membros da força de trabalho de segurança cibernética**

A identificação de tarefas nas funções de trabalho do NICE Framework permite que os educadores preparem os alunos com KSAs específicos, que poderão, portanto, demonstrar que possuem a capacidade de realizar tarefas de cibersegurança.

As instituições acadêmicas são uma parte crítica da preparação e educação da força de trabalho de segurança cibernética. A colaboração entre entidades públicas e privadas, utilizando o programa NICE, permite que essas instituições determinem o conhecimento geral e as habilidades necessárias. Por sua vez, desenvolver e elaborar currículos harmonizados usando a terminologia do NICE Framework permite que as instituições preparem os alunos com as habilidades que os empregadores julgam necessárias. À medida que aumenta o fluxo de alunos que encontram os empregos desejados em cibersegurança, mais alunos serão atraídos para programas semelhantes como opção de carreira.

### 3.4 Retenção e desenvolvimento de talentos altamente qualificados em cibersegurança

Um aspecto crítico de uma força de trabalho qualificada em cibersegurança envolve o desenvolvimento e a retenção dos talentos qualificados já integrados. Um funcionário atual já formou relacionamentos, e possui conhecimento institucional e experiência organizacional que são difíceis de substituir. Preencher novamente um cargo após a saída de um funcionário pode gerar novos custos de publicidade e contratação, e despesas com treinamento, além de diminuir a produtividade e a motivação geral. A seguinte lista ilustra algumas maneiras pelas quais o NICE Framework oferece suporte à retenção e ao desenvolvimento de talentos em cibersegurança:

- As organizações podem desenvolver planos de carreira que descrevam as qualificações necessárias para conjuntos de funções de trabalho cada vez mais desafiadores e em evolução, como os mencionados no NICE Framework.
- Uma compreensão detalhada dos KSAs e tarefas ajuda a equipe a entender as etapas específicas necessárias para desenvolver suas capacidades, estando prontos para ocupar uma posição desejada.
- Uma organização pode oferecer rodízio de funcionários para propiciar oportunidades de desenvolvimento e uso de novas habilidades.
- As organizações podem identificar funcionários que estão melhorando diligentemente os KSAs em áreas relevantes, reconhecendo aqueles que têm um bom desempenho.
- As organizações podem criar planos de desenvolvimento/melhoria para os funcionários, ajudando e orientando como adquirir os KSAs necessários para novas funções de trabalho.
- Oportunidades de treinamento em grupo podem ser identificadas para preparar os membros da equipe, com o intuito de aprimorar os seus conhecimentos, habilidades e competências relativas às funções de trabalho de uma organização.
- As organizações podem usar treinamentos e exames com base em habilidades e competências específicas da área de segurança cibernética para avaliar a proficiência em um ambiente realista.
- As organizações podem usar os funcionários existentes para atender às necessidades críticas de pessoal de segurança cibernética, aproveitando a possibilidade de analisar os currículos dos funcionários atuais para identificar os que possuem KSAs desejáveis.
- O NICE Framework é útil para os atuais funcionários que desejam ser transferidos de um determinado cargo, passando para uma função em cibersegurança. Uma organização pode descrever os KSAs necessários para permitir que um funcionário confiável, que exerça função de trabalho não relacionado à cibersegurança, se torne parte desta força de trabalho assumindo tarefas na área de cibersegurança.

## 4 Extensões

Organizações ou setores podem usar o NICE Framework para desenvolver publicações ou ferramentas adicionais que atendam às suas necessidades e para definir ou fornecer orientação sobre diferentes aspectos do desenvolvimento, planejamento, treinamento e educação da força de trabalho.

Novos materiais de referência que fazem referência cruzada com os componentes do NICE Framework serão compartilhados no site do NICE [\[5\]](#).

As seguintes áreas são alguns exemplos a partir dos quais publicações ou ferramentas adicionais podem ser desenvolvidas.

### 4.1 Competências

A Administração de Empregos e Treinamento do Departamento do Trabalho dos EUA [\[6\]](#) define uma competência como a capacidade de aplicar ou usar conhecimentos, habilidades, aptidões, comportamentos e características pessoais para desempenhar com sucesso tarefas de trabalho críticas, funções específicas ou trabalhar em uma determinada função ou posição. Além da lista de KSAs técnicos, os modelos de competência também consideram indicadores comportamentais e descrevem considerações não técnicas, como Eficácia Pessoal, Competências Acadêmicas e no Local de Trabalho. Informações adicionais sobre essas considerações estão disponíveis no site CareerOneStop do Departamento de Trabalho [\[7\]](#).

### 4.2 Títulos dos cargos

Os títulos dos cargos são uma descrição do cargo ou posição de um funcionário em uma organização. Um mapeamento de exemplos de cargos para áreas de especialidade ou funções de trabalho ajudaria as organizações a utilizar o NICE Framework.

### 4.3 Documentos de orientação e diretrizes de segurança cibernética

O Objetivo Estratégico nº 3 do NICE, Guia de Desenvolvimento de Carreira e Planejamento da Força de Trabalho, visa a apoiar os empregadores a atender às demandas do mercado e aprimorar o recrutamento, contratação, desenvolvimento e retenção de talentos em cibersegurança. Um dos propósitos dentro deste objetivo estratégico é divulgar e aumentar a conscientização sobre o NICE Framework e incentivar que seja adotado e utilizado. A adoção, neste caso, significa usar o NICE Framework como um recurso de referência para ações relacionadas ao treinamento e educação da força de trabalho em cibersegurança.

Uma forma de incentivar a adoção do NICE Framework é encorajar os autores de documentos com orientações e diretrizes na área de cibersegurança a fazerem uma referência cruzada dos componentes do NICE Framework no conteúdo que publicam. Como exemplo, três publicações são exploradas no Appendix D.

## Appendix A - Lista de componentes do NICE Framework

### A.1 Categorias de força de trabalho do NICE Framework

Tabela 1 fornece uma descrição de cada categoria descrita no NICE Framework. Cada categoria inclui uma abreviatura de dois caracteres (ex.: SP) para referência rápida da categoria e para validar a criação de identificadores de funções de trabalho do NICE Framework (consulte a Tabela 3 - Funções de Trabalho do NICE Framework). Esta lista será atualizada periodicamente [1]. A fonte definitiva para a versão mais atual deste material pode ser encontrada na Planilha de Referência para a Publicação Especial NIST 800-181 [4].

**Tabela 1 - Categorias de força de trabalho do NICE Framework**

<b>Categorias</b>	<b>Descrições</b>
Provisão de segurança (SP)	Idealiza, cria o design, adquire e/ou constrói sistemas seguros de tecnologia da informação (TI), sendo responsável por aspectos do sistema e/ou desenvolvimento de rede.
Operar e manter (OM)	Oferece suporte, administração e manutenção necessários para garantir o desempenho e a segurança eficaz e eficiente do sistema de tecnologia da informação (TI).
Supervisionar e governar (OV)	Oferece liderança, gerenciamento, direção, desenvolvimento e defesa para que a organização possa conduzir de forma efetiva o trabalho de segurança cibernética.
Proteger e defender (PR)	Identifica, analisa e faz a mitigação de ameaças a sistemas e/ou redes internas de tecnologia da informação (TI).
Analisar (AN)	Executa análises e avaliações altamente especializadas das informações recebidas sobre cibersegurança para determinar a sua utilidade em questões de inteligência.
Coletar e operar (CO)	Fornecer operações especializadas de negação e fraude, e coleta de informações de cibersegurança que podem ser usadas para desenvolver inteligência.
Investigar (IN)	Investiga eventos de cibersegurança ou crimes relacionados a sistemas de tecnologia da informação (TI), redes e evidências digitais.

## A.2 Áreas de especialidade do NICE Framework

Tabela 2 traz a descrição de cada área de especialidade do NICE Framework. Cada Área de Especialidade inclui uma sigla de três letras (ex.: RSK) para referência rápida da área de especialidade e para validar a criação de identificadores de funções de trabalho do NICE Framework (consulte a Tabela 3 - funções de trabalho do NICE Framework). Esta lista será atualizada periodicamente [1]. A fonte definitiva para a versão mais atual deste material pode ser encontrada na Planilha de Referência para a Publicação Especial NIST 800-181 [4].

**Tabela 2 - Áreas de especialidade do NICE Framework**

<b>Categorias</b>	<b>Áreas de Especialidade</b>	<b>Descrições das Áreas de Especialidade</b>
Provisão de segurança (SP)	Gestão de risco (RSK)	Supervisiona, avalia e apoia os processos de documentação, validação, avaliação e autorização necessários para garantir que os sistemas de tecnologia da informação (TI) atuais e novos atendam aos requisitos de cibersegurança e de riscos gerais para a organização. Garante abordagem adequada do risco, compliance, e confiança de perspectivas internas e externas.
	Desenvolvimento de software (DEV)	Desenvolve e escreve/codifica novas (ou modifica os existentes) aplicações de computador, software ou programas utilitários especializados, de acordo com as melhores práticas de garantia do software.
	Arquitetura de sistemas (ARC)	Desenvolve conceitos de sistemas e trabalha nas fases de capacidades do ciclo de vida de desenvolvimento de sistemas; transforma tecnologia e condições ambientais (ex.: lei e regulamentação) em processos e designs de sistemas e segurança.
	Pesquisa e desenvolvimento em tecnologia (TRD)	Realiza processos de avaliação e integração de tecnologia; fornece e apoia a capacidade de um protótipo e/ou avalia a sua utilidade.
	Planejamento de Requisitos de Sistemas (SRP)	Consulta os clientes para reunir e avaliar os requisitos funcionais e traduz tais requisitos em soluções técnicas. Fornece orientação aos clientes sobre a aplicabilidade dos sistemas de informação para atender às necessidades de negócios.
	Teste e avaliação (TST)	Desenvolve e realiza testes de sistemas para avaliar a conformidade com especificações e requisitos, aplicando princípios e métodos para planejamento de baixo custo, avaliação, verificação e validação de características técnicas, funcionais e de desempenho (incluindo interoperabilidade) de sistemas ou elementos de sistemas que incorporam TI.
	Desenvolvimento de Sistemas (SYS)	Trabalha nas fases de desenvolvimento do ciclo de vida de desenvolvimento de sistemas.

<b>Categorias</b>	<b>Áreas de Especialidade</b>	<b>Descrições das Áreas de Especialidade</b>
Operar e manter (OM)	Administração de dados (DTA)	Desenvolve e administra bancos de dados e/ou sistemas de gerenciamento de dados que permitem o armazenamento, consulta, proteção e utilização de dados.
	Gestão do conhecimento (KMG)	Gerencia e administra processos e ferramentas que permitem à organização identificar, documentar e acessar capital intelectual e conteúdo de informações.
	Atendimento ao cliente e suporte técnico (STS)	Aborda e soluciona problemas; instala, configura e fornece manutenção e treinamento em resposta aos requisitos ou consultas do cliente (ex.: suporte escalonado ao cliente). Normalmente fornece informações iniciais sobre o incidente para a Especialidade de Resposta a Incidentes (IR).
	Serviços de rede (NET)	Instala, configura, testa, opera, mantém e gerencia redes e seus firewalls, incluindo hardware (ex.: hubs, pontes, switches, multiplexadores, roteadores, cabos, servidores proxy e sistemas de distribuição de proteção), e software que permite o compartilhamento e transmissão no âmbito das informações para oferecer suporte à segurança e aos sistemas de informação.
	Administração de sistemas (ADM)	Instala, configura, soluciona problemas e mantém as configurações do servidor (hardware e software) para garantir sua confidencialidade, integridade e disponibilidade. Gerencia contas, firewalls e patches. Responsável pelo controle de acesso, senhas, criação e administração de contas.
	Análise de sistemas (ANA)	Estuda os sistemas informáticos e procedimentos atuais de uma organização e planeja soluções de sistemas de informação para ajudar a organização a funcionar de maneira mais segura, eficiente e eficaz. Une os negócios e a tecnologia da informação (TI) ao compreender as necessidades e limitações de ambas.
Supervisionar e governar (OV)	Orientação jurídica e advocacia (LGA)	Oferece orientações e recomendações juridicamente sólidas para a liderança e funcionários em inúmeros tópicos relevantes dentro do domínio pertinente ao assunto. Defende mudanças jurídicas e normativas e possíveis causas em nome do cliente por meio de uma ampla gama de produtos de trabalho escritos e orais, incluindo resumos e procedimentos legais.
	Treinamento, educação e conscientização (TEA)	Conduz treinamento de pessoal na área pertinente. Desenvolve, planeja, coordena, oferece e/ou avalia cursos, métodos e técnicas de treinamento, conforme apropriado.
	Gerenciamento de segurança cibernética (MGT)	Supervisiona o programa de segurança cibernética de um sistema de informação ou rede, incluindo o gerenciamento de implicações de segurança da informação dentro da organização, programa específico ou outra área de responsabilidade, para incluir estratégia, pessoal, infraestrutura, requisitos, aplicação de políticas, planejamento de emergência, conscientização de segurança e outros recursos.

<b>Categorias</b>	<b>Áreas de Especialidade</b>	<b>Descrições das Áreas de Especialidade</b>
	Planejamento Estratégico e Políticas (SPP)	Desenvolve normas e planos e/ou defende mudanças nas normas que apoiam iniciativas organizacionais do ciberespaço ou mudanças/aprimoramentos necessários.
	Liderança cibernética executiva (EXL)	Supervisiona, gerencia e/ou lidera o trabalho e os trabalhadores que desempenham funções e/ou trabalhos e operações cibernéticas.
	Gerenciamento de programas/projetos (PMA) e aquisição	Aplica conhecimentos sobre dados, informações, processos, interações organizacionais, habilidades e experiência analítica, bem como sistemas, redes e recursos de troca de informações para gerenciar programas de aquisição. Executa funções que regem programas de aquisição de hardware, software e sistema de informação e outras normas de gerenciamento de programas. Fornece suporte direto para aquisições que usam tecnologia da informação (TI) (incluindo Sistemas de Segurança Nacional), aplicando leis e normas relacionadas a TI, e fornece orientação relacionada a TI em todo o ciclo de vida da aquisição.
Proteger e defender (PR)	Análise de defesa da segurança cibernética (CDA)	Usa medidas defensivas e informações coletadas de uma variedade de fontes para identificar, analisar e relatar eventos que ocorrem ou podem ocorrer dentro da rede para proteger as informações, sistemas de informação e redes contra ameaças.
	Suporte de infraestrutura de defesa de segurança cibernética (INF)	Testa, implementa, implanta, mantém, analisa e administra o hardware e software de infraestrutura necessários para gerenciar com eficácia a rede e os recursos do provedor de serviços de defesa de rede de computadores. Monitora a rede para corrigir efetivamente as atividades não autorizadas.
	Resposta a incidentes (CIR)	Responde a crises ou situações urgentes dentro do domínio pertinente para mitigar ameaças imediatas e potenciais. Usa abordagens de mitigação, preparação, resposta e recuperação, conforme necessário, para maximizar a sobrevivência da vida, preservação da propriedade e segurança da informação. Investiga e analisa todas as atividades de respostas relevantes.
	Avaliação e gerenciamento de vulnerabilidades (VAM)	Realiza avaliações de ameaças e vulnerabilidades; determina desvios de configurações aceitáveis, normas empresariais e política local; avalia o nível de risco e desenvolve e/ou recomenda contramedidas de mitigação apropriadas em situações operacionais e não operacionais.
Analisar (AN)	Análise de ameaças (TWA)	Identifica e avalia as capacidades e atividades de criminosos de segurança cibernética ou entidades de inteligência estrangeiras; produz resultados para ajudar a inicializar ou apoiar a aplicação da lei em investigações ou atividades de contrainteligência.

<b>Categorias</b>	<b>Áreas de Especialidade</b>	<b>Descrições das Áreas de Especialidade</b>
	Análise de exploração (EXP)	Analisa as informações coletadas para identificar vulnerabilidades e potencial de exploração.
	Análise de todas as fontes (ASA)	Analisa informações sobre ameaças de várias fontes, disciplinas e agências em toda a Comunidade de Inteligência. Sintetiza e coloca informações de inteligência no contexto; estabelece insights sobre as possíveis implicações.
	Alvos (TGT)	Aplica o conhecimento atual de uma ou mais regiões, países, entidades e/ou tecnologias não estatais.
	Análise de linguagem (GNL)	Aplica conhecimento linguístico, cultural e técnico para apoiar a coleta, análise de informações e outras atividades de segurança cibernética.
Coletar e operar (CO)	Operações de coleta (CLO)	Executa a coleta usando estratégias adequadas e segundo prioridades estabelecidas para o processo de gerenciamento de coleta.
	Planejamento operacional cibernético (OPL)	Executa processo profundo de planejamento de segmentação e de cibersegurança. Reúne informações e desenvolve planos operacionais detalhados e requisitos de suporte de pedidos. Conduz planejamento estratégico e operacional em toda a gama de operações para informações integradas e no ciberespaço.
	Operações cibernéticas (OPS)	Executa atividades para coletar evidências sobre entidades de inteligência criminosas ou estrangeiras para mitigar ameaças possíveis ou em tempo real, proteger contra espionagem ou ameaças internas, sabotagem estrangeira, atividades terroristas internacionais ou para apoiar outras atividades de inteligência.
Investigar (IN)	Investigação cibernética (INV)	Aplica táticas, técnicas e procedimentos para uma gama completa de ferramentas investigativas e processos que incluem, por exemplo, técnicas de entrevista e interrogatório, vigilância, contravigilância e detecção de vigilância, e equilibra adequadamente os benefícios do processo contra a coleta de inteligência.
	Perícia digital (FOR)	Coleta, processa, preserva, analisa e apresenta evidências relacionadas a computador em apoio à mitigação de vulnerabilidade de rede, e/ou investigações criminais, de fraude, contrainteligência ou aplicação da lei.

### A.3 Funções de trabalho do NICE Framework

Tabela 3 fornece uma descrição de cada função de trabalho descrita no NICE Framework. Cada função de trabalho é identificada pela categoria e área de especialidade, seguida por um número sequencial (ex.: SP-RSK-001 é a primeira função de trabalho na categoria SP e área de especialidade RSK). Algumas das Descrições de funções de trabalho são originárias de documentos externos (ex.:

Comissão de Instrução sobre Sistemas de Segurança Nacional [CNSSI] 4009) e incluem essas informações na coluna de descrição. Esta lista será atualizada periodicamente [1]. A fonte definitiva para a versão mais atual deste material pode ser encontrada na Planilha de Referência para a Publicação Especial NIST 800-181 [4].

**Tabela 3 -Funções de trabalho do NICE Framework**

Categoria	Áreas de especialidade	Função de trabalho	ID da função de trabalho	Descrição da função de trabalho
Provisão de segurança (SP)	Gestão de Risco (RSK)	Dirigente Autorizador/Representante Designador	SP-RSK-001	Dirigente sênior ou executivo com autoridade para assumir formalmente a responsabilidade pela operação de um sistema de informação em nível aceitável de risco para as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais, indivíduos, outras organizações e a Nação (CNSSI 4009).
		Avaliador de controle de segurança	SP-RSK-002	Realiza avaliações abrangentes e independentes do gerenciamento, controles de segurança operacional e técnica, bem como aprimoramentos de controles empregados ou herdados por um sistema de tecnologia da informação (TI) para determinar a eficácia geral dos controles (conforme definido no NIST SP 800-37).
	Desenvolvimento de software (DEV)	Desenvolvedor de software	SP-DEV-001	Desenvolve, cria, mantém e escreve/codifica novas (ou modifica os existentes) aplicações de computador, software ou programas utilitários especializados.
		Avaliador de Software Seguro	SP-DEV-002	Analisa a segurança de aplicativos de computador novos ou existentes, software ou programas utilitários especializados e fornece resultados acionáveis.
Arquitetura de sistemas (ARC)	Arquiteto empresarial	SP-ARC-001	Desenvolve e mantém negócios, sistemas e processos de informação para apoiar as necessidades da missão empresarial; desenvolve regras e requisitos de tecnologia da informação (TI) que descrevem arquiteturas de linha de base e de destino.	

<b>Categoria</b>	<b>Áreas de especialidade</b>	<b>Função de trabalho</b>	<b>ID da função de trabalho</b>	<b>Descrição da função de trabalho</b>
		Arquiteto de segurança	SP-ARC-002	Garante que os requisitos de segurança necessários das partes interessadas para proteger a missão da organização e os processos de negócios sejam adequadamente implementados em todos os aspectos da arquitetura corporativa, incluindo modelos de referência, arquiteturas de segmento e solução, e os sistemas resultantes que suportam essas missões e processos de negócios.
	Pesquisa e desenvolvimento em tecnologia (TRD)	Especialista em pesquisa e desenvolvimento	SP-TRD-001	Realiza pesquisas de engenharia de software e sistemas para desenvolver novos recursos, garantindo que a segurança cibernética seja totalmente integrada. Realiza pesquisas abrangentes em tecnologia para avaliar vulnerabilidades potenciais em sistemas cibernéticos.
	Planejamento de requisitos de sistemas (SRP)	Planejador de requisitos de sistemas	SP-SRP-001	Consulta os clientes para avaliar os requisitos funcionais e traduz tais requisitos em soluções técnicas.
	Teste e avaliação (TST)	Especialista em teste e avaliação de sistemas	SP-TST-001	Planeja, prepara e executa testes de sistemas para avaliar os resultados em relação às especificações e requisitos, bem como analisar/relatar os resultados dos testes.
	Desenvolvimento de sistemas (SYS)	Desenvolvedor de segurança de sistemas de Informação	SP-SYS-001	Idealiza, desenvolve, testa e avalia a segurança do sistema de informações em todo o ciclo de vida de desenvolvimento de sistemas.
		Desenvolvedor de sistemas	SP-SYS-002	Idealiza, desenvolve, testa e avalia sistemas de informação em todo o ciclo de vida de desenvolvimento de sistemas.
Operar e manter (OM)	Administração de Dados (DTA)	Administrador de Banco de Dados	OM-DTA-001	Administra bancos de dados e/ou sistemas de gerenciamento de dados que permitem o armazenamento seguro, consulta, proteção e utilização de dados.

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

<b>Categoria</b>	<b>Áreas de especialidade</b>	<b>Função de trabalho</b>	<b>ID da função de trabalho</b>	<b>Descrição da função de trabalho</b>
		Analista de dados	OM-DTA-002	Examina dados de várias fontes distintas com o objetivo de fornecer informações sobre segurança e privacidade. Idealiza e implementa algoritmos personalizados, processos de fluxo de trabalho e layouts para conjuntos de dados complexos em escala corporativa usados para modelagem, mineração de dados e para fins de pesquisa.
	Gestão do conhecimento (KMG)	Gerente de conhecimentos	OM-KMG-001	Responsável por gerenciar e administrar processos e ferramentas que permitem à organização identificar, documentar e acessar capital intelectual e conteúdo das informações.
	Atendimento ao cliente e suporte técnico (STS)	Especialista em suporte técnico	OM-STS-001	Fornece suporte técnico para clientes que precisam de assistência utilizando hardware e software de nível de cliente de acordo com componentes de processo organizacional estabelecidos ou aprovados (ou seja, Plano Mestre de Gerenciamento de Incidentes, quando aplicável).
	Serviços de rede (NET)	Especialista em operações de rede	OM-NET-001	Planeja, implementa e opera serviços/sistemas de rede, para incluir hardware e ambientes virtuais.
	Administração de sistemas (ADM)	Administrador de sistemas	OM-ADM-001	Responsável por configurar e manter um sistema ou componentes específicos de um sistema (ex.: instalação, configuração e atualização de hardware e software; estabelecer e gerenciar contas de usuário; supervisionar ou conduzir tarefas de backup e recuperação; implementar controles de segurança operacionais e técnicos; e aderir às normas e procedimentos de segurança organizacional).
	Análise de sistemas (ANA)	Analista de segurança de sistemas	OM-ANA-001	Responsável pela análise e desenvolvimento da integração, testes, operações e manutenção de sistemas de segurança.
Supervisionar e governar (OV)	Orientação jurídica e advocacia (LGA)	Consultor jurídico cibernético	OV-LGA-001	Fornece aconselhamento jurídico e recomendações sobre tópicos relevantes relacionados ao direito cibernético.

<b>Categoria</b>	<b>Áreas de especialidade</b>	<b>Função de trabalho</b>	<b>ID da função de trabalho</b>	<b>Descrição da função de trabalho</b>
		Dirigente de Privacidade/Gerente de Compliance de Privacidade	OV-LGA-002	Desenvolve, supervisiona e apoia o programa e os funcionários de compliance de privacidade, bem como a governança/normas e necessidades de resposta a incidentes de executivos de privacidade e segurança e suas equipes.
	Treinamento, educação e conscientização (TEA)	Desenvolvedor de currículo instrucional cibernético	OV-TEA-001	Desenvolve, planeja, coordena e avalia cursos de treinamento/educação, métodos e técnicas cibernéticas, com base nas necessidades de instrução.
		Instrutor de cibernética	OV-TEA-002	Desenvolve e realiza treinamento ou educação de pessoal dentro do domínio cibernético.
	Gerenciamento de segurança cibernética (MGT)	Gerente de segurança de sistemas de informação	OV-MGT-001	Responsável pela segurança cibernética de um programa, organização, sistema ou enclave.
		Gerente de Segurança de Comunicações (COMSEC)	OV-MGT-002	Indivíduo que gerencia os recursos de Segurança de Comunicações (COMSEC) de uma organização (CNSSI 4009) ou principal custodiante para um Sistema de Gerenciamento de Chave Criptografada (CKMS).
	Planejamento estratégico e Políticas (SPP)	Desenvolvedor e gerente de força de trabalho cibernética	OV-SPP-001	Desenvolver planos, estratégias e orientação para a força de trabalho do ciberespaço em apoio aos requisitos de mão-de-obra, pessoal, treinamento e educação do ciberespaço, e para lidar com mudanças nas normas, doutrina, material, estrutura, e requisitos de educação e treinamento da força de trabalho.
		Planejador de Normas e Estratégias Cibernéticas	OV-SPP-002	Executar a autoridade de tomada de decisão e estabelecer uma visão e direcionamento para os recursos e/ou operações relacionados à cibernética em uma organização.
	Liderança Cibernética Executiva (EXL)	Liderança Cibernética Executiva	OV-EXL-001	Executa a autoridade de tomada de decisão e estabelece a visão e direção para os recursos e/ou operações cibernéticas relacionadas a uma organização.

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

<b>Categoria</b>	<b>Áreas de especialidade</b>	<b>Função de trabalho</b>	<b>ID da função de trabalho</b>	<b>Descrição da função de trabalho</b>
	Gerenciamento de Programas/Projetos (PMA) e Aquisição	Gerente de Programas	OV-PMA-001	Lidera, coordena, comunica, integra e é responsável pelo sucesso geral do programa, garantindo o alinhamento com as prioridades da agência ou da empresa.
		Gerente de Projetos de TI	OV-PMA-002	Gerencia diretamente projetos de tecnologia da informação.
		Gerente de Suporte de Produto	OV-PMA-003	Gerencia o pacote de funções de suporte necessárias para colocar em campo e manter a prontidão e a capacidade operacional dos sistemas e componentes.
		Gerente de Investimento/Portfólio de TI	OV-PMA-004	Gerencia um portfólio de investimentos em TI que se alinham com as necessidades gerais da missão e prioridades empresariais.
		Auditor de Programas de TI	OV-PMA-005	Realiza avaliações de um programa de TI ou de seus componentes individuais para determinar a conformidade com as normas publicadas.
Proteger e Defender (PR)	Análise de Defesa Cibernética (CDA)	Analista de Defesa Cibernética	PR-CDA-001	Usa dados coletados de diversas ferramentas de defesa cibernética (ex.: alertas IDS, firewalls, logs de tráfego de rede) para analisar eventos que ocorrem em seus ambientes com o objetivo de mitigar ameaças.
	Suporte de Infraestrutura de Defesa Cibernética (INF)	Especialista em Suporte de Infraestrutura de Defesa Cibernética	PR-INF-001	Testa, implementa, implanta, mantém e administra o hardware e software da infraestrutura.
	Resposta a Incidentes (CIR)	Respondente de Incidentes de Defesa Cibernética	PR-CIR-001	Investiga, analisa e responde a incidentes cibernéticos no ambiente de rede ou enclave.
	Avaliação e Gerenciamento de Vulnerabilidades (VAM)	Analista de Avaliação de Vulnerabilidades	PR-VAM-001	Executa avaliações de sistemas e redes dentro do ambiente de rede ou enclave e identifica onde esses sistemas/redes se desviam de configurações aceitáveis, políticas locais ou de enclave. Mede a eficácia da arquitetura de defesa em profundidade contra vulnerabilidades conhecidas.

<b>Categoria</b>	<b>Áreas de especialidade</b>	<b>Função de trabalho</b>	<b>ID da função de trabalho</b>	<b>Descrição da função de trabalho</b>
Analisar (AN)	Análise de Ameaças (TWA)	Analista de Ameaças/Alertas	AN-TWA-001	Desenvolve indicadores cibernéticos para manter a percepção sobre o status do ambiente operacional altamente dinâmico. Coleta, processa, analisa e dissemina avaliações de ameaças/alertas cibernéticos.
	Análise de Exploração (EXP)	Analista de Exploração	AN-EXP-001	Colabora para identificar lacunas de acesso e coleta que podem ser satisfeitas por meio de atividades de coleta e/ou preparação cibernética. Alavanca todos os recursos autorizados e técnicas analíticas para penetrar nas redes direcionadas.
	Análise de Todas as Fontes (ASA)	Analista de Todas as Fontes	AN-ASA-001	Analisa dados/informações de uma ou várias fontes para realizar a preparação do ambiente, responder às solicitações de informações e enviar coleta de inteligência e requisitos de produção em apoio ao planejamento e às operações.
		Especialista em Avaliação de Missão	AN-ASA-002	Desenvolve planos de avaliação e medidas de desempenho/eficácia. Conduz avaliações de eficácia estratégica e operacional conforme necessário para eventos cibernéticos. Determina se os sistemas tiveram o desempenho esperado e fornece informações para a determinação da eficácia operacional.
Destino (TGT)	Desenvolvedor de Destino	AN-TGT-001	Executa a análise do sistema de destino, cria e/ou mantém pastas de destino eletrônicas para incluir entradas da preparação do ambiente e/ou fontes de inteligência internas ou externas. Mantém coordenação com as atividades de destino de parceiros e organizações de inteligência e apresenta os destinos escolhidos para serem verificados e validados. Mantém coordenação com as atividades de destino de parceiros e organizações de inteligência, e apresenta os destinos escolhidos para serem verificados e validados.	

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

<b>Categoria</b>	<b>Áreas de especialidade</b>	<b>Função de trabalho</b>	<b>ID da função de trabalho</b>	<b>Descrição da função de trabalho</b>
		Analista de Rede de Destino	AN-TGT-002	Conduz análises avançadas de coleta e dados de código aberto para garantir a continuidade das redes de destino; traça o perfil dos destinos e suas atividades; e desenvolve técnicas para obter mais informações sobre os destinos. Determina como as redes de destino se comunicam, se movem, operam e vivem com base no conhecimento das tecnologias de destino, redes digitais e seus aplicativos.
	Análise de Linguagem (GNL)	Analista de Linguagem Multidisciplinar	AN-LNG-001	Aplica experiência específica em idiomas e culturas sobre destinos/ameaças e conhecimento técnico para processar, analisar e/ou disseminar informações de inteligência derivadas de linguagem, voz e/ou material gráfico. Cria e mantém bancos de dados em idiomas específicos, e recursos de trabalho para apoiar a execução de ações cibernéticas e garantir o compartilhamento de conhecimento crítico. Proporciona experiência específica em projetos interdisciplinares ou em que uma língua estrangeira seja intensamente utilizada.
Coletar e operar (CO)	Operações de Coleta (CLO)	Gerente de Coleta de Todas as Fontes	CO-CLO-001	Identifica autoridades de coleta e meio-ambiente; incorpora requisitos de informação prioritários no gerenciamento de coleta; desenvolve conceitos para atender às intenções manifestadas pela liderança. Determina os recursos e capacidades de coleta disponíveis, identifica novos recursos de coleta, constrói e divulga planos de coleta. Monitora a execução da coleta programada para garantir a execução eficaz do plano de coleta.
		Requisitos para Gerente de Coleta de Todas as Fontes	CO-CLO-002	Avalia as operações de coleta e desenvolve estratégias de requisitos de coleta com base em efeitos, usando fontes e métodos disponíveis para melhorar o processo. Desenvolve, processa, valida e coordena o envio de requisitos de coleta. Avalia o desempenho dos recursos e das operações de coleta.

<b>Categoria</b>	<b>Áreas de especialidade</b>	<b>Função de trabalho</b>	<b>ID da função de trabalho</b>	<b>Descrição da função de trabalho</b>
	Planejamento Operacional Cibernético (OPL)	Planejador Intel de Cibernética	CO-OPL-001	Desenvolve planos detalhados de inteligência para atender aos requisitos de operações cibernéticas. Colabora com planejadores de operações cibernéticas para identificar, validar e cobrar requisitos para coleta e análise. Participa na deleção de redes de destino, validação, sincronização e execução de ações cibernéticas. Sincroniza atividades de inteligência para apoiar os objetivos da organização no ciberespaço.
		Planejador de Operações Cibernéticas	CO-OPL-002	Desenvolve planos detalhados de realização ou suporte para várias operações cibernéticas aplicáveis por meio da colaboração com outros planejadores, operadores e/ou analistas. Participa na seleção, validação, sincronização e execução de redes de destino e viabiliza a integração durante a execução de ações cibernéticas.
		Planejador de Integração de Parceiros	CO-OPL-003	Trabalha para promover a cooperação além das fronteiras organizacionais ou nacionais entre parceiros de operações cibernéticas. Auxilia na integração de equipes cibernéticas parceiras, fornecendo orientação, recursos e colaboração para desenvolver as melhores práticas e facilitar o suporte organizacional para alcançar objetivos em ações cibernéticas integradas.
	Operações Cibernéticas (OPS)	Operador Cibernético	CO-OPS-001	Realiza coleta, processamento e/ou geolocalização de sistemas para explorar, localizar e/ou rastrear sistemas de destino de interesse. Executa navegação na rede, análise tática pericial e, quando orientado, executa operações de rede.
Investigar (IN)	Investigação Cibernética (INV)	Investigador de Crimes Cibernéticos	IN-INV-001	Identifica, coleta, examina e preserva evidências usando técnicas analíticas e investigativas controladas e documentadas.

Categoria	Áreas de especialidade	Função de trabalho	ID da função de trabalho	Descrição da função de trabalho
	Perícia Digital (FOR)	Analista de Perícia da Segurança Pública/Contraineligência	IN-FOR-001	Conduz investigações detalhadas sobre crimes cometidos através de computador, estabelecendo provas documentais ou físicas, incluindo mídia digital e registros associados a incidentes de invasão cibernética.
		Analista de Perícia de Defesa Cibernética	IN-FOR-002	Analisa a evidência digital e investiga incidentes de segurança do computador para derivar informações úteis para suportar a redução da vulnerabilidade do sistema/rede.

#### A.4 Tarefas do NICE Framework

.Tabela 4 traz uma lista de todas as tarefas que foram identificadas como parte de uma função de trabalho de segurança cibernética. Cada função de trabalho inclui um subconjunto das tarefas listadas aqui. Esta lista será atualizada periodicamente [1]. A fonte definitiva para a versão mais atual deste material pode ser encontrada na Planilha de Referência para a Publicação Especial NIST 800-181 [4].

**Tabela 4 - Tarefas do NICE Framework**

ID da Tarefa	Descrição da Tarefa
T0001	Adquirir e gerenciar os recursos necessários, incluindo suporte de liderança, recursos financeiros e de pessoal-chave na área de segurança, para apoiar as metas e objetivos de segurança da tecnologia da informação (TI) e reduzir o risco organizacional como um todo.
T0002	Adquirir os recursos necessários, incluindo recursos financeiros, para conduzir um programa eficaz de continuidade das operações da empresa.
T0003	Aconselhar a gerência sênior (ex.: Diretor de Informática [CIO]) sobre os níveis de risco e postura de segurança.
T0004	Aconselhar a gerência sênior (ex.: CIO) sobre a análise de custo-benefício dos programas, políticas, processos, sistemas e elementos de segurança da informação.
T0005	Aconselhar a liderança sênior ou Dirigente Autorizador apropriado sobre as mudanças que afetam a postura de segurança cibernética da organização.
T0006	Defender o posicionamento oficial da organização relativo aos procedimentos judiciais e legislativos.
T0007	Analisar e definir requisitos e especificações de dados.
T0008	Analisar e planejar as mudanças previstas nos requisitos de capacidade de dados.
T0009	Analisar as informações para determinar, recomendar e planejar o desenvolvimento de um novo aplicativo ou modificação de uma aplicação existente.
T0010	Analisar as políticas e configurações de defesa cibernética da organização e avaliar o compliance com os regulamentos e diretrizes organizacionais.
T0011	Analisar as necessidades do usuário e os requisitos de software para determinar a viabilidade do projeto dentro das restrições de tempo e custo.
T0012	Analisar as restrições de design, prós e contras, o sistema detalhado e o design de segurança, considerando o suporte adequado para o ciclo de vida.
T0013	Aplicar normas de codificação e teste, bem como ferramentas de teste de segurança, incluindo ferramentas de verificação de código de análise estática "fuzzing" e revisões de código.
T0014	Aplicar a documentação de código seguro.
T0015	Aplicar políticas de segurança a aplicativos que fazem interface uns com os outros, como aplicativos Business-to-Business (B2B).
T0016	Aplicar políticas de segurança para atender aos objetivos de segurança do sistema.
T0017	Aplicar os princípios da arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.
T0018	Avaliar a eficácia das medidas de segurança cibernética utilizadas pelos sistemas.
T0019	Avaliar ameaças e vulnerabilidades de sistemas informáticos para desenvolver um perfil de risco de segurança.
T0020	Desenvolver conteúdo para ferramentas de defesa cibernética.

ID da Tarefa	Descrição da Tarefa
T0021	Construir, testar e modificar protótipos de produtos usando modelos de trabalho ou modelos teóricos.
T0022	Capturar controles de segurança usados durante a fase de requisitos para integrar a segurança dentro do processo, visando a identificar os principais objetivos de segurança, e maximizar a segurança do software, ao mesmo tempo minimizando a interrupção dos planos e programações.
T0023	Caracterizar e analisar o tráfego da rede para identificar atividades anômalas e ameaças potenciais aos recursos de rede.
T0024	Coletar e manter os dados necessários para atender aos relatórios de segurança cibernética do sistema.
T0025	Comunicar o valor da segurança da tecnologia da informação (TI) em todos os níveis das partes interessadas da organização.
T0026	Compilar e escrever a documentação do desenvolvimento de programas e revisões subsequentes, inserindo comentários nas instruções codificadas para que outros possam entender os programas.
T0027	Realizar análises de arquivos de log, evidências e outras informações para determinar os melhores métodos para identificar os autores de uma invasão na rede.
T0028	Realizar e/ou apoiar testes de penetração autorizados em ativos de rede corporativa.
T0029	Realizar testes funcionais e de conectividade para garantir uma operacionalidade contínua.
T0030	Conduzir exercícios de treinamento interativo para criar um ambiente de aprendizagem eficaz.
T0031	Conduzir entrevistas com vítimas e testemunhas, bem como entrevistas ou interrogatórios com os suspeitos.
T0032	Realizar avaliações de impacto de privacidade (PIAs) no design de segurança do aplicativo para os controles de segurança apropriados, que protegem a confidencialidade e integridade das informações pessoalmente identificáveis (PII).
T0033	Conduzir análises de risco, estudo de viabilidade e/ou análise de trade-off para desenvolver, documentar e refinar requisitos e especificações funcionais.
T0034	Manter comunicação com analistas de sistemas, engenheiros, programadores e outros referente ao design de aplicativos e para obter informações sobre limitações e recursos do projeto, requisitos de desempenho e interfaces.
T0035	Configurar e otimizar hubs de rede, roteadores e switches (ex.: protocolos de nível superior, encapsulamento de dados).
T0036	Confirmar o que foi descoberto sobre uma invasão e descobrir novas informações, se possível, após identificar a invasão por meio de análise dinâmica.
T0037	Construir caminhos de acesso para conjuntos de informações (ex.: páginas de link) para facilitar o acesso dos usuários finais.
T0038	Desenvolver um modelo de ameaça com base em entrevistas e requisitos dos clientes.
T0039	Consultar os clientes para avaliar requisitos funcionais.
T0040	Consultar a equipe de engenharia para avaliar a interface entre hardware e software.
T0041	Coordenar e fornecer suporte técnico especializado para técnicos de defesa cibernética em toda a empresa para resolver incidentes de defesa cibernética.
T0042	Coordenar o trabalho com analistas de defesa cibernética para gerenciar e administrar a atualização de regras e assinaturas (ex.: sistemas de detecção/proteção de invasão, antivírus e listas negras de conteúdo) para aplicativos especializados de defesa cibernética.
T0043	Coordenar o trabalho com a equipe de defesa cibernética em toda a empresa para validar alertas de rede.

ID da Tarefa	Descrição da Tarefa
T0044	Colaborar com as partes interessadas para estabelecer a continuidade empresarial do programa de operações, estratégia e segurança da missão.
T0045	Coordenar com arquitetos e desenvolvedores de sistemas, conforme necessário, para fornecer supervisão no desenvolvimento de soluções de design.
T0046	Corrigir erros fazendo as alterações adequadas e verificando novamente o programa para garantir que os resultados desejados sejam produzidos.
T0047	Correlacionar dados de incidentes para identificar vulnerabilidades específicas e fazer recomendações que permitam uma correção rápida.
T0048	Criar uma duplicata pericial da evidência (ou seja, imagem pericial) que garanta que a evidência original não será modificada acidentalmente, para uso em processos de recuperação e análise de dados. Isso inclui, por exemplo, discos rígidos, disquetes, CDs, PDAs, telefones celulares, GPS e todos os formatos de fita.
T0049	Descriptografar dados apreendidos usando meios técnicos.
T0050	Definir e priorizar os recursos essenciais do sistema ou funções de negócios necessários para a restauração parcial ou total do sistema após um evento de falha catastrófica.
T0051	Definir os níveis apropriados de disponibilidade do sistema com base nas funções críticas e garantir que os requisitos do sistema identifiquem a recuperação de desastres apropriada e os requisitos de continuidade das operações para incluir qualquer failover/requisitos de site alternativo, requisitos de backup e requisitos de suporte de material para recuperação/restauração do sistema.
T0052	Definir o escopo e os objetivos do projeto com base nos requisitos do cliente.
T0053	Criar o design e desenvolver produtos habilitados para segurança cibernética ou cibersegurança.
T0054	Criar o design das políticas para grupos e listas de controle de acesso para garantir a compatibilidade com normas organizacionais, regras e necessidades de negócios.
T0055	Criar o design do hardware, sistemas operacionais e aplicativos de software para atender adequadamente aos requisitos de segurança cibernética.
T0056	Criar o design ou integrar recursos de backup de dados apropriados em designs gerais de sistemas e garantir que processos técnicos e procedimentais apropriados estejam presentes para backups de sistemas seguros e armazenamento protegido de dados de backup.
T0057	Criar o design, desenvolver e modificar sistemas de software, usando análises científicas e modelos matemáticos para prever e medir o resultado e o impacto do design.
T0058	Determinar o nível de garantia dos recursos desenvolvidos com base nos resultados dos testes.
T0059	Desenvolver um plano para investigar suposto crime, violação ou atividade suspeita utilizando computadores e a Internet.
T0060	Desenvolver uma compreensão das necessidades e requisitos de informações dos usuários finais.
T0061	Desenvolver e direcionar procedimentos e documentação de teste e validação de sistema.
T0062	Desenvolver e documentar requisitos, recursos e restrições para procedimentos e processos de design.
T0063	Desenvolver e documentar procedimentos operacionais padrão de administração de sistemas.
T0064	Revisar e validar programas, processos e requisitos de mineração de dados e armazenamento de dados.
T0065	Desenvolver e implementar procedimentos de backup e recuperação de rede.
T0066	Desenvolver e manter planos estratégicos.

ID da Tarefa	Descrição da Tarefa
T0067	Desenvolver arquiteturas ou componentes de sistema consistentes com as especificações técnicas.
T0068	Desenvolver normas, políticas e procedimentos referentes aos dados.
T0069	Desenvolver documentação de design de segurança detalhada para especificações de componentes e interfaces para apoiar o design e desenvolvimento do sistema.
T0070	Elaborar planos de recuperação de sistemas em desenvolvimento e continuidade das operações após desastres e garantir o teste antes que os sistemas entrem em um ambiente de produção.
T0071	Desenvolver/integrar projetos de cibersegurança para sistemas e redes com requisitos de segurança multinível ou requisitos para o processamento de vários níveis de classificação de dados aplicáveis principalmente a organizações governamentais (ex.: NÃO SIGILOSO, SECRETO e ULTRASSECRETO).
T0072	Desenvolver métodos para monitorar e medir riscos, compliance e esforços de garantia.
T0073	Desenvolver ou identificar materiais de conscientização e treinamento existentes que sejam apropriados para o público-alvo.
T0074	Desenvolver políticas, programas e diretrizes para implementação.
T0075	Fornecer um resumo técnico dos resultados de acordo com os procedimentos de relatório estabelecidos.
T0076	Desenvolver estratégias de mitigação de risco para resolver vulnerabilidades e recomendar mudanças de segurança para o sistema ou componentes do sistema conforme necessário.
T0077	Desenvolver código seguro e solução de erros.
T0078	Desenvolver contramedidas de segurança cibernética e estratégias de mitigação de risco específicas para sistemas e/ou aplicativos.
T0079	Desenvolver especificações para garantir que os esforços de risco, compliance e garantia estejam em conformidade com os requisitos de segurança, resiliência e confiabilidade no nível do aplicativo de software, sistema e ambiente de rede.
T0080	Desenvolver planos de teste para atender às especificações e requisitos.
T0081	Diagnosticar problema de conectividade de rede.
T0082	Documentar e atender aos requisitos de segurança da informação, arquitetura de segurança cibernética e engenharia de segurança de sistemas da organização durante todo o ciclo de vida da aquisição.
T0083	Redigir declarações de riscos de segurança preliminares ou residuais para o funcionamento do sistema.
T0084	Empregar processos seguros de gerenciamento de configuração.
T0085	Garantir que todas as operações de segurança do sistema e atividades de manutenção estejam devidamente documentadas e atualizadas conforme necessário.
T0086	Assegurar que a aplicação de patches de segurança para produtos comerciais integrados na concepção do sistema cumpra os prazos ditados pela autoridade de gestão para o ambiente operacional pretendido.
T0087	Assegurar que a cadeia de custódia seja obedecida em toda a mídia digital adquirida em conformidade com as Regras Federais de Evidência.
T0088	Garantir que os produtos habilitados para segurança cibernética ou outras tecnologias de compensação de controle de segurança reduzem o risco identificado até um nível aceitável.
T0089	Garantir que as ações de melhoria de segurança sejam avaliadas, validadas e implementadas conforme necessário.
T0090	Garantir que os sistemas e arquiteturas adquiridos ou desenvolvidos sejam consistentes com as diretrizes de arquitetura de segurança cibernética da organização.

ID da Tarefa	Descrição da Tarefa
T0091	Garantir que as inspeções, testes e análises de segurança cibernética sejam coordenados para o ambiente de rede.
T0092	Assegurar que os requisitos de segurança cibernética sejam integrados ao planejamento de continuidade para determinado sistema e/ou organização.
T0093	Garantir que os recursos de proteção e detecção sejam adquiridos ou desenvolvidos usando a abordagem de engenharia de segurança de SI, estando consistentes com a arquitetura de segurança cibernética no nível da organização.
T0094	Estabelecer e manter canais de comunicação com as partes interessadas.
T0095	Estabelecer a arquitetura global de segurança da informação empresarial (EISA) com a estratégia geral de segurança da organização.
T0096	Estabelecer relações (se for o caso), entre a equipe de resposta a incidentes e outros grupos, tanto internos (ex.: departamento jurídico) quanto externos (ex.: agências de aplicação da lei, fornecedores, profissionais de relações públicas).
T0097	Avaliar e aprovar os esforços de desenvolvimento para garantir que as proteções básicas de segurança sejam instaladas de maneira adequada.
T0098	Avaliar contratos para garantir a conformidade com os requisitos de financiamento, legais e de programas.
T0099	Avaliar a análise de custo-benefício, econômica e de risco no processo de tomada de decisão.
T0100	Avaliar fatores como formatos de relatório necessários, restrições de custo e necessidade de restrições de segurança para determinar a configuração do hardware.
T0101	Avaliar a eficácia e abrangência dos programas de treinamento existentes.
T0102	Avaliar a eficácia das leis, regulamentos, políticas, normas ou procedimentos.
T0103	Examinar os dados recuperados para obter informações relevantes para o problema em questão.
T0104	Combinar análises de ataques a redes de computadores com investigações e operações criminais e de contrainteligência.
T0105	Identificar componentes ou elementos, alocar funções de segurança para esses elementos e descrever as relações entre os elementos.
T0106	Identificar estratégias alternativas de segurança da informação para atender ao objetivo de segurança organizacional.
T0107	Identificar e direcionar a remediação de problemas técnicos encontrados durante o teste e implementação de novos sistemas (ex.: identificar e encontrar soluções para protocolos de comunicação que não são interoperáveis).
T0108	Identificar e priorizar funções críticas de negócios em colaboração com as partes interessadas organizacionais.
T0109	Identificar e priorizar funções essenciais do sistema ou subsistemas necessários para oferecer suporte aos recursos essenciais ou funções de negócios, visando a restauração ou recuperação após uma falha do sistema ou durante um evento de recuperação do sistema com base nos requisitos gerais de continuidade e disponibilidade.
T0110	Identificar e/ou determinar se um incidente de segurança é indicativo de uma violação da lei que requer ação legal específica.
T0111	Identificar falhas de codificação comuns e básicas de alto nível.
T0112	Identificar dados ou inteligência de valor probatório para apoiar contrainteligência e investigações criminais.
T0113	Identificar as evidências digitais para exame e análise de formas a evitar alterações não intencionais.
T0114	Identificar os elementos de prova do crime.

ID da Tarefa	Descrição da Tarefa
T0115	Identificar as implicações do programa de segurança de tecnologia da informação (TI) com respeito a novas tecnologias ou atualizações de tecnologia.
T0116	Identificar as partes interessadas ligadas às políticas organizacionais.
T0117	Identificar as implicações de segurança e aplicar metodologias em ambientes centralizados e descentralizados nos sistemas informáticos da empresa no desenvolvimento de software.
T0118	Identificar problemas de segurança relacionados à operação e gerenciamento de estado estável de software e incorporar medidas de segurança que devem ser tomadas quando um produto chega ao fim da sua vida útil.
T0119	Identificar, avaliar e recomendar produtos habilitados para segurança cibernética ou cibersegurança para uso em um sistema e garantir que os produtos recomendados estejam em conformidade com os requisitos de avaliação e validação da organização.
T0120	Identificar, coletar e capturar evidências documentais ou físicas para incluir mídia digital e registros associados a incidentes de invasão cibernética, investigações e operações.
T0121	Implementar novos procedimentos de design de sistema, procedimentos de teste e normas de qualidade.
T0122	Implementar projetos de segurança para sistemas novos ou existentes.
T0123	Implementar contramedidas de segurança cibernética específicas para sistemas e/ou aplicativos.
T0124	Incorporar soluções de vulnerabilidade de segurança cibernética em projetos de sistema (ex.: alertas de vulnerabilidade de segurança cibernética).
T0125	Instalar e manter o software do sistema operacional do dispositivo de infraestrutura de rede (ex.: IOS, firmware).
T0126	Instalar ou substituir hubs, roteadores e switches de rede.
T0127	Integrar e alinhar as políticas de segurança da informação e/ou cibersegurança para garantir que a análise do sistema atenda aos requisitos de segurança.
T0128	Integrar recursos automatizados para atualização ou patching de software de sistema em que for mais prático e desenvolver processos e procedimentos para atualização manual e patching de software de sistema, tendo como base os requisitos de cronograma de patch atuais e projetados para o ambiente operacional do sistema.
T0129	Integrar novos sistemas à arquitetura de rede existente.
T0130	Fazer interface com organizações externas (ex.: relações públicas, aplicação da lei, Comandante ou Inspetor Geral de Componentes) para garantir a disseminação adequada e precisa de incidentes e outras informações de Defesa de Rede de Computadores.
T0131	Interpretar e aplicar leis, regulamentos, políticas, normas ou procedimentos a questões específicas.
T0132	Interpretar e/ou aprovar requisitos de segurança relativos às capacidades das novas tecnologias da informação.
T0133	Interpretar os padrões de não conformidade para determinar seu impacto nos níveis de risco e/ou eficácia geral do programa de segurança cibernética da empresa.
T0134	Liderar e alinhar as prioridades de segurança de tecnologia da informação (TI) com a estratégia de segurança.
T0135	Liderar e supervisionar o orçamento para segurança da informação, alocação e contratação de pessoal.
T0136	Manter a segurança do sistema de linha de base de acordo com as políticas organizacionais.
T0137	Manter software de sistemas de gerenciamento de banco de dados.
T0138	Manter um kit de ferramentas de auditoria de defesa cibernética implantável (ex.: software e hardware de defesa cibernética especializado) para dar suporte às missões de auditoria de defesa cibernética.

ID da Tarefa	Descrição da Tarefa
T0139	Manter os serviços de replicação de diretório que permitem que as informações sejam replicadas automaticamente dos servidores traseiros para as unidades avançadas por meio de roteamento otimizado.
T0140	Manter a troca de informações por meio de funções de publicação, assinatura e alerta que permitem aos usuários enviar e receber informações críticas, conforme necessário.
T0141	Manter garantia de sistemas de informação e materiais de acreditação.
T0142	Manter conhecimento das políticas, regulamentos e documentos de compliance de defesa cibernética aplicáveis, especificamente relacionados à auditoria de defesa cibernética.
T0143	Fazer recomendações com base nos resultados do teste.
T0144	Gerenciar contas, direitos de rede e acesso a sistemas e equipamentos.
T0145	Gerenciar e aprovar pacotes de credenciamento (ex.: ISO/IEC 15026-2).
T0146	Gerenciar a compilação, catalogação, cache, distribuição e recuperação de dados.
T0147	Gerenciar o monitoramento de fontes de dados de segurança da informação para manter a consciencialização situacional organizacional.
T0148	Gerenciar a publicação de orientação de Defesa de Rede de Computadores (ex.: TCNOs, Conceito de Operações, Relatórios de Analistas de Rede, NTSM, MTOs) para o grupo constituinte da empresa.
T0149	Gerenciar a análise de ameaças ou alvos de informações de defesa cibernética e produção de informações sobre ameaças dentro da empresa.
T0150	Monitorar e avaliar o compliance de um sistema de acordo com os requisitos de segurança, resiliência e confiabilidade da tecnologia da informação (TI).
T0151	Monitorar e avaliar a eficácia das salvaguardas de segurança cibernética da empresa para garantir que forneçam o nível de proteção pretendido.
T0152	Monitorar e manter bancos de dados para garantir o melhor desempenho.
T0153	Monitorar a capacidade e o desempenho da rede.
T0154	Monitorar e relatar o uso de ativos e recursos de gestão do conhecimento.
T0155	Documentar e escalar incidentes (incluindo histórico, status e impacto potencial do evento para ações futuras) que podem causar impacto contínuo e imediato ao meio ambiente.
T0156	Supervisionar e fazer recomendações sobre o gerenciamento de configuração.
T0157	Supervisionar o programa de treinamento e conscientização sobre segurança da informação.
T0158	Participar de uma avaliação de risco de segurança da informação durante o processo de Avaliação e Autorização de Segurança.
T0159	Participar do desenvolvimento ou modificação dos planos e requisitos do programa de cibersegurança do ambiente de computador.
T0160	Corrigir vulnerabilidades da rede para garantir que as informações sejam protegidas contra terceiros.
T0161	Realizar a análise de arquivos de log de uma variedade de fontes (ex.: logs de hosts individuais, logs de tráfego de rede, logs de firewall e logs do sistema de detecção de invasões [IDS]) para identificar possíveis ameaças à segurança da rede.
T0162	Realizar backup e recuperação de bancos de dados para garantir a integridade dos dados.
T0163	Realizar a triagem de incidentes de defesa cibernética, para incluir a determinação quanto ao escopo, urgência e impacto potencial, identificando a vulnerabilidade específica e fazendo recomendações que permitam uma remediação rápida.
T0164	Realizar análise e relatórios de tendências de defesa cibernética.
T0165	Executar uma análise dinâmica para inicializar uma "imagem" de uma unidade (sem necessariamente ter a unidade original) para ver a invasão como o usuário pode ter visto, em um ambiente nativo.

ID da Tarefa	Descrição da Tarefa
T0166	Executar a correlação de eventos usando informações coletadas de uma variedade de fontes dentro da empresa para obter consciência situacional e determinar a eficácia de um ataque observado.
T0167	Executar a análise de assinatura de arquivo.
T0168	Executar a comparação de hash com o banco de dados estabelecido.
T0169	Executar testes de cibersegurança de aplicativos e/ou sistemas desenvolvidos.
T0170	Executar a coleta inicial e perícia de imagens e as inspecionar para discernir possíveis mitigações/remediações em sistemas corporativos.
T0171	Executar testes integrados de garantia de qualidade para funcionalidade de segurança e ataque de resiliência.
T0172	Executar análises periciais em tempo real (ex.: usando Helix juntamente com o LiveView).
T0173	Executar análise da linha de tempo.
T0174	Executar análises de necessidades para determinar oportunidades para novas e melhores soluções de processos de negócios.
T0175	Executar tarefas de resolução de incidentes de defesa cibernética em tempo real (ex.: coletas periciais, correlação e rastreamento de invasões, análise de ameaças e remediação direta do sistema) para apoiar as equipes de resposta a incidentes implantáveis (IRTs).
T0176	Executar uma programação segura e identificar possíveis falhas nos códigos para mitigar vulnerabilidades.
T0177	Executar análises de segurança, identificar brechas na arquitetura de segurança e desenvolver um plano de gerenciamento de riscos de segurança.
T0178	Executar análises de segurança e identificar falhas de segurança na arquitetura de segurança, resultando em recomendações para inclusão na estratégia de mitigação de riscos.
T0179	Executar análise de mídia estática.
T0180	Executar a administração do sistema em aplicativos e sistemas especializados de defesa cibernética (ex.: antivírus, auditoria e remediação) ou dispositivos de rede privada virtual (VPN), para incluir instalação, configuração, manutenção, backup e restauração.
T0181	Executar análise de risco (ex.: ameaça, vulnerabilidade e probabilidade de ocorrência) sempre que um aplicativo ou sistema passar por uma grande mudança.
T0182	Executar análises de malware de nível 1, 2 e 3.
T0183	Executar etapas de validação, comparando resultados reais com os resultados esperados e analisar as diferenças para identificar impactos e riscos.
T0184	Planejar e realizar revisões de autorização de segurança e desenvolvimento de casos de garantia para instalação inicial de sistemas e redes.
T0185	Planejar e gerenciar a entrega de projetos de gestão do conhecimento.
T0186	Planejar, executar e verificar os procedimentos de redundância de dados e recuperação do sistema.
T0187	Planejar e recomendar modificações ou ajustes com base nos resultados do exercício ou no ambiente do sistema.
T0188	Preparar relatórios de auditoria que identificam descobertas técnicas e processuais e fornecer estratégias/soluções recomendadas de remediação.
T0189	Preparar gráficos e diagramas detalhados de fluxo de trabalho que descrevem a entrada, a saída e a operação lógica, para convertê-las em uma série de instruções codificadas em linguagem de computador.
T0190	Preparar a mídia digital para imagens, garantindo a integridade dos dados (ex.: bloqueadores de gravação de acordo com os procedimentos operacionais padrão).
T0191	Preparar casos de uso para justificar a necessidade de soluções específicas de tecnologia da informação (TI).

ID da Tarefa	Descrição da Tarefa
T0192	Preparar, distribuir e manter planos, instruções, orientações e procedimentos operacionais padrão sobre a segurança das operações dos sistemas de rede.
T0193	Processar cenas de crime.
T0194	Documentar adequadamente todas as atividades de implementação, operações e manutenção de segurança de sistemas e atualizar conforme necessário.
T0195	Fornecer um fluxo gerenciado de informações relevantes (através de portais baseados na Web ou outros meios) com base nos requisitos da missão.
T0196	Fornecer orientação sobre custos de projetos, conceitos de design ou mudanças de design.
T0197	Fornecer uma avaliação técnica precisa do aplicativo de software, sistema ou rede, documentando a postura de segurança, recursos e vulnerabilidades, em conformidade com a segurança cibernética relevante.
T0198	Fornecer relatórios diários resumidos de eventos de rede e atividades relevantes para práticas de defesa cibernética.
T0199	Fornecer orientação de gerenciamento de risco da cadeia de suprimentos e segurança cibernética empresarial para o desenvolvimento dos Planos de Continuidade das Operações.
T0200	Fornecer feedback sobre os requisitos da rede, incluindo arquitetura e infraestrutura de rede.
T0201	Fornecer diretrizes para a implementação de sistemas desenvolvidos para clientes ou equipes de instalação.
T0202	Fornecer orientação sobre segurança cibernética à liderança.
T0203	Fornecer informações sobre os requisitos de segurança a serem incluídos em demonstrações de trabalho e outros documentos de aquisição apropriados.
T0204	Fornecer informações para planos de implementação e procedimentos operacionais padrão.
T0205	Fornecer informações para as atividades de processo para Gestão de Risco e documentação relacionada (ex.: planos de suporte ao ciclo de vida do sistema, conceito de operações, procedimentos operacionais e materiais de treinamento de manutenção).
T0206	Proporcionar, liderança e direcionamento ao pessoal de tecnologia da informação (TI), garantindo que a conscientização, noções básicas, conhecimentos e treinamento sobre segurança cibernética sejam fornecidos ao pessoal de operações, proporcional às suas responsabilidades.
T0207	Fornecer otimização contínua e suporte para a resolução de problemas.
T0208	Fornecer recomendações para possíveis melhorias e upgrades.
T0209	Fornecer recomendações sobre estruturas de dados e bancos de dados que garantam a produção correta e com qualidade de relatórios/informações gerenciais.
T0210	Fornecer recomendações sobre novas tecnologias e arquiteturas de banco de dados.
T0211	Fornecer informações relacionadas ao sistema sobre os requisitos de segurança cibernética a serem incluídos em demonstrações de trabalho e outros documentos de aquisição adequados.
T0212	Fornecer assistência técnica em questões de evidências digitais ao pessoal apropriado.
T0213	Fornecer documentos técnicos, relatórios de incidentes, resultados de exames de computador, resumos e outras informações de conscientização situacional para a sede administrativa.
T0214	Receber e analisar alertas de rede de várias fontes dentro da empresa e determinar possíveis causas de tais alertas.
T0215	Reconhecer uma possível violação de segurança e tomar as medidas adequadas para relatar o incidente, conforme exigido.
T0216	Reconhecer e relatar com precisão artefatos periciais indicativos de um determinado sistema operacional.

ID da Tarefa	Descrição da Tarefa
T0217	Abordar implicações de segurança na fase de aceitação do software, incluindo critérios de conclusão, aceitação e documentação de risco, critérios comuns e métodos de testes independentes.
T0218	Recomendar medidas novas ou revisadas de segurança, resiliência e confiabilidade com base nos resultados das revisões.
T0219	Recomendar alocações de recursos necessárias para operar e manter com segurança os requisitos de segurança cibernética de uma organização.
T0220	Resolver, conflitos em leis, regulamentos, políticas, normas e procedimentos.
T0221	Revisar documentos de autorização e garantia para confirmar que o nível de risco está dentro dos limites aceitáveis para cada aplicativo de software, sistema e rede.
T0222	Revisar as políticas existentes e propostas com as partes interessadas.
T0223	Revisar ou realizar auditorias de programas e projetos de tecnologia da informação (TI).
T0224	Revisar documentação de treinamento (ex.: Documentos de Conteúdo de Curso [CCD], planos de aula, textos dos alunos, exames, Cronogramas de Instrução [SOI] e descrições do curso).
T0225	Assegurar o dispositivo eletrônico ou a fonte de informação.
T0226	Servir em conselhos de administração responsáveis por políticas de agências e interações.
T0227	Recomendar políticas e coordenar a revisão e aprovação.
T0228	Armazenar, recuperar e manipular dados para análise dos recursos e requisitos do sistema.
T0229	Supervisionar ou gerenciar medidas protetoras ou corretivas quando um incidente de cibersegurança ou vulnerabilidade é descoberto.
T0230	Apoiar o design e a execução de cenários de exercício.
T0231	Fornecer suporte às atividades de teste e avaliação de segurança/certificação.
T0232	Testar e manter a infraestrutura de rede, incluindo dispositivos de software e hardware.
T0233	Rastrear e documentar incidentes de defesa cibernética desde a detecção inicial até a resolução final.
T0234	Acompanhar as conclusões e recomendações da auditoria para garantir que as ações de mitigação apropriadas sejam tomadas.
T0235	Traduzir requisitos funcionais em soluções técnicas.
T0236	Traduzir os requisitos de segurança em elementos de design de aplicativos, incluindo a documentação de elementos das superfícies de ataque de software, realizar a modelagem de ameaças e definir critérios específicos de segurança.
T0237	Solucionar problemas de hardware e software do sistema.
T0238	Extrair dados utilizando técnicas de escultura de dados (ex.: Kit de Ferramentas Periciais [FTK], Foremost).
T0239	Usar documentos federais e específicos para organizações já publicados para gerenciar operações de sistemas de ambiente de computação.
T0240	Capturar e analisar o tráfego de rede associado a atividades maliciosas usando ferramentas de monitoramento de rede.
T0241	Usar equipamentos e técnicas especializadas para catalogar, documentar, extrair, coletar, embalar e preservar evidências digitais.
T0242	Utilizar modelos e simulações para analisar ou prever o desempenho do sistema em diferentes condições de funcionamento.
T0243	Verificar e atualizar a documentação de segurança refletindo os recursos de design de segurança do aplicativo/sistema.

ID da Tarefa	Descrição da Tarefa
T0244	Verificar se as posturas de segurança do software/rede/sistema do aplicativo são implementadas conforme indicado, documentar os desvios e fazer as recomendações necessárias para corrigir esses desvios.
T0245	Verificar se a documentação de credenciamento e garantia do aplicativo de software/rede/sistema está em dia.
T0246	Escrever e publicar técnicas de defesa cibernética, orientação e relatórios sobre os resultados de incidentes para as devidas partes interessadas.
T0247	Escrever materiais didáticos (ex.: procedimentos operacionais padrão, manual de produção) para fornecer orientação detalhada à parte relevante da força de trabalho.
T0248	Promover a conscientização sobre questões de segurança com a gerência e garantir que princípios de segurança sólidos sejam refletidos na visão e nos objetivos da organização.
T0249	Pesquisar a tecnologia atual para entender os recursos do sistema ou rede necessários.
T0250	Identificar estratégias de recursos cibernéticos para o desenvolvimento de hardware e software customizados com base nos requisitos da missão.
T0251	Desenvolver processos de compliance de segurança e/ou auditorias para serviços externos (ex.: provedores de serviços em nuvem, data centers).
T0252	Realizar revisões necessárias conforme apropriado dentro do ambiente (ex.: vigilância técnica, revisões de contramedidas [TSCM], análises de contramedidas da TEMPEST).
T0253	Realizar análise binária superficial.
T0254	Supervisionar normas de políticas e estratégias de implementação para garantir que procedimentos e diretrizes cumpram as políticas de segurança cibernética.
T0255	Participar do processo de Governança de Riscos para fornecer riscos de segurança, mitigações e informações sobre outros riscos técnicos.
T0256	Avaliar a eficácia da função de aquisição ao abordar os requisitos de segurança da informação e os riscos da cadeia de suprimentos por meio de atividades de aquisição e recomendar melhorias.
T0257	Determinar o escopo, infraestrutura, recursos e o tamanho da amostra de dados para garantir que os requisitos do sistema sejam adequadamente demonstrados.
T0258	Fornecer detecção, identificação e alerta oportunos sobre possíveis ataques/invasões, atividades anômalas e atividades de uso indevido e distinguir esses incidentes dos eventos de atividades benignas.
T0259	Usar ferramentas de defesa cibernética para monitoramento contínuo e análise das atividades do sistema, para identificar atividades maliciosas.
T0260	Analisar atividades maliciosas identificadas para determinar fraquezas exploradas, métodos de exploração, efeitos no sistema e nas informações.
T0261	Auxiliar na identificação, priorização e coordenação da proteção da infraestrutura crítica de defesa cibernética e recursos fundamentais.
T0262	Empregar princípios e práticas de defesa em profundidade aprovados (ex.: defesa em vários locais defesas em camadas, robustez de segurança).
T0263	Identificar os requisitos de segurança específicos para um sistema de tecnologia da informação (TI) em todas as fases do ciclo de vida do sistema.
T0264	Garantir que os planos de ação e marcos ou planos de remediação estejam em vigor para as vulnerabilidades identificadas durante as avaliações de risco, auditorias, inspeções, etc.
T0265	Garantir a implementação e a funcionalidade bem-sucedidas dos requisitos de segurança e das políticas e procedimentos apropriados de tecnologia da informação (TI) que sejam consistentes com a missão e os objetivos da organização.
T0266	Realizar testes de penetração conforme necessário para aplicações novas ou atualizadas.

ID da Tarefa	Descrição da Tarefa
T0267	Criar o design de contramedidas e mitigações contra potenciais explorações de fraquezas e vulnerabilidades da linguagem de programação no sistema e nos elementos.
T0268	Definir e documentar como a implementação de um novo sistema ou novas interfaces entre sistemas impacta a postura de segurança do ambiente atual.
T0269	Projetar e desenvolver funções-chave de gerenciamento (relacionadas à segurança cibernética).
T0270	Analisar as necessidades e requisitos do usuário para planejar e conduzir o desenvolvimento de segurança do sistema.
T0271	Desenvolver projetos de cibersegurança para atender às necessidades operacionais específicas e fatores ambientais (ex.: controles de acesso, aplicativos automatizados, operações de rede, requisitos de alta integridade e disponibilidade, segurança/processamento multinível de vários níveis de classificação e processamento de Informações Confidenciais Compartimentadas).
T0272	Garantir que as atividades de design de segurança e desenvolvimento de segurança cibernética estejam devidamente documentadas (fornecendo uma descrição funcional da implementação de segurança) e atualizadas conforme necessário.
T0273	Desenvolver e documentar riscos da cadeia de suprimentos para elementos críticos do sistema, conforme apropriado.
T0274	Criar evidências auditáveis de medidas de segurança.
T0275	Oferecer suporte às atividades de compliance necessárias (ex.: verificar se as diretrizes de configuração de segurança do sistema estão sendo obedecidas, e que está havendo monitoramento de conformidade).
T0276	Participar do processo de aquisição conforme necessário, seguindo as práticas adequadas de gerenciamento de riscos da cadeia de suprimentos.
T0277	Verificar se todas as aquisições, compras e esforços de terceirização abordam os requisitos de segurança da informação consistentes com os objetivos da organização.
T0278	Coletar artefatos de invasão (ex.: código-fonte, malware, Trojans) e usar dados descobertos para permitir a mitigação de possíveis incidentes de defesa cibernética dentro da empresa.
T0279	Servir como perito técnico e ponto de contato com o pessoal da segurança pública e explicar detalhes do incidente conforme necessário.
T0280	Validar continuamente a organização no que se refere às políticas/diretrizes/procedimentos/regulamentos/leis para garantir o compliance.
T0281	Fazer previsões de solicitações contínuas de serviços e certificar-se de que as garantias de segurança sejam revisadas conforme necessário.
T0282	Definir e/ou implementar políticas e procedimentos para garantir a proteção da infraestrutura crítica conforme apropriado.
T0283	Colaborar com as partes interessadas para identificar e/ou desenvolver soluções adequadas.
T0284	Criar o design e desenvolver novas ferramentas/tecnologias relacionadas à segurança cibernética.
T0285	Executar a varredura de vírus em mídia digital.
T0286	Executar análise pericial do sistema de arquivos.
T0287	Realizar análises estáticas para montar uma "imagem" de uma unidade (sem necessariamente ter a unidade original).
T0288	Executar análises estáticas de malware.
T0289	Utilizar o kit de ferramentas periciais implantáveis para dar suporte às operações, conforme necessário.
T0290	Determinar táticas, técnicas e procedimentos (TTPs) para conjuntos de invasão.
T0291	Examinar as topologias de rede para entender os fluxos de dados através da rede.

ID da Tarefa	Descrição da Tarefa
T0292	Recomendar correções de vulnerabilidade do ambiente de computação.
T0293	Identificar e analisar anomalias no tráfego de rede usando metadados.
T0294	Realizar pesquisas, análises e correlações em uma ampla variedade de todos os conjuntos de dados de origem (indicações e avisos).
T0295	Validar alertas do sistema de detecção de invasões (IDS) no tráfego de rede usando ferramentas de análise de pacotes.
T0296	Isolar e remover o malware.
T0297	Identificar aplicativos e sistemas operacionais de um dispositivo de rede baseado no tráfego de rede.
T0298	Reconstruir um ataque ou atividade maliciosa com base no tráfego de rede.
T0299	Identificar atividades de mapeamento de rede e impressão digital do sistema operacional (SO).
T0300	Desenvolver e documentar requisitos de User Experience (UX) [experiência de usuário], incluindo arquitetura de informações e requisitos de interface do usuário.
T0301	Desenvolver e implementar processos de auditoria independente de segurança cibernética para software/redes/sistemas de aplicativos e supervisionar auditorias independentes em funcionamento para garantir que os processos e procedimentos operacionais e de pesquisa e design (P&D) estejam em conformidade com os requisitos organizacionais e obrigatórios de cibersegurança, sendo obedecidos precisamente pelos administradores de sistemas e outras equipes de cibersegurança ao realizar suas atividades diárias.
T0302	Desenvolver a linguagem dos contratos para garantir a segurança da cadeia de suprimentos, sistema, rede e operações.
T0303	Identificar e fazer a alavancagem do sistema de controle de versão em toda a empresa ao criar o design e desenvolver aplicativos seguros.
T0304	Implementar e integrar metodologias de ciclo de vida de desenvolvimento de sistema (SDLC) (ex.: IBM Rational Unified Process) no ambiente de desenvolvimento.
T0305	Executar os seguintes gerenciamentos: de configuração, problemas, capacidade e financeiro para bancos de dados e sistemas de gerenciamento de dados.
T0306	Oferecer suporte aos gerenciamentos de incidentes, de nível de serviço, de mudanças, versões, continuidade e disponibilidade para bancos de dados e sistemas de gerenciamento de dados.
T0307	Analisar arquiteturas de candidatos, alocar serviços de segurança e selecionar mecanismos de segurança.
T0308	Analisar dados de incidentes para tendências emergentes.
T0309	Avaliar a eficácia dos controles de segurança.
T0310	Auxiliar na construção de assinaturas que podem ser implementadas em ferramentas de rede de defesa cibernética em resposta a ameaças novas ou observadas dentro do ambiente de rede ou enclave.
T0311	Consultar os clientes sobre o design e a manutenção do sistema de software.
T0312	Coordenar funções com analistas de inteligência para correlacionar dados de avaliação de ameaças.
T0313	Criar o design e normas de qualidade de documentos.
T0314	Desenvolver um contexto de segurança do sistema, um conceito preliminar de segurança do sistema (CONOPS) e definir os requisitos de segurança do sistema de linha de base de acordo com os requisitos aplicáveis de segurança cibernética.
T0315	Desenvolver e oferecer treinamento técnico para instruir os demais ou para atender às necessidades do cliente.

ID da Tarefa	Descrição da Tarefa
T0316	Desenvolver ou auxiliar no desenvolvimento de módulos ou aulas de treinamento por computador.
T0317	Desenvolver ou auxiliar no desenvolvimento de atribuições de cursos.
T0318	Desenvolver ou auxiliar no desenvolvimento de avaliações de cursos.
T0319	Desenvolver ou auxiliar no desenvolvimento de normas de classificação e proficiência.
T0320	Auxiliar na elaboração de planos de desenvolvimento individual/coletivo, treinamento e/ou remediação.
T0321	Desenvolver ou auxiliar no desenvolvimento de metas e objetivos de aprendizagem.
T0322	Desenvolver ou auxiliar no desenvolvimento de materiais ou programas de treinamento no trabalho.
T0323	Desenvolver ou auxiliar no desenvolvimento de testes escritos para medir e avaliar a proficiência do aluno.
T0324	Direcionar a programação de software e desenvolvimento de documentação.
T0325	Documentar o propósito de um sistema e o conceito preliminar de segurança do sistema de operações.
T0326	Empregar processos de gerenciamento de configuração.
T0327	Avaliar as vulnerabilidades de infraestrutura de rede para melhorar os recursos que estão sendo desenvolvidos.
T0328	Avaliar arquiteturas e projetos de segurança para determinar a adequação do design de segurança e arquitetura propostos ou fornecidos em resposta aos requisitos contidos em documentos de aquisição.
T0329	Seguir as normas e processos do ciclo de vida de engenharia de software e sistemas.
T0330	Manter sistemas de entrega de mensagens assegurados.
T0331	Manter o rastreamento de incidentes e o banco de dados de soluções.
T0332	Notificar os gerentes responsáveis, respondentes de incidentes cibernéticos, e membros da equipe de provedores de serviços de segurança cibernética sobre suspeitas de incidentes cibernéticos e articular o histórico, status e impacto potencial do evento para medidas adicionais de acordo com o plano de resposta a incidentes cibernéticos da organização.
T0334	Assegurar que todos os componentes do sistema possam ser integrados e alinhados (ex.: procedimentos, bancos de dados, políticas, software e hardware).
T0335	Construir, instalar, configurar e testar hardware dedicado de defesa cibernética.
T0336	Retirado: Integrado com o T0228
T0337	Supervisionar e atribuir trabalhos a programadores, designers, tecnólogos e técnicos, além de outros engenheiros e pessoal científico.
T0338	Escrever especificações funcionais detalhadas que documentam o processo de desenvolvimento da arquitetura.
T0339	Liderar esforços para promover o uso da gestão do conhecimento e compartilhamento de informações pela organização.
T0340	Atuar como principal parte interessada nos processos e funções operacionais de tecnologia da informação subjacentes (TI) que oferecem suporte ao serviço, além de fornecer orientação e monitorar todas as atividades significativas para que o serviço seja desempenhado com sucesso.
T0341	Defender o financiamento adequado para recursos de treinamento cibernético, para incluir cursos internos e fornecidos pelo setor, bem como instrutores e materiais relacionados.
T0342	Analisar as fontes de dados para fornecer recomendações acionáveis.
T0343	Analisar uma possível crise para garantir a proteção do público, do pessoal e dos recursos.
T0344	Avaliar todos os processos de gerenciamento de configuração (alterar configuração/gerenciamento de liberação).

ID da Tarefa	Descrição da Tarefa
T0345	Avaliar a eficácia e a eficiência da instrução de acordo com a facilidade do uso da tecnologia instrucional e da aprendizagem do aluno, transferência de conhecimentos e nível de satisfação.
T0346	Avaliar o comportamento da vítima, testemunha ou suspeito no que se refere à investigação.
T0347	Avaliar a validade dos dados de origem e as conclusões subsequentes.
T0348	Auxiliar na avaliação do impacto da implementação e manutenção de uma infraestrutura de defesa cibernética dedicada.
T0349	Coletar métricas e dados de tendências.
T0350	Conduzir uma análise de mercado para identificar, avaliar e recomendar produtos comerciais e governamentais fora da prateleira e produtos de código aberto para uso dentro de um sistema, para garantir que os produtos recomendados estejam em conformidade com os requisitos de avaliação e validação da organização.
T0351	Conduzir testes de hipóteses utilizando processos estatísticos.
T0352	Realizar avaliações das necessidades de aprendizagem e identificar os requisitos.
T0353	Consultar analistas de sistemas, engenheiros, programadores, entre outros, para o design de aplicativos.
T0354	Coordenar e gerenciar o serviço global fornecido a um cliente de ponta a ponta.
T0355	Coordenar funções com especialistas em assuntos internos e externos para garantir que as normas de qualificação existentes reflitam os requisitos funcionais da organização e atendam às normas do setor.
T0356	Coordenar funções com as partes interessadas da força de trabalho organizacional para garantir a alocação e distribuição adequadas de ativos de capital humano.
T0357	Criar exercícios de aprendizagem interativa para estabelecer um ambiente de aprendizagem eficaz.
T0358	Criar o design e desenvolver a funcionalidade de administração e gerenciamento de sistemas para usuários de acesso privilegiado.
T0359	Criar o design, implementar, testar e avaliar interfaces seguras entre sistemas de informação, sistemas físicos e/ou tecnologias incorporadas.
T0360	Determinar a extensão das ameaças e recomendar cursos de ação ou contramedidas para mitigar riscos.
T0361	Desenvolver e facilitar métodos de coleta de dados.
T0362	Desenvolver e implementar descrições de cargos padronizados com base em funções de trabalho cibernético estabelecidas.
T0363	Desenvolver e analisar procedimentos de recrutamento, contratação e retenção de acordo com as políticas de RH vigentes.
T0364	Desenvolver uma estrutura de classificação para o campo de carreira cibernética, incluindo requisitos para entrada nesta carreira e outras nomenclaturas, como códigos e identificadores.
T0365	Desenvolver ou auxiliar no desenvolvimento de políticas de treinamento e protocolos para treinamento cibernético.
T0366	Desenvolver percepções estratégicas derivadas de grandes conjuntos de dados.
T0367	Desenvolver metas e objetivos para o currículo em cibernética.
T0368	Verificar se os campos de carreira cibernética estão sendo gerenciados de acordo com as políticas e diretrizes organizacionais de RH.
T0369	Verificar se as políticas e processos de gestão da força de trabalho cibernética estão em cumprimento dos requisitos legais e organizacionais em relação à igualdade de oportunidades, diversidade e práticas justas de contratação/emprego.

ID da Tarefa	Descrição da Tarefa
T0370	Verificar se os acordos de nível de serviço (SLAs) e os contratos subjacentes já foram definidos, e estabelecem claramente para o cliente uma descrição do serviço e as medidas para monitoramento.
T0371	Estabelecer limites aceitáveis para o aplicativo de software, rede ou sistema.
T0372	Estabelecer e coletar métricas para monitorar e validar a prontidão da força de trabalho cibernética, incluindo a análise de dados para avaliar o status dos cargos identificados e preenchidos, e cargos que foram ocupados com pessoal qualificado.
T0373	Estabelecer e supervisionar processos de isenção para entrada no campo de carreira cibernética e requisitos de qualificação de treinamento.
T0374	Estabelecer planos de carreira cibernética para permitir a progressão de carreira, desenvolvimento e crescimento deliberados, dentro e entre os campos de carreira cibernética.
T0375	Estabelecer normas de elementos de mão de obra, de quadro de pessoal e elementos de dados de qualificação para cumprir os requisitos de gerenciamento e emissão de relatórios da força de trabalho cibernética.
T0376	Estabelecer, identificar, implementar e avaliar programas de gestão da força de trabalho cibernética de acordo com os requisitos organizacionais.
T0377	Solicitar feedback sobre a satisfação do cliente e o desempenho dos serviços internos para promover a melhoria contínua.
T0378	Incorporar o processo de atualizações de manutenção de sistemas orientados ao risco para resolver deficiências do sistema (periodicamente e fora do ciclo).
T0379	Gerenciar o relacionamento interno com os proprietários de processos de tecnologia da informação (TI) que oferecem suporte ao serviço, auxiliando na definição e pactuação de acordos de nível operacional (OLAs).
T0380	Planejar estratégias instrucionais como palestras, demonstrações, exercícios interativos, apresentações multimídia, cursos em vídeo, cursos baseados na Web para um ambiente de aprendizagem mais eficaz, juntamente com educadores e treinadores.
T0381	Apresentar informações técnicas para públicos técnicos e não técnicos.
T0382	Apresentar dados em formatos criativos.
T0383	Programar algoritmos personalizados.
T0384	Promover a conscientização entre os gestores sobre as políticas e estratégias cibernéticas, conforme apropriado, e garantir que princípios sólidos se reflitam na missão, visão e metas da organização.
T0385	Oferecer recomendações acionáveis às partes críticas interessadas, com base na análise de dados e conclusões.
T0386	Proporcionar apoio investigativo criminal ao advogado durante o processo judicial.
T0387	Analisar e aplicar normas de qualificação para o campo de carreira cibernética.
T0388	Analisar e aplicar políticas organizacionais relacionadas ou que influenciam a força de trabalho cibernética.
T0389	Analisar relatórios de desempenho do serviço identificando quaisquer problemas e variações significativas, iniciando, quando necessário, ações corretivas e garantindo que todas as questões pendentes sejam resolvidas.
T0390	Examinar/avaliar a eficácia da força de trabalho cibernética para ajustar normas de habilidade e/ou qualificação.
T0391	Apoiar a integração de pessoal qualificado da força de trabalho cibernética em processos de desenvolvimento do ciclo de vida de sistemas de informação.
T0392	Utilizar documentação ou recursos técnicos para implementar um novo método matemático, de ciência de dados ou ciência da computação.

ID da Tarefa	Descrição da Tarefa
T0393	Validar as especificações e requisitos para testabilidade.
T0394	Trabalhar com outros gerentes de serviços e proprietários de produtos para equilibrar e priorizar serviços que atendam às necessidades, restrições e objetivos gerais do cliente.
T0395	Escrever e publicar análises pós-ação.
T0396	Processar imagens com ferramentas apropriadas, dependendo dos objetivos do analista.
T0397	Executar análise de registro do Windows.
T0398	Executar o monitoramento de arquivos e registros no sistema de execução após identificar a invasão através de análise dinâmica.
T0399	Inserir informações de mídia no banco de dados de rastreamento (ex.: ferramenta de rastreamento de produtos) para a mídia digital que foi adquirida.
T0400	Correlacionar dados de incidentes e executar relatórios de defesa cibernética.
T0401	Manter o kit de ferramentas de defesa cibernética implantável (ex.: software/hardware especializado em defesa cibernética) para apoiar a missão da Equipe de Resposta a Incidentes.
T0402	Alocar de forma eficiente a capacidade de armazenamento na concepção de sistemas de gerenciamento de dados.
T0403	Ler, interpretar, escrever, modificar e executar scripts simples (ex.: Perl, VBScript) nos sistemas Windows e UNIX (ex.: aqueles que executam tarefas como: analisar arquivos grandes de dados, automatizar tarefas manuais e buscar/processar dados remotos).
T0404	Utilizar diferentes linguagens de programação para escrever código, abrir arquivos, ler arquivos e gravar saída para diferentes arquivos.
T0405	Utilizar linguagem de código aberto como “R” e aplicar técnicas quantitativas (ex.: estatísticas descritivas e inferenciais, amostragem, design experimental, testes paramétricos e não paramétricos de diferença, regressão de mínimos quadrados ordinários, linha geral).
T0406	Verificar se as atividades de design e desenvolvimento estão devidamente documentadas (fornecendo uma descrição funcional da implementação) e atualizadas conforme necessário.
T0407	Participar do processo de aquisição, conforme necessário.
T0408	Interpretar e fazer vigorar leis, estatutos e documentos regulatórios aplicáveis e os integra às políticas.
T0409	Solucionar problemas de design e processo de protótipos em todas as fases de design, desenvolvimento e pré-lançamento do produto.
T0410	Identificar recursos funcionais e relacionados à segurança para encontrar oportunidades de desenvolvimento de novos recursos e para explorar ou mitigar vulnerabilidades.
T0411	Identificar e/ou desenvolver ferramentas de engenharia reversa para melhorar os recursos e detectar vulnerabilidades.
T0412	Realizar revisões de importação/exportação para aquisição de sistemas e softwares.
T0413	Desenvolver recursos de gerenciamento de dados (ex.: gerenciamento de chave criptográfica centralizado baseado em nuvem) para incluir suporte à força de trabalho móvel.
T0414	Desenvolver requisitos de cadeia de suprimentos, sistemas, rede, desempenho e segurança cibernética.
T0415	Garantir que os requisitos da cadeia de suprimentos, sistema, rede, desempenho e segurança cibernética sejam incluídos na linguagem do contrato e entrem em vigor.
T0416	Habilitar aplicativos com codificação pública, aproveitando as bibliotecas de infraestrutura de chave pública (PKI) existentes, incorporando o gerenciamento de certificados e as funcionalidades de criptografia, quando apropriado.
T0417	Identificar e alavancar os serviços de segurança no âmbito da empresa ao elaborar o design e desenvolver aplicativos seguros (ex.: Enterprise PKI, Servidor de Identidade Federada, solução Enterprise Antivírus), quando apropriado.

ID da Tarefa	Descrição da Tarefa
T0418	Instalar, atualizar e solucionar problemas de sistemas/servidores.
T0419	Adquirir e manter conhecimento prático das questões constitucionais que surgem em leis, regulamentos, políticas, acordos, normas, procedimentos ou outras questões relevantes.
T0420	Administrar bancadas de testes, para testar e avaliar aplicativos, infraestrutura de hardware, regras/assinaturas, controles de acesso e configurações de plataformas gerenciadas por provedores de serviço.
T0421	Gerenciar a indexação/catalogação, armazenamento e acesso aos conhecimentos organizacionais explícitos (ex.: documentos impressos, arquivos digitais).
T0422	Implementar normas, requisitos e especificações de gerenciamento de dados.
T0423	Analisar ameaças geradas por computador para contrainteligência ou atividade criminosa.
T0424	Analisar e fornecer informações às partes interessadas que apoiarão o desenvolvimento de aplicativos de segurança ou modificação de um aplicativo de segurança existente.
T0425	Analisar a política cibernética organizacional.
T0426	Analisar os resultados dos testes de software, hardware ou interoperabilidade.
T0427	Analisar as necessidades e requisitos do usuário durante o planejamento da arquitetura.
T0428	Analisar as necessidades de segurança e os requisitos de software para determinar a viabilidade do projeto dentro de restrições de tempo, custos e mandados de segurança.
T0429	Avaliar as necessidades normativas e colaborar com as partes interessadas para desenvolver políticas de governança para atividades cibernéticas.
T0430	Reunir e preservar provas usadas na acusação de crimes de computador.
T0431	Verificar a disponibilidade de hardware, funcionalidade, integridade e eficiência do sistema.
T0432	Coletar e analisar artefatos de invasão (ex.: código fonte, malware e configuração do sistema) e usar dados descobertos para permitir a mitigação de possíveis incidentes de defesa cibernética dentro da empresa.
T0433	Realizar análises de arquivos de registro, evidências e outras informações para determinar os melhores métodos para identificar os autores de uma invasão de rede ou outros crimes.
T0434	Conduzir o enquadramento de alegações para identificar adequadamente supostas violações da lei, regulamentos ou políticas/orientação.
T0435	Realizar manutenção periódica do sistema, incluindo limpeza (física e eletronicamente), verificações de disco, reinicializações de rotina, despejos de dados e testes.
T0436	Realizar testes de programas e aplicativos de software para garantir que as informações desejadas sejam produzidas e que as instruções e os níveis de segurança estejam corretos.
T0437	Correlacionar treinamento e aprendizado com os requisitos e missão de negócios.
T0438	Criar, editar e gerenciar listas de controle de acesso à rede em sistemas especializados de defesa cibernética (ex.: firewalls e sistemas de prevenção de invasões).
T0439	Detectar e analisar dados criptografados, estenografia, fluxos de dados alternativos e outras formas de dados ocultos.
T0440	Capturar e integrar recursos essenciais do sistema ou funções de negócios necessárias para restauração parcial ou completa do sistema após um evento de falha catastrófico.
T0441	Definir e integrar ambientes de missão atuais e futuros.
T0442	Criar cursos de capacitação adaptados ao público e ao ambiente físico.
T0443	Oferecer cursos de capacitação adaptados ao público e ambientes físicos/virtuais.
T0444	Introduzir conceitos, procedimentos, software, equipamentos e/ou aplicações tecnológicas aos alunos.
T0445	Criar o design/integrar uma estratégia cibernética para descrever a visão, missão e objetivos que se alinham com o plano estratégico da organização.

ID da Tarefa	Descrição da Tarefa
T0446	Criar o design, desenvolver, integrar e atualizar medidas de segurança do sistema que forneçam confidencialidade, integridade, disponibilidade, autenticação e não repúdio.
T0447	Criar o design de hardware, sistemas operacionais e aplicativos de software para atender adequadamente aos requisitos.
T0448	Desenvolver a arquitetura corporativa ou os componentes do sistema necessários para atender às necessidades do usuário.
T0449	Criar o design para requisitos de segurança para garantir que os requisitos sejam atendidos em todos os sistemas e/ou aplicativos.
T0450	Criar o design para o currículo de treinamento e conteúdo do curso com base nos requisitos.
T0451	Participar do desenvolvimento de currículo de treinamento e conteúdo do curso.
T0452	Projetar, construir, implementar e manter uma estrutura de gerenciamento de conhecimento que forneça aos usuários finais acesso ao capital intelectual da organização.
T0453	Determinar e desenvolver leads e identificar fontes de informação para identificar e/ou processar os responsáveis por uma invasão ou outros crimes.
T0454	Definir os requisitos de segurança da linha de base de acordo com as diretrizes aplicáveis.
T0455	Desenvolver procedimentos de teste e validação de sistemas de software, programação e documentação.
T0456	Desenvolver procedimentos seguros de teste e validação de software.
T0457	Desenvolver procedimentos de teste e validação do sistema, programação e documentação.
T0458	Cumprir os procedimentos operacionais padrão de administração de sistemas da organização.
T0459	Implementar aplicativos de mineração de dados e armazenamento de dados.
T0460	Desenvolver e implementar programas de mineração de dados e armazenamento de dados.
T0461	Implementar e fazer vigorar políticas e procedimentos locais de uso de rede.
T0462	Desenvolver procedimentos e teste de failover para transferência de operações do sistema para um site alternativo com base nos requisitos de disponibilidade do sistema.
T0463	Desenvolver estimativas de custos para sistemas novos ou modificados.
T0464	Desenvolver documentação de design detalhado para especificações de componentes e interfaces para suportar o design e o desenvolvimento do sistema.
T0465	Desenvolver diretrizes para implementação.
T0466	Desenvolver estratégias de mitigação para resolver problemas de riscos de custo, cronograma, desempenho e segurança.
T0467	Assegurar que o treinamento atenda aos objetivos e metas de treinamento em segurança cibernética, educação ou conscientização.
T0468	Fazer diagnóstico e resolver incidentes, problemas e eventos do sistema relatados pelo cliente.
T0469	Analisar e relatar tendências de postura de segurança organizacional.
T0470	Analisar e relatar tendências de postura de segurança do sistema.
T0471	Documentar condição original de evidência digital e/ou associada (ex.: através de fotografias digitais, relatórios escritos, verificação da função hash).
T0472	Elaborar, contratar pessoal e publicar políticas sobre cibernética.
T0473	Documentar e atualizar todas as atividades de definição e arquitetura, conforme necessário.
T0474	Fornecer análises e decisões jurídicas aos inspetores gerais, dirigentes de privacidade, pessoal de supervisão e compliance, sobre o cumprimento das políticas de segurança cibernética e aos requisitos legais e regulatórios relevantes.
T0475	Avaliar controles de acesso adequados com base em princípios de privilégio mínimo e a “necessidade de saber”.
T0476	Avaliar o impacto das mudanças nas leis, regulamentos, políticas, normas e procedimentos.

ID da Tarefa	Descrição da Tarefa
T0477	Garantir a execução da recuperação de desastres e a continuidade das operações.
T0478	Fornecer orientações sobre leis, regulamentos, políticas, normas ou procedimentos para a gerência, funcionários ou clientes.
T0479	Empregar sistemas de tecnologia da informação (TI) e mídia de armazenamento digital para resolver, investigar e/ou processar crimes cibernéticos e fraudes cometidas contra pessoas e propriedades.
T0480	Identificar componentes ou elementos, alocar componentes funcionais abrangentes para incluir funções de segurança e descrever as relações entre os elementos.
T0481	Identificar e abordar questões de planejamento e gerenciamento da força de trabalho cibernética (ex.: recrutamento, retenção e treinamento).
T0482	Fazer recomendações baseadas na análise de tendências para melhorias em soluções de software e hardware para aprimorar a experiência do cliente.
T0483	Identificar potenciais conflitos com a implementação de quaisquer ferramentas de defesa cibernética (ex.: teste e otimização de ferramentas e assinaturas).
T0484	Determinar as necessidades de proteção (ou seja, controles de segurança) para os sistemas de informação e redes e documentar adequadamente.
T0485	Implementar medidas de segurança para resolver, vulnerabilidades, mitigar riscos e recomendar alterações de segurança no sistema ou nos seus componentes, conforme necessário.
T0486	Implementar requisitos de Controle de Risco (RMF)/Avaliação e Autorização de Segurança (SA&A) para sistemas dedicados de defesa cibernética dentro da empresa, além de documentar e manter registros para eles.
T0487	Facilitar a implementação de leis novas ou revisadas, regulamentos, ordens executivas, políticas, normas ou procedimentos.
T0488	Implementar projetos para sistemas novos ou existentes.
T0489	Implementar medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.
T0490	Instalar e configurar sistemas de gerenciamento de banco de dados e software.
T0491	Instalar e configurar equipamentos de hardware, software e periféricos para usuários do sistema de acordo com as normas organizacionais.
T0492	Garantir a integração e implementação de Cross-Domain Solutions CDS [soluções de domínio cruzado] em um ambiente seguro.
T0493	Liderar e supervisionar o orçamento, alocação e contratação de pessoal.
T0494	Administrar contas, direitos de rede e acesso a sistemas e equipamentos.
T0495	Gerenciar pacotes de credenciamento (ex.: O/IEC 15026-2).
T0496	Executar gestão/inventário de ativos de recursos de tecnologia da informação (TI).
T0497	Gerenciar processo de planejamento de tecnologia da informação (TI) para garantir que as soluções desenvolvidas atendam às necessidades do cliente.
T0498	Gerenciar os recursos do sistema/servidor, incluindo desempenho, capacidade, disponibilidade, facilidade de manutenção e capacidade de recuperação.
T0499	Mitigar/corrigir deficiências de segurança identificadas durante testes de segurança/certificação e/ou recomendar aceitação de risco para o líder sênior ou respectivo representante autorizado.
T0500	Modificar e manter o software existente para corrigir erros, adaptá-lo a novos hardwares ou atualizar interfaces e melhorar o desempenho.
T0501	Monitorar e manter a configuração do sistema/servidor.
T0502	Monitorar e reportar o desempenho do sistema de computador em nível de cliente.

ID da Tarefa	Descrição da Tarefa
T0503	Monitorar fontes de dados externos (ex.: sites de fornecedores de defesa cibernética, equipes de resposta a emergências de computador, foco de segurança) para manter a atual condição em termos de ameaça de defesa cibernética e determinar quais os problemas de segurança que podem impactar a empresa.
T0504	Avaliar e monitorar a segurança cibernética relacionada às práticas de implementação e testes do sistema.
T0505	Monitorar a aplicação rigorosa de políticas cibernéticas, princípios e práticas na prestação de serviços de planejamento e gestão.
T0506	Chegar a um consenso sobre as mudanças propostas nas políticas pelas partes interessadas.
T0507	Supervisionar a instalação, implementação, configuração e suporte de componentes do sistema.
T0508	Verificar se existem requisitos mínimos de segurança para todas as aplicações.
T0509	Realizar uma avaliação de risco de segurança da informação.
T0510	Coordenar as funções de resposta a incidentes.
T0511	Realizar testes de desenvolvimento em sistemas que estão sendo produzidos.
T0512	Realizar testes de interoperabilidade em sistemas que trocam informações eletrônicas com outros sistemas.
T0513	Realizar testes operacionais.
T0514	Diagnosticar hardware de sistema/servidor defeituoso.
T0515	Realizar reparos no hardware do sistema/servidor defeituoso.
T0516	Realizar testes, revisão e/ou avaliação de programas seguros para identificar possíveis falhas nos códigos e mitigar vulnerabilidades.
T0517	Integrar resultados quanto à identificação de lacunas na arquitetura de segurança.
T0518	Executar revisões de segurança e identificar falhas de segurança na arquitetura.
T0519	Planejar e coordenar a apresentação de técnicas e formatos de sala de aula (ex.: palestras, demonstrações, exercícios interativos, apresentações multimídia) para haver um ambiente de aprendizado mais eficaz.
T0520	Planejar técnicas e formatos educacionais não presenciais (ex.: cursos em vídeo, mentoria, cursos baseados na web).
T0521	Planejar a estratégia de implementação para garantir que os componentes da empresa possam ser integrados e alinhados.
T0522	Elaborar documentos legais e outros relevantes (ex.: depoimentos, resumos, atestados, declarações, apelações, alegações, descobertas).
T0523	Preparar relatórios para documentar a investigação seguindo normas e requisitos legais.
T0524	Promover o compartilhamento de conhecimento entre proprietários/usuários de informações através dos processos e sistemas operacionais de uma organização.
T0525	Fornecer orientação para gerenciamento de risco da cadeia de suprimentos e segurança cibernética empresarial.
T0526	Fornecer recomendações de segurança cibernética à liderança com base em ameaças e vulnerabilidades significativas.
T0527	Fornecer informações aos planos de implementação e procedimentos operacionais padrão à medida que se relacionam com a segurança dos sistemas de informação.
T0528	Fornecer informações sobre planos de implementação, procedimentos operacionais padrão, documentação de manutenção e materiais de treinamento de manutenção.
T0529	Fornecer orientação sobre políticas para gerenciamento cibernético, funcionários e usuários.
T0530	Elaborar um relatório de análise de tendências e impacto.
T0531	Solucionar problemas de interface de hardware/software e interoperabilidade.

ID da Tarefa	Descrição da Tarefa
T0532	Analisar imagens periciais e outras fontes de dados (ex.: dados voláteis) para recuperação de informações potencialmente relevantes.
T0533	Revisar, realizar ou participar de auditorias de programas e projetos cibernéticos.
T0534	Realizar análises periódicas/revisões de conteúdo de curso para exatidão, alinhamento de completude e atualizações (ex.: documentos de conteúdo do curso, planos de aula, textos dos alunos, exames, cronograma de instrução e descrições de cursos).
T0535	Recomendar revisões do currículo e do conteúdo do curso com base no feedback de sessões de treinamento anteriores.
T0536	Servir como consultor interno e orientador em sua própria área de atuação (ex.: técnico, direitos autorais, mídia impressa, mídia eletrônica).
T0537	Oferecer suporte ao CIO na formulação de políticas relacionadas ao ciberespaço.
T0538	Fornecer suporte para atividades de teste e avaliação.
T0539	Testar, avaliar e verificar hardware e/ou software para determinar a conformidade com especificações e requisitos definidos.
T0540	Registrar e gerenciar os dados de teste.
T0541	Rastrear os requisitos do sistema para idealizar o design de componentes e realizar análises de lacunas.
T0542	Traduzir os recursos propostos em requisitos técnicos.
T0544	Verificar a estabilidade, interoperabilidade, portabilidade e/ou a escalabilidade da arquitetura do sistema.
T0545	Trabalhar com as partes interessadas para resolver incidentes de segurança de computador e conformidade com vulnerabilidades.
T0546	Escrever e publicar recomendações de defesa cibernética, relatórios e white papers sobre os resultados de incidentes para as devidas partes interessadas.
T0547	Pesquisar e avaliar as tecnologias e normas disponíveis para atender às necessidades dos clientes.
T0548	Fornecer aconselhamento e opiniões para Planos de Recuperação, Contingência e Continuidade das Operações após um desastre.
T0549	Realizar avaliações de risco e vulnerabilidades técnicas (avaliação de tecnologia) e não técnicas (avaliação de pessoas e operações) em áreas relevantes com foco em tecnologia (ex.: ambiente de computação local, rede e infraestrutura, limite de enclave, infraestrutura de suporte e aplicativos).
T0550	Fazer recomendações sobre a seleção de controles de segurança econômicos para mitigar riscos (ex.: proteção de informações, sistemas e processos).
T0551	Elaborar e publicar documentos de segurança da cadeia de suprimentos e gestão de riscos.
T0552	Revisar e aprovar uma norma de segurança/gestão de risco da cadeia de suprimentos.
T0553	Aplicar funções de segurança cibernética (ex.: criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.
T0554	Determinar e documentar patches de software ou a extensão das versões que deixariam o software vulnerável.
T0555	Documentar como a implementação de um novo sistema ou nova interface entre sistemas impacta o ambiente atual e o ambiente-alvo, incluindo, mas não se limitando à postura de segurança.
T0556	Avaliar e idealizar o design das funções de gerenciamento da segurança relacionadas ao ciberespaço.
T0557	Integrar as principais funções de gerenciamento relacionadas ao ciberespaço.
T0558	Analisar as necessidades e requisitos do usuário para planejar e conduzir o desenvolvimento do sistema.

ID da Tarefa	Descrição da Tarefa
T0559	Desenvolver projetos para atender às necessidades operacionais específicas e fatores ambientais (ex.: controles de acesso, aplicativos automatizados, operações de rede).
T0560	Colaborar em projetos de cibersegurança para atender às necessidades operacionais específicas e fatores ambientais (ex.: controles de acesso, aplicativos automatizados, operações de rede, requisitos de alta integridade e disponibilidade, segurança/processamento multinível de vários níveis de classificação e processamento de Informações Confidenciais Compartimentadas).
T0561	Caracterizar com precisão os sistemas de destino.
T0562	Ajustar as operações de coleta ou o plano de coleta para resolver problemas/desafios identificados e sincronizar as coletas com os requisitos operacionais gerais.
T0563	Fornecer informações para a análise, design, desenvolvimento ou aquisição de recursos utilizados para o cumprimento dos objetivos.
T0564	Analisar o feedback para determinar até que ponto os produtos e serviços de coleta estão atendendo aos requisitos.
T0565	Analisar os pedidos de coleta recebidos.
T0566	Analisar a arquitetura operacional interna, ferramentas e procedimentos para melhorar o desempenho.
T0567	Analisar a arquitetura operacional de destino para obter acesso.
T0568	Analisar planos, diretrizes, orientações e políticas referentes aos fatores que influenciam a estrutura operacional e os requisitos de gerenciamento da coleta (ex.: duração, escopo, requisitos de comunicação, acordos interagências/internacionais).
T0569	Responder aos pedidos de informação.
T0570	Aplicar e utilizar recursos cibernéticos autorizados para permitir o acesso a redes direcionadas.
T0571	Aplicar a experiência específica em normas e processos para facilitar o desenvolvimento, negociação, contratação de pessoal e planos e/ou memorandos de entendimento.
T0572	Aplicar a coleta cibernética, preparação de ambiente e experiência específica em engajamento para permitir novas operações de exploração e/ou coleta contínua, ou em suporte às necessidades do cliente.
T0573	Avaliar e aplicar fatores de riscos do ambiente operacional ao processo de gerenciamento de coleta.
T0574	Aplicar e obedecer a estatutos, leis, regulamentos e normas aplicáveis.
T0575	Coordenar para oferecer suporte de inteligência às atividades de planejamento operacional.
T0576	Avaliar a inteligência de todas as fontes e recomendar alvos para apoiar os objetivos de operação cibernética.
T0577	Avaliar a eficiência dos sistemas de troca e gerenciamento de informações existentes.
T0578	Avaliar o desempenho dos ativos de coleta em relação às especificações prescritas.
T0579	Avaliar as vulnerabilidades do destino e/ou os recursos operacionais para determinar o curso de ação.
T0580	Avaliar a eficácia das coletas no sentido de satisfazer lacunas de informações prioritárias, utilizando recursos e métodos disponíveis, e ajustar as estratégias e os requisitos de coleta para estarem em conformidade.
T0581	Auxiliar e aconselhar parceiros interagências na identificação e desenvolvimento de melhores práticas para facilitar o apoio operacional à realização dos objetivos da organização.
T0582	Oferecer experiência específica para o desenvolvimento de um plano de ação.
T0583	Fornecer experiência específica sobre o assunto para o desenvolvimento de um quadro operacional comum.

ID da Tarefa	Descrição da Tarefa
T0584	Manter uma imagem de inteligência comum.
T0585	Fornecer experiência específica sobre o assunto para o desenvolvimento de indicadores específicos de operações cibernéticas.
T0586	Auxiliar na coordenação, validação e gestão de requisitos, planos e/ou atividades de coleta de todas as fontes.
T0587	Auxiliar no desenvolvimento e refinamento de requisitos prioritários de informações.
T0588	Oferecer experiência específica para o desenvolvimento de medidas de efetividade e medidas de atuação.
T0589	Auxiliar na identificação de falhas de coleta de informações.
T0590	Habilitar a sincronização dos planos de suporte de inteligência entre organizações parceiras, conforme necessário.
T0591	Executar análises para atividades de exploração de infraestrutura de destinos.
T0592	Fornecer informações para a identificação de critérios de sucesso relacionados com a cibersegurança.
T0593	Breve ameaça e/ou situações atuais de destino.
T0594	Construir e manter pastas eletrônicas de destino.
T0595	Classificar documentos de acordo com as diretrizes de classificação.
T0596	Encerrar os pedidos por informações assim que forem atendidos.
T0597	Colaborar com analistas de inteligência/organizações de destino envolvidas em áreas relacionadas.
T0598	Colaborar com as organizações de desenvolvimento para criar e implantar as ferramentas necessárias para alcançar os objetivos.
T0599	Colaborar com outros clientes, organizações de inteligência e redes de destino envolvidas em áreas cibernéticas relacionadas.
T0600	Colaborar com outras organizações parceiras internas e externas em questões de acesso e operação de destino.
T0601	Colaborar com outros membros da equipe ou organizações parceiras para desenvolver um programa diversificado de materiais informativos (ex.: páginas da Web, briefings, materiais de impressão).
T0602	Colaborar com o cliente para definir os requisitos de informações.
T0603	Comunicar novos desenvolvimentos, avanços, desafios e lições aprendidas à liderança e clientes internos e externos.
T0604	Comparar os ativos alocados e disponíveis com a demanda por coleta, conforme declarado nos requerimentos.
T0605	Compilar lições aprendidas com a execução das atividades de gerenciamento de coleta, comparando-as aos objetivos de coleta da organização.
T0606	Compilar, integrar e/ou interpretar dados de todas as fontes para inteligência ou valor de vulnerabilidade em relação a alvos específicos.
T0607	Identificar e realizar análises de comunicações do alvo para identificar informações essenciais em apoio às operações.
T0608	Realizar análises de tecnologias digitais físicas e lógicas (ex.: sem fio, SCADA, telecom) para identificar possíveis caminhos de acesso.
T0609	Realizar a habilitação de acesso de computadores sem fio e redes digitais.
T0610	Realizar coleta e processamento de computadores sem fio e redes digitais.
T0611	Realizar avaliações de fim de operação.
T0612	Realizar exploração de computadores sem fio e redes digitais.
T0613	Realizar uma coordenação formal e informal dos requisitos de coleta de acordo com as diretrizes e procedimentos estabelecidos.

ID da Tarefa	Descrição da Tarefa
T0614	Realizar uma análise técnica e de metas independentes, incluindo informações específicas de destino (ex.: culturais, organizacionais, políticas) que resultem em acesso.
T0615	Realizar pesquisas e análises aprofundadas.
T0616	Realizar análises de reconhecimento de rede e vulnerabilidade de sistemas dentro de uma rede.
T0617	Realizar análises nodais.
T0618	Realizar atividades na rede para controlar e exfiltrar dados de tecnologias implantadas.
T0619	Realizar atividades on-net e off-net para controlar e exfiltrar dados de tecnologias automatizadas implantadas.
T0620	Realizar a coleta de dados de código aberto através de várias ferramentas online.
T0621	Realizar controle de qualidade para determinar a validade e relevância das informações coletadas sobre redes.
T0622	Desenvolver, revisar e implementar todos os níveis de orientação de planejamento em apoio às operações cibernéticas.
T0623	Realizar levantamento de computadores e redes digitais.
T0624	Realizar pesquisa e análise de destino.
T0625	Considerar a eficiência e a eficácia dos ativos e recursos de coleta se/quando aplicados em relação aos requisitos prioritários de informações.
T0626	Construir planos de coleta e matrizes utilizando orientações e procedimentos estabelecidos.
T0627	Contribuir para o planejamento de um curso de ação em caso de crise das operações cibernéticas.
T0628	Contribuir para o desenvolvimento de ferramentas de apoio às decisões da organização, se necessário.
T0629	Contribuir para o desenvolvimento, alocação de pessoal e coordenação de políticas de operações cibernéticas, normas de desempenho, planos e pacotes de aprovação com os devidos tomadores de decisão internos e/ou externos.
T0630	Incorporar ativos de inteligência ao projeto geral dos planos de operações cibernéticas.
T0631	Coordenar a alocação de recursos dos ativos de coleta relativos aos requisitos de coleta priorizados com leads de disciplina de coleta.
T0632	Coordenar a inclusão do plano de coleta na documentação adequada.
T0633	Coordenar a verificação de destino com parceiros apropriados.
T0634	Retardar ou redirecionar ativos e recursos de coleta direta.
T0635	Manter coordenação com parceiros de inteligência e defesa cibernética para obter informações essenciais relevantes.
T0636	Manter coordenação com planejadores de inteligência para garantir que os gerentes de coleta recebam requisitos de informações.
T0637	Manter coordenação com a equipe de planejamento de inteligência para avaliar a capacidade de realizar as tarefas de inteligência que lhes foram atribuídas.
T0638	Coordenar, produzir e rastrear os requisitos de inteligência.
T0639	Coordenar, sincronizar e elaborar seções de inteligência aplicáveis referentes aos planos de operações cibernéticas.
T0640	Usar estimativas de inteligência para combater possíveis ações do destino.
T0641	Criar estratégias abrangentes de exploração que identifiquem vulnerabilidades técnicas ou operacionais exploráveis.
T0642	Manter todos cientes das estruturas internas e externas, pontos fortes e empregabilidade de pessoal em organizações cibernéticas.
T0643	Implantar ferramentas para um sistema de destino e utilizá-las assim que forem implantadas (ex.: backdoors, sniffers).

ID da Tarefa	Descrição da Tarefa
T0644	Detectar explorações contra redes e hosts direcionados e reagir apropriadamente.
T0645	Determinar o curso de ação para abordar mudanças nos objetivos, orientação e ambiente operacional.
T0646	Determinar o gerenciamento de bancos de dados de páginas na Web, bibliotecas e armazenamento de coletas existentes.
T0647	Determinar como os fatores identificados afetam a forma e a função da arquitetura de tarefas, coleta, processamento, exploração e disseminação.
T0648	Determinar indicadores (ex.: medidas de eficácia) mais adequados a objetivos específicos de operação cibernética.
T0649	Determinar organizações e/ou escalões com autoridade de coleta referente a todos os ativos de coleta acessíveis.
T0650	Determinar quais são as tecnologias usadas por um determinado destino.
T0651	Desenvolver um método para comparar relatórios de coleta com requisitos pendentes para identificar lacunas de informações.
T0652	Desenvolver materiais de inteligência de todas as fontes.
T0653	Aplicar técnicas analíticas para obter mais informações de destino.
T0654	Desenvolver e manter planos deliberados e/ou de crise.
T0655	Desenvolver e revisar orientações específicas de operações cibernéticas para integração em atividades de planejamento mais amplas.
T0656	Desenvolver e revisar orientações de inteligência para integração no apoio ao planejamento e execução de operações cibernéticas.
T0657	Desenvolver instruções de coordenação por disciplina de coleta para cada fase de uma operação.
T0658	Desenvolver planos e orientações sobre operações cibernéticas para garantir que as decisões de execução e alocação de recursos estejam alinhadas com os objetivos da organização.
T0659	Desenvolver suporte de inteligência detalhado para os requisitos de operações cibernéticas.
T0660	Desenvolver requisitos de informações necessários para responder às solicitações de informações prioritárias.
T0661	Desenvolver medidas de efetividade e de desempenho.
T0662	Alocar ativos de coleta com base na orientação, prioridades e/ou ênfase operacional da liderança.
T0663	Desenvolver a avaliação de eficácia das munições ou materiais de avaliação operacional.
T0664	Desenvolver novas técnicas para obter e manter acesso aos sistemas de destino.
T0665	Desenvolver ou participar no desenvolvimento de normas para fornecer, solicitar e/ou obter suporte de parceiros externos para sincronizar operações cibernéticas.
T0666	Desenvolver ou modelar estratégias, políticas e atividades internacionais de engajamento cibernético para atender aos objetivos da organização.
T0667	Desenvolver potenciais cursos de ação.
T0668	Desenvolver procedimentos para fornecer feedback aos gestores de coleta, gestores de ativos e centros de processamento, exploração e disseminação.
T0669	Desenvolver estratégias e processos para planejamento, operações e desenvolvimento de capacidades de parceiros.
T0670	Desenvolver, implementar e recomendar mudanças nos procedimentos e políticas de planejamento adequados.
T0671	Desenvolver, manter e avaliar acordos de segurança de cooperação cibernética com parceiros externos.
T0672	Elaborar, documentar e validar a estratégia de operação cibernética e os documentos de planejamento.

ID da Tarefa	Descrição da Tarefa
T0673	Divulgar relatórios para informar os principais decisores sobre questões de coleta.
T0674	Disseminar mensagens de tarefa e planos de coleta.
T0675	Realizar e documentar uma avaliação dos resultados da coleta por meio de procedimentos estabelecidos.
T0676	Elaborar requisitos de coleta e produção de inteligência cibernética.
T0677	Editar ou executar scripts simples (ex.: Perl, VBScript) nos sistemas Windows e UNIX.
T0678	Engajar os clientes para que entendam suas próprias necessidades e aspirações quanto à inteligência.
T0679	Garantir que os esforços de planejamento operacional sejam efetivamente transicionados para as operações atuais.
T0680	Assegurar que as atividades de planejamento de inteligência sejam integradas e sincronizadas com cronogramas de planejamento operacional.
T0681	Estabelecer caminhos alternativos de processamento, exploração e divulgação para resolver questões ou problemas identificados.
T0682	Validar a ligação que existe entre solicitações de coleta, requisitos críticos de informações e requisitos prioritários de inteligência solicitados pela liderança.
T0683	Estabelecer atividades de gestão de processamento, exploração e disseminação utilizando orientações e/ou procedimentos aprovados.
T0684	Estimar os efeitos operacionais gerados através de atividades cibernéticas.
T0685	Avaliar os processos de tomada de decisão referentes a ameaças.
T0686	Identificar vulnerabilidades de ameaças.
T0687	Identificar ameaças às vulnerabilidades da Força Azul.
T0688	Avaliar os recursos disponíveis para alcançar os efeitos desejados e recomendar soluções eficientes.
T0689	Avaliar até que ponto as informações coletadas e/ou produzidas de inteligência satisfazem as solicitações de informações.
T0690	Avaliar as estimativas de inteligência para apoiar o ciclo de planejamento.
T0691	Avaliar as condições que afetam o emprego dos recursos disponíveis de inteligência cibernética.
T0692	Gerar e avaliar a eficácia das estratégias de análise de rede.
T0693	Avaliar até que ponto as operações de coleta estão sincronizadas com os requisitos operacionais.
T0694	Avaliar a eficácia das operações de coleta em relação ao que foi planejado para este propósito.
T0695	Examinar metadados e conteúdos relacionados à interceptação, tendo uma compreensão da significância das redes de destino.
T0696	Explorar dispositivos de rede, dispositivos de segurança e/ou terminais ou ambientes usando vários métodos ou ferramentas.
T0697	Facilitar a habilitação do acesso por meios físicos e/ou sem fio.
T0698	Facilitar continuamente a atualização da inteligência, vigilância e visualização para gerentes de quadros operacionais comuns.
T0699	Facilitar interações entre os principais decisores de parceiros internos e externos para sincronizar e integrar os cursos de ação em apoio aos objetivos.
T0700	Facilitar o compartilhamento de "melhores práticas" e "lições aprendidas" em toda a comunidade de operações cibernéticas.
T0701	Colaborar com os desenvolvedores, transmitindo conhecimento técnico sobre ferramentas e redes de destino visando aprimorar o desenvolvimento de ferramentas.

ID da Tarefa	Descrição da Tarefa
T0702	Formular estratégias de coleta baseadas no conhecimento dos recursos disponíveis de disciplina de inteligência e métodos de coleta que alinham recursos de coleta multidisciplinar e acessos aos destinos e seus observáveis.
T0703	Coletar e analisar dados (ex.: medidas de eficácia) para determinar a eficácia e fornecer relatórios para atividades subsequentes.
T0704	Incorporar as operações cibernéticas e os planos de suporte de segurança de comunicações aos objetivos da organização.
T0705	Incorporar inteligência e contrainteligência para apoiar o desenvolvimento de planos.
T0706	Reunir informações sobre redes através de técnicas tradicionais e alternativas, (ex.: análise de redes sociais, encadeamento de chamadas, análise de tráfego.)
T0707	Gerar pedidos de informação.
T0708	Identificar táticas de ameaça e metodologias.
T0709	Identificar todos os recursos e limitações disponíveis de inteligência de parceiros que suportem operações cibernéticas.
T0710	Identificar e avaliar os recursos, requisitos e vulnerabilidades críticas de ameaças.
T0711	Identificar, redigir, avaliar e priorizar os requisitos relevantes de inteligência ou informação.
T0712	Identificar e gerenciar prioridades de cooperação em segurança com parceiros externos.
T0713	Identificar e encaminhar requisitos de inteligência para fins de designação de requisitos prioritários de informações.
T0714	Identificar fóruns de colaboração que possam servir como mecanismos para coordenar processos, funções e resultados com organizações especificadas e grupos funcionais.
T0715	Identificar lacunas de coleta e potenciais estratégias de coleta em relação às informações de destino.
T0716	Identificar requisitos e procedimentos de coordenação com as autoridades de coleta designadas.
T0717	Identificar elementos-alvo críticos.
T0718	Identificar lacunas e falhas de inteligência.
T0719	Identificar lacunas e deficiências cibernéticas para o planejamento operacional cibernético.
T0720	Identificar lacunas em nossa compreensão da tecnologia de destino e desenvolver abordagens inovadoras de coleta.
T0721	Identificar questões ou problemas que possam interromper e/ou degradar a eficácia da arquitetura de processamento, exploração e divulgação.
T0722	Identificar os componentes da rede e sua funcionalidade para permitir a análise e o desenvolvimento de destino.
T0723	Identificar potenciais disciplinas de coleta para aplicação conforme os requisitos prioritários de informações.
T0724	Identificar pontos potenciais de força e vulnerabilidade dentro de uma rede.
T0725	Identificar e mitigar riscos à capacidade de gerenciamento de coleta para apoiar o plano, as operações e o ciclo de destino.
T0726	Identificar a necessidade, o escopo e o prazo para a produção derivada da preparação do ambiente de inteligência aplicável.
T0727	Identificar, localizar e rastrear destinos por meio de técnicas de análise geoespacial.
T0728	Fornecer informações ou desenvolver cursos de ação com base em fatores de ameaça.
T0729	Informar os parceiros externos sobre os efeitos potenciais de políticas e orientações novas ou revisadas sobre as atividades de parceria de operações cibernéticas.
T0730	Informar as partes interessadas (ex.: gestores de coleta, gestores de ativos, centros de processamento, exploração e divulgação) dos resultados de avaliação utilizando procedimentos estabelecidos.

ID da Tarefa	Descrição da Tarefa
T0731	Iniciar solicitações para orientar o trabalho e auxiliar na gestão da coleta.
T0732	Integrar os esforços de planejamento cibernético/segmentação com outras organizações.
T0733	Interpretar as avaliações de preparações ambientais para determinar um curso de ação.
T0734	Emitir pedidos de informação.
T0735	Liderar e coordenar o suporte de inteligência ao planejamento operacional.
T0736	Liderar ou permitir operações de exploração em apoio aos objetivos da organização e aos requisitos de destino.
T0737	Vincular os requisitos de coleta prioritária aos ativos e recursos ideais.
T0738	Manter a consciencialização sobre os avanços nas tecnologias de hardware e software (ex.: participar de treinamentos ou conferências, leitura) e suas potenciais implicações.
T0739	Manter relacionamentos com parceiros internos e externos envolvidos em planejamento cibernético ou áreas relacionadas.
T0740	Manter a conscientização situacional e a funcionalidade da infraestrutura operacional orgânica.
T0741	Manter a conscientização situacional sobre os requisitos de inteligência cibernética e do trabalho associado.
T0742	Manter a conscientização situacional das capacidades e atividades dos parceiros.
T0743	Manter a consciencialização situacional para determinar se as mudanças no ambiente operacional requerem revisão do plano.
T0744	Manter listas de destino (ou seja, RTL, JTL, CTL, etc.).
T0745	Fazer recomendações para orientar a coleta em suporte às necessidades do cliente.
T0746	Modificar os requisitos de coleta conforme necessário.
T0747	Monitorar e avaliar operações cibernéticas integradas para identificar oportunidades para atender aos objetivos da organização.
T0748	Monitorar e relatar mudanças nas disposições de ameaças, atividades, táticas, capacidades, objetivos, etc., conforme se relacionam aos conjuntos de problemas de alerta de operações cibernéticas designados.
T0749	Monitorar e informar sobre atividades de ameaça validadas.
T0750	Monitorar a conclusão dos esforços de coleta realocados.
T0751	Monitorar sites de código aberto para conteúdo hostil direcionado a interesses organizacionais ou a parceiros.
T0752	Monitorar o ambiente operacional e informar sobre atividades contraditórias que preenchem os requisitos prioritários de informações da liderança.
T0753	Monitorar o status operacional e a eficácia da arquitetura de processamento, exploração e divulgação.
T0754	Monitorar as redes de destino para fornecer indicações e avisos sobre alterações de comunicações de destino ou falhas de processamento.
T0755	Monitorar o ambiente operacional em busca de fatores potenciais e riscos para o processo de gerenciamento da operação de coleta.
T0756	Operar e manter sistemas automatizados para obter e manter o acesso aos sistemas de destino.
T0757	Otimizar o mix de ativos e recursos de coleta para aumentar a eficácia e a eficiência contra informações essenciais associadas a requisitos prioritários de inteligência.
T0758	Produzir inteligência de operações cibernéticas oportunas, compiladas e de todas as fontes e/ou produtos de inteligência de advertências e indicações (ex.: avaliações de ameaças, briefings, estudos de inteligência, estudos sobre países).
T0759	Contribuir para a revisão e refinamento das políticas para incluir avaliações das consequências de endossar ou não endossar tal norma.

ID da Tarefa	Descrição da Tarefa
T0760	Fornecer conhecimento específico sobre o assunto para equipes de planejamento, grupos de coordenação e forças-tarefa, conforme necessário.
T0761	Fornecer conhecimento e suporte a fóruns de planejamento/desenvolvimento e grupos de trabalho, conforme apropriado.
T0763	Realizar esforços de planejamento estratégico de longo alcance com parceiros internos e externos em atividades cibernéticas.
T0764	Fornecer conhecimento específico sobre determinado assunto para planejar esforços com parceiros internos e externos de operações cibernéticas.
T0765	Fornecer conhecimentos específicos para o desenvolvimento de exercícios.
T0766	Propor uma política que regule as interações com grupos de coordenação externa.
T0767	Realizar análise de conteúdo e/ou de metadados para atender aos objetivos da organização.
T0768	Realizar atividades cibernéticas para degradar/remover informações residentes em computadores e redes de computadores.
T0769	Realizar atividades de automação direcionadas.
T0770	Caracterizar sites.
T0771	Fornecer conhecimentos específicos para caracterizações de sites.
T0772	Preparar e fornecer conhecimentos específicos sobre exercícios.
T0773	Priorizar os requisitos de coleta para plataformas de coleta com base nos recursos da plataforma.
T0774	Processar dados exfiltrados para análise e/ou divulgação aos clientes.
T0775	Produzir reconstruções de rede.
T0776	Produzir produtos de análise de sistema de destino.
T0777	Executar o perfil dos administradores de rede ou sistema e suas atividades.
T0778	Providenciar o perfil do destino e suas atividades.
T0779	Fornecer assessoria/assistência aos tomadores de decisão de operações e inteligência com redesignação de ativos e recursos de coleta em resposta a situações operacionais dinâmicas.
T0780	Fornecer assessoria e defesa da causa para promover o planejamento de coletas como componente integrado aos planos estratégicos de campanha e outros planos adaptativos.
T0781	Fornecer recomendações precisas e de reengajamento.
T0782	Fornecer análises e suporte para avaliação de eficácia.
T0783	Fornecer suporte de inteligência atual a partes interessadas internas/externas críticas, conforme apropriado.
T0784	Fornecer orientações e conselhos cibernéticos sobre a entrada de dados referentes aos planos de suporte de inteligência.
T0785	Fornecer avaliação e feedback necessários para melhorar a produção de inteligência, relatórios de inteligência, requisitos de coleta e operações.
T0786	Fornecer informações e avaliações com o propósito de informar a liderança e clientes; desenvolver e aprimorar os objetivos; apoiar o planejamento e a execução das operações; e avaliar os efeitos das operações.
T0787	Fornecer informações para o desenvolvimento e refinamento dos objetivos, prioridades, estratégias, planos e programas de operações cibernéticas.
T0788	Fornecer informações e auxiliar nas avaliações de eficácia pós-ação.
T0789	Fornecer informações e auxiliar no desenvolvimento de planos e orientações.
T0790	Fornecer informações para direcionamento das avaliações de eficácia para a aceitação da liderança.
T0791	Fornecer informações aos elementos administrativos e logísticos de um plano de apoio operacional.

ID da Tarefa	Descrição da Tarefa
T0792	Fornecer análise de inteligência e suporte a exercícios designados, atividades de planejamento e operações sensíveis ao tempo.
T0793	Fornecer suporte de eficácia a exercícios designados e/ou operações sensíveis ao tempo.
T0794	Fornecer recomendações para operações e reengajamento.
T0795	Fornecer suporte de planejamento entre parceiros internos e externos.
T0796	Fornecer informações de geolocalização acionáveis em tempo real.
T0797	Fornecer recomendações sobre destino que atendam aos objetivos de liderança.
T0798	Fornecer produtos direcionados e suporte de segmentação conforme designado.
T0799	Fornecer suporte de segmentação sensível ao tempo.
T0800	Fornecer aviso oportuno de intenções ou atividades iminentes ou hostis que possam afetar objetivos, recursos ou capacidades da organização.
T0801	Recomendar o refinamento, adaptação, término e execução de planos operacionais, conforme apropriado.
T0802	Analisar fontes de informação adequadas para determinar a validade e a relevância das informações coletadas.
T0803	Reconstruir redes em formato de diagrama ou relatório.
T0804	Registrar as atividades de coleta de informações e/ou preparação do ambiente em relação aos destinos durante as operações criadas para obter efeitos cibernéticos.
T0805	Reportar eventos e invasões significativas derivadas da inteligência.
T0806	Solicitar o processamento específico da disciplina, exploração e disseminação das informações coletadas, usando os ativos e recursos de coleta da disciplina de acordo com as orientações e/ou procedimentos aprovados.
T0807	Pesquisar tendências de comunicação em tecnologias emergentes (em redes de computadores e telefonia, satélite, cabo e sem fio) em fontes abertas e classificadas.
T0808	Revisar e compreender os objetivos de liderança organizacional e orientação para o planejamento.
T0809	Revisar os recursos dos ativos de coleta alocados.
T0810	Revisar as orientações de coleta de inteligência para precisão/aplicabilidade.
T0811	Revisar a lista de requisitos de coleta priorizados e informações essenciais.
T0812	Revisar e atualizar o plano de coleta abrangente, conforme necessário.
T0813	Revisar, aprovar, priorizar e encaminhar requisitos operacionais para pesquisa, desenvolvimento e/ou aquisição de recursos cibernéticos.
T0814	Revisar a matriz de coleta com base na disponibilidade de ativos e recursos ideais.
T0815	Higienizar e minimizar informações para proteger fontes e métodos.
T0816	Analisar o escopo do esforço de planejamento de inteligência cibernética.
T0817	Servir como um canal de informações de equipes parceiras, identificando especialistas no assunto que possam auxiliar na investigação de situações complexas ou incomuns.
T0818	Servir como contato para parceiros externos.
T0819	Solicitar e gerenciar até o final do processo, o feedback dos solicitantes sobre a qualidade, o prazo e a eficácia da coleta em relação aos requisitos de coleta.
T0820	Especificar alterações no plano de coleta e/ou ambiente operacional que exijam redefinição de tarefas ou redirecionamento de ativos e recursos de coleta.
T0821	Especificar coletas e/ou tarefas específicas da disciplina que devem ser executadas a curto prazo.
T0822	Enviar solicitações de informações à seção de gerenciamento de requisitos de coleta para processamento como solicitações de coleta.
T0823	Enviar ou responder a pedidos de eliminação de conflitos das operações cibernéticas.
T0824	Apoiar a identificação e documentação de efeitos colaterais.

ID da Tarefa	Descrição da Tarefa
T0825	Sincronizar as atividades de engajamento internacional cibernético e os requisitos de recursos associados, conforme apropriado.
T0826	Sincronizar partes cibernéticas de planos de cooperação em segurança.
T0827	Sincronizar o emprego integrado de todos os ativos de coleta de inteligência orgânica e parceiros disponíveis usando recursos e técnicas de colaboração em curso.
T0828	Testar e avaliar ferramentas desenvolvidas localmente para uso operacional.
T0829	Testar ferramentas e técnicas internas desenvolvidas, em relação às ferramentas de destino.
T0830	Rastrear o status das solicitações de informações, incluindo as que foram processadas como solicitações de coleta e requisitos de produção, utilizando procedimentos estabelecidos.
T0831	Traduzir solicitações de coleta em requisitos de coleta específicos de disciplinas aplicáveis.
T0832	Usar resultados de feedback (ex.: lições aprendidas) para identificar oportunidades para melhorar a eficiência e eficácia do gerenciamento da coleta.
T0833	Validar solicitações de informações de acordo com critérios estabelecidos.
T0834	Trabalhar em estreita colaboração com planejadores, analistas de inteligência e gerentes de coleta para garantir que os requisitos de inteligência e planos de coleta sejam precisos e atualizados.
T0835	Trabalhar em estreita colaboração com planejadores, analistas e gerentes de coleta para identificar lacunas de inteligência e garantir que os requisitos de inteligência sejam precisos e atualizados.
T0836	Documentar as lições aprendidas que transmitem os resultados de eventos e/ou exercícios.
T0837	Aconselhar gestores e operadores sobre questões linguísticas e culturais que impactam os objetivos da organização.
T0838	Analisar e processar informações utilizando linguagem e/ou conhecimento cultural.
T0839	Avaliar, documentar e aplicar a motivação e/ou quadro de referência de um destino para facilitar as oportunidades de análise, segmentação e coleta.
T0840	Colaborar em linhas organizacionais internas e/ou externas para melhorar a coleta, análise e divulgação.
T0841	Realizar pesquisas de destinos de todas as fontes para incluir o uso de materiais de código aberto no idioma de destino.
T0842	Realizar análises de comunicações de destino para identificar informações essenciais em apoio aos objetivos da organização.
T0843	Realizar a revisão de qualidade e fornecer feedback sobre materiais transcritos ou traduzidos.
T0844	Avaliar e interpretar metadados para identificar padrões, anomalias ou eventos, otimizando, portanto, a segmentação, análise e processamento.
T0845	Identificar táticas de ameaça cibernética e metodologias.
T0846	Identificar as comunicações de destino dentro da rede global.
T0847	Manter-se ciente das ferramentas de comunicação de destino, técnicas e características das redes de comunicação de destino (ex.: capacidade, funcionalidade, percursos, nodes críticos) e suas potenciais implicações para segmentação, coleta e análise.
T0848	Fornecer feedback aos gestores de coleta para melhorar a coleta e análise futura.
T0849	Realizar a identificação de idioma estrangeiro e dialetos em dados iniciais de origem.
T0850	Realizar ou oferecer suporte às análises e mapeamentos técnicos de rede.
T0851	Fornecer requisitos e feedback para otimizar o desenvolvimento de ferramentas de processamento de idiomas.
T0852	Realizar a análise e documentação das redes sociais conforme apropriado.
T0853	Digitalizar, identificar e priorizar material gráfico ou de voz (incluindo comunicações máquina a máquina) na língua do alvo.

ID da Tarefa	Descrição da Tarefa
T0854	Oferecer dicas críticas ou sensíveis ao tempo para clientes apropriados.
T0855	Transcrever materiais de voz de destino na língua de destino.
T0856	Traduzir (ex.: literalmente, na essência e/ou resumos) o material gráfico de destino.
T0857	Traduzir (literalmente, na essência e/ou resumos) material de voz de destino.
T0858	Identificar terminologia de língua estrangeira dentro de programas de computador (ex.: comentários, nomes variáveis).
T0859	Fornecer suporte à análise de idiomas em tempo real (ex.: operações ao vivo).
T0860	Identificar terminologia relacionada à tecnologia/cibernética no idioma de destino.
T0861	Trabalhar com o assessor jurídico, relações exteriores e empresas para garantir que os serviços existentes e novos estejam em compliance com as obrigações de privacidade e segurança de dados.
T0862	Trabalhar com a assessoria e gestão jurídica, departamentos e comitês-chave para garantir que a organização tenha e mantenha o consentimento adequado de privacidade e confidencialidade, formulários de autorização e avisos de informações e materiais, que reflitam as práticas e requisitos jurídicos atuais da organização.
T0863	Coordenar com os órgãos reguladores adequados para garantir que programas, políticas e procedimentos envolvendo direitos civis, liberdades civis e considerações de privacidade sejam abordados de forma integrada e abrangente.
T0864	Manter contato com órgãos reguladores e credenciadores.
T0865	Trabalhar com as relações exteriores para desenvolver relacionamentos com reguladores e outros funcionários do governo responsáveis por questões de privacidade e segurança de dados.
T0866	Manter conhecimento atualizado das leis de privacidade federais e estaduais aplicáveis e normas de credenciamento, e monitorar os avanços nas tecnologias de privacidade da informação para garantir a adaptação e o compliance da organização.
T0867	Assegurar-se de que todos os processos e/ou bancos de dados estejam registrados junto às autoridades locais de privacidade/proteção de dados, quando necessário.
T0868	Trabalhar com equipes de negócios e a administração sênior para garantir a conscientização sobre as "melhores práticas" para questões de privacidade e segurança de dados.
T0869	Trabalhar com a gerência sênior da organização para estabelecer um Comitê de Supervisão da Privacidade em toda a organização.
T0870	Exercer um papel de liderança para as atividades do Comitê de Supervisão de Privacidade
T0871	Colaborar em políticas e procedimentos de privacidade cibernética e segurança
T0872	Colaborar com o pessoal de cibersegurança no processo de avaliação de riscos de segurança para abordar o compliance de privacidade e mitigação de riscos
T0873	Manter contato com a Gestão Sênior visando desenvolver planos estratégicos para a coleta, uso e compartilhamento de informações de forma a maximizar o seu valor ao cumprir as normas de privacidade aplicáveis
T0874	Fornecer orientação estratégica aos dirigentes corporativos sobre recursos e tecnologia da informação.
T0875	Auxiliar o Diretor de Segurança no desenvolvimento e implementação de uma infraestrutura de informações
T0876	Coordenar com o Diretor de Conformidade Corporativa sobre os procedimentos para documentar e relatar autodivulgações de qualquer evidência de violações de privacidade.
T0877	Trabalhar em colaboração com unidades organizacionais aplicáveis no monitoramento dos direitos de acesso do consumidor às informações.
T0878	Servir como contato para assuntos de privacidade da informação para usuários de sistemas de tecnologia

ID da Tarefa	Descrição da Tarefa
T0879	Servir de contato para o departamento de sistemas de informação
T0880	Desenvolver materiais de treinamento sobre privacidade e outras comunicações para aumentar a compreensão dos funcionários sobre as políticas de privacidade da empresa, práticas e procedimentos de manipulação de dados e obrigações legais
T0881	Supervisionar, direcionar, oferecer e garantir a realização de treinamento inicial e orientação sobre privacidade a todos os funcionários, voluntários, contratados, alianças, associados de negócios e terceiros, conforme apropriado.
T0882	Realizar atividades de treinamento e conscientização sobre privacidade
T0883	Trabalhar com as Relações Exteriores para desenvolver relacionamentos com organizações de consumidores e outras ONGs com interesse em questões de privacidade e segurança de dados — e gerenciar a participação da empresa em eventos públicos relacionados à privacidade e segurança de dados.
T0884	Trabalhar com a administração da organização, departamento jurídico e outras partes relacionadas para representar os interesses de privacidade de informações da organização com partes externas, incluindo órgãos governamentais, que se comprometem a adotar ou alterar a legislação, regulamentação ou padrão de privacidade.
T0885	Relatar periodicamente sobre o status do programa de privacidade para o Conselho, CEO ou outro indivíduo ou comitê responsável
T0886	Trabalhar com as Relações Exteriores para responder à imprensa e a outros questionamentos sobre a preocupação com os dados dos consumidores e funcionários
T0887	Proporcionar liderança para o programa de privacidade da organização
T0888	Direcionar e supervisionar especialistas em privacidade e coordenar programas de privacidade e segurança de dados com executivos seniores, em âmbito global, para garantir a consistência em toda a organização
T0889	Garantir o cumprimento das práticas de privacidade e a aplicação consistente de sanções por descumprimento das políticas de privacidade para todos os indivíduos na força de trabalho da organização, força de trabalho estendida e para todos os associados em cooperação com Recursos Humanos, o dirigente de segurança da informação, administração e assessoria jurídica, conforme for o caso.
T0890	Desenvolver sanções adequadas por não cumprimento às políticas e procedimentos de privacidade corporativa
T0891	Resolver alegações de descumprimento das políticas de privacidade corporativa ou aviso de práticas de informação
T0892	Desenvolver e coordenar uma estrutura de gestão de risco e compliance referente à privacidade.
T0893	Fazer uma revisão abrangente dos projetos de privacidade e dados da empresa e garantir que estejam consistentes com as metas e políticas de privacidade e segurança de dados da empresa.
T0894	Desenvolver e gerenciar procedimentos corporativos para garantir que o desenvolvimento de novos produtos e serviços seja consistente com as políticas de privacidade e obrigações legais da empresa
T0895	Estabelecer um processo para receber, documentar, rastrear, investigar e agir, frente a todas as reclamações relativas às políticas e procedimentos de privacidade da organização.
T0896	Estabelecer com a administração e operações um mecanismo para rastrear o acesso a informações protegidas sobre saúde, dentro da competência da organização e conforme exigido por lei, e permitir que indivíduos qualificados analisem ou recebam um relatório sobre tal atividade.

ID da Tarefa	Descrição da Tarefa
T0897	Oferecer liderança no planejamento, design e avaliação de projetos relacionados à privacidade e segurança
T0898	Estabelecer um programa interno de auditoria de privacidade
T0899	Revisar periodicamente o programa de privacidade considerando mudanças nas leis, políticas ou regulamentos da empresa
T0900	Fornecer orientação sobre desenvolvimento e auxiliar na identificação, implementação e manutenção das políticas e procedimentos sobre privacidade das informações organizacionais em coordenação com a administração, gerência e assessoria jurídica da organização.
T0901	Garantir que o uso de tecnologias mantenha, e não destrua, as proteções de privacidade no uso, coleta e divulgação de informações pessoais.
T0902	Monitorar o desenvolvimento e as operações de sistemas para estarem em compliance com a segurança e privacidade
T0903	Realizar avaliações de impacto de privacidade referentes às regras propostas sobre a privacidade das informações pessoais, incluindo o tipo de informação e o número de pessoas afetadas.
T0904	Realizar avaliações periódicas sobre o impacto das informações sobre privacidade e atividades contínuas de monitoramento de compliance, em coordenação com outras funções e avaliações operacionais da organização de aderência ao compliance.
T0905	Analisar todos os planos de segurança da informação relacionados ao sistema para garantir o alinhamento das práticas de segurança com a privacidade.
T0906	Trabalhar com todos os funcionários da organização envolvidos com qualquer aspecto da liberação de informações protegidas para garantir a coordenação com as políticas, procedimentos e requisitos legais da organização
T0907	Responsabilizar-se e administrar solicitações individuais de liberação ou divulgação de informações pessoais e/ou protegidas
T0908	Desenvolver e gerenciar procedimentos para vetar e auditar fornecedores para o cumprimento das políticas de privacidade e segurança de dados e requisitos legais
T0909	Participar da implementação e do monitoramento contínuo de compliance referente a todos os acordos de parceiros comerciais e associados de negócios, para garantir que todas as questões, requisitos e responsabilidades de privacidade sejam abordados
T0910	Agir como, ou trabalhar com a assessoria jurídica quanto aos contratos de parceiros de negócios
T0911	Mitigar efeitos de determinado uso ou divulgação de informações pessoais por funcionários ou parceiros de negócios
T0912	Desenvolver e aplicar procedimentos de ação corretiva
T0913	Decidir sobre um curso de ação referente a todas as reclamações sobre políticas e procedimentos relativos à privacidade da organização em coordenação e colaboração com outras funções semelhantes e, quando necessário, com a assessoria jurídica.
T0914	Aderir ao programa de conformidade de privacidade da organização, trabalhando em estreita colaboração com o Dirigente de Privacidade, Diretor de Segurança da Informação e outros líderes empresariais para garantir o cumprimento das leis e regulamentos federais e estaduais sobre privacidade
T0915	Identificar e corrigir possíveis lacunas de compliance da empresa e/ou áreas de risco para garantir o compliance às normas de privacidade.
T0916	Gerenciar incidentes e violações de privacidade juntamente com o Dirigente de Privacidade, Diretor de Segurança da Informação, assessoria jurídica e as unidades de negócios

ID da Tarefa	Descrição da Tarefa
T0917	Coordenar medidas com o Diretor de Segurança da Informação para garantir o alinhamento das práticas de segurança e privacidade.
T0918	Estabelecer, implementar e manter políticas e procedimentos em toda a organização para cumprir as normas de privacidade
T0919	Assegurar que a empresa mantenha avisos de privacidade e confidencialidade adequados, além de materiais, formulários de consentimento e autorização
T0920	Desenvolver e manter comunicações e treinamentos adequados para promover e instruir todos os integrantes da força de trabalho e membros do conselho sobre questões e requisitos de compliance de privacidade, e as consequências se houver descumprimento.
T0921	Determinar os requisitos dos parceiros de negócios relacionados ao programa de privacidade da organização.
T0922	Estabelecer e administrar um processo para recebimento, documentação, rastreamento, investigação e medidas corretivas, conforme apropriado, referentes às reclamações sobre as políticas e procedimentos de privacidade da empresa.
T0923	Colaborar com as agências reguladoras competentes e outras entidades jurídicas, além dos dirigentes da organização, em qualquer revisão ou investigação sobre compliance.
T0924	Realizar atividades contínuas de monitoramento de compliance sobre privacidade.
T0925	Monitorar avanços em tecnologias sobre privacidade das informações para garantir a aderências e o compliance organização.
T0926	Desenvolver ou auxiliar no desenvolvimento de materiais de treinamento de privacidade e outras comunicações para aumentar a compreensão dos funcionários sobre políticas de privacidade da empresa, práticas e procedimentos de tratamento de dados e obrigações legais.
T0927	Nomear e orientar uma equipe de especialistas em segurança de TI.
T0928	Colaborar com as principais partes interessadas para estabelecer um programa de gestão de risco de cibersegurança.
T0929	Identificar e atribuir indivíduos a funções específicas associadas à execução da Estrutura de Gestão de Riscos.
T0930	Estabelecer uma estratégia de gestão de risco para a organização que inclua uma determinação de tolerância ao risco.
T0931	Identificar as missões, funções de negócios e processos de missão/negócios aos quais o sistema oferecerá suporte.
T0932	Identificar as partes interessadas em segurança para que se envolvam no desenvolvimento, implementação, operação e manutenção de um sistema.
T0933	Identificar as partes interessadas em segurança para que se envolvam no desenvolvimento, implementação, operação e manutenção de um sistema.
T0934	Identificar os ativos das partes interessadas que requerem proteção.
T0935	Realizar uma avaliação inicial de risco dos ativos das partes interessadas que deve ser atualizada continuamente.
T0936	Definir as necessidades de proteção e requisitos de segurança das partes interessadas.
T0937	Determinar a implantação de um sistema dentro da arquitetura corporativa.
T0938	Identificar controles comuns em toda a organização que estão disponíveis para serem herdados pelos sistemas organizacionais.
T0939	Realizar uma categorização de segurança de segundo nível para sistemas organizacionais com o mesmo nível de impacto.
T0940	Determinar o limite de determinado sistema.
T0941	Identificar os requisitos de segurança alocados em determinado sistema e na organização.

ID da Tarefa	Descrição da Tarefa
T0942	Identificar os tipos de informações a serem processadas, armazenadas ou transmitidas por um sistema.
T0943	Categorizar o sistema e documentar os resultados de categorização de segurança como parte dos requisitos do sistema.
T0944	Descrever as características de um sistema.
T0945	Registrar o sistema junto aos escritórios de gestão/programa organizacional apropriados.
T0946	Selecionar os controles de segurança para determinado sistema e documentar a descrição funcional das implementações de controle que foram idealizadas em um plano de segurança.
T0947	Desenvolver uma estratégia para monitorar a eficácia do controle de segurança; coordenar a estratégia de nível de sistema com a organização e a estratégia de monitoramento em nível de processo de missão/negócios.
T0948	Revisar e aprovar planos de segurança.
T0949	Implementar os controles de segurança especificados em um plano de segurança ou outra documentação do sistema.
T0950	Documentar mudanças na implementação planejada de controle de segurança e estabelecer a linha de base de configuração para determinado sistema.
T0951	Desenvolver, revisar e aprovar um plano para avaliar os controles de segurança em um sistema e na organização.
T0952	Avaliar os controles de segurança de acordo com os procedimentos de avaliação definidos em um plano de avaliação de segurança.
T0953	Preparar um relatório de avaliação de segurança documentando os problemas, resultados e recomendações derivados da avaliação do controle de segurança.
T0954	Implementar um curso de ação inicial de remediação referente aos controles de segurança, com base nas conclusões e recomendações de um relatório de avaliação de segurança; reavaliar controles remediados.
T0955	Preparar um plano de ação e marcos de referência, tendo como base as conclusões e recomendações provenientes de um relatório de avaliação de segurança, excluindo qualquer medida tomada como remediação.
T0956	Montar um pacote de autorização para ser enviado a um dirigente autorizado para adjudicação.
T0957	Determinar o risco decorrente da operação ou uso de um sistema ou da provisão ou uso de controles comuns.
T0958	Identificar e implementar um curso de ação preferido em resposta a determinado risco.
T0959	Determinar se o risco da operação, o uso do sistema ou o provisionamento ou uso dos controles comuns são aceitáveis.
T0960	Monitorar as mudanças em um sistema e seu ambiente de operação.
T0961	Avaliar se os controles de segurança utilizados e herdados pelo sistema estão em conformidade com as estratégias de monitoramento definidas pela organização.
T0962	Responder ao risco com base nos resultados das atividades de monitoramento contínuo, da avaliação de risco, e dos itens pendentes em um plano de ação e marcos de referência.
T0963	Atualizar um plano de segurança, relatório de avaliação de segurança e plano de ação e marcos de referência com base nos resultados do processo de monitoramento contínuo.
T0964	Informar a situação de segurança de um sistema (incluindo a eficácia dos controles de segurança) a um dirigente autorizado, de maneira contínua, e de acordo com a estratégia de monitoramento.
T0965	Analisar continuamente a situação de segurança de um sistema (incluindo a eficácia dos controles de segurança) para determinar se o risco permanece aceitável.

ID da Tarefa	Descrição da Tarefa
T0966	Implementar uma estratégia de descarte do sistema que execute as ações necessárias quando um sistema for removido do serviço.
T0967	Patrocinar e promover um monitoramento contínuo dentro da organização.
T0968	Designar funcionários conforme necessário para um acompanhamento contínuo e adequado de grupos de trabalho.
T0969	Identificar requisitos de emissão de relatórios para apoiar atividades de monitoramento contínuo.
T0970	Estabelecer métricas de pontuação e classificação para medir a eficácia do programa de monitoramento contínuo.
T0971	Determinar como integrar um programa de monitoramento contínuo às estruturas e políticas mais amplas de governança de segurança da informação dentro da organização.
T0972	Usar métricas contínuas de pontuação e classificação do monitoramento para tomar decisões sobre investimentos em segurança da informação para solucionar questões persistentes.
T0973	Garantir que a equipe de monitoramento contínuo tenha o treinamento e os recursos (ex.: pessoal e orçamento) necessários para desempenhar as funções lhe foram atribuídas.
T0974	Trabalhar com analistas de risco organizacional para garantir que o monitoramento contínuo de relatórios englobe os níveis adequados da organização.
T0975	Trabalhar com os analistas de risco organizacional para garantir que as métricas de risco sejam definidas de forma realista para apoiar o monitoramento contínuo.
T0976	Trabalhar com dirigentes organizacionais para garantir que os dados oriundos da ferramenta de monitoramento contínuo forneçam a percepção da situação dos níveis de risco.
T0977	Estabelecer gatilhos de limites de risco inaceitáveis para dados de monitoramento contínuo.
T0978	Trabalhar junto a funcionários organizacionais para estabelecer categorias de relatórios de nível de sistema que possam ser usados pelo programa de monitoramento contínuo da organização.
T0980	Designar uma pessoa qualificada para ser responsável pela gestão e implementação do programa de monitoramento contínuo.
T0981	Identificar os principais interessados em monitoramento contínuo e estabelecer um processo para mantê-los informados sobre o programa.
T0982	Identificar os requisitos para os relatórios da organização focados em segurança, que são atendidos pelo programa de monitoramento contínuo.
T0983	Usar os dados de monitoramento contínuo para tomar decisões de investimento em segurança da informação, visando a resolver questões persistentes.
T0984	Definir gatilhos dentro do programa de monitoramento contínuo que podem ser usados para definir o risco inaceitável, o que resulta em uma tomada de decisão para resolvê-lo.
T0985	Estabelecer métricas de pontuação e classificação para medir a eficácia do programa de monitoramento contínuo.
T0986	Trabalhar junto a gestores de segurança para estabelecer requisitos adequados de emissão de relatórios de monitoramento contínuo em nível de sistema.
T0987	Usar as ferramentas e tecnologias de monitoramento contínuo para avaliar o risco continuamente.
T0988	Estabelecer requisitos adequados de emissão de relatórios em adesão aos critérios identificados no programa de monitoramento contínuo para uso na avaliação de controle automatizado.
T0989	Usar métodos de avaliação não automatizados onde os dados das ferramentas e tecnologias de monitoramento contínuo ainda não são de suficiência ou qualidade adequadas.

ID da Tarefa	Descrição da Tarefa
T0990	Desenvolver processos com o grupo de auditoria externa sobre como compartilhar informações sobre o programa de monitoramento contínuo e seu impacto na avaliação do controle de segurança.
T0991	Identificar os requisitos de relatórios para uso em avaliação automatizada de controle para dar suporte ao monitoramento contínuo.
T0992	Determinar como os resultados de monitoramento contínuo serão usados na autorização contínua.
T0993	Estabelecer ferramentas de monitoramento contínuo, bem como tecnologias e procedimentos de controle de acesso.
T0994	Garantir que o controle de acesso contínuo de ferramentas e tecnologias seja gerenciado adequadamente.
T0995	Estabelecer um processo para fornecer ajuda técnica aos mitigadores de monitoramento contínuo.
T0996	Coordenar os requisitos de relatórios de monitoramento contínuo para vários usuários.
T0997	Estabelecer responsabilidades para apoiar a implementação de cada ferramenta ou tecnologia de monitoramento contínuo.
T0998	Estabelecer uma ligação com o grupo de trabalho de pontuação e métricas para apoiar o monitoramento contínuo.
T0999	Estabelecer e operar um processo para gerenciar a introdução de novos riscos para oferecer suporte ao monitoramento contínuo.
T1000	Estabelecer questões de configuração de monitoramento contínuo e subgrupo de coordenação.
T1001	Estabelecer ferramentas de monitoramento contínuo e requisitos de medição/gerenciamento de desempenho de tecnologias.
T1002	Usar pontuações e classificação para motivar e avaliar o desempenho, ao mesmo tempo abordando questões para apoiar o monitoramento contínuo
T1003	Trabalhar com gerentes de segurança (ou seja, proprietários de sistemas, gerentes de segurança do sistema de informação, agentes de segurança do sistema de informação, etc.) para estabelecer requisitos adequados de emissão de relatórios para monitoramento contínuo em nível de sistema.
T1004	Usar ferramentas de monitoramento contínuo para avaliar o risco continuamente.
T1005	Usar os dados de monitoramento contínuo para tomar decisões de investimento em segurança da informação, visando a resolver questões persistentes.
T1006	Responder aos problemas sinalizados durante o monitoramento contínuo, para escalar e coordenar uma resposta.
T1007	Examinar os resultados do programa de monitoramento contínuo e atenuar riscos em tempo hábil.

## A.5 Descrições de Conhecimento do NICE Framework

Tabela 5 fornece uma listagem dos vários tipos de informações aplicadas diretamente ao desempenho de uma função. Os IDs de conhecimento/descrições selecionados contidos nesta lista estão também incluídos em cada função de trabalho na lista detalhada de funções de trabalho no Apêndice B. As seis primeiras descrições são comuns a todas as funções de trabalho de segurança cibernética. Esta lista será atualizada periodicamente [1]. A fonte definitiva para a versão mais atual deste material pode ser encontrada na Planilha de Referência para a Publicação Especial NIST 800-181 [4].

**Tabela 5 - Descrições de Conhecimentos do NICE Framework**

ID de KSA	Descrição
K0001	Conhecimento de conceitos e protocolos de rede de computadores e metodologias de segurança de rede.
K0002	Conhecimento de processos de gestão de riscos (ex.: métodos de avaliação e mitigação de riscos).
K0003	Conhecimento de leis, regulamentos, políticas e ética no que se refere à segurança cibernética e privacidade.
K0004	Conhecimento dos princípios de segurança cibernética e privacidade.
K0005	Conhecimento de ameaças e vulnerabilidades cibernéticas.
K0006	Conhecimento de impactos operacionais específicos de lapsos de cibersegurança.
K0007	Conhecimento de métodos de autenticação, autorização e controle de acesso.
K0008	Conhecimento dos processos de negócios aplicáveis e operações de organizações de clientes.
K0009	Conhecimento das vulnerabilidades de aplicativos.
K0010	Conhecimento de métodos, princípios e conceitos de comunicação que suportam a infraestrutura de rede.
K0011	Conhecimento de recursos e aplicações de equipamentos de rede, incluindo roteadores, switches, pontes, servidores, mídia de transmissão e hardware relacionado.
K0012	Conhecimento de recursos e análise de requisitos.
K0013	Conhecimento das ferramentas de avaliação de defesa cibernética e vulnerabilidade e suas capacidades.
K0014	Conhecimento de estruturas de dados complexas.
K0015	Conhecimento de algoritmos de computador.
K0016	Conhecimento dos princípios da programação de computadores
K0017	Conhecimento de conceitos e práticas de processamento de dados periciais digitais.
K0018	Conhecimento de algoritmos de criptografia
K0019	Conhecimento de criptografia e conceitos de gerenciamento de chaves criptográficas
K0020	Conhecimento da administração de dados e políticas de padronização de dados.
K0021	Conhecimento de backup e recuperação de dados.
K0022	Conhecimento dos princípios de mineração de dados e armazenamento de dados.
K0023	Conhecimento de sistemas de gerenciamento de banco de dados, idiomas de consulta, relacionamentos de tabela e visualizações.
K0024	Conhecimento de sistemas de banco de dados.
K0025	Conhecimento de gestão de direitos digitais.
K0026	Conhecimento da continuidade dos negócios e continuidade da recuperação dos planos operacionais após desastres.

ID de KSA	Descrição
K0027	Conhecimento da arquitetura de segurança da informação corporativa da organização.
K0028	Conhecimento dos requisitos de avaliação e validação da organização.
K0029	Conhecimento das conexões de Rede Local e Ampla da organização.
K0030	Conhecimento de engenharia elétrica aplicada à arquitetura de computador (ex.: placas de circuito, processadores, chips e hardware de computador).
K0031	Conhecimento de sistemas de mensagens corporativas e software associado.
K0032	Conhecimento de resiliência e redundância.
K0033	Conhecimento dos mecanismos de controle de acesso de host/rede (ex.: lista de controle de acesso, listas de recursos).
K0034	Conhecimento de serviços de rede e interações de protocolos que fornecem comunicações de rede.
K0035	Conhecimento de instalação, integração e otimização de componentes do sistema.
K0036	Conhecimento dos princípios de interação homem-computador.
K0037	Conhecimento do processo de Avaliação e Autorização de Segurança.
K0038	Conhecimento dos princípios de segurança cibernética e privacidade usados para gerenciar riscos relacionados ao uso, processamento, armazenamento e transmissão de informações ou dados.
K0039	Conhecimento dos princípios e métodos de segurança cibernética e privacidade que se aplicam ao desenvolvimento de software.
K0040	Conhecimento das fontes de disseminação de informações de vulnerabilidade (ex.: alertas, avisos, errata e boletins).
K0041	Conhecimento de categorias de incidentes, respostas a incidentes e cronogramas para respostas.
K0042	Conhecimento de metodologias de resposta e resolução após incidentes.
K0043	Conhecimento dos princípios e métodos de análise do padrão da indústria que são organizacionalmente aceitos.
K0044	Conhecimento dos princípios de cibersegurança, privacidade e requisitos organizacionais (relevantes para confidencialidade, integridade, disponibilidade, autenticação, não repúdio).
K0045	Conhecimento dos princípios de engenharia de sistemas de segurança da informação (NIST SP 800-160).
K0046	Conhecimento de metodologias e técnicas de detecção de invasões para detectar invasões baseadas em host e rede.
K0047	Conhecimento de conceitos e frameworks arquitetônicos de tecnologia da informação (TI).
K0048	Conhecimento dos requisitos da Estrutura de Gestão de Risco (RMF).
K0049	Conhecimento dos princípios e métodos de segurança da tecnologia da informação (TI) (ex.: firewalls, zonas desmilitarizadas, criptografia).
K0050	Conhecimento dos princípios e conceitos sobre rede de área local e rede de longa distância, incluindo o gerenciamento de largura de banda.
K0051	Conhecimento de linguagem de programação de baixo nível (ex.: idiomas de montagem).
K0052	Conhecimentos de matemática (ex.: logaritmos, trigonometria, álgebra linear, cálculo, estatística e análise operacional.)
K0053	Conhecimento de medidas ou indicadores de desempenho e disponibilidade do sistema.
K0054	Conhecimento dos métodos atuais do setor para avaliar, implementar e disseminar ferramentas e procedimentos de avaliação, implementação e disseminação de segurança em tecnologia da informação (TI), monitoramento, detecção e remediação utilizando conceitos e recursos baseados em políticas.
K0055	Conhecimento de microprocessadores.

ID de KSA	Descrição
K0056	Conhecimento de acesso à rede, gestão de identidade e acesso (ex.: infraestrutura de chaves públicas, Oauth, OpenID, SAML, SPML).
K0057	Conhecimento de dispositivos e funções de hardware de rede.
K0058	Conhecimento dos métodos de análise de tráfego de rede.
K0059	Conhecimento de novas e emergentes tecnologias da informação (TI) e tecnologias de cibersegurança.
K0060	Conhecimento de sistemas operacionais.
K0061	Conhecimento de como o tráfego flui através da rede (ex.: Protocolo de Controle de Transmissão [TCP] e Protocolo de Internet [IP], Modelo de Interconexão de Sistema Aberto [OSI], Biblioteca de Infraestrutura de Tecnologia da Informação, versão atual [ITIL]).
K0062	Conhecimento de análise em nível de pacote.
K0063	Conhecimento de conceitos paralelos e distribuídos de computação.
K0064	Conhecimento de ferramentas e técnicas de ajuste de desempenho.
K0065	Conhecimento de controles de acesso adaptativos baseados em normas e riscos.
K0066	Conhecimento de Avaliações de Impacto de Privacidade.
K0067	Conhecimento de conceitos de engenharia de processos.
K0068	Conhecimento de estruturas e lógica de linguagem de programação.
K0069	Conhecimento de linguagens de consulta, como SQL (linguagem de consulta estruturada).
K0070	Conhecimento de ameaças e vulnerabilidades de segurança de sistemas e aplicativos (ex.: estouro de buffer, código móvel, scripting entre sites, linguagem processual/linguagem de consulta estruturada [PL/SQL] e injeções, condições de corrida, canal oculto, replay, ataques orientados para o retorno, código malicioso).
K0071	Conhecimento de conceitos de tecnologia de acesso remoto.
K0072	Conhecimento dos princípios e técnicas de gestão de recursos.
K0073	Conhecimento de técnicas seguras de gerenciamento de configuração. (por exemplo, Guias de Implementação Técnica de Segurança (STIGs), práticas recomendadas de segurança cibernética em ciscsecurity.org).
K0074	Conhecimento de conceitos-chave no gerenciamento de segurança (ex.: Gerenciamento de versão, Gerenciamento de patch).
K0075	Conhecimento das ferramentas, métodos e técnicas de design de sistemas de segurança.
K0076	Conhecimento de teorias, conceitos e métodos de administração de servidores e engenharia de sistemas.
K0077	Conhecimento dos sistemas operacionais do servidor e cliente.
K0078	Conhecimento de ferramentas de diagnóstico de servidor e técnicas de identificação de falhas.
K0079	Conhecimento dos princípios de depuração de software.
K0080	Conhecimento de ferramentas, métodos e técnicas de design de software.
K0081	Conhecimento de modelos de desenvolvimento de software (ex.: Modelo Cascata, Modelo Espiral).
K0082	Conhecimento de engenharia de software.
K0083	Conhecimento de fontes, características e usos dos ativos de dados da organização.
K0084	Conhecimento de princípios e métodos de análise estruturada.
K0086	Conhecimento de ferramentas, métodos e técnicas de design de sistemas, incluindo ferramentas automatizadas de análise e design de sistemas.
K0087	Conhecimento de software de sistemas e normas de design organizacional, políticas e abordagens autorizadas (ex.: diretrizes da Organização Internacional para Padronização [ISO]) relacionadas ao design do sistema.

ID de KSA	Descrição
K0088	Conhecimento de conceitos de administração de sistemas.
K0089	Conhecimento de ferramentas de diagnóstico de sistemas e técnicas de identificação de falhas.
K0090	Conhecimento dos princípios de gerenciamento do ciclo de vida do sistema, incluindo segurança de software e usabilidade.
K0091	Conhecimento de sistemas de testes e métodos de avaliação.
K0092	Conhecimento de processos de integração tecnológica.
K0093	Conhecimento de conceitos de telecomunicações (ex.: canal de comunicação, Orçamento de Links de Sistemas, Eficiência Espectral, Multiplexação).
K0094	Conhecimento dos recursos e funcionalidades associados às tecnologias de criação de conteúdo (ex.: wikis, redes sociais, sistemas de gerenciamento de conteúdo, blogs).
K0095	Conhecimento dos recursos e funcionalidades associados a diversas tecnologias para organização e gerenciamento de informações (ex.: bancos de dados, motores de bookmarking).
K0096	Conhecimento dos recursos e funcionalidades de várias tecnologias colaborativas (ex.: groupware, SharePoint).
K0097	Conhecimento das características das mídias de armazenamento de dados físicos e virtuais.
K0098	Conhecimento da estrutura de relatórios e processos do Provedor de Serviços de Defesa Cibernética dentro da sua própria organização.
K0100	Conhecimento da arquitetura de tecnologia da informação corporativa (TI).
K0101	Conhecimento dos objetivos e metas da tecnologia da informação corporativa (TI) da organização.
K0102	Conhecimento do processo de engenharia de sistemas.
K0103	Conhecimento do tipo e frequência da manutenção de hardware de rotina.
K0104	Conhecimento de segurança da Rede Privada Virtual (VPN).
K0105	Conhecimento de serviços na web (ex.: arquitetura orientada a serviços, Protocolo de Acesso a Objetos Simples e linguagem de descrição de serviços na Web).
K0106	Conhecimento do que constitui um ataque de rede e a relação de um ataque de rede com ameaças e vulnerabilidades.
K0107	Conhecimento de investigações, relatórios, ferramentas investigativas e leis/regulamentos.
K0108	Conhecimento de conceitos, terminologia e operações de uma ampla gama de mídias de comunicação (redes de computadores e telefonia, satélite, fibra, e sem fio).
K0109	Conhecimento de componentes e arquiteturas de computadores físicos, incluindo as funções de vários componentes e periféricos (ex.: CPUs, Network Interface Cards, armazenamento de dados).
K0110	Conhecimento de táticas, técnicas e procedimentos contraditórios.
K0111	Conhecimento de ferramentas de rede (por exemplo, ping, traceroute, nslookup)
K0112	Conhecimento de princípios de defesa em profundidade e arquitetura de segurança de rede.
K0113	Conhecimento de diferentes tipos de comunicação de rede (ex.: LAN, WAN, MAN, WLAN, WWAN).
K0114	Conhecimento de dispositivos eletrônicos (ex.: sistemas/componentes de computador, dispositivos de controle de acesso, câmeras digitais, scanners digitais, organizadores eletrônicos, discos rígidos, cartões de memória, modems, componentes de rede, aparelhos de rede, dispositivos de controle doméstico em rede, impressoras, dispositivos de armazenamento removíveis, telefones, copiadoras, máquinas de fac-símile, etc.).
K0115	Conhecimento da tecnologia que pode ser explorada.
K0116	Conhecimento de extensões de arquivo (ex.: .dll, .bat, .zip, .pcap, .gzip).

ID de KSA	Descrição
K0117	Conhecimento das implementações do sistema de arquivos (ex.: New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
K0118	Conhecimento de processos para apreensão e preservação de provas digitais.
K0119	Conhecimento de metodologias de hackers.
K0120	Conhecimento de como as necessidades de informação e os requisitos de coleta são traduzidos, rastreados e priorizados em toda a extensão da empresa.
K0121	Conhecimento dos princípios e técnicas de gestão de programas de segurança da informação e gerenciamento de projetos.
K0122	Conhecimento de implicações investigativas de hardware, sistemas operacionais e tecnologias de rede.
K0123	Conhecimento de governança jurídica relacionada à admissibilidade (ex.: Regras de Evidência).
K0124	Conhecimento de múltiplos domínios cognitivos e ferramentas e métodos aplicáveis para o aprendizado em cada domínio.
K0125	Conhecimento de processos de coleta, embalagem, transporte e armazenamento de provas eletrônicas, mantendo cadeia de custódia.
K0126	Conhecimento de Práticas de Gestão de Riscos da Cadeia de Suprimentos (NIST SP 800-161)
K0127	Conhecimento da natureza e função da estrutura de informações relevante (ex.: Infraestrutura Nacional de Informações).
K0128	Conhecimento de tipos e coleta de dados persistentes.
K0129	Conhecimento de ferramentas de linha de comando (ex.: mkdir, mv, ls, passwd, grep).
K0130	Conhecimento de tecnologias de virtualização, desenvolvimento e manutenção de máquinas virtuais.
K0131	Conhecimento de coleta de webmail, técnicas de pesquisa/análise, ferramentas e cookies.
K0132	Conhecimento de quais arquivos do sistema (ex.: arquivos de log, de registro, ou de configuração) contêm informações relevantes e onde encontrar esses arquivos no sistema.
K0133	Conhecimento dos tipos de dados periciais digitais e como reconhecê-los.
K0134	Conhecimento de perícia implantável.
K0135	Conhecimento de tecnologias de filtragem na Web.
K0136	Conhecimento das capacidades de diferentes sistemas e métodos de comunicação eletrônica (ex.: e-mail, VOIP, IM, fóruns na Web, Transmissões diretas em vídeo).
K0137	Conhecimento da variedade de redes existentes (ex.: PBX, LANs, WANs, WIFI, SCADA).
K0138	Conhecimento de Wi-Fi.
K0139	Conhecimento de linguagens de computador interpretadas e compiladas.
K0140	Conhecimento de técnicas seguras de codificação.
K0141	Retirada – Integrada ao K0420
K0142	Conhecimento de processos de gestão de coletas, capacidades e limitações.
K0143	Conhecimento de sistemas de coleta front-end, incluindo coleta de tráfego, filtragem e seleção.
K0144	Conhecimento da dinâmica social dos invasores de computador em um contexto global.
K0145	Conhecimento de ferramentas de correlação de eventos de segurança.
K0146	Conhecimento dos principais processos de negócios/missões da organização.
K0147	Conhecimento de problemas emergentes de segurança, riscos e vulnerabilidades.
K0148	Conhecimento das normas de controle de importação/exportação e órgãos responsáveis com o propósito de reduzir o risco da cadeia de suprimentos.

ID de KSA	Descrição
K0149	Conhecimento da abordagem de tolerância ao risco e/ou gerenciamento de riscos da organização.
K0150	Conhecimento do programa, funções e responsabilidades de resposta a incidentes corporativos.
K0151	Conhecimento de ameaças atuais e emergentes/vetores de ameaças.
K0152	Conhecimento dos princípios e métodos de segurança da tecnologia da informação relacionadas a software (TI) (ex.: modularização, camadas, abstração, ocultação de dados, simplicidade/minimização).
K0153	Conhecimento do processo de garantia da qualidade do software.
K0154	Conhecimento de normas, processos e práticas de gerenciamento de risco da cadeia de suprimentos.
K0155	Conhecimento da lei de evidências eletrônicas.
K0156	Conhecimento das regras legais de evidência e procedimento judicial.
K0157	Conhecimento de políticas, procedimentos e regulamentos de defesa cibernética e segurança da informação.
K0158	Conhecimento das políticas de segurança do usuário de tecnologia da informação organizacional (TI) (ex.: criação de conta, regras de senha, controle de acesso).
K0159	Conhecimento de Voz sobre IP (VoIP).
K0160	Conhecimento dos vetores de ataques comuns na camada de rede.
K0161	Conhecimento de diferentes classes de ataques (ex.: ataques passivos, ativos, internos, próximos, de distribuição).
K0162	Conhecimento de ciberataques (por exemplo, script kiddies, ameaças internas, patrocinado por um estado não-nação e patrocinado por uma nação).
K0163	Conhecimento dos requisitos críticos de aquisição de tecnologia da informação (TI).
K0164	Conhecimento dos requisitos de funcionalidade, qualidade e segurança e como eles se aplicarão a itens específicos de fornecimento (ou seja, elementos e processos).
K0165	Conhecimento de avaliação/ameaça de risco.
K0167	Conhecimento das técnicas de endurecimento de sistemas, redes e sistemas operacionais.
K0168	Conhecimento das leis e estatutos aplicáveis (ex.: nos Títulos 10, 18, 32, 50 no Código dos EUA), Diretrizes Presidenciais, diretrizes do Poder Executivo e/ou diretrizes e procedimentos legais administrativos/criminais.
K0169	Conhecimento das políticas, requisitos e procedimentos de gerenciamento de riscos da cadeia de suprimentos de tecnologia da informação (TI).
K0170	Conhecimento de sistemas críticos de infraestrutura com tecnologia de comunicação da informação cujo design não leva em consideração a segurança do sistema.
K0171	Conhecimento de técnicas de engenharia reversa de hardware.
K0172	Conhecimento de middleware (ex.: barramento de serviço empresarial e enfileiramento de mensagens).
K0174	Conhecimento de protocolos de networking.
K0175	Conhecimento de técnicas de engenharia reversa de software.
K0176	Conhecimento de esquemas de linguagem de marcação extensível (XML).
K0177	Conhecimento dos estágios do ataque cibernético (ex.: reconhecimento, varredura, enumeração, obtenção de acesso, escalonamento de privilégios, manutenção do acesso, exploração da rede, cobertura de rastros).
K0178	Conhecimento de metodologias, ferramentas e práticas seguras de implantação de software.

ID de KSA	Descrição
K0179	Conhecimento de conceitos de arquitetura de segurança de rede, incluindo topologia, protocolos, componentes e princípios (ex.: aplicação de defesa em profundidade).
K0180	Conhecimento dos princípios, modelos, métodos (ex.: monitoramento de desempenho de sistemas de rede) e ferramentas.
K0182	Conhecimento de ferramentas e técnicas de escultura de dados (ex.: Foremost).
K0183	Conhecimento de conceitos de engenharia reversa.
K0184	Conhecimento de táticas, técnicas e procedimentos antipericiais \.
K0185	Conhecimento de configuração de design de laboratório de perícia e aplicações de suporte (ex.: VMWare, Wireshark).
K0186	Conhecimento de procedimentos e ferramentas de depuração.
K0187	Conhecimento de abuso de tipo de arquivo por adversários com comportamento anômalo.
K0188	Conhecimento de ferramentas de análise de malware (ex.: Oily Debug, Ida Pro).
K0189	Conhecimento de malware com detecção de máquina virtual (ex.: malware com reconhecimento virtual, malware com reconhecimento de depurador e malware descompactado que procura sequências relacionadas à VM no dispositivo de exibição do seu computador).
K0190	Conhecimento de metodologias de criptografia.
K0191	Impacto de implementação de assinaturas para vírus, malware e ataques.
K0192	Conhecimento das portas e serviços do Windows/Unix.
K0193	Conhecimento de recursos avançados de segurança de remediação de dados em bancos de dados.
K0194	Conhecimento de tecnologias e conceitos de gestão de conhecimento baseados em nuvem relacionados à segurança, governança, compras e administração.
K0195	Conhecimento de normas e metodologias de classificação de dados com base na sensibilidade e outros fatores de risco.
K0196	Conhecimento de Regulamentos de Importação/Exportação relacionados à criptografia e outras tecnologias de segurança.
K0197	Conhecimento da interface de programação de aplicativos de acesso ao banco de dados (ex.: Conectividade de Banco de Dados Java [JDBC]).
K0198	Conhecimento de conceitos de melhoria de processos organizacionais e modelos de maturidade de processos (ex.: Integração de Modelo de Maturidade da Capacidade (CMMI) para Desenvolvimento, CMMI para Serviços e CMMI para Aquisições).
K0199	Conhecimento de conceitos de arquitetura de segurança e modelos de referência em arquitetura corporativa (ex.: Zachman, Federal Enterprise Architecture [FEA]).
K0200	Conhecimento de conceitos de gestão de serviços para redes e normas relacionados (ex.: Biblioteca de Infraestrutura de Tecnologia da Informação, versão atual [ITIL]).
K0201	Conhecimento de técnicas e conceitos de rotação de chaves simétricas.
K0202	Conhecimento dos conceitos e funções de firewall do aplicativo (ex.: ponto único de autenticação/auditoria/aplicação de políticas, varredura de mensagens devido ao conteúdo malicioso, anonimização de dados para conformidade PCI e PII, varredura de proteção contra perda de dados, operações criptográficas aceleradas, segurança SSL, processamento REST/JSON).
K0203	Conhecimento de modelos de segurança (ex.: modelo Bell-LaPadula, modelo de integridade Biba, modelo de integridade Clark-Wilson).
K0204	Conhecimento de técnicas de avaliação de aprendizagem (rubricas, planos de avaliação, testes, questionários).
K0205	Conhecimento de técnicas básicas de endurecimento do sistema, rede e sistema operativo.
K0206	Conhecimento de princípios e técnicas de hacking éticos.

ID de KSA	Descrição
K0207	Conhecimento de análise de circuitos.
K0208	Conhecimento de serviços de treinamento baseado em computador e e-learning.
K0209	Conhecimento de técnicas de comunicação secretas.
K0210	Conhecimento de conceitos de backup e restauração de dados.
K0211	Conhecimento de requisitos de confidencialidade, integridade e disponibilidade.
K0212	Conhecimento de produtos de software habilitados para segurança cibernética.
K0213	Conhecimento de modelos instrutivos de design e avaliação (ex.: ADDIE, modelo Smith/Ragan, Eventos de Instrução de Gagne, modelo de avaliação de Kirkpatrick).
K0214	Conhecimento da Metodologia de Avaliação de Estruturas de Gestão de Risco.
K0215	Conhecimento de políticas de treinamento organizacional.
K0216	Conhecimento dos níveis de aprendizagem (ou seja, Taxonomia da Aprendizagem de Bloom).
K0217	Conhecimento de Sistemas de Gestão de Aprendizagem e o seu uso na gestão da aprendizagem.
K0218	Conhecimento de estilos de aprendizagem (ex.: assimilador, auditivo, cinestésico).
K0220	Conhecimento dos modos de aprendizagem (ex.: aprendizagem rotineira, observação).
K0221	Conhecimento do modelo OSI e protocolos de rede subjacentes (ex.: TCP/IP).
K0222	Conhecimento de leis relevantes, autoridades legais, restrições e regulamentos relativos às atividades de defesa cibernética.
K0223	Retirado – integrado ao K0073
K0224	Conhecimento dos conceitos de administração de sistemas para sistemas operacionais tais como, por exemplo, Unix/Linux, IOS, Android e Windows.
K0226	Conhecimento de sistemas de treinamento organizacional.
K0227	Conhecimento de vários tipos de arquiteturas de computador.
K0228	Conhecimento da taxonomia e teoria da ontologia semântica.
K0229	Conhecimento de aplicativos que podem registrar erros, exceções e falhas de aplicativos e login.
K0230	Conhecimento dos modelos de serviço em nuvem e como esses modelos podem limitar a resposta a incidentes.
K0231	Conhecimento de protocolos, processos e técnicas de gestão de crises.
K0233	Conhecimento da Estrutura Nacional da Força de Trabalho em Cibersegurança, funções de trabalho e tarefas associadas, conhecimentos, habilidades e aptidões.
K0234	Conhecimento de recursos cibernéticos de espectro completo (ex.: defesa, ataque, exploração).
K0235	Conhecimento de como alavancar centros de pesquisa e desenvolvimento, think tanks, pesquisa acadêmica e sistemas industriais.
K0236	Conhecimento de como utilizar Hadoop, Java, Python, SQL, Hive e Pig para explorar dados.
K0237	Conhecimento das melhores práticas do setor para service desk.
K0238	Conhecimento da teoria e princípios da aprendizagem de máquina.
K0239	Conhecimento de técnicas e métodos de produção de mídia, comunicação e divulgação, incluindo formas alternativas de informar via mídia escrita, oral e visual.
K0240	Conhecimento de sistemas de segurança multinível e soluções de domínio cruzado.
K0241	Conhecimento de políticas, processos e procedimentos de recursos humanos organizacionais.
K0242	Conhecimento de políticas de segurança organizacional.

ID de KSA	Descrição
K0243	Conhecimento de políticas, processos e procedimentos de formação organizacional e educação.
K0244	Conhecimento de comportamentos físicos e fisiológicos que podem indicar atividade suspeita ou anormal.
K0245	Conhecimento de princípios e processos para a realização de treinamento e educação precisa de avaliação.
K0246	Conhecimento de conceitos, procedimentos, softwares, equipamentos e aplicações tecnológicas relevantes.
K0247	Conhecimento de processos de acesso remoto, ferramentas e recursos relacionados ao suporte ao cliente.
K0248	Conhecimento de teoria estratégica e prática.
K0249	Conhecimento de tecnologias, processos e estratégias de sustentação.
K0250	Conhecimento de processos de Teste e Avaliação para alunos.
K0251	Conhecimento do processo judicial, incluindo a apresentação de fatos e provas.
K0252	Conhecimento dos princípios e métodos de treinamento e educação para a elaboração de currículos, ensino e instrução para indivíduos e grupos, e como mensurar os efeitos do treinamento e da educação.
K0253	Retirado – Integrado no K0227
K0254	Conhecimento de análise binária.
K0255	Conhecimento de conceitos de arquitetura de rede, incluindo topologia, protocolos e componentes.
K0257	Conhecimento dos requisitos de aquisição/aprovisionamento de tecnologia da informação (TI).
K0258	Conhecimento de procedimentos de teste, princípios e metodologias (ex.: Integração de Recursos e Modelos de Maturidade (CMMI)).
K0259	Conhecimento de conceitos e metodologias de análise de malware.
K0260	Conhecimento dos normas de segurança de dados de Informações Pessoalmente Identificáveis (PII).
K0261	Conhecimento das normas de segurança de dados da Indústria de Cartões de Pagamento (PCI).
K0262	Conhecimento das normas de segurança de dados de Informações de Saúde Pessoal (PHI).
K0263	Conhecimento de políticas, requisitos e procedimentos de gerenciamento de riscos de tecnologia da informação (TI).
K0264	Conhecimento do planejamento para proteção de programas (ex.: tecnologia da informação (TI) políticas de segurança/gerenciamento de risco da cadeia de suprimentos, técnicas antiadulteração e requisitos).
K0265	Conhecimento de infraestrutura que suporta a tecnologia da informação (TI) para segurança, desempenho e confiabilidade.
K0266	Conhecimento de como avaliar a confiabilidade do fornecedor e/ou produto.
K0267	Conhecimento de leis, políticas, procedimentos ou governança relevantes à segurança cibernética para infraestruturas críticas.
K0268	Conhecimento de identificação de rastro pericial.
K0269	Conhecimento de arquitetura de comunicações móveis.
K0270	Conhecimento do processo de vida de aquisição/aprovisionamento.
K0271	Conhecimento de estruturas de sistemas operacionais e internos (ex.: gestão de processos, estrutura de diretórios, aplicações instaladas).
K0272	Conhecimento das ferramentas de análise de rede utilizadas para identificar vulnerabilidades de comunicações de software.

ID de KSA	Descrição
K0274	Conhecimento de registros de transmissão (ex.: Bluetooth, Identificação de Radiofrequência (RFID), Rede Infravermelha (IR), Fidelidade Sem Fio (Wi-Fi). Paging, celular, antenas parabólicas, Voice over Internet Protocol (VoIP)) e técnicas de interferência para permitir a transmissão de informações indesejáveis ou impedir que os sistemas instalados operem corretamente.
K0275	Conhecimento de técnicas de gestão de configuração.
K0276	Conhecimento de gestão de segurança.
K0277	Conhecimento de criptografia de dados atuais e emergentes (ex.: criptografia de coluna e espaço de tabela, criptografia de arquivo e disco) recursos de segurança em bancos de dados (ex.: recursos de gerenciamento de chave criptográfica integrados).
K0278	Conhecimento dos recursos atuais e emergentes de segurança de remediação de dados em bancos de dados.
K0280	Conhecimento de teorias, conceitos e métodos de engenharia de sistemas.
K0281	Conhecimento de catálogos de serviços de tecnologia da informação (TI).
K0282	Retirado – Integrado ao K0200
K0283	Conhecimento de casos de uso relacionados à colaboração e sincronização de conteúdo em plataformas (ex.: Mobile, PC, nuvem).
K0284	Conhecimento do desenvolvimento e aplicação do sistema de gerenciamento de credenciais do usuário.
K0285	Conhecimento da implementação de sistemas de custódia de chaves corporativas para suportar criptografia de dados em repouso.
K0286	Conhecimento de tipologias de camadas N (ex.: incluindo sistemas operacionais de servidor e cliente).
K0287	Conhecimento do programa de classificação de informações de uma organização e procedimentos para comprometimento das informações.
K0288	Conhecimento de modelos de segurança padrão da indústria.
K0289	Conhecimento de ferramentas de diagnóstico de sistema/servidor e técnicas de identificação de falhas.
K0290	Conhecimento de testes de segurança de sistemas e métodos de avaliação.
K0291	Conhecimento dos conceitos e normas arquitetônicas de tecnologia da informação corporativa (TI) (ex.: linha de base, design validado e arquiteturas de destino.)
K0292	Conhecimento das operações e processos e gerenciamento de incidentes, problemas e eventos.
K0293	Conhecimento de integração das metas e objetivos da organização na arquitetura.
K0294	Conhecimento da operação, manutenção e segurança do sistema de TI necessário para manter o funcionamento adequado do equipamento.
K0295	Conhecimento dos princípios de confidencialidade, integridade e disponibilidade.
K0296	Conhecimento de recursos, aplicativos e potenciais vulnerabilidades de equipamentos de rede, incluindo hubs, roteadores, switches, pontes, servidores, mídia de transmissão e hardware relacionado.
K0297	Conhecimento de design de contramedidas para riscos de segurança identificados.
K0298	Conhecimento de contramedidas para riscos de segurança identificados.
K0299	Conhecimento para determinar como um sistema de segurança deve funcionar (incluindo sua capacidade de resiliência e confiabilidade) e como as mudanças nas condições, operações ou ambiente afetarão esses resultados.
K0300	Conhecimento de mapeamento de rede e recriação de topologias de rede.
K0301	Conhecimento da análise em nível de pacote usando ferramentas apropriadas (ex.: Wireshark, tcpdump).

ID de KSA	Descrição
K0302	Conhecimento do funcionamento básico de computadores.
K0303	Conhecimento do uso de ferramentas de sub-redes.
K0304	Conhecimento de conceitos e práticas de processamento de dados periciais digitais.
K0305	Conhecimento de ocultação de dados (ex.: algoritmos de criptografia e estenografia).
K0308	Conhecimento de criptografia.
K0309	Conhecimento de tecnologias emergentes que têm potencial de exploração.
K0310	Conhecimento de metodologias de hackers.
K0311	Conhecimento de indicadores do setor úteis para identificar tendências tecnológicas.
K0312	Conhecimento de princípios, políticas e procedimentos de coleta de inteligência, incluindo autoridades legais e restrições.
K0313	Conhecimento de organizações externas e instituições acadêmicas com foco cibernético (ex.: currículo cibernético/treinamento e Pesquisa & Desenvolvimento).
K0314	Conhecimento das potenciais vulnerabilidades de cibersegurança das tecnologias do setor.
K0315	Conhecimento dos principais métodos, procedimentos e técnicas de coleta de informações e produção, emissão de relatórios e compartilhamento de informações.
K0316	Conhecimento de planos de operação empresarial ou militar, planos de operação conceitual, ordens, políticas e regras permanentes de engajamento.
K0317	Conhecimento dos procedimentos utilizados para documentar e consultar incidentes, problemas e eventos relatados.
K0318	Conhecimento das ferramentas de linha de comando do sistema operacional.
K0319	Conhecimento das capacidades técnicas de entrega e suas limitações.
K0320	Conhecimento dos critérios de avaliação e validação da organização.
K0321	Conhecimento de conceitos de engenharia aplicados à arquitetura de computação e hardware/software de computador associado.
K0322	Conhecimento de sistemas embarcados.
K0323	Conhecimento das metodologias de tolerância a falhas do sistema.
K0324	Conhecimento de ferramentas e aplicativos do Sistema de Detecção de invasões (IDS)/Sistema de Prevenção de invasões (IPS).
K0325	Conhecimento da Teoria da Informação (ex.: codificação de origem, codificação de canais, teoria da complexidade do algoritmo e compressão de dados).
K0326	Conhecimento das zonas desmilitarizadas.
K0330	Conhecimento de recursos de sucesso para identificar as soluções para problemas de sistema menos comuns e mais complexos.
K0332	Conhecimento de protocolos de rede como TCP/IP, configuração dinâmica do host, Domain Name System DNS, (sistema de nomes de domínio) e serviços de diretório.
K0333	Conhecimento dos processos de design de rede, para incluir a compreensão dos objetivos de segurança, objetivos operacionais e escolhas apropriadas.
K0334	Conhecimento de análise de tráfego de rede (ferramentas, metodologias, processos).
K0335	Conhecimento das tecnologias cibernéticas atuais e emergentes.
K0336	Conhecimento dos métodos de autenticação de acesso.
K0337	Retirado – Integrado em K0007
K0338	Conhecimento de técnicas de mineração de dados.
K0339	Conhecimento de como usar ferramentas de análise de rede para identificar vulnerabilidades.
K0341	Conhecimento das políticas de divulgação externa e regulamentos de controle de importação/exportação relacionados à segurança cibernética.
K0342	Conhecimento de princípios, ferramentas e técnicas de teste de penetração.

ID de KSA	Descrição
K0343	Conhecimento de técnicas de análise de causas básicas.
K0344	Conhecimento do ambiente de ameaças de uma organização.
K0346	Conhecimento de princípios e métodos para integração de componentes do sistema.
K0347	Conhecimento e compreensão do design operacional.
K0349	Conhecimento de tipos de sites, administração, funções e sistema de gerenciamento de conteúdo (CMS).
K0350	Conhecimento de sistemas de planejamento de organização aceitos.
K0351	Conhecimento dos estatutos, leis, regulamentos e políticas aplicáveis que regem o direcionamento e a exploração cibernética.
K0352	Conhecimento de formas de necessidades de suporte de inteligência, tópicos e áreas de foco.
K0353	Conhecimento de possíveis circunstâncias que resultariam em mudanças nas autoridades de gestão de coleta.
K0354	Conhecimento de procedimentos relevantes para relatórios e divulgação.
K0355	Conhecimento de todas as fontes para relatórios e procedimentos de divulgação.
K0356	Conhecimento de ferramentas e técnicas analíticas para linguagem, voz e/ou material gráfico.
K0357	Conhecimento de construções analíticas e seu uso na avaliação do ambiente operacional.
K0358	Conhecimento de normas analíticas e propósito dos níveis de confiança da inteligência.
K0359	Conhecimento de processos aprovados de disseminação de inteligência.
K0361	Conhecimento da disponibilidade, capacidades e limitações dos ativos.
K0362	Conhecimento de métodos e técnicas de ataque (DDoS, força bruta, spoofing, etc.).
K0363	Conhecimento de procedimentos de auditoria e registro (incluindo registro baseado em servidor).
K0364	Conhecimento das bases de dados disponíveis e ferramentas necessárias para avaliar o trabalho adequado de coleta.
K0367	Conhecimento de testes de penetração.
K0368	Conhecimento de implantes que permitem atividades de coleta cibernética e/ou preparação.
K0371	Conhecimento dos princípios dos processos de desenvolvimento de coleta (ex.: Reconhecimento de Números Discados, Análise de Redes Sociais).
K0372	Conhecimento de conceitos de programação (ex.: níveis, estruturas, linguagens compiladas vs. interpretadas).
K0373	Conhecimento de aplicativos básicos de software (ex.: armazenamento e backup de dados, aplicativos de banco de dados) e os tipos de vulnerabilidades encontradas nesses aplicativos.
K0375	Conhecimento de vulnerabilidades de aplicativos sem fio.
K0376	Conhecimento de clientes internos e externos e organizações parceiras, incluindo necessidades de informações, objetivos, estrutura, capacidades, etc.
K0377	Conhecimento de classificação e normas, políticas e procedimentos de controle de marcas.
K0379	Conhecimento de organizações dos clientes, incluindo necessidades de informações, objetivos, estrutura, capacidades, etc.
K0380	Conhecimento de ferramentas e ambientes colaborativos.
K0381	Conhecimento de danos colaterais e estimativa de impactos.
K0382	Conhecimento das capacidades e limitações da coleta.
K0383	Conhecimento dos recursos de coleta, acessos, especificações de desempenho e restrições utilizadas para satisfazer o plano de coleta.
K0384	Conhecimento da funcionalidade de gestão de coleta (ex.: cargos, funções, responsabilidades, produtos, requisitos de emissão de relatórios).
K0385	Retirado – Integrado em K0142

ID de KSA	Descrição
K0386	Conhecimento de ferramentas de gestão de coleta.
K0387	Conhecimento do processo de planejamento e plano de coleta.
K0388	Conhecimento de técnicas de pesquisa/análise de coleta e ferramentas para lista de chat/amigos, tecnologias emergentes, VOIP, Media Over IP, VPN, VSAT/wireless, web mail e cookies.
K0389	Conhecimento de fontes de coleta, incluindo fontes convencionais e não convencionais.
K0390	Conhecimento de estratégias de coleta.
K0391	Conhecimento de sistemas de coleta, capacidades e processos.
K0392	Conhecimento de infecções comuns de computador/rede (vírus, Trojan, etc.) e métodos de infecção (portas, anexos, etc.).
K0393	Conhecimento de dispositivos de rede comuns e suas configurações.
K0394	Conhecimento de bancos de dados e ferramentas de relatórios comuns.
K0395	Conhecimento dos fundamentos de rede de computadores (ou seja, componentes básicos do computador de uma rede, tipos de redes, etc.) .
K0396	Conhecimento de conceitos de programação de computadores, incluindo linguagens de computador, programação, testes, depuração e tipos de arquivos.
K0397	Conhecimento de conceitos de segurança em sistemas operacionais (ex.: Linux, Unix.)
K0398	Conhecimento de conceitos relacionados a sites (ex.: servidores/páginas da web, hospedagem, DNS, registro, linguagens da web, como HTML).
K0399	Conhecimento do planejamento de um curso de ação em caso de crises, e procedimentos de planejamento sensíveis ao tempo.
K0400	Conhecimento do planejamento de um curso de ação mediante uma crise para operações cibernéticas.
K0401	Conhecimento de critérios para avaliação de produtos de coleta.
K0402	Conhecimento de fatores de criticidade e vulnerabilidade (por exemplo, valor, recuperação, amortecimento, contramedidas) para a seleção de destinos e aplicabilidade ao domínio cibernético.
K0403	Conhecimento de capacidades, limitações e contribuições criptológicas para operações cibernéticas.
K0404	Conhecimento dos requisitos atuais de coleta.
K0405	Conhecimento dos conjuntos atuais de invasão baseados em computador.
K0406	Conhecimento de softwares e metodologias atuais para defesa ativa e endurecimento do sistema.
K0407	Conhecimento das necessidades de informação do cliente.
K0408	Conhecimento dos princípios, capacidades, limitações e efeitos das ações cibernéticas (ou seja, defesa cibernética, coleta de informações, preparação do ambiente, ataque cibernético).
K0409	Conhecimento dos recursos de inteligência cibernética/coleta de informações e repositórios.
K0410	Conhecimento das leis cibernéticas e seus efeitos no planejamento cibernético.
K0411	Conhecimento das leis cibernéticas e considerações legais e seus efeitos no planejamento cibernético.
K0412	Conhecimento do léxico/terminologia cibernética.
K0413	Conhecimento dos objetivos, políticas e legalidades da operação cibernética.
K0414	Conhecimento de processos de suporte ou habilitação de operações cibernéticas.
K0415	Conhecimento da terminologia/léxico de operações cibernéticas.
K0416	Conhecimento de operações cibernéticas.
K0417	Conhecimento da terminologia de comunicações de dados (ex.: protocolos de rede, Ethernet, IP, criptografia, dispositivos ópticos, mídia removível).

ID de KSA	Descrição
K0418	Conhecimento do processo de fluxo de dados para coleta de terminais ou ambientais.
K0419	Conhecimento de administração e manutenção de banco de dados.
K0420	Conhecimento da teoria de banco de dados.
K0421	Conhecimento de bancos de dados, portais e veículos de divulgação associados.
K0422	Conhecimento de processos e procedimentos de desconflito.
K0423	Conhecimento de relatórios de desconflito para incluir interação com organização externa.
K0424	Conhecimento de técnicas de negação e engano.
K0425	Conhecimento de diferentes objetivos de organização em todos os níveis, incluindo subordinado, lateral e superior.
K0426	Conhecimento de direcionamento dinâmico e deliberado.
K0427	Conhecimento de algoritmos de criptografia e recursos/ferramentas cibernéticas (ex.: SSL, PGP).
K0428	Conhecimento de algoritmos de criptografia e ferramentas para redes de áreas locais sem fio (WLANs).
K0429	Conhecimento de gerenciamento da informação em toda a empresa.
K0430	Conhecimento de estratégias e técnicas de evasão.
K0431	Conhecimento de tecnologias de comunicação em evolução/emergentes.
K0432	Conhecimento de questões existentes, emergentes e de longo alcance relacionadas à estratégia, política e organização de operações cibernéticas.
K0433	Conhecimento das implicações periciais da estrutura e funcionamento do sistema operacional.
K0435	Conhecimento de conceitos, princípios, limitações e efeitos cibernéticos fundamentais.
K0436	Conhecimento de conceitos fundamentais de operações cibernéticas, terminologia/léxico (ex.: preparação do ambiente, ataque cibernético, defesa cibernética), princípios, capacidades, limitações e efeitos.
K0437	Conhecimento dos componentes do sistema de controle geral de supervisão e aquisição de dados (SCADA).
K0438	Conhecimento da arquitetura de comunicações móveis celulares (ex.: LTE, CDMA, GSM/EDGE e UMTS/HSPA).
K0439	Conhecimento das autoridades governamentais para segmentação.
K0440	Conhecimento dos produtos de segurança baseados em host e como esses produtos afetam a exploração e reduzem a vulnerabilidade.
K0442	Conhecimento de como as tecnologias convergentes impactam as operações cibernéticas (ex.: digital, telefonia, sem fio).
K0443	Conhecimento de como hubs, switches, roteadores, trabalham juntos no design de uma rede.
K0444	Conhecimento de como funcionam os aplicativos da Internet (e-mail SMTP, e-mail baseado na Web, clientes de chat, VOIP).
K0445	Conhecimento de como as modernas redes digitais e de telefonia impactam as operações cibernéticas.
K0446	Conhecimento de como os modernos sistemas de comunicação sem fio impactam as operações cibernéticas.
K0447	Conhecimento de como coletar, visualizar e identificar informações essenciais sobre alvos de interesse de metadados (ex.: e-mail, http).
K0448	Conhecimento de como estabelecer prioridades para os recursos.
K0449	Conhecimento de como extrair, analisar e usar metadados.
K0450	Retirado – Integrado em K0036
K0451	Conhecimento de processos de identificação e emissão de relatórios.

ID de KSA	Descrição
K0452	Conhecimento da implementação de sistemas Unix e Windows que fornecem autenticação e registro de raios, DNS, correio, serviço web, servidor FTP, DHCP, firewall e SNMP.
K0453	Conhecimento de indicações e advertências.
K0454	Conhecimento das necessidades de informação.
K0455	Conhecimento de conceitos de segurança da informação, facilitando tecnologias e métodos.
K0456	Conhecimento das capacidades e limitações de inteligência.
K0457	Conhecimento dos níveis de confiança da inteligência.
K0458	Conhecimento de disciplinas de inteligência.
K0459	Conhecimento dos requisitos de emprego de inteligência (ex.: logística, suporte de comunicações, manobrabilidade, restrições legais, etc.).
K0460	Conhecimento da preparação da inteligência do meio ambiente e processos similares.
K0461	Conhecimento de processos de produção de inteligência.
K0462	Conhecimento de princípios de relatórios de inteligência, políticas, procedimentos e veículos, incluindo formatos de relatórios, critérios de reportabilidade (requisitos e prioridades), práticas de divulgação, autoridades legais e restrições.
K0463	Conhecimento de sistemas de atribuição de tarefas de requisitos de inteligência.
K0464	Conhecimento de suporte de inteligência para o planejamento, execução e avaliação.
K0465	Conhecimento das capacidades e ferramentas de operações cibernéticas de parceiros internos e externos.
K0466	Conhecimento de processos internos e externos de inteligência de parceiros e desenvolvimento de requisitos de informação e informações essenciais.
K0467	Conhecimento das capacidades e limitações da organização de parceiros internos e externos (aqueles com tarefas, cobranças, processamento, exploração e divulgação).
K0468	Conhecimento de relatórios de parceiros internos e externos.
K0469	Conhecimento de táticas internas para antecipar e/ou emular capacidades e ações de ameaças.
K0470	Conhecimento de Internet e protocolos de roteamento.
K0471	Conhecimento de endereçamento de rede da Internet (endereços IP, roteamento, interdomínio sem classe, numeração da porta TCP/UDP).
K0472	Conhecimento de sistemas de detecção de invasões e desenvolvimento de assinaturas.
K0473	Conhecimento de conjuntos de invasão.
K0474	Conhecimento dos principais atores de ameaças cibernéticas e suas ações.
K0475	Conhecimento dos principais fatores do ambiente operacional e da ameaça.
K0476	Conhecimento de ferramentas e técnicas de processamento de linguagem.
K0477	Conhecimento da intenção e objetivos da liderança.
K0478	Conhecimento de considerações legais na segmentação.
K0479	Conhecimento de análise e características de malware.
K0480	Conhecimento de malware.
K0481	Conhecimento de métodos e técnicas utilizados para detectar diversas atividades de exploração.
K0482	Conhecimento dos métodos para apuração da postura e disponibilidade do ativo de cobrança.
K0483	Conhecimento de métodos para integrar e resumir informações de qualquer fonte potencial.
K0484	Conhecimento de coleta de ponto médio (processo, objetivos, organização, alvos, etc.).
K0485	Conhecimento de administração de rede.
K0486	Conhecimento de construção de rede e topologia.

ID de KSA	Descrição
K0487	Conhecimento de segurança de rede (por exemplo, criptografia, firewalls, autenticação, potes de mel, proteção de perímetro).
K0488	Conhecimento de implementações de segurança de rede (ex.: IDS, IPS, listas de controle de acesso), incluindo sua função e colocação em uma rede.
K0489	Conhecimento de topologia de rede.
K0490	Retirado – Integrado em K0058
K0491	Conhecimento de fundamentos de comunicação de rede e Internet (ex.: dispositivos, configuração de dispositivos, hardware, software, aplicativos, portas/protocolos, endereçamento, arquitetura e infraestrutura de rede, roteamento, sistemas operacionais, etc.).
K0492	Conhecimento de metodologias de coleta não tradicionais.
K0493	Conhecimento de técnicas de ofuscação (ex.: TOR/Onion/anonimizadores, VPN/VPS, criptografia).
K0494	Conhecimento de objetivos, situação, ambiente operacional, status e disposição dos recursos internos e externos de coleta de parceiros disponíveis para apoiar o planejamento.
K0495	Conhecimento de operações contínuas e futuras.
K0496	Conhecimento de restrições de ativos operacionais.
K0497	Conhecimento de avaliação de eficácia operacional.
K0498	Conhecimento de processos de planejamento operacional.
K0499	Conhecimento de segurança de operações.
K0500	Conhecimento de sistemas de coleta para organizações e/ou parceiros, recursos e processos (ex.: processadores de coleta e protocolo).
K0501	Conhecimento dos programas, estratégias e recursos de operações cibernéticas da organização.
K0502	Conhecimento das ferramentas e/ou métodos de apoio à decisão da organização.
K0503	Conhecimento dos formatos de organização de relatórios de disponibilidade de recursos e ativos, sua relevância operacional e impacto na coleta de inteligência.
K0504	Conhecimento de questões, objetivos e operações da organização em cibersegurança, bem como regulamentos e diretivas normativas que regem as operações cibernéticas.
K0505	Conhecimento dos objetivos da organização e demanda associada à gestão de coletas.
K0506	Conhecimento dos objetivos da organização, prioridades de liderança e riscos de tomada de decisão.
K0507	Conhecimento da exploração de redes digitais por organizações ou parceiros.
K0508	Conhecimento das políticas e conceitos de planejamento da organização para fazer parcerias com organizações internas e/ou externas.
K0509	Conhecimento das autoridades organizacionais e parceiras quanto às responsabilidades e contribuições para alcançar os objetivos.
K0510	Conhecimento das políticas, ferramentas, capacidades e procedimentos organizacionais e de parceiros.
K0511	Conhecimento da hierarquia organizacional e processos cibernéticos de tomada de decisão.
K0512	Conhecimento dos conceitos de planejamento organizacional.
K0513	Conhecimento das prioridades organizacionais, autoridades legais e processos de envio de requisitos.
K0514	Conhecimento das estruturas organizacionais e capacidades de inteligência associadas.
K0516	Conhecimento de dispositivos de rede físicos e lógicos e infraestrutura para incluir hubs, switches, roteadores, firewalls, etc.
K0517	Conhecimento do processo de aprovação da revisão pós-implementação (PIR).

ID de KSA	Descrição
K0518	Conhecimento do início da atividade de planejamento.
K0519	Conhecimento de cronogramas de planejamento adaptativo, ação contra crises e planejamento sensível ao tempo.
K0520	Conhecimento dos princípios e práticas relacionados ao desenvolvimento de destino, como conhecimento de destino, associações, sistemas de comunicação e infraestrutura.
K0521	Conhecimento de informações prioritárias, como ela é derivada, onde é publicada, como acessar, etc.
K0522	Conhecimento das necessidades e arquiteturas de exploração e disseminação da produção.
K0523	Conhecimento de produtos e nomenclatura de grandes fornecedores (ex.: suítes de segurança - Trend Micro, Symantec, McAfee, Outpost e Panda) e como esses produtos afetam a exploração e reduzem vulnerabilidades.
K0524	Conhecimento de leis, regulamentos e políticas relevantes.
K0525	Conhecimento de produtos necessários de planejamento de inteligência associados ao planejamento operacional cibernético.
K0526	Conhecimento de estratégias de pesquisa e gestão do conhecimento.
K0527	Conhecimento de estratégias de gestão e mitigação de riscos.
K0528	Conhecimento de sistemas de comunicação baseados em satélite.
K0529	Conhecimento de scripting
K0530	Conhecimento de hardware de segurança e opções de software, incluindo os artefatos de rede que eles induzem e seus efeitos na exploração.
K0531	Conhecimento das implicações de segurança das configurações de software.
K0532	Conhecimento de língua de destino especializada (ex.: siglas, jargão, terminologia técnica, palavras de código).
K0533	Conhecimento de identificadores de destino específicos e seu uso.
K0534	Conhecimento de processos de gestão, atribuição e alocação de pessoal.
K0535	Conhecimento de estratégias e ferramentas para pesquisa de destino.
K0536	Conhecimento da estrutura, abordagem e estratégia de ferramentas de exploração (ex.: sniffers, keyloggers) e técnicas (ex.: obter acesso backdoor, coletar / exfiltrar dados, conduzir análise de vulnerabilidade de outros sistemas na rede).
K0538	Conhecimento de estruturas de organizações do destino e de ameaças, recursos críticos e vulnerabilidades críticas
K0539	Conhecimento dos perfis de comunicação do alvo e seus elementos-chave (ex.: associações, atividades, infraestrutura de comunicação do alvo).
K0540	Conhecimento de ferramentas e técnicas de comunicação de destino.
K0541	Conhecimento das referências culturais, dialetos, expressões, idiomas e abreviações de destino.
K0542	Conhecimento do desenvolvimento de destino (ex.: conceitos, funções, responsabilidades, produtos, etc.).
K0543	Conhecimento do tempo estimado de reparação e recuperação de destino.
K0544	Conhecimento de técnicas de coleta de inteligência de destino, preparação operacional e ciclos de vida.
K0545	Conhecimento de línguas de destino.
K0546	Conhecimento do desenvolvimento de listas de destino (ex.: Restricted, Joint, Candidate, etc. ).
K0547	Conhecimento de métodos e procedimentos de destino.
K0548	Conhecimento de atores e procedimentos cibernéticos ou ameaça de destino.
K0549	Conhecimento de procedimentos de verificação e validação de destino.

ID de KSA	Descrição
K0550	Conhecimento de destino, incluindo eventos atuais relacionados, perfil de comunicação, atores e história (linguagem, cultura) e/ou quadro de referência.
K0551	Conhecimento de ciclos de segmentação.
K0552	Conhecimento de mecanismos de tarefa.
K0553	Conhecimento de processos de tarefas para ativos de coleta orgânicos e subordinados.
K0554	Conhecimento de tarefas, coleta, processamento, exploração e divulgação.
K0555	Conhecimento dos protocolos de rede TCP/IP.
K0556	Conhecimento dos fundamentos das telecomunicações.
K0557	Conhecimento de coleta terminal ou ambiental (processo, objetivos, organização, alvos, etc.).
K0558	Conhecimento das ferramentas e aplicativos disponíveis associados aos requisitos de coleta e gestão da coleta.
K0559	Conhecimento da estrutura básica, arquitetura e design de aplicações convergentes.
K0560	Conhecimento da estrutura básica, arquitetura e design de redes de comunicação modernas.
K0561	Conhecimento dos princípios básicos da segurança de rede (ex.: criptografia, firewalls, autenticação, potes de mel, proteção de perímetro).
K0562	Conhecimento das capacidades e limitações de recursos de coleta novos e emergentes, acessos e/ou processos.
K0563	Conhecimento das capacidades, limitações e metodologias de tarefas de coletas internas e externas, conforme se aplicam às atividades cibernéticas planejadas.
K0564	Conhecimento das características das redes de comunicação direcionadas (ex.: capacidade, funcionalidade, caminhos, nós críticos).
K0565	Conhecimento dos protocolos comuns de rede e roteamento (ex.: TCP/IP), serviços (ex.: web, e-mail, DNS) e como eles interagem para fornecer comunicações de rede.
K0566	Conhecimento dos requisitos críticos de informações e como eles são usados no planejamento.
K0567	Conhecimento do fluxo de dados desde a origem da coleta até repositórios e ferramentas.
K0568	Conhecimento da definição de gestão de coleta e autoridade de gestão de coleta.
K0569	Conhecimento da arquitetura de tarefas, coletas, processamento, exploração e disseminação existentes.
K0570	Conhecimento dos fatores de ameaças que podem impactar as operações de coleta.
K0571	Conhecimento do ciclo de feedback nos processos de coleta.
K0572	Conhecimento das funções e capacidades das equipes internas que emulam atividades de ameaça para beneficiar a organização.
K0573	Conhecimento dos fundamentos da perícia digital para extrair inteligência acionável.
K0574	Conhecimento do impacto da análise de linguagem nas funções do operador on-net.
K0575	Conhecimento dos impactos das estimativas de pessoal de parceiros internos e externos.
K0576	Conhecimento do ambiente da informação.
K0577	Conhecimento das estruturas de inteligência, processos e sistemas relacionados.
K0578	Conhecimento dos requisitos de inteligência desenvolvimento e solicitação de processos de informação.
K0579	Conhecimento da organização, papéis e responsabilidades de subelementos superiores, inferiores e adjacentes.
K0580	Conhecimento do formato estabelecido da organização para o plano de coleta.
K0581	Conhecimento dos ciclos de planejamento, operações e segmentação da organização.
K0582	Conhecimento do planejamento organizacional e processo de alocação de pessoal.

ID de KSA	Descrição
K0583	Conhecimento dos planos/diretrizes/orientações organizacionais que descrevem os objetivos.
K0584	Conhecimento das políticas/procedimentos organizacionais para transferência temporária da autoridade de coleta.
K0585	Conhecimento da estrutura organizacional no que se refere a operações cibernéticas de espectro total, incluindo as funções, responsabilidades e inter-relacionamentos entre elementos internos distintos.
K0586	Conhecimento dos resultados do curso de ação e análise de exercícios.
K0587	Conhecimento dos POC's, bancos de dados, ferramentas e aplicações necessárias para estabelecer produtos de preparação e vigilância ambiental.
K0588	Conhecimento dos requisitos prioritários de informações dos níveis - subordinado, lateral e superior da organização.
K0589	Conhecimento do processo utilizado para avaliar o desempenho e o impacto das operações.
K0590	Conhecimento dos processos para sincronizar procedimentos de avaliação operacional com o processo crítico de exigência de informações.
K0591	Conhecimento das responsabilidades de produção e análise orgânica e capacidade de produção.
K0592	Conhecimento da finalidade e contribuição dos modelos de destino.
K0593	Conhecimento da variedade de operações cibernéticas e suas necessidades de suporte de inteligência subjacentes, tópicos e áreas de foco.
K0594	Conhecimento das relações entre estados finais, objetivos, efeitos, linhas de operação, etc.
K0595	Conhecimento das relações entre objetivos operacionais, requisitos de inteligência e tarefas de produção de inteligência.
K0596	Conhecimento do processo de solicitação de informações.
K0597	Conhecimento do papel das operações de rede no apoio e facilitação de outras operações da organização.
K0598	Conhecimento da estrutura e intenção dos planos específicos, orientações e autorizações da organização.
K0599	Conhecimento da estrutura, arquitetura e design de redes digitais e de telefonia modernas.
K0600	Conhecimento da estrutura, arquitetura e design de sistemas modernos de comunicação sem fio.
K0601	Conhecimento dos sistemas/arquitetura/comunicações utilizados para coordenação.
K0602	Conhecimento de disciplinas e capacidades de coleta.
K0603	Conhecimento das maneiras pelas quais alvos ou ameaças usam a Internet.
K0604	Conhecimento de ameaças/sistemas alvo.
K0605	Conhecimento de tipping, cueing, mixagem e redundância.
K0606	Conhecimento dos processos e técnicas de desenvolvimento de transcrição (ex.: literal, essência, resumos).
K0607	Conhecimento de processos e técnicas de tradução.
K0608	Conhecimento das estruturas e interiores dos sistemas operacionais Unix/Linux e Windows (ex.: gerenciamento de processos, estrutura de diretórios, aplicativos instalados).
K0609	Conhecimento de tecnologias de máquinas virtuais.
K0610	Conhecimento de produtos de virtualização (VMware, Virtual PC).
K0611	Retirado – Integrado ao K0131
K0612	Conhecimento do que constitui uma "ameaça" a uma rede.
K0613	Conhecimento de quem são os planejadores operacionais da organização, como e onde eles podem ser contatados e quais são as suas expectativas.

ID de KSA	Descrição
K0614	Conhecimento de tecnologias sem fio (ex.: celular, satélite, GSM) para incluir a estrutura básica, arquitetura e design de sistemas modernos de comunicação sem fio.
K0615	Conhecimento das declarações de divulgação de privacidade com base nas leis vigentes.
K0616	Conhecimento do monitoramento contínuo, seus processos e atividades do programa de Diagnóstico e Mitigação Contínua (MDL).
K0617	Conhecimento de avaliações automatizadas de controle de segurança
K0618	Conhecimento de gerenciamento de ativos de hardware e o valor de rastrear a localização e configuração de dispositivos e softwares em rede, em todos os departamentos, locais, instalações e, potencialmente, apoiar funções de negócios.
K0619	Conhecimento de gerenciamento de ativos de software e o valor de rastrear a localização e configuração de dispositivos e softwares em rede, em todos os departamentos, locais, instalações e, potencialmente, apoiar funções de negócios.
K0620	Conhecimento de tecnologias e ferramentas de monitoramento contínuo.
K0621	Conhecimento de pontuação de risco.
K0622	Conhecimento de controles relacionados ao uso, processamento, armazenamento e transmissão de dados.
K0623	Conhecimento de metodologias de avaliação de riscos.
K0624	Conhecimento dos riscos de segurança de aplicativos (ex.: lista dos 10 principais do Open Web Application Security Project (Projeto Aberto de Segurança em Aplicações Web))
K0625	Conhecimento de que patches e atualizações de software são impraticáveis para alguns dispositivos em rede.
K0626	Conhecimento de mecanismos de atualização seguros.
K0627	Conhecimento da importância da filtragem de entrada para proteger contra ameaças automatizadas que dependem de endereços de rede falsificados.
K0628	Conhecimento de competições cibernéticas como forma de desenvolver habilidades, proporcionando experiência prática em situações simuladas do mundo real.
K0629	Conhecimento da lista branca/negra
K0630	Conhecimento das mais recentes técnicas de invasão, métodos e invasões documentadas externas à organização.

## A.6 Descrições de Habilidades do NICE Framework

A Tabela 6 fornece uma lista de habilidades de segurança cibernética. Uma habilidade é a competência observável para realizar um ato psicomotor aprendido. As descrições de habilidades selecionadas nesta lista estão incluídas para cada função de trabalho na Lista Detalhada de Função de Trabalho no Apêndice B. Esta lista será atualizada periodicamente [1]. A fonte definitiva para a versão mais atual deste material pode ser encontrada na Planilha de Referência para a Publicação Especial NIST 800-181 [4].

**Tabela 6 - Descrições de Habilidades do NICE Framework**

ID de Habilidade	Descrição
S0001	Habilidade na realização de varreduras e reconhecimento de vulnerabilidades em sistemas de segurança.
S0002	Habilidade na alocação da capacidade de armazenamento no design de sistemas de gerenciamento de dados.
S0003	Habilidade de identificar, capturar, conter e relatar malware.
S0004	Habilidade na análise da capacidade de tráfego de rede e características de desempenho.
S0005	Habilidade na aplicação e incorporação de tecnologias da informação em soluções propostas.
S0006	Habilidade na aplicação de princípios de confidencialidade, integridade e disponibilidade.
S0007	Habilidade na aplicação de controles de acesso de host/rede (ex.: lista de controle de acesso).
S0008	Habilidade na aplicação de princípios e técnicas de análise de sistemas específicos da organização.
S0009	Habilidade na avaliação da robustez dos sistemas e projetos de segurança.
S0010	Habilidade na condução de recursos e análise de requisitos.
S0011	Habilidade na realização de pesquisas de informação.
S0012	Habilidade na realização de mapeamento de conhecimento (ex.: mapa de repositórios de conhecimento).
S0013	Habilidade na realização de consultas e desenvolvimento de algoritmos para analisar estruturas de dados.
S0014	Habilidade na condução da depuração de software.
S0015	Habilidade na realização de eventos de teste.
S0016	Habilidade na configuração e otimização de software.
S0017	Habilidade na criação e utilização de modelos matemáticos ou estatísticos.
S0018	Habilidade na criação de políticas que reflitam os objetivos de segurança do sistema.
S0019	Habilidade na criação de programas que validam e processam múltiplas entradas, incluindo argumentos de linha de comando, variáveis ambientais e fluxos de entrada.
S0020	Habilidade no desenvolvimento e implantação de assinaturas.
S0021	Habilidade na concepção de uma estrutura de análise de dados (ex.: os tipos de dados que um teste deve gerar e como analisar os dados).
S0022	Habilidade na concepção de contramedidas para identificar riscos de segurança.
S0023	Habilidade na concepção de controles de segurança com base em princípios e conceitos de segurança cibernética.
S0024	Habilidade no projeto da integração de soluções de hardware e software.

ID de Habilidade	Descrição
S0025	Habilidade na detecção de invasões baseadas em host e rede através de tecnologias de detecção de invasões (ex.: Snort).
S0026	Habilidade na determinação de um nível apropriado de rigor de teste para um determinado sistema.
S0027	Habilidade para determinar como um sistema de segurança deve funcionar (incluindo suas capacidades de resiliência e confiabilidade) e como as mudanças nas condições, operações ou ambiente afetarão esses resultados.
S0028	Habilidade no desenvolvimento de dicionários de dados.
S0029	Habilidade no desenvolvimento de modelos de dados.
S0030	Habilidade no desenvolvimento de cenários de testes baseados em operações.
S0031	Habilidade no desenvolvimento e aplicação de controles de acesso ao sistema de segurança.
S0032	Habilidade no desenvolvimento, teste e implementação de planos de contingência e recuperação de infraestrutura de rede.
S0033	Habilidade no diagnóstico de problemas de conectividade.
S0034	Habilidade em discernir as necessidades de proteção (ou seja, controles de segurança) de sistemas de informação e redes.
S0035	Habilidade em estabelecer um esquema de roteamento.
S0036	Habilidade na avaliação da adequação dos projetos de segurança.
S0037	Habilidade na geração de consultas e relatórios.
S0038	Habilidade na identificação de medidas ou indicadores de desempenho do sistema e as ações necessárias para melhorar ou corrigir o desempenho, em relação às metas do sistema.
S0039	Habilidade na identificação de possíveis causas de degradação do desempenho ou disponibilidade do sistema e início de ações necessárias para mitigar essa degradação.
S0040	Habilidade na implementação, manutenção e melhoria das práticas estabelecidas de segurança de rede.
S0041	Habilidade na instalação, configuração e solução de problemas dos componentes LAN e WAN, como roteadores, hubs e switches.
S0042	Habilidade na manutenção de bancos de dados. (ex.: backup, restauração, exclusão de dados, arquivos de registro de transações, etc.).
S0043	Habilidade na manutenção dos serviços de diretório. (ex.: Microsoft Active Directory, LDAP, etc.).
S0044	Habilidade em imitar comportamentos de ameaça.
S0045	Habilidade na otimização do desempenho do banco de dados.
S0046	Habilidade na realização de análises em nível de pacote usando ferramentas apropriadas (ex.: Wireshark, tcpdump).
S0047	Habilidade na preservação da integridade das evidências de acordo com os procedimentos operacionais padrão ou normas nacionais.
S0048	Habilidade em testes de integração de sistemas.
S0049	Habilidade na medição e reportagem do capital intelectual.
S0050	Habilidade na modelagem de design e em construir casos de uso (ex.: linguagem de modelagem unificada).
S0051	Habilidade no uso de ferramentas e técnicas de teste de penetração.
S0052	Habilidade no uso de técnicas de engenharia social. (ex.: phishing, baiting, tailgating, etc.).
S0053	Habilidade em sintonizar sensores.

ID de Habilidade	Descrição
S0054	Habilidade no uso de metodologias de manuseio de incidentes.
S0055	Habilidade no uso de tecnologias de gestão do conhecimento.
S0056	Habilidade no uso de ferramentas de gerenciamento de rede para analisar padrões de tráfego de rede (ex.: protocolo simples de gerenciamento de rede).
S0057	Habilidade no uso de analisadores de protocolo.
S0058	Habilidade em usar as ferramentas adequadas para reparar software, hardware e equipamentos periféricos de um sistema.
S0059	Habilidade no uso de dispositivos VPN - Virtual Private Network [rede privada virtual] e criptografia.
S0060	Habilidade na escrita de código em uma linguagem de programação atualmente compatível (ex.: Java, C++).
S0061	Habilidade para escrever planos de teste.
S0062	Habilidade na análise de despejo de memória para extrair informações.
S0063	Habilidade na coleta de dados de uma variedade de recursos de defesa cibernética.
S0064	Habilidade no desenvolvimento e execução de programas de treinamento técnico e currículos.
S0065	Habilidade na identificação e extração de dados de interesse pericial em diversos meios de comunicação (ex.: perícia de mídia).
S0066	Habilidade na identificação de lacunas nas capacidades técnicas.
S0067	Habilidade na identificação, modificação e manipulação de componentes aplicáveis do sistema dentro do Windows, Unix ou Linux (ex.: senhas, contas de usuário, arquivos).
S0068	Habilidade na coleta, processamento, embalagem, transporte e armazenamento de provas eletrônicas para evitar alteração, perda, dano físico ou destruição de dados.
S0069	Habilidade em configurar uma estação de trabalho pericial.
S0070	Habilidade em falar com outras pessoas para transmitir informações de maneira eficaz.
S0071	Habilidade no uso de suítes de ferramentas periciais (ex.: EnCase, Sleuthkit, FTK).
S0072	Habilidade no uso de regras científicas e métodos para resolver problemas.
S0073	Habilidade no uso de máquinas virtuais. (ex.: Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
S0074	Habilidade em desmontar fisicamente PCs.
S0075	Habilidade na realização de análises periciais em múltiplos ambientes do sistema operacional (ex.: sistemas de dispositivos móveis).
S0076	Habilidade na configuração e utilização de ferramentas de proteção de computador baseadas em software (ex.: firewalls de software, software antivírus, anti-spyware).
S0077	Habilidade em proteger as comunicações de rede.
S0078	Habilidade em reconhecer e categorizar tipos de vulnerabilidades e ataques associados.
S0079	Habilidade na proteção de uma rede contra malware. (ex.: NIPS, anti-malware, restringir/prevenir dispositivos externos, filtros de spam) .
S0080	Habilidade na realização de avaliações de danos.
S0081	Habilidade no uso de ferramentas de análise de rede para identificar vulnerabilidades. (ex.: fuzzing, nmap, etc. ).
S0082	Habilidade na avaliação de planos de teste para aplicabilidade e completude.
S0083	Habilidade na integração de ferramentas de teste de segurança da caixa preta em processo de garantia de qualidade de lançamentos de software.
S0084	Habilidade na configuração e utilização de componentes de proteção de rede (ex.: Firewalls, VPNs, sistemas de detecção de invasão de rede).
S0085	Habilidade na realização de auditorias ou revisões de sistemas técnicos.

ID de Habilidade	Descrição
S0086	Habilidade em avaliar a confiabilidade do fornecedor e/ou produto.
S0087	Habilidade em análise profunda do código malicioso capturado (ex.: análise pericial de malware).
S0088	Habilidade no uso de ferramentas de análise binária (ex.: Hexedit, código de comando xxd, hexdump).
S0089	Habilidade em funções hash unilaterais (ex.: Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).
S0090	Habilidade em analisar código anômalo como malicioso ou benigno.
S0091	Habilidade na análise de dados voláteis.
S0092	Habilidade na identificação de técnicas de ofuscação.
S0093	Habilidade em interpretar resultados do depurador para verificar táticas, técnicas e procedimentos.
S0094	Habilidade na leitura de dados hexadecimais.
S0095	Habilidade na identificação de técnicas comuns de codificação (por exemplo, Disjunção Exclusiva [XOR], Código Padrão Americano para Intercâmbio de Informações [ASCII], Unicode, Base64, Uuencode, Codificador Uniforme de Recursos [URL]).
S0096	Habilidade na leitura e interpretação de assinaturas (ex.: snort).
S0097	Habilidade na aplicação de controles de segurança.
S0100	Habilidade em utilizar ou desenvolver atividades de aprendizagem (ex.: cenários, jogos instrucionais, exercícios interativos).
S0101	Habilidade na utilização de tecnologias (ex.: SmartBoards, sites, computadores, projetores) para fins instrucionais.
S0102	Habilidade na aplicação de recursos técnicos de entrega.
S0103	Habilidade na avaliação do poder preditivo e da generalização subsequente de um modelo.
S0104	Habilidade na realização de Revisões de Prontidão de Teste.
S0106	Habilidade em pré-processamento de dados ex.: imputação, redução de dimensionalidade, normalização, transformação, extração, filtragem, suavização).
S0107	Habilidade na concepção e documentação geral das estratégias de Teste e Avaliação do programa.
S0108	Habilidade no desenvolvimento da força de trabalho e normas de qualificação de cargos.
S0109	Habilidade na identificação de padrões ou relacionamentos ocultos.
S0110	Habilidade na identificação de requisitos de infraestrutura de Teste e Avaliação (pessoas, faixas, ferramentas, instrumentação).
S0111	Habilidade em interagir com os clientes.
S0112	Habilidade no gerenciamento de ativos de teste, recursos de teste e pessoal de teste para garantir a conclusão eficaz dos eventos de teste.
S0113	Habilidade na realização de conversões de formato para criar uma representação padrão dos dados.
S0114	Habilidade na realização de análise de sensibilidade.
S0115	Habilidade na preparação de relatórios de Teste e Avaliação.
S0116	Habilidade em projetar soluções de segurança multinível/domínio cruzado.
S0117	Habilidade no fornecimento de estimativa de recursos de Teste e Avaliação.
S0118	Habilidade no desenvolvimento de ontologias semânticas compreensíveis pela máquina.
S0119	Habilidade em Análise de Regressão (ex.: Stepwise Hierárquico, Modelo Linear Generalizado, Quadrados Mínimos Ordinários, Métodos Baseados em Árvores, Logística).

ID de Habilidade	Descrição
S0120	Habilidade em revisar logs para identificar evidências de invasões anteriores.
S0121	Habilidade em técnicas de endurecimento de sistema, rede e SO. (ex.: remover serviços desnecessários, políticas sobre senhas, segmentação de rede, ativação de registro, privilégio mínimo, etc.).
S0122	Habilidade no uso de métodos de design.
S0123	Habilidade em análise de transformação (ex.: agregação, enriquecimento, processamento).
S0124	Habilidade na solução de problemas e diagnóstico de anomalias de infraestrutura de defesa cibernética e trabalho através de resolução.
S0125	Habilidade no uso de estatísticas e técnicas descritivas básicas (ex.: normalidade, distribuição de modelos, gráficos de dispersão).
S0126	Habilidade no uso de ferramentas de análise de dados (ex.: Excel, STATA SAS, SPSS).
S0127	Habilidade no uso de ferramentas de mapeamento de dados.
S0128	Habilidade no uso de mão-de-obra e sistemas de TI para quadro de pessoal.
S0129	Habilidade no uso de técnicas de identificação e remoção de outliers.
S0130	Habilidade na escrita de scripts usando R, Python, PIG, HIVE, SQL, etc.
S0131	Habilidade na análise de malware.
S0132	Habilidade na realização de análises em nível de bits.
S0133	Habilidade no processamento de provas digitais, para incluir a proteção e a realização de cópias legalmente sólidas de evidências.
S0134	Habilidade na realização de revisões de sistemas.
S0135	Habilidade no design seguro do plano de teste (ex.: unidade, integração, sistema, aceitação).
S0136	Habilidade em princípios de gerenciamento de sistemas de rede, modelos, métodos (ex.: monitoramento de desempenho de sistemas de ponta a ponta) e ferramentas.
S0137	Habilidade em conduzir avaliações de vulnerabilidade de aplicativos.
S0138	Habilidade no uso de criptografia de chave pública (PKI) e recursos de assinatura digital em aplicativos (ex.: e-mail S/MIME, tráfego SSL).
S0139	Habilidade na aplicação de modelos de segurança (ex.: modelo Bell-LaPadula, modelo de integridade Biba, modelo de integridade Clark-Wilson).
S0140	Habilidade na aplicação do processo de engenharia de sistemas.
S0141	Habilidade na avaliação de projetos de sistemas de segurança.
S0142	Habilidade na realização de pesquisas para solucionar problemas novos no nível do cliente.
S0143	Habilidade na condução do planejamento, gerenciamento e manutenção do sistema/servidor.
S0144	Habilidade na correção de problemas físicos e técnicos que impactam o desempenho do sistema/servidor.
S0145	Habilidade na integração e aplicação de políticas que atendam aos objetivos de segurança do sistema.
S0146	Habilidade na criação de políticas que permitam que os sistemas atendam aos objetivos de desempenho (ex.: roteamento de tráfego, SLAs, especificações de CPU).
S0147	Habilidade na avaliação de controles de segurança com base em princípios e conceitos de segurança cibernética. (ex.: CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
S0148	Habilidade em projetar a integração de processos e soluções tecnológicas, incluindo sistemas legados e modernas linguagens de programação.

ID de Habilidade	Descrição
S0149	Habilidade no desenvolvimento de aplicativos que podem registrar e lidar com erros, exceções e falhas de aplicativos e registro.
S0150	Habilidade na implementação e teste de planos de contingência e recuperação de infraestrutura de rede.
S0151	Habilidade na solução de problemas de componentes do sistema com falha (ex.: servidores)
S0152	Habilidade na tradução de requisitos operacionais em necessidades de proteção (ex.: controles de segurança).
S0153	Habilidade na identificação e antecipação de problemas de desempenho, disponibilidade, capacidade ou configuração do sistema/servidor.
S0154	Habilidade na instalação de upgrades de sistemas e componentes. (ex.: servidores, aparelhos, dispositivos de rede).
S0155	Habilidade no monitoramento e otimização do desempenho do sistema/servidor.
S0156	Habilidade na realização de análises em nível de pacote.
S0157	Habilidade na recuperação de sistemas/servidores com falha. (ex.: software de recuperação, clusters failover, replicação, etc.) .
S0158	Habilidade na administração do sistema operacional. (ex.: manutenção de conta, backups de dados, manter o desempenho do sistema, instalar e configurar novo hardware/software).
S0159	Habilidade na configuração e validação de estações de trabalho de rede e periféricos de acordo com as normas e/ou especificações aprovadas.
S0160	Habilidade no uso de modelagem de design (ex.: linguagem de modelagem unificada).
S0161	Retirada – Integrada em S0160
S0162	Habilidade em sub-redes.
S0163	Retirada – Integrada em S0060
S0164	Habilidade na avaliação da aplicação de normas criptográficas.
S0166	Habilidade na identificação de lacunas em capacidades técnicas de entrega.
S0167	Habilidade no reconhecimento de vulnerabilidades em sistemas de segurança. (ex.: varredura de vulnerabilidade e conformidade).
S0168	Habilidade na criação de sub-redes físicas ou lógicas que separam uma rede interna de área local (LAN) de outras redes não confiáveis.
S0169	Habilidade na realização de análise de tendências.
S0170	Habilidade na configuração e utilização de componentes de proteção de computador (ex.: firewalls de hardware, servidores, roteadores, conforme apropriado).
S0171	Habilidade na realização de avaliações de impacto/risco.
S0172	Habilidade na aplicação de técnicas seguras de codificação.
S0173	Habilidade no uso de ferramentas de correlação de eventos de segurança.
S0174	Habilidade no uso de ferramentas de análise de código.
S0175	Habilidade na realização de análise de causa-raiz.
S0176	Habilidade em atividades de planejamento administrativo, para incluir a elaboração de planos de apoio funcionais e específicos, preparação e gerenciamento de correspondências e procedimentos de contratação.
S0177	Habilidade na análise das redes de comunicação de destino.
S0178	Habilidade na análise de dados essenciais de rede (ex.: arquivos de configuração do roteador, protocolos de roteamento).
S0179	Habilidade na análise de ferramentas de processamento de idiomas para fornecer feedback para melhorar o desenvolvimento de ferramentas.

ID de Habilidade	Descrição
S0180	Retirada – Integrada em S0062
S0181	Habilidade na análise de dados de coleta de ponto médio.
S0182	Habilidade na análise de comunicações de destino internas e externas coletadas de LANs sem fio.
S0183	Habilidade na análise de dados de coleta de terminais ou ambientes.
S0184	Habilidade de analisar o tráfego para identificar dispositivos de rede.
S0185	Habilidade na aplicação de métodos analíticos tipicamente utilizados para apoiar o planejamento e justificar estratégias e cursos de ação recomendados.
S0186	Habilidade na aplicação de procedimentos de planejamento em caso de crises.
S0187	Habilidade na aplicação de vários métodos analíticos, ferramentas e técnicas (ex.: hipóteses concorrentes; cadeia de raciocínio; métodos de cenário; detecção de negação e engano; alto impacto-baixa probabilidade; análise de rede/associação ou link; análises Bayesianas, Delphi e de Padrão).
S0188	Habilidade na avaliação do quadro de referência de um alvo (ex.: motivação, capacidade técnica, estrutura organizacional, sensibilidades).
S0189	Habilidade na avaliação e/ou estimativa dos efeitos gerados durante e após operações cibernéticas.
S0190	Habilidade na avaliação de ferramentas atuais para identificar melhorias necessárias.
S0191	Habilidade na avaliação da aplicabilidade das ferramentas analíticas disponíveis para diversas situações.
S0192	Habilidade na auditoria de firewalls, perímetros, roteadores e sistemas de detecção de invasões.
S0193	Habilidade no cumprimento das restrições legais para informações direcionadas.
S0194	Habilidade na realização de pesquisas não atribuíveis.
S0195	Habilidade na realização de pesquisas usando todas as fontes disponíveis.
S0196	Habilidade na realização de pesquisas usando deep web.
S0197	Habilidade na realização de análises de redes sociais, análise de listas de amigos e/ou análise de cookies.
S0198	Habilidade na realização de análises de redes sociais.
S0199	Habilidade na criação e extração de informações importantes de capturas de pacotes.
S0200	Habilidade na criação de requisitos de coleta em apoio às atividades de aquisição de dados.
S0201	Habilidade na criação de planos de apoio a operações remotas. (ex.: locais quentes/mornos/frios/sites alternativos, recuperação de desastres) .
S0202	Habilidade em técnicas de mineração de dados (ex.: sistemas de arquivos de pesquisa) e análise.
S0203	Habilidade na definição e caracterização de todos os aspectos pertinentes do ambiente operacional.
S0204	Habilidade em descrever dados de origem ou garantia em um mapa de rede.
S0205	Habilidade na determinação de opções de segmentação adequadas através da avaliação dos recursos disponíveis em relação aos efeitos desejados.
S0206	Habilidade para determinar patches instalados em vários sistemas operacionais e na identificação de assinaturas de patches.
S0207	Habilidade na determinação do efeito de várias configurações de roteador e firewall em padrões de tráfego e desempenho de rede em ambientes LAN e WAN.
S0208	Habilidade na determinação da localização física dos dispositivos de rede.

ID de Habilidade	Descrição
S0209	Habilidade no desenvolvimento e execução de programas abrangentes de avaliação de operações cibernéticas para avaliar e validar características de desempenho operacional.
S0210	Habilidade no desenvolvimento de relatórios de inteligência.
S0211	Habilidade no desenvolvimento ou recomendação de abordagens ou soluções analíticas para problemas e situações para as quais as informações estão incompletas ou não existe precedente.
S0212	Habilidade na disseminação de itens de maior valor de inteligência em tempo hábil.
S0213	Habilidade em documentar e comunicar informações técnicas e programáticas complexas.
S0214	Habilidade na avaliação de acessos para o valor da inteligência.
S0215	Habilidade na avaliação e interpretação de metadados.
S0216	Habilidade na avaliação dos recursos disponíveis contra os efeitos desejados para fornecer cursos eficazes de ação.
S0217	Habilidade na avaliação de fontes de dados para relevância, confiabilidade e objetividade.
S0218	Habilidade na avaliação de informações para confiabilidade, validade e relevância.
S0219	Habilidade na avaliação de informações para reconhecer relevância, prioridade, etc.
S0220	Habilidade na exploração/consulta de bancos de dados de coleta organizacional e/ou de parceiros.
S0221	Habilidade na extração de informações de capturas de pacotes.
S0222	Habilidade na análise de fusão
S0223	Habilidade na geração de planos de operação em apoio aos requisitos de missão e destino.
S0224	Habilidade em entender o significado das comunicações de destino.
S0225	Habilidade de identificar as redes de comunicação de um destino.
S0226	Habilidade em identificar as características da rede de um destino.
S0227	Habilidade de identificar interpretações analíticas alternativas para minimizar resultados imprevistos.
S0228	Habilidade de identificar elementos de destino críticos, para serem incluídos no domínio cibernético.
S0229	Habilidade de identificar ameaças cibernéticas que podem comprometer interesses da organização e/ou parceiros.
S0230	Retirada – integrada em S0066
S0231	Habilidade de identificar como um alvo se comunica.
S0232	Habilidade de identificar lacunas e limitações de inteligência.
S0233	Habilidade de identificar questões linguísticas que podem ter impacto nos objetivos da organização.
S0234	Habilidade de identificar leads para o desenvolvimento de alvos.
S0235	Habilidade de identificar idiomas e dialetos regionais não-alvo
S0236	Habilidade de identificar dispositivos que funcionam em cada nível de modelos de protocolo.
S0237	Habilidade de identificar a localização e rastreamento de alvos através de técnicas de análise geoespacial
S0238	Habilidade na priorização de informações no que se refere às operações.
S0239	Habilidade na interpretação de linguagens de programação compiladas e interpretativas.
S0240	Habilidade em interpretar metadados e conteúdos, conforme aplicados por sistemas de coleta.

ID de Habilidade	Descrição
S0241	Habilidade de interpretar resultados de traceroute, conforme se aplicam à análise e reconstrução da rede.
S0242	Habilidade de interpretar resultados do scanner de vulnerabilidade para identificar vulnerabilidades.
S0243	Habilidade em gestão do conhecimento, incluindo experiência em documentação técnica (ex.: página Wiki).
S0244	Habilidade no gerenciamento de relacionamentos com os clientes, incluindo determinar as necessidades/requisitos dos clientes, gerenciar as expectativas e demonstrar compromisso em entregar resultados de qualidade.
S0245	Habilidade na navegação de software de visualização de rede.
S0246	Habilidade na normalização de números.
S0247	Habilidade na execução da fusão de dados derivados da inteligência existente para permitir uma coleta nova e contínua.
S0248	Habilidade na realização de análises do sistema de destino.
S0249	Habilidade na preparação e apresentação de briefings.
S0250	Habilidade na preparação de planos e correspondências relacionadas.
S0251	Habilidade em priorizar material de linguagem de destino.
S0252	Habilidade no processamento de dados coletados para análise de acompanhamento.
S0253	Habilidade no fornecimento de análises sobre assuntos relacionados ao destino (ex.: exemplo, linguagem, cultura, comunicações).
S0254	Habilidade em fornecer análises para auxiliar na redação de relatórios em fases após a ação.
S0255	Habilidade em fornecer informações de geolocalização em tempo real e acionáveis utilizando infraestruturas de destino.
S0256	Habilidade em fornecer compreensão dos sistemas alvo ou ameaça através da análise de identificação e links de relacionamentos físicos, funcionais ou comportamentais.
S0257	Habilidade na leitura, interpretação, escrita, modificação e execução de scripts simples (ex.: PERL, VBS) em sistemas Windows e Unix (ex.: aqueles que executam tarefas como analisar grandes arquivos de dados, automatizar tarefas manuais e buscar/processar dados remotos).
S0258	Habilidade em reconhecer e interpretar atividades maliciosas da rede no tráfego.
S0259	Habilidade em reconhecer técnicas de negação e engano do alvo.
S0260	Habilidade em reconhecer oportunidades de ponto médio e informações essenciais.
S0261	Habilidade em reconhecer a relevância da informação.
S0262	Habilidade em reconhecer mudanças significativas nos padrões de comunicação de um alvo.
S0263	Habilidade no reconhecimento de informações técnicas que podem ser usadas para leads em análise de metadados.
S0264	Habilidade em reconhecer informações técnicas que podem ser usadas para leads para habilitar operações remotas (dados incluem usuários, senhas, endereços de e-mail, faixas de IP do destino, frequência no comportamento DNI, servidores de correio, servidores de domínio, informações de cabeçalho SMTP).
S0265	Habilidade em reconhecer informações técnicas que podem ser usadas para o desenvolvimento de alvos, incluindo o desenvolvimento de inteligência.
S0266	Habilidade em linguagens de programação relevantes (ex.: C++, Python, etc.).
S0267	Habilidade em linha de comando remoto e uso de ferramentas de interface gráfica de usuário (GUI).
S0268	Habilidade na pesquisa de informações essenciais.

ID de Habilidade	Descrição
S0269	Habilidade na pesquisa de vulnerabilidades e explorações utilizadas no tráfego.
S0270	Habilidade em engenharia reversa (ex.: edição hexadecimal, utilitários de empacotamento binário, depuração e análise de strings) para identificar a função e propriedade de ferramentas remotas.
S0271	Habilidade na revisão e edição de produtos de avaliação.
S0272	Habilidade na revisão e edição de produtos de inteligência de várias fontes para operações cibernéticas.
S0273	Habilidade em revisar e editar planos.
S0274	Habilidade na revisão e edição de materiais-alvo.
S0275	Habilidade em administração de servidores.
S0276	Habilidade em pesquisa, coleta e análise de metadados LAN sem fio.
S0277	Habilidade em sintetizar, analisar e priorizar o significado entre os conjuntos de dados.
S0278	Habilidade em adaptar a análise aos níveis necessários (ex.: classificação e organizacional).
S0279	Habilidade no desenvolvimento de alvos em suporte direto a operações de coleta.
S0280	Habilidade na identificação de anomalias de rede de destino (ex.: invasões, fluxo de dados ou processamento, implementação direcionada de novas tecnologias).
S0281	Habilidade em escrita técnica.
S0282	Habilidade em testar e avaliar ferramentas para implementação.
S0283	Habilidade em transcrever comunicações na língua alvo.
S0284	Habilidade na tradução de materiais gráficos e/ou de voz na língua alvo.
S0285	Habilidade em usar operadores booleanos para construir consultas simples e complexas.
S0286	Habilidade em usar bancos de dados para identificar informações relevantes do alvo.
S0287	Habilidade no uso de dados geoespaciais e na aplicação de recursos geoespaciais.
S0288	Habilidade no uso de múltiplas ferramentas analíticas, bancos de dados e técnicas (ex.: Notebook do Analista, A-Space, Anchory, M3, pensamento divergente/convergente, gráficos de links, matrizes, etc.).
S0289	Habilidade no uso de vários mecanismos de pesquisa (ex.: Google, Yahoo, LexisNexis, DataStar) e ferramentas na realização de pesquisas de código aberto.
S0290	Habilidade no uso de redes não atribuíveis.
S0291	Habilidade no uso de métodos de pesquisa, incluindo fontes múltiplas e diferentes para reconstruir uma rede-alvo.
S0292	Habilidade no uso de bancos de dados de segmentação e pacotes de software.
S0293	Habilidade no uso de ferramentas, técnicas e procedimentos para explorar remotamente e estabelecer persistência em um alvo.
S0294	Habilidade em usar ferramentas de rastreamento de rota e interpretar os resultados conforme se aplicam à análise e reconstrução de rede.
S0295	Habilidade no uso de várias ferramentas de coleta de dados de código aberto (comércio on-line, DNS, correio, etc.).
S0296	Habilidade em utilizar feedback para melhorar processos, produtos e serviços.
S0297	Habilidade na utilização de espaços de trabalho e/ou ferramentas colaborativas virtuais (ex.: IWS, VTCs, salas de bate-papo, SharePoint).
S0298	Habilidade em verificar a integridade de todos os arquivos. (ex.: checksums, OR exclusivo, hashes seguros, restrições de verificação, etc.).
S0299	Habilidade em análise de alvo de rede sem fio, templating e geolocalização.
S0300	Habilidade em escrever (e enviar) requisitos para atender lacunas em capacidades técnicas.

ID de Habilidade	Descrição
S0301	Habilidade em escrever sobre fatos e ideias de forma clara, convincente e organizada.
S0302	Habilidade em escrever relatórios de eficácia.
S0303	Habilidade em escrever, revisar e editar produtos de inteligência/avaliação relacionados à cibernética de várias fontes.
S0304	Habilidade para acessar informações sobre ativos atuais disponíveis, utilização.
S0305	Habilidade para acessar os bancos de dados onde os planos/diretrizes/orientações são mantidos.
S0306	Habilidade para analisar orientações estratégicas para questões que requerem esclarecimentos e/ou orientação adicional.
S0307	Habilidade para analisar alvos ou fontes de ameaças de força e moral.
S0308	Habilidade para antecipar os requisitos de emprego da capacidade de inteligência.
S0309	Habilidade para antecipar o alvo principal ou atividades de ameaça que provavelmente exigirão uma decisão por parte da liderança.
S0310	Habilidade para aplicar normas analíticas para avaliar produtos de inteligência.
S0311	Habilidade para aplicar os recursos, limitações e metodologias de tarefas das plataformas, sensores, arquiteturas e aparelhos disponíveis conforme se aplicam aos objetivos da organização.
S0312	Habilidade para aplicar o processo utilizado para avaliar o desempenho e o impacto das operações cibernéticas.
S0313	Habilidade para articular uma declaração/exigência de necessidades e integrar novos e emergentes recursos de coleta, acessos e/ou processos em operações de coleta.
S0314	Habilidade para articular recursos de inteligência disponíveis para apoiar a execução do plano.
S0315	Habilidade para articular as necessidades dos planejadores conjuntos para os analistas de todas as fontes.
S0316	Habilidade para associar lacunas de inteligência a requisitos prioritários de informações e observáveis.
S0317	Habilidade para comparar indicadores/observáveis aos requisitos.
S0318	Habilidade para conceituar a totalidade do processo de inteligência nos múltiplos domínios e dimensões.
S0319	Habilidade para converter requisitos de inteligência em tarefas de produção de inteligência.
S0320	Habilidade para coordenar o desenvolvimento de produtos de inteligência sob medida.
S0321	Habilidade para correlacionar prioridades de inteligência à alocação de recursos/ativos de inteligência.
S0322	Habilidade para elaborar indicadores de progresso/sucesso operacional.
S0323	Habilidade para criar e manter documentos de planejamento atualizados e rastreamento de serviços/produção.
S0324	Habilidade para determinar a viabilidade da coleta.
S0325	Habilidade para desenvolver um plano de coleta que mostre claramente a disciplina que pode ser usada para coletar as informações necessárias.
S0326	Habilidade para distinguir entre recursos nocionais e reais e sua aplicabilidade ao plano em desenvolvimento.
S0327	Habilidade para garantir que a estratégia de coleta aproveite todos os recursos disponíveis.
S0328	Habilidade para avaliar fatores do ambiente operacional comparado aos objetivos e requisitos de informações.

ID de Habilidade	Descrição
S0329	Habilidade para avaliar solicitações de informações para determinar se existem informações de resposta.
S0330	Habilidade para avaliar as capacidades, limitações e metodologias de atribuição de tarefas orgânicas, teatrais, nacionais, de coalizão e outras capacidades de coleta.
S0331	Habilidade para expressar oralmente e por escrito a relação entre as limitações da capacidade de inteligência e o risco de tomada de decisão e os impactos na operação geral.
S0332	Habilidade para extrair informações de ferramentas e aplicativos disponíveis associados aos requisitos de coleta e gerenciamento de operações de coleta.
S0333	Habilidade para representar graficamente materiais de suporte de decisão contendo estimativas de inteligência e capacidade de parceiros.
S0334	Habilidade para identificar e aplicar tarefas, coleta, processamento, exploração e disseminação às disciplinas de coleta associadas.
S0335	Habilidade para identificar lacunas de inteligência.
S0336	Habilidade para identificar quando os requisitos de informações prioritárias são satisfeitos.
S0337	Habilidade para implementar procedimentos estabelecidos para avaliar as atividades de gestão de coleta e operações.
S0338	Habilidade para interpretar as orientações de planejamento para discernir o nível de suporte analítico necessário.
S0339	Habilidade para interpretar relatórios de prontidão, sua relevância operacional e impacto na coleta de inteligência.
S0340	Habilidade para monitorar o alvo ou situação de ameaça e fatores ambientais.
S0341	Habilidade para monitorar os efeitos de ameaças aos recursos do parceiro e manter uma estimativa de execução.
S0342	Habilidade para otimizar o desempenho do sistema de coleta através de ajustes repetidos, testes e reajuste.
S0343	Habilidade para orquestrar equipes de planejamento de inteligência, coordenar o suporte de coleta e produção e monitorar o status.
S0344	Habilidade para preparar e entregar relatórios, apresentações e briefings, incluindo o uso de recursos visuais ou tecnologia de apresentação.
S0345	Habilidade para relacionar recursos/ativos de inteligência aos requisitos de inteligência previstos.
S0346	Habilidade para resolver requisitos conflitantes de coleta.
S0347	Habilidade para revisar especificações de desempenho e informações históricas sobre ativos de coleta.
S0348	Habilidade para especificar coletas e/ou tarefas que devem ser realizadas em curto prazo.
S0349	Habilidade para sincronizar os procedimentos de avaliação operacional com o processo de exigência de informações críticas.
S0350	Habilidade para sincronizar atividades de planejamento e o suporte de inteligência necessário.
S0351	Habilidade para traduzir as capacidades, limitações e metodologias de atribuição de tarefas orgânicas, teatrais, nacionais, de coalizão e outras capacidades de coleta.
S0352	Habilidade para usar ferramentas e ambientes colaborativos para operações de coleta.
S0353	Habilidade para usar sistemas e/ou ferramentas para rastrear os requisitos de coleta e determinar se estão sendo satisfeitos.

ID de Habilidade	Descrição
S0354	Habilidade na criação de políticas que reflitam os principais objetivos empresariais de privacidade.
S0355	Habilidade na negociação de acordos com fornecedores e na avaliação das práticas de privacidade dos fornecedores.
S0356	Habilidade na comunicação com todos os níveis de gestão, incluindo membros do Conselho (por exemplo, habilidades interpessoais, capacidade de aproximação, habilidades de escuta eficazes, uso adequado de estilo e linguagem para o público).
S0357	Habilidade para antecipar novas ameaças à segurança.
S0358	Habilidade para se manter ciente da evolução das infraestruturas técnicas.
S0359	Habilidade de usar o pensamento crítico para analisar padrões e relacionamentos organizacionais.
S0360	Habilidade para analisar e avaliar recursos e ferramentas de operações cibernéticas de parceiros internos e externos.
S0361	Habilidade para analisar e avaliar processos internos e externos de inteligência de parceiros e o desenvolvimento de requisitos de informações de rotina e informações essenciais.
S0362	Habilidade para analisar e avaliar as capacidades e limitações internas e externas de organizações parceiras (aquelas com responsabilidades de tarefa, coleta, processamento, exploração e divulgação).
S0363	Habilidade para analisar e avaliar relatórios de parceiros internos e externos.
S0364	Habilidade para desenvolver percepções sobre o contexto do ambiente de ameaças de uma organização
S0365	Habilidade para preparar resposta a incidentes para modelos de serviço em nuvem.
S0366	Habilidade para identificar recursos de sucesso e encontrar soluções para problemas de sistema menos comuns e mais complexos.
S0367	Habilidade para aplicar princípios de cibersegurança e privacidade aos requisitos organizacionais (relevantes para confidencialidade, integridade, disponibilidade, autenticação, não repúdio).
S0368	Habilidade para usar pontuação de risco para informar abordagens baseadas em desempenho e econômicas para ajudar as organizações a identificar, avaliar e gerenciar riscos de cibersegurança.
S0369	Habilidade para identificar fontes, características e usos dos ativos de dados da organização.
S0370	Habilidade para usar a estrutura de relatório e os processos do provedor de serviços de defesa cibernética dentro da própria organização.
S0371	Habilidade para responder e tomar medidas locais em resposta aos alertas de compartilhamento de ameaças de provedores de serviços.
S0372	Habilidade para traduzir, rastrear e priorizar as necessidades de informações e os requisitos de coleta de inteligência em toda a empresa.
S0373	Habilidade para garantir que as informações de responsabilidade sejam coletadas para os componentes da infraestrutura da cadeia de suprimentos do sistema de informações e tecnologia de informação e comunicações.
S0374	Habilidade para identificar problemas de segurança cibernética e privacidade decorrentes de conexões com clientes internos e externos e organizações parceiras.

## A.7 Descrições de Capacidades do NICE Framework

A Tabela 7 fornece uma lista de capacidades de segurança cibernética. Capacidade significa competência para realizar um comportamento observável ou um comportamento que resulta em um produto observável. As descrições de capacidade selecionadas nesta lista estão incluídas em cada função de trabalho na listagem detalhada da função de trabalho no apêndice B. Esta listagem será atualizada periodicamente [1]. A fonte definitiva para a versão mais atual deste material pode ser encontrada na Planilha de Referência para a Publicação Especial NIST 800-181 [4].

**Tabela 7 - Descrições de Aptidões do NICE Framework**

ID de Aptidão	Descrição
A0001	Aptidão para identificar problemas de segurança sistêmicos com base na análise de dados de vulnerabilidade e configuração.
A0002	Aptidão para combinar a tecnologia adequada do repositório de conhecimento para uma determinada aplicação ou ambiente.
A0003	Aptidão para determinar a validade dos dados de tendência da tecnologia.
A0004	Aptidão para desenvolver currículo que explique sobre o tópico no nível adequado para o público-alvo.
A0005	Aptidão para descriptografar coletas de dados digitais.
A0006	Aptidão para preparar e fornecer briefings sobre educação e conscientização para garantir que os sistemas, a rede e os usuários de dados estejam cientes e sigam as políticas e procedimentos de segurança dos sistemas.
A0007	Aptidão para adaptar a análise de código para questões específicas do aplicativo.
A0008	Aptidão para aplicar os métodos, normas e abordagens para descrever, analisar e documentar a arquitetura de tecnologia da informação corporativa (TI) de uma organização (ex.: Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).
A0009	Aptidão para aplicar normas de gerenciamento de riscos da cadeia de suprimentos.
A0010	Aptidão para analisar malware.
A0011	Aptidão para responder perguntas de forma clara e concisa.
A0012	Aptidão para fazer perguntas esclarecedoras.
A0013	Aptidão para comunicar informações, conceitos ou ideias complexas de forma confiante e bem organizada por meios verbais, escritos e/ou visuais.
A0014	Aptidão para se comunicar efetivamente ao escrever.
A0015	Aptidão para realizar varreduras de vulnerabilidade e reconhecer vulnerabilidades em sistemas de segurança.
A0016	Aptidão para facilitar discussões em pequenos grupos.
A0017	Aptidão para medir a compreensão e o nível de conhecimento do aprendiz.
A0018	Aptidão para preparar e apresentar briefings.
A0019	Aptidão para produzir documentação técnica.
A0020	Aptidão para fornecer feedback eficaz aos alunos para melhorar a aprendizagem.
A0021	Aptidão para usar e entender conceitos matemáticos complexos (ex.: matemática discreta).
A0022	Aptidão para aplicar princípios de aprendizagem de adultos.
A0023	Aptidão para elaborar avaliações válidas e confiáveis.
A0024	Aptidão para desenvolver direcionamento claro e materiais instrucionais.
A0025	Aptidão para definir com precisão incidentes, problemas e eventos no sistema de tickets de problemas.

ID de Aptidão	Descrição
A0026	Aptidão para analisar dados de teste.
A0027	Aptidão para aplicar os objetivos e metas de uma organização para desenvolver e manter a arquitetura.
A0028	Aptidão para avaliar e prever requisitos de mão de obra para atender aos objetivos organizacionais.
A0029	Aptidão para construir estruturas de dados complexas e linguagens de programação de alto nível.
A0030	Aptidão para coletar, verificar e validar dados de teste.
A0031	Aptidão para conduzir e implementar pesquisas de mercado para entender os recursos governamentais e do setor e preços adequados.
A0032	Aptidão para desenvolver currículo para uso dentro de um ambiente virtual.
A0033	Aptidão para desenvolver políticas, planos e estratégia em conformidade com leis, regulamentos, políticas e políticas de apoio às atividades cibernéticas organizacionais.
A0034	Aptidão para desenvolver, atualizar e/ou manter procedimentos operacionais padrão (SOPs).
A0035	Aptidão para destrinchar um problema e examinar as inter-relações entre dados que podem parecer não relacionados.
A0036	Aptidão para identificar falhas básicas de codificação comuns em alto nível.
A0037	Aptidão para alavancar as melhores práticas e lições aprendidas de organizações externas e instituições acadêmicas que lidam com questões cibernéticas.
A0038	Capacidade de otimizar sistemas para atender aos requisitos de desempenho corporativo.
A0039	Aptidão para supervisionar o desenvolvimento e atualização da estimativa de custo do ciclo de vida.
A0040	Capacidade de traduzir dados e testar resultados em conclusões avaliativas.
A0041	Aptidão para usar ferramentas de visualização de dados (ex.: Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tableau, Raphael.js).
A0042	Capacidade de desenvolver oportunidades de carreira.
A0043	Aptidão para realizar análises periciais em Windows e Unix/Linux, e para esses ambientes também.
A0044	Capacidade de aplicar estruturas de linguagem de programação (ex.: revisão de código fonte) e lógica.
A0045	Aptidão para avaliar/garantir a confiabilidade do fornecedor e/ou produto.
A0046	Capacidade de monitorar e avaliar o impacto potencial das tecnologias emergentes em leis, regulamentos e/ou políticas.
A0047	Aptidão para desenvolver softwares seguro de acordo com metodologias, ferramentas e práticas seguras de implantação de software.
A0048	Aptidão para aplicar conceitos de arquitetura de segurança de rede, incluindo topologia, protocolos, componentes e princípios (ex.: aplicação de defesa em profundidade).
A0049	Capacidade de aplicar ferramentas, métodos e técnicas de design de sistema seguro.
A0050	Aptidão para aplicar ferramentas, métodos e técnicas de design de sistemas, incluindo análise automatizada de sistemas e ferramentas de design.
A0051	Aptidão para executar processos de integração de tecnologia.
A0052	Capacidade de operar equipamentos de rede, incluindo hubs, roteadores, switches, pontes, servidores, mídia de transmissão e hardware relacionado.
A0053	Aptidão para determinar a validade dos dados de tendência da força de trabalho.
A0054	Capacidade de aplicar a metodologia de Instructional System Design (ISD).
A0055	Aptidão para operar ferramentas de rede comuns (ex.: ping, traceroute, nslookup).
A0056	Aptidão para garantir que as práticas de segurança sejam seguidas durante todo o processo de aquisição.

ID de Aptidão	Descrição
A0057	Aptidão para adaptar o currículo que aborda o tópico no nível apropriado para o público-alvo.
A0058	Aptidão para de executar a linha de comando do sistema operacional (ex.: ipconfig, netstat, dir, nbtstat).
A0059	Aptidão para operar os caminhos LAN/WAN da organização.
A0060	Aptidão para construir arquiteturas e frameworks.
A0061	Aptidão para projetar arquiteturas e frameworks.
A0062	Aptidão para monitorar medidas ou indicadores de desempenho e disponibilidade do sistema.
A0063	Aptidão para operar diferentes sistemas e métodos de comunicação eletrônica (ex.: e-mail, VOIP, IM, fóruns da web, Direct Video Broadcasts).
A0064	Aptidão para interpretar e traduzir os requisitos do cliente em recursos operacionais.
A0065	Aptidão para monitorar fluxos de tráfego através da rede.
A0066	Aptidão para fornecer de forma precisa e completa todos os dados usados em produtos de inteligência, avaliação e/ou planejamento.
A0067	Aptidão para se adaptar e operar em um ambiente de trabalho diverso, imprevisível, desafiador e acelerado.
A0068	Aptidão para aplicar processos de desenvolvimento de planejamento e recrutamento aprovados.
A0069	Aptidão para aplicar habilidades e estratégias colaborativas.
A0070	Aptidão para aplicar habilidades críticas de leitura/pensamento.
A0071	Aptidão para aplicar linguagem e conhecimento cultural à análise.
A0072	Aptidão para articular claramente os requisitos de inteligência, transformando-os em questões de pesquisas bem formuladas e variáveis de rastreamento de dados para fins de rastreamento de investigações.
A0073	Aptidão para articular claramente os requisitos de inteligência, transformando-os em questões de pesquisas bem formuladas e pedidos de informações.
A0074	Aptidão para colaborar efetivamente com outras pessoas.
A0076	Aptidão para coordenar e colaborar com analistas quanto aos requisitos de vigilância e desenvolvimento de informações essenciais.
A0077	Aptidão para coordenar operações cibernéticas com outras funções da organização ou atividades de suporte.
A0078	Aptidão para coordenar, colaborar e disseminar informações para organizações subordinadas, laterais e de alto nível.
A0079	Aptidão para empregar corretamente cada organização ou elemento no plano de coleta e matriz.
A0080	Aptidão para desenvolver ou recomendar abordagens ou soluções analíticas para situações e problemas para os quais as informações estão incompletas ou não existe precedente.
A0081	Aptidão para desenvolver ou recomendar soluções de planejamento para situações e problemas para os quais não existe precedente.
A0082	Aptidão para colaborar efetivamente por meio de equipes virtuais.
A0083	Aptidão para avaliar a confiabilidade, validade e relevância de informações.
A0084	Aptidão para avaliar, analisar e sintetizar grandes quantidades de dados (que podem ser fragmentados e contraditórios) em produtos combinados de segmentação/inteligência de alta qualidade.
A0085	Capacidade de discernimento quando as políticas não são bem definidas.
A0086	Aptidão para expandir o acesso à rede realizando análise e coleta de alvos para identificar alvos de interesse.

ID de Aptidão	Descrição
A0087	Capacidade de concentrar esforços de pesquisa para atender às necessidades de tomada de decisão do cliente.
A0088	Aptidão para funcionar com eficiência em um ambiente dinâmico e acelerado.
A0089	Capacidade de funcionar em um ambiente colaborativo, buscando consulta contínua com outros analistas e especialistas — tanto internos quanto externos à organização — para alavancar conhecimentos analíticos e técnicos.
A0090	Aptidão para identificar parceiros externos com interesses comuns em operações cibernéticas.
A0091	Aptidão para identificar lacunas de inteligência.
A0092	Aptidão para identificar/descrever vulnerabilidades de um alvo.
A0093	Aptidão para identificar/descrever técnicas/métodos para realizar exploração técnica do alvo.
A0094	Aptidão para interpretar e aplicar leis, regulamentos, políticas e orientações relevantes para os objetivos cibernéticos da organização.
A0095	Aptidão para interpretar e traduzir exigências do cliente em ações operacionais.
A0096	Aptidão para interpretar e entender conceitos complexos e em rápida evolução.
A0097	Aptidão para monitorar as operações do sistema e reagir a eventos em resposta a gatilhos e/ou observação de tendências ou atividades incomuns.
A0098	Aptidão para participar como membro de equipes de planejamento, grupos de coordenação e forças-tarefa, conforme necessário.
A0099	Aptidão para executar táticas, técnicas e procedimentos de coleta de rede para incluir recursos/ferramentas de descryptografia.
A0100	Aptidão para executar procedimentos de coleta sem fio para incluir recursos/ferramentas de descryptografia.
A0101	Aptidão para reconhecer e mitigar vieses cognitivos que podem afetar a análise.
A0102	Aptidão para reconhecer e mitigar enganos em relatórios e análises.
A0103	Aptidão para revisar a precisão e completude de materiais processados na língua de alvo .
A0104	Aptidão para selecionar o implante apropriado para atingir metas operacionais.
A0105	Aptidão para adequar informações técnicas e de planejamento ao nível de compreensão de um cliente.
A0106	Aptidão para pensar criticamente.
A0107	Aptidão para pensar como os atores de ameaças.
A0108	Aptidão para entender objetivos e efeitos.
A0109	Aptidão para utilizar múltiplas fontes de inteligência em todas as disciplinas de inteligência.
A0110	Aptidão para monitorar os avanços nas leis de privacidade da informação para garantir a adaptação e conformidade organizacional.
A0111	Aptidão para trabalhar em departamentos e unidades de negócios para implementar os princípios e programas de privacidade da organização e alinhar objetivos de privacidade aos objetivos de segurança.
A0112	Aptidão para monitorar avanços em tecnologias de privacidade da informação para garantir adaptação e conformidade organizacional.
A0113	Aptidão para determinar se um incidente de segurança viola um princípio de privacidade ou padrão normativo que exige ações legais específicas.
A0114	Aptidão para desenvolver ou obter currículo que aborde o tema no nível apropriado para o alvo.
A0115	Aptidão para trabalhar em departamentos e unidades de negócios para implementar os princípios e programas de privacidade da organização e alinhar objetivos de privacidade aos objetivos de segurança.

ID de Aptidão	Descrição
A0116	Aptidão para priorizar e alocar recursos de cibersegurança de forma correta e eficiente.
A0117	Aptidão para relacionar estratégia, negócios e tecnologia no contexto da dinâmica organizacional.
A0118	Aptidão para entender questões de tecnologia, gestão e liderança relacionadas aos processos da organização e resolução de problemas.
A0119	Aptidão para entender os conceitos e questões básicas relacionadas à cibernética e seu impacto organizacional.
A0120	Aptidão para compartilhar insights significativos sobre o contexto do ambiente de ameaças de uma organização que melhorem sua postura de gerenciamento de riscos.
A0121	Aptidão para conceptualizar resposta a incidentes para modelos de serviço em nuvem.
A0122	Aptidão para conceptualizar recursos para encontrar soluções para problemas menos comuns e mais complexos de sistemas.
A0123	Aptidão para aplicar princípios de cibersegurança e privacidade aos requisitos organizacionais (relevantes para confidencialidade, integridade, disponibilidade, autenticação, não repúdio).
A0124	Aptidão para estabelecer e manter avaliações automatizadas de controle de segurança
A0125	Aptidão para redigir uma declaração de divulgação de privacidade com base nas leis vigentes.
A0126	Aptidão para rastrear a localização e a configuração de dispositivos e software de rede em vários departamentos, locais, instalações e, potencialmente, oferecer suportes às funções de negócios.
A0127	Aptidão para implantar tecnologias e ferramentas de monitoramento contínuo.
A0128	Aptidão para aplicar técnicas para detectar invasões baseadas em host e rede usando tecnologias de detecção de invasões.
A0129	Aptidão para garantir que os processos de gestão da segurança da informação estejam integrados a processos estratégicos e de planejamento operacional.
A0130	Aptidão para garantir que dirigentes seniores da organização forneçam segurança da informação referente às informações e sistemas que dão suporte às operações e ativos sob seu controle.
A0131	Aptidão para garantir que a organização tenha pessoal treinado adequadamente para auxiliar no cumprimento dos requisitos de segurança em vigor, Ordens Executivas, políticas, diretivas, instruções, normas e diretrizes.
A0132	Aptidão para coordenar medidas com a liderança sênior de uma organização no sentido de fornecer uma abordagem abrangente, holística e extensiva para lidar com riscos - uma abordagem que forneça uma maior compreensão das operações integradas da organização.
A0133	Aptidão para coordenar abordagens com a liderança sênior de uma organização no sentido de desenvolver uma estratégia de gestão de riscos, fornecendo uma visão estratégica dos riscos relacionados à segurança da organização.
A0134	Aptidão para coordenar com a liderança sênior de uma organização no sentido de facilitar o compartilhamento de informações relacionadas a riscos entre dirigentes autorizados e outros líderes seniores dentro da organização.
A0135	Aptidão para coordenar abordagens junto à liderança sênior de uma organização no sentido de fornecer supervisão para todas as atividades relacionadas à gestão de risco da organização para ajudar a garantir decisões de aceitação de risco que sejam consistentes e eficazes.
A0136	Aptidão para coordenar esforços com a liderança sênior de uma organização para garantir que as decisões de autorização considerem todos os fatores necessários para o sucesso da missão e dos negócios.

ID de Aptidão	Descrição
A0137	Aptidão para coordenar com a liderança sênior de uma organização a possibilidade de fornecer um fórum para considerar as fontes de risco em toda a organização (incluindo risco agregado) referentes às operações e ativos organizacionais, indivíduos, outras organizações e a Nação.
A0138	Aptidão para coordenar com a liderança sênior de uma organização a possibilidade de promover a cooperação e a colaboração entre os dirigentes autorizados para que incluam ações de autorização que exijam responsabilidade compartilhada.
A0139	Aptidão para coordenar esforços com a liderança sênior de uma organização para garantir que a responsabilidade compartilhada de apoiar funções organizacionais de missão/negócios usando provedores externos de sistemas, serviços e aplicativos, receba a visibilidade necessária, sendo elevada ao nível das autoridades de tomada de decisão apropriadas.
A0140	Aptidão para coordenar com a liderança sênior de uma organização a possibilidade de identificar a postura de risco organizacional com base no risco agregado da operação e uso dos sistemas pelos quais a organização é responsável.
A0141	Aptidão para trabalhar em estreita colaboração com dirigentes autorizados e seus representantes designados para ajudar a garantir que um programa de segurança seja efetivamente implementado em toda a organização, resultando em segurança adequada para todos os sistemas organizacionais e ambientes operacionais.
A0142	Aptidão para trabalhar em estreita colaboração com dirigentes autorizados e seus representantes designados para ajudar a garantir que as considerações sobre segurança sejam integradas em ciclos de programação/planejamento/orçamento, arquiteturas corporativas e ciclos de vida de aquisição/desenvolvimento de sistemas.
A0143	Aptidão para trabalhar em estreita colaboração com dirigente autorizados e seus representantes designados para ajudar a garantir que os sistemas organizacionais e controles comuns sejam cobertos por planos de segurança aprovados e possuam autorizações atualizadas.
A0144	Aptidão para trabalhar em estreita colaboração com funcionários autorizados e seus representantes designados para ajudar a garantir que as atividades relacionadas à segurança exigida em toda a organização sejam realizadas de forma eficiente, econômica e em tempo hábil.
A0145	Aptidão para trabalhar em estreita colaboração com funcionários autorizados e seus representantes designados para ajudar a garantir a existência de relatórios centralizados de atividades relacionadas à segurança.
A0146	Aptidão para estabelecer regras de uso e proteção adequadas da informação e manter essa responsabilidade mesmo quando as informações são compartilhadas ou fornecidas a outras organizações.
A0147	Aptidão para aprovar planos de segurança, memorandos de acordo ou entendimento, planos de ação e marcos, e determinar se mudanças significativas nos sistemas ou ambientes de operação requerem nova autorização.
A0148	Aptidão para servir como o elo principal entre o arquiteto corporativo e o engenheiro de segurança de sistemas e coordenar com os proprietários do sistema, provedores de controle comum e agentes de segurança do sistema sobre a alocação de controles de segurança como sendo específicos do sistema, híbridos ou comuns.

ID de Aptidão	Descrição
A0149	Aptidão para manter estreita coordenação com os dirigentes de segurança do sistema, no sentido de aconselhar dirigentes autorizados, diretores de informação, dirigentes seniores de segurança da informação e o dirigente responsável pela gestão de risco/executivo de risco (função), sobre uma série de questões relacionadas à segurança (ex.: estabelecer limites para o sistema; avaliar a gravidade das fraquezas e deficiências no sistema; planos de ação e marcos de referência; abordagens de mitigação de riscos; alertas de segurança e potenciais efeitos adversos resultantes das vulnerabilidades identificadas).
A0150	Aptidão para realizar atividades de engenharia de segurança de sistemas (NIST SP 800-160).
A0151	Aptidão para capturar e refinar os requisitos de segurança e garantir que sejam efetivamente integrados objetivamente aos produtos e sistemas componentes, por meio da arquitetura, design, desenvolvimento e configuração de segurança.
A0152	Aptidão para empregar práticas recomendadas ao implementar controles de segurança dentro de um sistema, incluindo metodologias de engenharia de software; princípios de engenharia de sistemas e segurança; design seguro, arquitetura segura e técnicas seguras de codificação.
A0153	Aptidão para coordenar as atividades relacionadas à segurança juntamente com arquitetos de segurança, agentes de segurança da informação seniores, proprietários de sistemas, provedores de controle comum e agentes de segurança do sistema.
A0154	Aptidão para conduzir uma avaliação abrangente dos controles de segurança gerenciais e operacionais, bem como técnicas e melhorias de controle utilizadas no sistema ou herdadas por determinado sistema, com o intuito de determinar a eficácia dos controles (ex.: até que ponto os controles de segurança foram implementados corretamente, se estão funcionando de acordo com a expectativa e produzindo o resultado desejado no que diz respeito ao cumprimento dos requisitos de segurança para o sistema).
A0155	Aptidão para apresentar uma avaliação da gravidade das fraquezas ou deficiências descobertas no sistema e em seu ambiente de operação e recomendar ações corretivas para solucionar as vulnerabilidades identificadas.
A0156	Aptidão para elaborar o relatório final de avaliação de segurança contendo os resultados e conclusões sobre a avaliação.
A0157	Aptidão para avaliar um plano de segurança e garantir que ele forneça um conjunto de controles de segurança que atenda aos requisitos estabelecidos para o sistema.
A0158	Aptidão para garantir que os requisitos funcionais e de segurança sejam devidamente abordados em um contrato e que o contratante atenda a tais requisitos conforme previsto no contrato.
A0159	Aptidão para interpretar as informações coletadas por ferramentas de rede (ex.: Nslookup, Ping e Traceroute).
A0160	Aptidão para traduzir, rastrear e priorizar necessidades de informações e requisitos de coleta de inteligência em toda a empresa.
A0161	Aptidão para integrar requisitos de segurança da informação no processo de aquisição, usando controles de segurança de linha de base aplicáveis como uma das fontes para requisitos de segurança, garantindo um processo robusto de controle de qualidade de software e estabelecendo múltiplas fontes (ex.: rotas de entrega para elementos críticos do sistema).
A0162	Aptidão para garantir a segurança do sistema de informações, do pessoal de aquisições, departamento jurídico e outros consultores e partes interessadas apropriadas que estejam participando da tomada de decisão referente à definição/revisão da concepção do sistema e que estejam envolvidos no processo decisório ou são responsáveis por aprovar decisões importantes que impactam o sistema e o ciclo de vida de todos os sistemas.

ID de Aptidão	Descrição
A0162	Aptidão para identificar aspectos singulares do ambiente e hierarquia de Segurança das Comunicações (COMSEC).
A0163	Aptidão para interpretar a terminologia, diretrizes e procedimentos de Segurança das Comunicações (COMSEC).
A0164	Aptidão para identificar as funções e responsabilidades do pessoal nomeado para a Segurança das Comunicações (COMSEC).
A0165	Aptidão para gerenciar os procedimentos de contabilidade, controle e uso de materiais de Segurança das Comunicações (COMSEC).
A0166	Aptidão para identificar tipos de Incidentes de Segurança das Comunicações (COMSEC) e como eles são relatados
A0167	Aptidão para reconhecer a importância da auditoria da Segurança das Comunicações (COMSEC) referente a materiais e contas.
A0168	Aptidão para identificar os requisitos de contabilidade em processo para a Segurança das Comunicações (COMSEC)
A0170	Aptidão para identificar sistemas de infraestrutura críticos com tecnologia de comunicação da informação que foram idealizados sem considerações de segurança do sistema.
A0171	Aptidão para realizar avaliação das necessidades de treinamento e educação.
A0172	Aptidão para configurar sub-redes físicas ou lógicas que separam uma rede local interna (LAN) de outras redes não confiáveis.
A0173	Aptidão para reconhecer que as mudanças nos sistemas ou no ambiente podem mudar os riscos residuais em relação à apetência pelo risco.
A0174	Aptidão para encontrar e navegar na dark web usando a rede TOR para localizar mercados e fóruns.
A0175	Aptidão para examinar mídia digital em várias plataformas de sistema operacional.
A0176	Aptidão para manter bancos de dados. (ex.: backup, restauração, exclusão de dados, arquivos de registro de transações, etc.).

## Appendix B – Lista de Detalhes da Função de Trabalho

Este apêndice fornece uma descrição detalhada de cada função de trabalho do NICE Framework. Para cada função de trabalho, a lista abaixo fornece as seguintes informações:

- O nome da função de trabalho;
- Um ID de função de trabalho do NICE Framework exclusivo, com base nas abreviações da Categoria do NICE Framework e área de especialidade à qual pertence tal função de trabalho;
- A área de especialidade na qual reside a função de trabalho;
- A categoria na qual reside a função de trabalho;
- Uma descrição da função de trabalho;
- Uma lista das tarefas do NICE Framework que uma pessoa em um cargo de segurança cibernética que inclui a função de trabalho deve desempenhar;
- Uma lista das áreas de conhecimentos do NICE Framework que se espera que uma pessoa em um cargo de segurança cibernética que inclui tal função de trabalho saiba desempenhar;
- Uma lista das habilidades do NICE Framework que se espera que uma pessoa em um cargo de segurança cibernética que inclui tal função de trabalho deve possuir;
- Uma lista das aptidões do NICE Framework que uma pessoa em um cargo de segurança cibernética que inclui tal função de trabalho deve demonstrar.

As tabelas abaixo descrevem as funções de trabalho do NICE Framework juntamente com uma lista simples de tarefas, conhecimentos, habilidades e aptidões. A fonte definitiva para a versão mais atual deste material pode ser encontrada na Planilha de Referência para a Publicação Especial NIST 800-181 [4]. A Planilha de Referência fornece listas mais detalhadas das tarefas, conhecimentos, habilidades e aptidões. As funções de trabalho serão atualizadas periodicamente [1].

### B.1 Provisão de Segurança (SP)

<b>Nome das funções de trabalho</b>	<b>Oficial Autorizado</b>
<b>ID da função de trabalho</b>	<b>SP-RSK-001</b>
<b>Área de especialidade</b>	<b>Gestão de Risco (RSK)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Diretor sênior ou executivo com autoridade para assumir formalmente a responsabilidade pela operação de um sistema de informação em um nível aceitável de risco para as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais, indivíduos, outras organizações e a Nação (CNSSI 4009).

<b>Tarefas</b>	T0145, T0221, T0371, T0495
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624
<b>Habilidades</b>	S0034, S0367
<b>Aptidões</b>	A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170

<b>Nome das funções de trabalho</b>	<b>Avaliador de Controle de Segurança</b>
<b>ID da função de trabalho</b>	<b>SP-RSK-002</b>
<b>Área de especialidade</b>	<b>Gestão de Risco (RSK)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Realizar avaliações abrangentes e independentes do gerenciamento operacional e técnico de controles de segurança, além de aprimoramentos dos controles utilizados ou herdados por um sistema de tecnologia da informação (TI), para determinar a eficácia geral dos controles (conforme definido no NIST 800-37).
<b>Tarefas</b>	T0145, T0184, T0221, T0244, T0251, T0371, T0495, T0177, T0178, T0181, T0205, T0243, T0255, T0264, T0265, T0268, T0272, T0275, T0277, T0309, T0344
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0013, K0018, K0019, K0018, K0021, K0024, K0026, K0027, K0028, K0029, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0056, K0059, K0070, K0084, K0089, K0098, K0100, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0287, K0322, K0342, K0622, K0624
<b>Habilidades</b>	S0001, S0006, S0027, S0034, S0038, S0073, S0078, S0097, S0100, S0110, S0111, S0112, S0115, S0120, S0124, S0128, S0134, S0135, S0136, S0137, S0138, S0141, S0145, S0147, S0171, S0172, S0173, S0174, S0175, S0176, S0177, S0184, S0232, S0233, S0234, S0235, S0236, S0237, S0238, S0239, S0240, S0241, S0242, S0243, S0244, S0248, S0249, S0250, S0251, S0252, S0254, S0271, S0273, S0278, S0279, S0280, S0281, S0296, S0304, S0305, S0306, S0307, S0325, S0329, S0332, S0367, S0370, S0374
<b>Aptidões</b>	A0001, A0011, A0012, A0013, A0014, A0015, A0016, A0018, A0019, A0023, A0026, A0030, A0035, A0036, A0040, A0056, A0069, A0070, A0082, A0083, A0084, A0085, A0086, A0087, A0088, A0089, A0090, A0091, A0092, A0093, A0094, A0095, A0096, A0098, A0101, A0106, A0108, A0109, A0117, A0118, A0119, A0111, A0112, A0114, A0115, A0116, A0119, A0123, A0170

<b>Nome da função de trabalho</b>	<b>Desenvolvedor de Software</b>
<b>ID da função de trabalho</b>	<b>SP-DEV-001</b>

<b>Área de especialidade</b>	<b>Desenvolvimento de software (DEV)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Desenvolver, criar, manter e escrever/codificar novos (ou modificar os existentes) aplicativos de computador, software ou programas utilitários especializados.
<b>Tarefas</b>	T0009, T0011, T0013, T0014, T0022, T0026, T0034, T0040, T0046, T0057, T0077, T0100, T0111, T0117, T0118, T0171, T0176, T0181, T0189, T0217, T0228, T0236, T0267, T0303, T0311, T0324, T0337, T0416, T0417, T0436, T0455, T0500, T0553, T0554
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0332, K0342, K0343, K0624
<b>Habilidades</b>	S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175, S0367
<b>Aptidões</b>	A0007, A0021, A0047, A0123, A0170

<b>Nome da Função de Trabalho</b>	<b>Avaliador de Software Seguro</b>
<b>ID da função de trabalho</b>	<b>SP-DEV-002</b>
<b>Área de especialidade</b>	<b>Desenvolvimento de software (DEV)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Analisar a segurança de aplicativos de computador novos ou existentes, software ou programas utilitários especializados e fornecer resultados acionáveis.
<b>Tarefas</b>	T0013, T0014, T0022, T0038, T0040, T0100, T0111, T0117, T0118, T0171, T0181, T0217, T0228, T0236, T0266, T0311, T0324, T0337, T0424, T0428, T0436, T0456, T0457, T0516, T0554
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0178, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0342, K0343, K0624
<b>Habilidades</b>	S0001, S0022, S0031, S0034, S0083, S0135, S0138, S0174, S0175, S0367
<b>Aptidões</b>	A0021, A0123, A0170

<b>Nome da Função de Trabalho</b>	<b>Arquiteto Empresarial</b>
<b>ID da função de trabalho</b>	<b>SP-ARC-001</b>
<b>Área de especialidade</b>	<b>Arquitetura de Sistemas (ARC)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>

<b>Descrição da função de trabalho</b>	Desenvolver e manter negócios, sistemas e processos de informação para apoiar as necessidades da missão empresarial; desenvolver regras e requisitos de tecnologia da informação (TI) que descrevem arquiteturas de linha de base e de destino.
<b>Tarefas</b>	T0051, T0084, T0090, T0108, T0196, T0205, T0307, T0314, T0328, T0338, T0427, T0440, T0448, T0473, T0517, T0521, T0542, T0555, T0557
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0024, K0027, K0028, K0030, K0035, K0037, K0043, K0044, K0052, K0056, K0060, K0061, K0063, K0074, K0075, K0082, K0091, K0093, K0102, K0170, K0179, K0180, K0198, K0200, K0203, K0207, K0211, K0212, K0214, K0227, K0240, K0264, K0275, K0286, K0287, K0291, K0293, K0299, K0322, K0323, K0325, K0326, K0332, K0333, K0487, K0516
<b>Habilidades</b>	S0005, S0024, S0027, S0050, S0060, S0122, S0367, S0374
<b>Aptidões</b>	A0008, A0015, A0027, A0038, A0051, A0060, A0123, A0170

<b>Nome da Função de Trabalho</b>	<b>Arquiteto de Segurança</b>
<b>ID da função de trabalho</b>	<b>SP-ARC-002</b>
<b>Área de especialidade</b>	<b>Arquitetura de Sistemas (ARC)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Garantir que os requisitos de segurança das partes interessadas, necessários para proteger a missão da organização e os processos de negócios, sejam adequadamente abordados em todos os aspectos da arquitetura corporativa, incluindo modelos de referência, arquiteturas de segmento e solução, e os sistemas resultantes que suportam tais missões e processos de negócios.
<b>Tarefas</b>	T0050, T0051, T0071, T0082, T0084, T0090, T0108, T0177, T0196, T0203, T0205, T0268, T0307, T0314, T0328, T0338, T0427, T0448, T0473, T0484, T0542, T0556
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0015, K0018, K0019, K0024, K0026, K0027, K0030, K0035, K0036, K0037, K0043, K0044, K0052, K0055, K0056, K0057, K0059, K0060, K0061, K0063, K0071, K0074, K0082, K0091, K0092, K0093, K0102, K0170, K0180, K0198, K0200, K0202, K0211, K0212, K0214, K0227, K0240, K0260, K0261, K0262, K0264, K0275, K0277, K0286, K0287, K0291, K0293, K0320, K0322, K0323, K0325, K0326, K0332, K0333, K0336, K0565, K0599
<b>Habilidades</b>	S0005, S0022, S0024, S0027, S0050, S0059, S0061, S0076, S0116, S0122, S0138, S0139, S0152, S0168, S0170, S367, S0374
<b>Aptidões</b>	A0008, A0014, A0015, A0027, A0038, A0048, A0049, A0050, A0061, A0123, A0148, A0149, A0170, A0172

<b>Nome da Função de Trabalho</b>	<b>Especialista em Pesquisa e Desenvolvimento</b>
<b>ID da função de trabalho</b>	<b>SP-TRD-001</b>
<b>Área de especialidade</b>	<b>Pesquisa e Desenvolvimento em Tecnologia (TRD)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Realizar pesquisas de engenharia de software e sistemas para desenvolver novos recursos, garantindo que a segurança cibernética seja totalmente integrada. Realizar pesquisas abrangente em tecnologia para avaliar vulnerabilidades potenciais em sistemas cibernéticos.
<b>Tarefas</b>	T0064, T0249, T0250, T0283, T0284, T0327, T0329, T0409, T0410, T0411, T0413, T0547
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0059, K0090, K0126, K0169, K0170, K0171, K0172, K0174, K0175, K0176, K0179, K0202, K0209, K0267, K0268, K0269, K0271, K0272, K0288, K0296, K0310, K0314, K0321, K0342, K0499
<b>Habilidades</b>	S0005, S0017, S0072, S0140, S0148, S0172
<b>Aptidões</b>	A0001, A0018, A0019, A0170

<b>Nome da Função de Trabalho</b>	<b>Planejador de Requisitos de Sistemas</b>
<b>ID da função de trabalho</b>	<b>SP-SRP-001</b>
<b>Área de especialidade</b>	<b>Planejamento de Requisitos de Sistemas (SRP)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Consultar os clientes para avaliar os requisitos funcionais e traduzir tais requisitos em soluções técnicas.
<b>Tarefas</b>	T0033, T0039, T0045, T0052, T0062, T0127, T0156, T0174, T0191, T0235, T0273, T0300, T0313, T0325, T0334, T0454, T0463, T0497
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0012, K0018, K0019, K0032, K0035, K0038, K0043, K0044, K0045, K0047, K0055, K0056, K0059, K0060, K0061, K0063, K0066, K0067, K0073, K0074, K0086, K0087, K0090, K0091, K0093, K0101, K0102, K0126, K0163, K0164, K0168, K0169, K0170, K0180, K0200, K0267, K0287, K0325, K0332, K0333, K0622
<b>Habilidades</b>	S0005, S0006, S0008, S0010, S0050, S0134, S0367
<b>Aptidões</b>	A0064, A0123, A0170

<b>Nome da Função de Trabalho</b>	<b>Especialista em Teste e Avaliação de Sistemas</b>
<b>ID da função de trabalho</b>	<b>SP-TST-001</b>
<b>Área de especialidade</b>	<b>Teste e Avaliação (TST)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Planejar, preparar e executar testes de sistemas para avaliar os resultados em relação às especificações e requisitos, bem como analisar/relatar os resultados dos testes.
<b>Tarefas</b>	T0058, T0080, T0125, T0143, T0257, T0274, T0393, T0426, T0511, T0512, T0513, T0539, T0540
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0028, K0037, K0044, K0057, K0088, K0091, K0102, K0139, K0126, K0169, K0170, K0179, K0199, K0203, K0212, K0250, K0260, K0261, K0262, K0287, K0332
<b>Habilidades</b>	S0015, S0021, S0026, S0030, S0048, S0060, S0061, S0082, S0104, S0107, S0110, S0112, S0115, S0117, S0367
<b>Aptidões</b>	A0026, A0030, A0040, A0123

<b>Nome da Função de Trabalho</b>	<b>Desenvolvedor de Segurança de Sistemas de Informação</b>
<b>ID da função de trabalho</b>	<b>SP-SYS-001</b>
<b>Área de especialidade</b>	<b>Desenvolvimento de Sistemas (SYS)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Idealizar, desenvolver, testar e avaliar a segurança do sistema de informações em todo o ciclo de vida de desenvolvimento de sistemas.
<b>Tarefas</b>	T0012, T0015, T0018, T0019, T0021, T0032, T0053, T0055, T0056, T0061, T0069, T0070, T0076, T0078, T0105, T0107, T0109, T0119, T0122, T0124, T0181, T0201, T0205, T0228, T0231, T0242, T0269, T0270, T0271, T0272, T0304, T0326, T0359, T0446, T0449, T0466, T0509, T0518, T0527, T0541, T0544
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
<b>Habilidades</b>	S0001, S0022, S0023, S0024, S0031, S0034, S0036, S0085, S0145, S0160, S0367
<b>Aptidões</b>	A0001, A0008, A0012, A0013, A0015, A0019, A0026, A0040, A0048, A0049, A0050, A0056, A0061, A0074, A0089, A0098, A0108, A0119, A0123, A0170

<b>Nome da Função de Trabalho</b>	<b>Desenvolvedor de Sistemas</b>
<b>ID da função de trabalho</b>	<b>SP-SYS-002</b>
<b>Área de especialidade</b>	<b>Desenvolvimento de Sistemas (SYS)</b>
<b>Categoria</b>	<b>Provisão de Segurança (SP)</b>
<b>Descrição da função de trabalho</b>	Idealizar, desenvolver, testar e avaliar sistemas de informação em todo o ciclo de vida de desenvolvimento de sistemas.
<b>Tarefas</b>	T0012, T0021, T0053, T0056, T0061, T0067, T0070, T0107, T0109, T0119, T0181, T0201, T0205, T0228, T0242, T0304, T0326, T0350, T0358, T0359, T0378, T0406, T0447, T0449, T0464, T0466, T0480, T0488, T0518, T0528, T0538, T0541, T0544, T0558, T0559, T0560
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0207, K0212, K0227, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
<b>Habilidades</b>	S0018, S0022, S0023, S0024, S0025, S0031, S0034, S0036, S0060, S0085, S0097, S0136, S0145, S0146, S0160, S0367
<b>Aptidões</b>	A0123, A0170

**B.2 Operar e Manter (OM)**

<b>Nome da Função de Trabalho</b>	<b>Administrador de Banco de Dados</b>
<b>ID da função de trabalho</b>	<b>OM-DTA-001</b>
<b>Área de especialidade</b>	<b>Administração de Dados (DTAA)</b>
<b>Categoria</b>	<b>Operar e Manter (OM)</b>
<b>Descrição da função de trabalho</b>	Administrar bancos de dados e/ou sistemas de gerenciamento de dados que permitam o armazenamento seguro, a consulta e utilização de dados.
<b>Tarefas</b>	T0008, T0137, T0139, T0140, T0146, T0152, T0162, T0210, T0305, T0306, T0330, T0422, T0459, T0490
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0020, K0021, K0022, K0023, K0025, K0031, K0056, K0060, K0065, K0069, K0083, K0097, K0197, K0260, K0261, K0262, K0277, K0278, K0287, K0420
<b>Habilidades</b>	S0002, S0013, S0037, S0042, S0045
<b>Aptidões</b>	A0176

<b>Nome da Função de Trabalho</b>	<b>Analista de Dados</b>
<b>ID da função de trabalho</b>	<b>OM-DTA-002</b>
<b>Área de especialidade</b>	<b>Administração de Dados (DTA)</b>
<b>Categoria</b>	<b>Operar e Manter (OM)</b>
<b>Descrição da função de trabalho</b>	Examinar dados de várias fontes distintas com o objetivo de fornecer informações sobre segurança e privacidade. Idealizar e implementar algoritmos personalizados, processos de fluxo de trabalho e layouts para conjuntos de dados complexos de escala corporativa usados para modelagem, mineração de dados e fins de pesquisa.
<b>Tarefas</b>	T0007, T0008, T0068, T0146, T0195, T0210, T0342, T0347, T0349, T0351, T0353, T0361, T0366, T0381, T0382, T0383, T0385, T0392, T0402, T0403, T0404, T0405, T0460
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0016, K0020, K0022, K0023, K0025, K0031, K0051, K0052, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0420
<b>Habilidades</b>	S0013, S0017, S0202, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160, S0369
<b>Aptidões</b>	A0029, A0035, A0036, A0041, A0066

<b>Nome da Função de Trabalho</b>	<b>Gerente de Conhecimentos</b>
<b>ID da função de trabalho</b>	<b>OM-KMG-001</b>
<b>Área de especialidade</b>	<b>Gestão do Conhecimento (KMG)</b>
<b>Categoria</b>	<b>Operar e Manter (OM)</b>
<b>Descrição da função de trabalho</b>	Responsável por gerenciar e administrar processos e ferramentas que permitem à organização identificar, documentar e acessar capital intelectual e conteúdo de informações.
<b>Tarefas</b>	T0037, T0060, T0154, T0185, T0209, T0339, T0421, T0452, T0524
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0094, K0095, K0096, K0146, K0194, K0195, K0228, K0260, K0261, K0262, K0283, K0287, K0315, K0338, K0420
<b>Habilidades</b>	S0011, S0012, S0049, S0055
<b>Aptidões</b>	A0002

<b>Nome da Função de Trabalho</b>	<b>Especialista em Suporte Técnico</b>
<b>ID da função de trabalho</b>	<b>OM-STS-001</b>
<b>Área de especialidade</b>	<b>Atendimento ao cliente e suporte técnico (STS)</b>
<b>Categoria</b>	<b>Operar e Manter (OM)</b>
<b>Descrição da função de trabalho</b>	Fornecer suporte técnico aos clientes que precisam de assistência utilizando hardware e software em nível de cliente, e de acordo com componentes de processo organizacional estabelecidos ou aprovados. (ex.: Plano Mestre de Gerenciamento de Incidentes, quando aplicável).
<b>Tarefas</b>	T0125, T0237, T0308, T0315, T0331, T0468, T0482, T0491, T0494, T0496, T0502, T0530
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0053, K0088, K0109, K0114, K0116, K0194, K0224, K0237, K0242, K0247, K0260, K0261, K0262, K0287, K0292, K0294, K0302, K0317, K0330
<b>Habilidades</b>	S0039, S0058, S0142, S0159, S0365
<b>Aptidões</b>	A0025, A0034, A0122

<b>Nome da Função de Trabalho</b>	<b>Especialista em Operações de Rede</b>
<b>ID da função de trabalho</b>	<b>OM-NET-001</b>
<b>Área de especialidade</b>	<b>Serviços de Rede (NET)</b>
<b>Categoria</b>	<b>Operar e Manter (OM)</b>
<b>Descrição da função de trabalho</b>	Planejar, implementar e operar serviços/sistemas de rede, para incluir hardware e ambientes virtuais.
<b>Tarefas</b>	T0035, T0065, T0081, T0121, T0125, T0126, T0129, T0153, T0160, T0200, T0232

<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0011, K0029, K0038, K0049, K0050, K0053, K0061, K0071, K0076, K0093, K0104, K0108, K0111, K0113, K0135, K0136, K0137, K0138, K0159, K0160, K0179, K0180, K0200, K0201, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622
<b>Habilidades</b>	S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170
<b>Aptidões</b>	A0052, A0055, A0058, A0059, A0062, A0063, A0065, A0159

<b>Nome da Função de Trabalho</b>	<b>Administrador de Sistemas</b>
<b>ID da função de trabalho</b>	<b>OM-ADM-001</b>
<b>Área de especialidade</b>	<b>Administração de Sistemas (ADM)</b>
<b>Categoria</b>	<b>Operar e Manter (OM)</b>
<b>Descrição da função de trabalho</b>	Responsável por configurar e manter um sistema ou componentes específicos de um sistema (ex.: instalação, configuração e atualização de hardware e software; estabelecer e gerenciar contas de usuário; supervisionar ou conduzir tarefas de backup e recuperação; implementar controles de segurança operacionais e técnicos; e aderir às políticas e procedimentos de segurança organizacional).
<b>Tarefas</b>	T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0260, K0261, K0262, K0274, K0280, K0289, K0318, K0332, K0346
<b>Habilidades</b>	S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158
<b>Aptidões</b>	S0154, S0158

<b>Nome da Função de Trabalho</b>	<b>Analista de Segurança de Sistemas</b>
<b>ID da função de trabalho</b>	<b>OM-ANA-001</b>
<b>Área de especialidade</b>	<b>Análise de Sistemas (ANA)</b>
<b>Categoria</b>	<b>Operar e Manter (OM)</b>
<b>Descrição da função de trabalho</b>	Responsável pela análise e desenvolvimento da integração, testes, operações e manutenção de sistemas de segurança.
<b>Tarefas</b>	T0015, T0016, T0017, T0085, T0086, T0088, T0123, T0128, T0169, T0177, T0187, T0194, T0202, T0205, T0243, T0309, T0344, T0462, T0469, T0470, T0475, T0477, T0485, T0489, T0492, T0499, T0504, T0508, T0526, T0545, T0548
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0019, K0024, K0035, K0036, K0040, K0044, K0049, K0052, K0056, K0060, K0061, K0063, K0075, K0082, K0093, K0102, K0179, K0180, K0200, K0203, K0227, K0260, K0261, K0262, K0263, K0266, K0267, K0275, K0276, K0281, K0284, K0285, K0287, K0290, K0297, K0322, K0333, K0339
<b>Habilidades</b>	S0024, S0027, S0031, S0036, S0060, S0141, S0147, S0167, S0367
<b>Aptidões</b>	A0015, A0123

**B.3 Supervisorar e Governar (OV)**

<b>Nome da Função de Trabalho</b>	<b>Consultor Jurídico Cibernético</b>
<b>ID da função de trabalho</b>	<b>OV-LGA-001</b>
<b>Área de especialidade</b>	<b>Aconselhamento jurídico e defesa (LGA)</b>
<b>Categoria</b>	<b>Supervisorar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Fornecer orientação jurídica e recomendações sobre tópicos relevantes relacionados ao direito cibernético.
<b>Tarefas</b>	T0006, T0098, T0102, T0131, T0220, T0419, T0434, T0465, T0474, T0476, T0478, T0487, T0522
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0059, K0107, K0157, K0261, K0262, K0267, K0312, K0316, K0341, K0615
<b>Habilidades</b>	S0356
<b>Aptidões</b>	A0046

<b>Nome da Função de Trabalho</b>	<b>Diretor de Privacidade/Gerente de Compliance de Privacidade</b>
<b>ID da função de trabalho</b>	<b>OV-LGA-002</b>
<b>Área de especialidade</b>	<b>Orientação jurídica e defesa (LGA)</b>
<b>Categoria</b>	<b>Supervisorar e Governar (OV)</b>
<b>Descrição da Função de Trabalho</b>	Desenvolver e supervisionar o programa e os funcionários envolvidos no programa de compliance de privacidade, oferecendo suporte ao compliance de privacidade, governança/políticas e necessidades de resposta a incidentes de executivos no âmbito de privacidade e segurança e suas equipes.
<b>Tarefas</b>	T0003, T0004, T0029, T0930, T0032, T0066, T0098, T0099, T0131, T0133, T0188, T0381, T0384, T0478, T0861, T0862, T0863, T0864, T0865, T0866, T0867, T0868, T0869, T0870, T0871, T0872, T0873, T0874, T0875, T0876, T0877, T0878, T0879, T0880, T0881, T0882, T0883, T0884, T0885, T0886, T0887, T0888, T0889, T0890, T0891, T0892, T0893, T0894, T0895, T0896, T0897, T0898, T0899, T0900, T0901, T0902, T0903, T0904, T0905, T0906, T0907, T0908, T0909, T0910, T0911, T0912, T0913, T0914, T0915, T0916, T0917, T0918, T0919
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0066, K0168, K0612, K0613, K0614, K0615
<b>Habilidades</b>	S0354, S0355, S0356
<b>Aptidões</b>	A0024, A0033, A0034, A0104, A0105, A0110, A0111, A0112, A0113, A0114, A0115, A0125

<b>Nome da Função de Trabalho</b>	<b>Desenvolvedor de Currículo Instrucional Cibernético</b>
<b>ID da função de trabalho</b>	<b>OV-TEA-001</b>
<b>Área de especialidade</b>	<b>Treinamento, Educação e Conscientização (TEA)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Desenvolver, planejar, coordenar e avaliar cursos de treinamento/educação cibernética, métodos e técnicas com base nas necessidades de instrução.
<b>Tarefas</b>	T0230, T0247, T0248, T0249, T0345, T0352, T0357, T0365, T0367, T0380, T0437, T0442, T0450, T0451, T0534, T0536, T0926
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0124, K0146, K0147, K0204, K0208, K0213, K0216, K0217, K0220, K0243, K0239, K0245, K0246, K0250, K0252, K0287, K0628
<b>Habilidades</b>	S0064, S0066, S0070, S0102, S0166, S0296
<b>Aptidões</b>	A0004, A0013, A0015, A0018, A0019, A0022, A0024, A0032, A0054, A0057, A0055, A0057, A0058, A0063, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

<b>Nome da Função de Trabalho</b>	<b>Instrutor de Cibernética</b>
<b>ID da função de trabalho</b>	<b>OV-TEA-002</b>
<b>Área de especialidade</b>	<b>Treinamento, Educação e Conscientização (TEA)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Desenvolver e realizar treinamento ou educação de pessoal dentro do domínio cibernético.
<b>Tarefas</b>	T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0352, T0365, T0367, T0381, T0382, T0395, T0443, T0444, T0450, T0451, T0467, T0519, T0520, T0535, T0536, T0926
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0245, K0246, K0250, K0252, K0287, K0313, K0319, K0628
<b>Habilidades</b>	S0001, S0004, S0006, S0051, S0052, S0053, S0055, S0056, S0057, S0060, S0064, S0070, S0073, S0075, S0076, S0081, S0084, S0097, S0100, S0101, S0121, S0131, S0156, S0184, S0270, S0271, S0281, S0293, S0301, S0356, S0358
<b>Aptidões</b>	A0006, A0011, A0012, A0013, A0014, A0015, A0016, A0017, A0018, A0019, A0020, A0022, A0023, A0024, A0032, A0055, A0057, A0057, A0058, A0063, A0066, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

<b>Nome da Função de Trabalho</b>	<b>Gerente de Segurança de Sistemas de Informação</b>
<b>ID da função de trabalho</b>	<b>OV-MGT-001</b>
<b>Área de especialidade</b>	<b>Gerenciamento de Segurança Cibernética (MGT)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Responsável pela segurança cibernética de um programa, organização, sistema ou enclave.
<b>Tarefas</b>	T0001, T0002, T0003, T0004, T0005, T0024, T0025, T0044, T0089, T0091, T0092, T0093, T0095, T0097, T0099, T0106, T0115, T0130, T0132, T0133, T0134, T0135, T0147, T0148, T0149, T0151, T0157, T0158, T0159, T0192, T0199, T0206, T0211, T0213, T0215, T0219, T0227, T0229, T0234, T0239, T0248, T0254, T0255, T0256, T0263, T0264, T0265, T0275, T0276, T0277, T0280, T0281, T0282
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0018, K0021, K0026, K0033, K0038, K0040, K0042, K0043, K0046, K0048, K0053, K0054, K0058, K0059, K0061, K0070, K0072, K0076, K0077, K0087, K0090, K0092, K0101, K0106, K0121, K0126, K0149, K0150, K0151, K0163, K0167, K0168, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0267, K0287, K0332, K0342, K0622, K0624
<b>Habilidades</b>	S0018, S0027, S0086
<b>Aptidões</b>	A0128, A0161, A0170

<b>Nome da Função de Trabalho</b>	<b>Gerente de Segurança das Comunicações (COMSEC)</b>
<b>ID da função de trabalho</b>	<b>OV-MGT-002</b>
<b>Área de especialidade</b>	<b>Gerenciamento de Segurança Cibernética (MGT)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Indivíduo que gerencia os recursos de Segurança das Comunicações (COMSEC) de uma organização (CNSSI 4009) ou principal custodiante de um Sistema de Gerenciamento de Chave Criptográfica (CKMS).
<b>Tarefas</b>	T0003, T0004, T0025, T0044, T0089, T0095, T0099, T0215, T0229
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0038, K0042, K0090, K0101, K0121, K0126, K0163, K0267, K0285, K0287, K0622
<b>Habilidades</b>	S0027, S0059, S0138
<b>Aptidões</b>	A0162, A0163, A0164, A0165, A0166, A0167, A0168

<b>Nome da Função de Trabalho</b>	<b>Desenvolvedor e Gerente da Força de Trabalho Cibernética</b>
<b>ID da função de trabalho</b>	<b>OV-SPP-001</b>
<b>Área de especialidade</b>	<b>Planejamento Estratégico e Políticas (SPP)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Desenvolver planos, estratégias e orientação para a força de trabalho do ciberespaço em apoio aos requisitos de mão-de-obra, pessoal, treinamento e educação do ciberespaço e para lidar com mudanças nas políticas, doutrina, material, estrutura de força e requisitos de educação e treinamento da força de trabalho.
<b>Tarefas</b>	T0001, T0004, T0025, T0044, T0074, T0094, T0099, T0116, T0222, T0226, T0341, T0352, T0355, T0356, T0362, T0363, T0364, T0365, T0368, T0369, T0372, T0373, T0374, T0375, T0376, T0384, T0387, T0388, T0390, T0391, T0408, T0425, T0429, T0437, T0441, T0445, T0472, T0481, T0505, T0506, T0529, T0533, T0536, T0537, T0552
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0072, K0101, K0127, K0146, K0147, K0168, K0169, K0204, K0215, K0233, K0234, K0241, K0243, K0309, K0311, K0313, K0335
<b>Habilidades</b>	S0108, S0128
<b>Aptidões</b>	A0023, A0028, A0033, A0037, A0042, A0053

<b>Nome da Função de Trabalho</b>	<b>Planejador de políticas e estratégias cibernéticas</b>
<b>ID da função de trabalho</b>	<b>OV-SPP-002</b>
<b>Área de especialidade</b>	<b>Planejamento Estratégico e Desenvolvimento de Políticas (SPP)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Desenvolver e manter planos, estratégias e políticas de segurança cibernética para apoiar e se alinhar com iniciativas de segurança cibernética organizacional e compliance regulatório.
<b>Tarefas</b>	T0074, T0094, T0222, T0226, T0341, T0369, T0384, T0390, T0408, T0425, T0429, T0441, T0445, T0472, T0505, T0506, T0529, T0533, T0537
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0168, K0234, K0248, K0309, K0311, K0313, K0335, K0624
<b>Habilidades</b>	S0176, S0250
<b>Aptidões</b>	A0003, A0033, A0037

<b>Nome da Função de Trabalho</b>	<b>Liderança Cibernética Executiva</b>
<b>ID da função de trabalho</b>	<b>OV-EXL-001</b>
<b>Área de especialidade</b>	<b>Liderança Cibernética Executiva (EXL)</b>

<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Executar a autoridade de tomada de decisão e estabelecer uma visão e direcionamento para os recursos e/ou operações cibernéticas relacionados a uma organização.
<b>Tarefas</b>	T0001, T0002, T0004, T0006, T0025, T0066, T0130, T0134, T0135, T0148, T0151, T0227, T0229, T0229, T0248, T0254, T0263, T0264, T0282, T0337, T0356, T0429, T0445, T0509, T0763, T0871, T0872, T0927, T0928
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0070, K0106, K0314, K0296, K0147, K0624, K0628
<b>Habilidades</b>	S0018, S0356, S0357, S0358, S0359
<b>Aptidões</b>	A0033, A0070, A0085, A0094, A0105, A0106, A0116, A0117, A0118, A0119, A0129, A0130, A0130

<b>Nome da Função de Trabalho</b>	<b>Gerente de Programas</b>
<b>ID da função de trabalho</b>	<b>OV-PMA-001</b>
<b>Área de especialidade</b>	<b>Gerenciamento e Aquisição de Programas/Projetos (PMA)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Liderar, coordenar, comunicar, integrar, sendo ainda responsável pelo sucesso geral do programa, garantindo o alinhamento com as prioridades da agência ou da empresa.
<b>Tarefas</b>	T0066, T0072, T0174, T0199, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0377, T0379, T0407, T0412, T0414, T0415, T0481, T0493, T0551
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
<b>Habilidades</b>	S0038, S0372
<b>Aptidões</b>	A0009, A0039, A0045, A0056,

<b>Nome da Função de Trabalho</b>	<b>Gerente de Projetos de Tecnologia da Informação (TI)</b>
<b>ID da função de trabalho</b>	<b>OV-PMA-002</b>
<b>Área de especialidade</b>	<b>Gerenciamento e Aquisição de Programas/Projetos (PMA)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Gerenciar diretamente projetos de tecnologia da informação.
<b>Tarefas</b>	T0072, T0174, T0196, T0199, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0340, T0354, T0370, T0377, T0379, T0389, T0394, T0407, T0412, T0414, T0415, T0481, T0493, T0551
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0012, K0043, K0047, K0048, K0059, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270

<b>Habilidades</b>	S0038, S0372
<b>Aptidões</b>	A0009, A0039, A0045, A0056

<b>Nome da Função de Trabalho</b>	<b>Gerente de Suporte de Produto</b>
<b>ID da função de trabalho</b>	<b>OV-PMA-003</b>
<b>Área de especialidade</b>	<b>Gerenciamento e Aquisição de Programas/Projetos (PMA)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Gerenciar o pacote de funções de suporte necessárias para colocar em campo e manter a prontidão e a capacidade operacional dos sistemas e componentes.
<b>Tarefas</b>	T0072, T0174, T0196, T0204, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0370, T0377, T0389, T0394, T0412, T0414, T0493, T0525, T0551, T0553
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0048, K0059, K0072, K0090, K0120, K0126, K0148, K0150, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0249, K0257, K0270
<b>Habilidades</b>	S0038, S0372
<b>Aptidões</b>	A0009, A0031, A0039, A0045, A0056

<b>Nome da Função de Trabalho</b>	<b>Gerente de Investimento/Portfólio de TI</b>
<b>ID da função de trabalho</b>	<b>OV-PMA-004</b>
<b>Área de especialidade</b>	<b>Gerenciamento e Aquisição de Programas/Projetos (PMA)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Gerenciar um portfólio de investimentos em TI que esteja alinhado às necessidades gerais da missão e prioridades empresariais.
<b>Tarefas</b>	T0220, T0223, T0277, T0302, T0377, T0415, T0493, T0551
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0072, K0120, K0126, K0146, K0154, K0165, K0169, K0235, K0257, K0270
<b>Habilidades</b>	S0372
<b>Aptidões</b>	A0039

<b>Nome da Função de Trabalho</b>	<b>Auditor de Programas de TI</b>
<b>ID da função de trabalho</b>	<b>OV-PMA-005</b>
<b>Área de especialidade</b>	<b>Gerenciamento e Aquisição de Programas/Projetos (PMA)</b>
<b>Categoria</b>	<b>Supervisionar e Governar (OV)</b>
<b>Descrição da função de trabalho</b>	Realizar avaliações de um programa de TI ou de seus componentes individuais, para determinar o compliance e aderência aos normas estabelecidos.
<b>Tarefas</b>	T0072, T0207, T0208, T0223, T0256, T0389, T0412, T0415
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0047, K0048, K0072, K0090, K0120, K0126, K0148, K0154, K0165, K0169, K0198, K0200, K0235, K0257, K0270
<b>Habilidades</b>	S0038, S0085, S0372
<b>Aptidões</b>	A0056

**B.4 Proteger e Defender (PR)**

<b>Nome da Função de Trabalho</b>	<b>Analista de Defesa Cibernética</b>
<b>ID da função de trabalho</b>	<b>PR-CDA-001</b>
<b>Área de especialidade</b>	<b>Análise de Defesa Cibernética (CDA)</b>
<b>Categoria</b>	<b>Proteger e Defender (PR)</b>
<b>Descrição da função de trabalho</b>	Utilizar dados coletados de uma variedade de ferramentas de defesa cibernética (ex.: alertas de IDS, firewalls, registros de tráfego de rede) para analisar eventos que ocorrem dentro de seus ambientes com o propósito de mitigar ameaças.
<b>Tarefas</b>	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
<b>Habilidades</b>	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
<b>Aptidões</b>	A0010, A0015, A0066, A0123, A0128, A0159

<b>Nome da Função de Trabalho</b>	<b>Especialista em Suporte de Infraestrutura de Defesa Cibernética</b>
<b>ID da função de trabalho</b>	<b>PR-INF-001</b>
<b>Área de especialidade</b>	<b>Suporte de Infraestrutura de Defesa Cibernética (INF)</b>
<b>Categoria</b>	<b>Proteger e Defender (PR)</b>
<b>Descrição da função de trabalho</b>	Testar, implementar, implantar, manter e administrar o hardware e software da infraestrutura.
<b>Tarefas</b>	T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0058, K0061, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0332, K0334
<b>Habilidades</b>	S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124, S0367
<b>Aptidões</b>	A0123

<b>Nome da Função de Trabalho</b>	<b>Respondente a Incidentes de Defesa Cibernética</b>
<b>ID da função de trabalho</b>	<b>PR-CIR-001</b>
<b>Área de especialidade</b>	<b>Resposta a Incidentes (CIR)</b>
<b>Categoria</b>	<b>Proteger e Defender (PR)</b>
<b>Descrição da função de trabalho</b>	Investigar, analisar e responder a incidentes cibernéticos no ambiente de rede ou enclave.
<b>Tarefas</b>	T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, T0510
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0230, K0259, K0287, K0332, K0565, K0624
<b>Habilidades</b>	S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365
<b>Aptidões</b>	A0121, A0128

<b>Nome da Função de Trabalho</b>	<b>Analista de Avaliação de Vulnerabilidades</b>
<b>ID da função de trabalho</b>	<b>PR-VAM-001</b>
<b>Área de especialidade</b>	<b>Avaliação e Gerenciamento de Vulnerabilidade (VAM)</b>
<b>Categoria</b>	<b>Proteger e Defender (PR)</b>
<b>Descrição da função de trabalho</b>	Executar avaliações de sistemas e redes dentro do NE ou enclave e identificar onde esses sistemas/redes se desviam de configurações aceitáveis, norma para o enclave ou norma local. Medir a eficácia da arquitetura de defesa em profundidade contra vulnerabilidades conhecidas.
<b>Tarefas</b>	T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0089, K0106, K0139, K0161, K0162, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0332, K0342, K0344, K0624
<b>Habilidades</b>	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364, S0367
<b>Aptidões</b>	A0001, A0044, A0120, A0123

**B.5 Analisar (AN)**

<b>Nome da Função de Trabalho</b>	<b>Analista de Ameaças/Alertas</b>
<b>ID da função de trabalho</b>	<b>AN-TWA-001</b>
<b>Área de especialidade</b>	<b>Analista de Alertas/Ameaças (TWA)</b>
<b>Categoria</b>	<b>Analisar (AN)</b>
<b>Descrição da função de trabalho</b>	Desenvolver indicadores cibernéticos para manter a percepção sobre o status do ambiente operacional altamente dinâmico. Coletar, processar, analisar e disseminar avaliações de ameaças/alertas cibernéticos.
<b>Tarefas</b>	T0569, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0660, T0685, T0687, T0707, T0708, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0783, T0785, T0786, T0792, T0800, T0805, T0834
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0415, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0471, K0480, K0499, K0511, K0516, K0556, K0560, K0561, K0565, K0603, K0604, K0610, K0612, K0614
<b>Habilidades</b>	S0194, S0196, S0203, S0211, S0218, S0227, S0228, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303
<b>Aptidões</b>	A0013, A0066, A0072, A0080, A0082, A0083, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109

<b>Nome da Função de Trabalho</b>	<b>Analista de Exploração</b>
<b>ID da função de trabalho</b>	<b>AN-EXP-001</b>
<b>Área de especialidade</b>	<b>Análise de Exploração (EXP)</b>
<b>Categoria</b>	<b>Analisar (AN)</b>
<b>Descrição da função de trabalho</b>	Colaborar na identificação de lacunas de acesso e coleta que podem ser preenchidas por meio de atividades de coleta e/ou preparação cibernética. Alavancar todos os recursos autorizados e técnicas analíticas para penetrar nas redes direcionadas.
<b>Tarefas</b>	T0028, T0266, T0570, T0572, T0574, T0591, T0600, T0603, T0608, T0614, T0641, T0695, T0701, T0720, T0727, T0736, T0738, T0754, T0775, T0777
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0131, K0142, K0143, K0177, K0224, K0349, K0362, K0417, K0444, K0471, K0560, K0351, K0354, K0368, K0371, K0376, K0379, K0388, K0393, K0394, K0397, K0418, K0430, K0443, K0447, K0451, K0470, K0473, K0484, K0487, K0489, K0509, K0510, K0523, K0529, K0535, K0544, K0557, K0559, K0608
<b>Habilidades</b>	S0066, S0184, S0199, S0200, S0201, S0204, S0207, S0214, S0223, S0236, S0237, S0239, S0240, S0245, S0247, S0258, S0260, S0264, S0269, S0279, S0286, S0290, S0294, S0300
<b>Aptidões</b>	A0013, A0066, A0080, A0084, A0074, A0086, A0092, A0093, A0104

<b>Nome da Função de Trabalho</b>	<b>Analista de Todas as Fontes</b>
<b>ID da função de trabalho</b>	<b>AN-ASA-001</b>
<b>Área de especialidade</b>	<b>Análise de Todas as Fontes (ASA)</b>
<b>Categoria</b>	<b>Analisar (AN)</b>
<b>Descrição da função de trabalho</b>	Analisar dados/informações de uma ou várias fontes para realizar a preparação do ambiente, responder às solicitações de informações e enviar coleta de inteligência e requisitos de produção em apoio ao planejamento e às operações.
<b>Tarefas</b>	T0569, T0582, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0642, T0660, T0678, T0685, T0686, T0687, T0707, T0708, T0710, T0713, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0771, T0782, T0783, T0785, T0786, T0788, T0789, T0792, T0797, T0800, T0805, T0834
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0221, K0349, K0357, K0362, K0377, K0392, K0395, K0405, K0409, K0410, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0457, K0458, K0460, K0464, K0465, K0469, K0471, K0480, K0507, K0511, K0516, K0533, K0542, K0549, K0551, K0556, K0560, K0561, K0565, K0577, K0598, K0603, K0604, K0610, K0612, K0614
<b>Habilidades</b>	S0194, S0203, S0211, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303, S0189, S0254, S0360
<b>Aptidões</b>	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0085, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0108, A0109

<b>Nome da Função de Trabalho</b>	<b>Especialista em Avaliação de Missão</b>
<b>ID da função de trabalho</b>	<b>AN-ASA-002</b>
<b>Área de especialidade</b>	<b>Análise de Todas as Fontes (ASA)</b>
<b>Categoria</b>	<b>Analisar (AN)</b>
<b>Descrição da função de trabalho</b>	Desenvolver planos de avaliação e medidas de desempenho/eficácia. Realizar avaliações de eficácia estratégica e operacional para eventos cibernéticos, conforme necessário. Determinar se os sistemas tiveram o desempenho esperado e fornecer informações para a determinar a eficácia operacional.
<b>Tarefas</b>	T0582, T0583, T0585, T0586, T0588, T0589, T0593, T0597, T0611, T0615, T0617, T0624, T0660, T0661, T0663, T0678, T0684, T0685, T0686, T0707, T0718, T0748, T0749, T0752, T0758, T0761, T0782, T0783, T0785, T0786, T0788, T0789, T0793, T0797, T0834
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0410, K0414, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0457, K0460, K0464, K0465, K0469, K0471, K0480, K0507, K0511, K0516, K0549, K0551, K0556, K0560, K0561, K0565, K0598, K0603, K0604, K0610, K0612, K0614
<b>Habilidades</b>	S0189, S0194, S0203, S0211, S0216, S0218, S0227, S0228, S0229, S0249, S0254, S0256, S0271, S0278, S0285, S0288, S0289, S0292, S0296, S0297, S0303, S0360

<b>Aptidões</b>	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109, A0085, A0108
-----------------	--

<b>Nome da Função de Trabalho</b>	<b>Desenvolvedor de Destino</b>
<b>ID da função de trabalho</b>	<b>AN-TGT-001</b>
<b>Área de especialidade</b>	<b>Destino (TGT)</b>
<b>Categoria</b>	<b>Analisar (AN)</b>
<b>Descrição da função de trabalho</b>	Executar a análise do sistema de destino, criar e/ou manter pastas de destino eletrônicas para incluir entradas da preparação do ambiente e/ou fontes de inteligência internas ou externas. Manter coordenação com as atividades de destino de parceiros e organizações de inteligência e apresentar os destinos potenciais para verificação e validação.
<b>Tarefas</b>	T0597, T0617, T0707, T0582, T0782, T0797, T0588, T0624, T0661, T0663, T0684, T0642, T0710, T0561, T0594, T0599, T0633, T0650, T0652, T0688, T0717, T0731, T0744, T0769, T0770, T0776, T0781, T0790, T0794, T0798, T0799, T0802, T0815, T0824, T0835
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0142, K0177, K0349, K0351, K0357, K0362, K0379, K0381, K0392, K0395, K0402, K0409, K0413, K0417, K0426, K0427, K0431, K0436, K0437, K0439, K0440, K0444, K0445, K0446, K0449, K0457, K0458, K0460, K0461, K0464, K0465, K0466, K0471, K0473, K0478, K0479, K0497, K0499, K0507, K0516, K0533, K0542, K0543, K0546, K0547, K0549, K0551, K0555, K0556, K0560, K0561, K0565, K0598, K0603, K0604, K0614
<b>Habilidades</b>	S0194, S0203, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0189, S0228, S0216, S0292, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0302, S0360, S0361
<b>Aptidões</b>	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

<b>Nome da Função de Trabalho</b>	<b>Analista de Rede de Destino</b>
<b>ID da função de trabalho</b>	<b>AN-TGT-002</b>
<b>Área de especialidade</b>	<b>Destino (TGT)</b>
<b>Categoria</b>	<b>Analisar (AN)</b>
<b>Descrição da função de trabalho</b>	Conduzir análises avançadas de coleta e dados de código aberto para garantir a continuidade das redes de destino; traçar o perfil dos destinos e suas atividades; e desenvolver técnicas para obter mais informações sobre os destinos. Determinar como os destinos se comunicam, se movem, operam e vivem com base no conhecimento de tecnologias de destino, redes digitais e os aplicativos nelas inseridos.
<b>Tarefas</b>	T0617, T0707, T0582, T0797, T0624, T0710, T0599, T0650, T0802, T0595, T0606, T0607, T0621, T0653, T0692, T0706, T0715, T0722, T0745, T0765, T0767, T0778, T0803, T0807

<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0177, K0349, K0362, K0444, K0471, K0392, K0395, K0431, K0436, K0440, K0445, K0449, K0516, K0379, K0473, K0413, K0439, K0479, K0547, K0487, K0544, K0559, K0389, K0403, K0424, K0442, K0462, K0472, K0483, K0499, K0500, K0520, K0550, K0567, K0592, K0599, K0600
<b>Habilidades</b>	S0194, S0203, S0229, S0256, S0228, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0177, S0178, S0181, S0183, S0191, S0197, S0217, S0219, S0220, S0225, S0231, S0234, S0244, S0246, S0259, S0261, S0262, S0263, S0268, S0277, S0280, S0291, S0301
<b>Aptidões</b>	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

<b>Nome da Função de Trabalho</b>	<b>Analista de Linguagem Multidisciplinar</b>
<b>ID da função de trabalho</b>	<b>AN-LNG-001</b>
<b>Área de especialidade</b>	<b>Análise de Linguagem (GNL)</b>
<b>Categoria</b>	<b>Analisar (AN)</b>
<b>Descrição da função de trabalho</b>	Aplicar experiência específica em idiomas e culturas sobre destinos/ameaças e conhecimento técnico para processar, analisar e/ou disseminar informações de inteligência derivadas de linguagem, voz e/ou material gráfico. Criar e manter bancos de dados em idiomas específicos e recursos de trabalho para apoiar a execução de ações cibernéticas e garantir o compartilhamento de conhecimento crítico. Proporcionar experiência específica em projetos interdisciplinares ou intensivos em língua estrangeira.
<b>Tarefas</b>	T0650, T0606, T0715, T0745, T0761, T0837, T0838, T0839, T0840, T0841, T0842, T0843, T0844, T0845, T0846, T0847, T0848, T0849, T0850, T0851, T0852, T0853, T0854, T0855, T0856, T0857, T0858, T0859, T0860
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0143, K0177, K0431, K0449, K0413, K0487, K0462, K0520, K0550, K0567, K0599, K0600, K0417, K0377, K0356, K0359, K0391, K0396, K0398, K0407, K0416, K0476, K0488, K0491, K0493, K0499, K0524, K0532, K0539, K0540, K0541, K0545, K0548, K0564, K0571, K0574, K0579, K0596, K0606, K0607
<b>Habilidades</b>	S0187, S0217, S0244, S0259, S0262, S0277, S0218, S0184, S0290, S0179, S0188, S0193, S0195, S0198, S0210, S0212, S0215, S0224, S0226, S0232, S0233, S0235, S0241, S0251, S0253, S0265, S0283, S0284
<b>Aptidões</b>	A0013, A0089, A0071, A0103

**B.6 Coletar e Operar (CO)**

<b>Nome da Função de Trabalho</b>	<b>Gerente de Coleta de Todas as Fontes</b>
<b>ID da função de trabalho</b>	<b>CO-CLO-001</b>
<b>Área de especialidade</b>	<b>Operações de Coleta (CLO)</b>
<b>Categoria</b>	<b>Coletar e Operar (CO)</b>
<b>Descrição da função de trabalho</b>	Identificar autoridades de coleta e meio ambiente; incorporar requisitos de informação prioritários no gerenciamento de coleta; desenvolver conceitos para cumprir as determinações da liderança. Determinar os recursos e capacidades de coleta disponíveis, identificar novos recursos de coleta, construir e divulgar planos de coleta. Monitorar a execução da coleta programada para garantir a execução eficaz do plano de coleta.
<b>Tarefas</b>	T0562, T0564, T0568, T0573, T0578, T0604, T0605, T0625, T0626, T0631, T0632, T0634, T0645, T0646, T0647, T0649, T0651, T0657, T0662, T0674, T0681, T0683, T0698, T0702, T0714, T0716, T0721, T0723, T0725, T0734, T0737, T0750, T0753, T0755, T0757, T0773, T0779, T0806, T0809, T0810, T0811, T0812, T0814, T0820, T0821, T0827
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0431, K0449, K0417, K0579, K0596, K0444, K0471, K0392, K0395, K0440, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0405, K0480, K0610, K0612, K0353, K0361, K0364, K0380, K0382, K0383, K0386, K0387, K0390, K0401, K0404, K0412, K0419, K0425, K0435, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0482, K0492, K0495, K0496, K0498, K0503, K0505, K0513, K0521, K0522, K0526, K0527, K0552, K0553, K0554, K0558, K0562, K0563, K0569, K0570, K0580, K0581, K0583, K0584, K0587, K0588, K0601, K0605, K0613
<b>Habilidades</b>	S0238, S0304, S0305, S0311, S0313, S0316, S0317, S0324, S0325, S0327, S0328, S0330, S0332, S0334, S0335, S0336, S0339, S0342, S0344, S0347, S0351, S0352, S0362
<b>Aptidões</b>	A0069, A0070, A0076, A0078, A0079

<b>Nome da Função de Trabalho</b>	<b>Gerente de Requisitos de Coleta de Todas as Fontes</b>
<b>ID da função de trabalho</b>	<b>CO-CLO-002</b>
<b>Área de especialidade</b>	<b>Operações de Coleta (CLO)</b>
<b>Categoria</b>	<b>Coletar e Operar (CO)</b>
<b>Descrição da função de trabalho</b>	Avaliar as operações de coleta e desenvolver estratégias para os requisitos de coleta com base em efeitos, usando fontes e métodos disponíveis para melhoria do processo. Desenvolver, processar, validar e coordenar o envio de requisitos de coleta. Avaliar o desempenho dos recursos e das operações de coleta.
<b>Tarefas</b>	T0564, T0568, T0578, T0605, T0651, T0714, T0725, T0734, T0809, T0810, T0811, T0565, T0577, T0580, T0596, T0602, T0613, T0668, T0673, T0675, T0682, T0689, T0693, T0694, T0730, T0746, T0780, T0819, T0822, T0830, T0831, T0832, T0833
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0353, K0361, K0364, K0380, K0382, K0383, K0384, K0386, K0387, K0390, K0395, K0401, K0404, K0412, K0417, K0419, K0421, K0425, K0427, K0431, K0435, K0444, K0445, K0446, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0480, K0482, K0492, K0495, K0496, K0498, K0505, K0513, K0516, K0521, K0526, K0527, K0552, K0554, K0558, K0560, K0561, K0562, K0563, K0565, K0568, K0569, K0570, K0579, K0580, K0581, K0584, K0587, K0588, K0596, K0605, K0610, K0612
<b>Habilidades</b>	S0304, S0305, S0316, S0317, S0327, S0330, S0334, S0335, S0336, S0339, S0344, S0347, S0352, S0329 S0337, S0346, S0348, S0353, S0362
<b>Aptidões</b>	A0069, A0070, A0078

<b>Nome da Função de Trabalho</b>	<b>Planejador Intel de Cibernética</b>
<b>ID da função de trabalho</b>	<b>CO-OPL-001</b>
<b>Área de especialidade</b>	<b>Planejamento Operacional Cibernético (OPL)</b>
<b>Categoria</b>	<b>Coletar e Operar (CO)</b>
<b>Descrição da função de trabalho</b>	Desenvolver planos detalhados de inteligência para atender aos requisitos de operações cibernéticas. Colaborar com planejadores de operações cibernéticas para identificar, validar e cobrar requisitos para coleta e análise. Participar da seleção de redes de destino, validação, sincronização e execução de ações cibernéticas. Sincronizar atividades de inteligência para apoiar os objetivos da organização no ciberespaço.
<b>Tarefas</b>	T0734, T0563, T0575, T0576, T0579, T0581, T0587, T0590, T0592, T0601, T0627, T0628, T0630, T0636, T0637, T0638, T0639, T0640, T0648, T0656, T0659, T0667, T0670, T0676, T0680, T0690, T0691, T0705, T0709, T0711, T0719, T0726, T0728, T0733, T0735, T0739, T0743, T0760, T0763, T0772, T0784, T0801, T0808, T0816, T0836
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0120, K0431, K0417, K0444, K0395, K0445, K0560, K0427, K0446, K0561, K0565, K0480, K0610, K0612, K0435, K0471, K0392, K0440, K0405, K0377, K0349, K0362, K0436, K0379, K0403, K0460, K0464, K0556, K0603, K0614, K0465, K0507, K0598, K0511, K0414, K0577, K0347, K0350, K0352, K0355, K0358, K0399, K0400, K0408, K0411, K0422, K0432, K0455, K0456, K0459, K0463, K0494, K0499, K0501, K0502, K0504, K0506, K0508, K0512, K0514, K0517, K0518, K0519, K0525, K0538, K0566, K0572, K0575, K0578, K0582, K0585, K0586, K0589, K0590, K0591, K0593, K0594, K0595, K0599, K0602
<b>Habilidades</b>	S0218, S0203, S0249, S0278, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0272, S0273, S0306, S0307, S0308, S0309, S0310, S0312, S0314, S0315, S0318, S0319, S0320, S0321, S0322, S0323, S0331, S0333, S0338, S0340, S0341, S0343, S0345, S0350, S0360
<b>Aptidões</b>	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105, A0160

<b>Nome da Função de Trabalho</b>	<b>Planejador de Operações Cibernéticas</b>
<b>ID da função de trabalho</b>	<b>CO-OPL-002</b>
<b>Área de especialidade</b>	<b>Planejamento Operacional Cibernético (OPL)</b>
<b>Categoria</b>	<b>Coletar e Operar (CO)</b>
<b>Descrição da função de trabalho</b>	Desenvolver planos detalhados para realizar ou oferecer suporte a várias operações cibernéticas aplicáveis por meio da colaboração com outros planejadores, operadores e/ou analistas. Participar na seleção, validação, sincronização e execução de redes de destino e viabilizar a integração durante a execução de ações cibernéticas.
<b>Tarefas</b>	T0734, T0563, T0579, T0581, T0592, T0627, T0628, T0640, T0648, T0667, T0670, T0680, T0690, T0719, T0733, T0739, T0743, T0763, T0772, T0801, T0836, T0571, T0622, T0635, T0654, T0655, T0658, T0665, T0672, T0679, T0699, T0703, T0704, T0732, T0741, T0742, T0747, T0764, T0787, T0791, T0795, T0813, T0823
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0347, K0349, K0350, K0352, K0362, K0377, K0379, K0392, K0395, K0399, K0400, K0403, K0408, K0411, K0414, K0417, K0422, K0431, K0432, K0435, K0436, K0444, K0445, K0446, K0455, K0464, K0465, K0471, K0480, K0494, K0497, K0499, K0501, K0502, K0504, K0506, K0507, K0508, K0511, K0512, K0514, K0516, K0518, K0519, K0525, K0534, K0538, K0556, K0560, K0561, K0565, K0566, K0572, K0576, K0582, K0585, K0586, K0589, K0590, K0593, K0594, K0597, K0598, K0599, K0603, K0610, K0612, K0614
<b>Habilidades</b>	S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349, S0360
<b>Aptidões</b>	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

<b>Nome da Função de Trabalho</b>	<b>Planejador de Integração de Parceiros</b>
<b>ID da função de trabalho</b>	<b>CO-OPL-003</b>
<b>Área de especialidade</b>	<b>Planejamento Operacional Cibernético (OPL)</b>
<b>Categoria</b>	<b>Coletar e Operar (CO)</b>
<b>Descrição da função de trabalho</b>	Trabalhar para promover a cooperação além das fronteiras organizacionais ou nacionais entre parceiros de operações cibernéticas. Auxiliar na integração de equipes cibernéticas parceiras, fornecendo orientação, recursos e colaboração para desenvolver as melhores práticas e facilitar o suporte organizacional, visando alcançar os objetivos em ações cibernéticas integradas.
<b>Tarefas</b>	T0581, T0582, T0627, T0670, T0739, T0763, T0772, T0836, T0571, T0635, T0665, T0699, T0732, T0747, T0764, T0787, T0795, T0823, T0601, T0760, T0784, T0629, T0666, T0669, T0671, T0700, T0712, T0729, T0759, T0766, T0817, T0818, T0825, T0826

<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0431, K0417, K0444, K0395, K0435, K0392, K0377, K0362, K0436, K0379, K0403, K0465, K0507, K0598, K0511, K0414, K0350, K0400, K0408, K0411, K0422, K0432, K0455, K0499, K0501, K0504, K0506, K0508, K0512, K0514, K0538, K0585, K0599
<b>Habilidades</b>	S0218, S0249, S0296, S0297, S0185, S0186, S0213, S0250, S0326, S0360
<b>Aptidões</b>	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

<b>Nome da Função de Trabalho</b>	<b>Operador Cibernético</b>
<b>ID da função de trabalho</b>	<b>CO-OPS-001</b>
<b>Área de especialidade</b>	<b>Operações Cibernéticas (OPS)</b>
<b>Categoria</b>	<b>Coletar e Operar (CO)</b>
<b>Descrição da função de trabalho</b>	Realizar coleta, processamento e/ou geolocalização de sistemas para explorar, localizar e/ou rastrear sistemas de destino de interesse. Executar navegação na rede, análise tática pericial e, quando orientado, executar operações na rede.
<b>Tarefas</b>	T0566, T0567, T0598, T0609, T0610, T0612, T0616, T0618, T0619, T0620, T0623, T0643, T0644, T0664, T0677, T0696, T0697, T0724, T0740, T0756, T0768, T0774, T0796, T0804, T0828, T0829
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0051, K0109, K0142, K0224, K0363, K0372, K0373, K0375, K0379, K0403, K0406, K0420, K0423, K0428, K0427, K0429, K0430, K0433, K0438, K0440, K0452, K0468, K0481, K0485, K0486, K0480, K0516, K0528, K0530, K0531, K0536, K0560, K0565, K0573, K0608, K0609
<b>Habilidades</b>	S0062, S0183, S0236, S0182, S0190, S0192, S0202, S0206, S0221, S0242, S0243, S0252, S0255, S0257, S0266, S0267, S0270, S0275, S0276, S0281, S0282, S0293, S0295, S0298, S0299, S0363
<b>Aptidões</b>	A0095, A0097, A0099, A0100

**B.7 Investigar (IN)**

<b>Nome da Função de Trabalho</b>	<b>Investigador de Crimes Cibernéticos</b>
<b>ID da função de trabalho</b>	<b>IN-INV-001</b>
<b>Área de especialidade</b>	<b>Investigação Cibernética (INV)</b>
<b>Categoria</b>	<b>Investigar (IN)</b>
<b>Descrição da função de trabalho</b>	Identificar, coletar, examinar e preservar evidências usando técnicas analíticas e investigativas controladas e documentadas.
<b>Tarefas</b>	[ <b>Nota:</b> Várias atividades só podem ser realizadas por pessoas com Autoridade de Aplicação da Lei ou Contraineligência.]  T0031, T0059, T0096, T0103, T0104, T0110, T0112, T0113, T0114, T0120, T0193, T0225, T0241, T0343, T0346, T0360, T0386, T0423, T0430, T0433, T0453, T0471, T0479, T0523
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0046, K0070, K0107, K0110, K0114, K0118, K0123, K0125, K0128, K0144, K0155, K0156, K0168, K0209, K0231, K0244, K0251, K0351, K0624
<b>Habilidades</b>	S0047, S0068, S0072, S0086
<b>Aptidões</b>	A0174, A0175

<b>Nome da Função de Trabalho</b>	<b>Analista de Perícia da Segurança Pública/Contraineligência</b>
<b>ID da função de trabalho</b>	<b>IN-FOR-001</b>
<b>Área de especialidade</b>	<b>Perícia Digital (FOR)</b>
<b>Categoria</b>	<b>Investigar (IN)</b>
<b>Descrição da função de trabalho</b>	Realizar investigações profundas sobre crimes baseados em computador que estabelecem evidências documentais ou físicas, para incluir mídia digital e registros associados a incidentes de invasão cibernética.
<b>Tarefas</b>	T0027, T0036, T0048, T0075, T0087, T0103, T0113, T0120, T0165, T0167, T0168, T0172, T0173, T0179, T0182, T0190, T0193, T0212, T0216, T0238, T0240, T0241, T0246, T0253, T0285, T0286, T0287, T0288, T0289, T0432, T0439, T0471, T0532
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0060, K0070, K0077, K0078, K0107, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0305, K0624
<b>Habilidades</b>	S0032, S0046, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093
<b>Aptidões</b>	A0005, A0175

<b>Nome da Função de Trabalho</b>	<b>Analista de Perícia de Defesa Cibernética</b>
<b>ID da função de trabalho</b>	<b>IN-FOR-002</b>
<b>Área de especialidade</b>	<b>Perícia Digital (FOR)</b>
<b>Categoria</b>	<b>Investigar (IN)</b>
<b>Descrição da função de trabalho</b>	Analisar a evidência digital e investigar incidentes de segurança do computador para derivar informações úteis em apoio à redução da vulnerabilidade do sistema/rede.
<b>Tarefas</b>	T0027, T0036, T0048, T0049, T0075, T0087, T0103, T0113, T0165, T0167, T0168, T0172, T0173, T0175, T0179, T0182, T0190, T0212, T0216, T0238, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0546
<b>Conhecimentos</b>	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0224, K0254, K0255, K0301, K0304, K0347, K0624
<b>Habilidades</b>	S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133, S0156
<b>Aptidões</b>	A0005, A0043

## Appendix C – Ferramentas de Desenvolvimento da Força de Trabalho

### C.1 Kit de Ferramentas de Desenvolvimento da Força de Trabalho em Cibersegurança do DHS

O Kit de ferramentas de desenvolvimento da força de trabalho em cibersegurança (CWDT) [8] ajuda as organizações entenderem as necessidades de força de trabalho e de recrutamento em cibersegurança, para proteger as suas informações, bem como as informações dos clientes e redes. Este kit de ferramentas inclui tipos de carreira em cibersegurança e recursos de recrutamento para contratar e reter os melhores talentos. O CWDT proporciona ferramentas para ajudar a entender os riscos e fazer o inventário da força de trabalho em segurança cibernética de uma organização. As ferramentas do CWDT alavancam as áreas de especialidade, KSAs e tarefas do NICE Framework. O CWDT observa que a primeira etapa de preparação para se construir e organizar uma força de trabalho em segurança cibernética é ter uma visão compartilhada. Ter uma visão compartilhada significa apoiar os líderes conforme eles reagem às mudanças ambientais e fornecer dados para melhor ajustar os recursos, identificar padrões de trabalho e destacar áreas de risco potencial. Esse entendimento é especialmente importante em um ambiente que passa por mudanças constantes, como é o caso da segurança cibernética. O CWDT inclui um Modelo de Maturidade em Capacitação (CMM) para o Planejamento da Força de Trabalho em Cibersegurança, que é uma ferramenta de autoavaliação para ajudar uma organização a avaliar a maturidade da sua capacidade de planejamento da força de trabalho em cibersegurança.

O (CWDT) oferece perfis que servem de orientação, com enfoque em reter os funcionários em todos os níveis, seja profissionais de nível básico, médio ou com vasta experiência em cibersegurança.

#### C.1.1 Níveis de Proficiência e Planos de Carreira

Desenvolver e compartilhar planos de carreira em cibersegurança com os funcionários os ajudará a identificar os seus próprios níveis de proficiência para que possam fazer avanços de carreira.

O CWDT inclui um processo de três etapas para desenvolver planos de carreira em segurança cibernética em determinada organização.

- Etapa 1 – Familiarize-se com os níveis de proficiência e analisar os planos de carreira usados como modelo.
- Etapa 2 – Usar um modelo do CWDT para criar planos de carreira em cibersegurança, específicos e customizados para a sua organização, preenchendo as "*Experiências e credenciais sugeridas*", "*Competências e exemplos de habilidades/KSAs*" e "*Atividades de treinamento e desenvolvimento sugeridas*".
- Etapa 3 – Compartilhar planos de carreira com os gerentes e funcionários de cibersegurança.

## C.2 Ferramenta de Construção de Excelência em Cibersegurança de Baldrige

Quando uma organização determinar efetivamente quais serão os requisitos de cibersegurança (por meio de uma auditoria de segurança cibernética ou uma autoavaliação), ela poderá usar o NICE Framework como referência para identificar as funções de trabalho e tarefas que ajudarão a atender tais requisitos. Mesmo sabendo que alguns termos generalizados, como "profissionais de cibernética", tenham sido historicamente usados para mensurar as necessidades, a especificidade fornecida pelo NICE Framework proporciona uma abordagem mais ampla para descrever as dezenas de funções discretas de trabalho que são necessárias. Ao identificar as competências exigidas e as que estão disponíveis, bem como identificar lacunas entre as habilidades exigidas e as que estão disponíveis, a organização pode determinar quais são as necessidades críticas. O NICE Framework ajuda uma organização a responder às seguintes perguntas, extraídas da Ferramenta de Excelência em Cibersegurança de Baldrige [9], sobre como manter um ambiente de força de trabalho eficaz e coeso para alcançar seus objetivos de cibersegurança:

- Como você avalia a sua capacidade de força de trabalho e as necessidades de capacidade relacionadas à segurança cibernética?
- Como você organiza e gerencia a sua força de trabalho em cibersegurança para estabelecer funções e responsabilidades?
- Como você prepara a sua força de trabalho para as constantes mudanças em termos de necessidades de competência e capacidade de cibersegurança?

À medida que mais organizações avaliam a força de trabalho em cibersegurança, o léxico de fácil entendimento do NICE Framework permite melhor avaliação das competências e capacidades em várias organizações, setores da indústria e regiões.

## C.3 Ferramenta para elaborar uma descrição de cargo

A ferramenta PushbuttonPD da Iniciativa de Suporte ao Gerenciamento DHS Cyberskills [10] permite que gerentes, supervisores e especialistas de RH elaborem rapidamente uma descrição do cargo de funcionário federal (PD) sem a necessidade de treinamento extensivo ou conhecimento prévio da classificação de cargos. A ferramenta foi criada para integrar a linguagem de várias fontes e normas oficiais de missão crítica, referentes aos deveres, tarefas e KSAs, visando a capturar rapidamente os requisitos exigidos pelo funcionário responsável pela contratação, apresentando tais requisitos em um pacote de contratação robusto que pode ser facilmente integrado aos processos atuais da agência de RH. Qualquer organização pode utilizar a Ferramenta PushbuttonPD e verificar como ela integra o material do NICE Framework em uma descrição de cargo.

## Appendix D – Referência Cruzada para Documentos de Orientações e Diretrizes

O Objetivo Estratégico nº 3 do NICE, Guia de Desenvolvimento de Carreira e Planejamento da Força de Trabalho, visa orientar os empregadores para que possam atender às demandas do mercado e reforçar o nível de recrutamento, contratação, desenvolvimento e retenção de talentos em cibersegurança. Um dos propósitos dentro deste objetivo estratégico é divulgar e aumentar a conscientização sobre a o NICE Framework e incentivar a sua adoção e utilização. A adoção, neste caso, significa usar o NICE Framework como um recurso de referência para ações relacionadas ao treinamento e educação da força de trabalho em cibersegurança.

Uma maneira de incentivar a adoção do NICE Framework é sugerir aos autores que escrevem orientações e diretrizes sobre segurança cibernética ou redigem documentos sobre esse tópico, que façam uma referência cruzada de algum conteúdo com os componentes no NICE Framework. O apêndice D inclui exemplos de referências cruzadas em publicações que podem incentivar a adoção do NICE Framework.

### D.1 Cybersecurity Framework

Em 2014, o NIST lançou o Framework for Improving Critical Infrastructure Cybersecurity [11],[Guia para Melhorar a Segurança Cibernética da Infraestrutura Crítica] comumente referido como Cybersecurity Framework. O guia foi desenvolvido em resposta à Ordem Executiva (EO) 13636 [12], e fornece uma abordagem baseada em desempenho e economicamente viável para ajudar as organizações a identificar, avaliar e gerenciar riscos de cibersegurança. Ele foi construído após uma série de workshops públicos, convocados pelo NIST, para que as pessoas tivessem um entendimento mais amplo das normas e metodologias que seriam mais úteis para instituir uma gestão de risco eficaz, e como as boas práticas voluntárias em vigor podem ser implementadas para incrementar a segurança cibernética.

Um documento complementar ao Cybersecurity Framework, intitulado NIST Roadmap for Improving Critical Infrastructure Cybersecurity [*Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica do NIST*] [13] aponta para a necessidade de uma força de trabalho em cibersegurança que seja qualificada para atender às necessidades exclusivas de cibersegurança da infraestrutura crítica. O Guia indica que, conforme os ambientes de ameaça e tecnologia da cibersegurança evoluem, a força de trabalho deve continuar se adaptando ao design, desenvolvimento, implementação e manutenção de melhorias contínuas às práticas necessárias de cibersegurança.

O Cybersecurity Framework consiste em três partes: Framework Core (núcleo), Framework Implementation Tiers (níveis) e Framework Profiles (perfis). Cada componente do Cybersecurity Framework reforça a conexão entre os que comandam os negócios de uma empresa e as atividades de cibersegurança. Os elementos do Framework Core funcionam juntos, da seguinte maneira:

- **As funções** organizam as atividades básicas de cibersegurança em seu nível mais alto. As funções - identificar, proteger, detectar, responder e recuperar - são descritas detalhadamente abaixo:

- **Categorias** são as subdivisões de uma Função categorizadas em grupos de resultados de cibersegurança diretamente ligados às necessidades e atividades programáticas.
- **As subcategorias** dividem ainda mais uma categoria em resultados específicos de atividades técnicas e/ou de gestão. Elas fornecem um conjunto de resultados que, apesar de não serem exaustivos, ajudam a validar a realização dos resultados em cada Categoria.
- **Referências informativas** são seções específicas sobre normas, diretrizes e práticas comuns entre setores críticos de infraestrutura que ilustram determinado método para alcançar os resultados associados a cada Subcategoria. As Referências Informativas apresentadas no Framework Core são ilustrativas, mas não exaustivas. Elas representam a orientação intersetorial mais frequentemente referenciada durante o processo de desenvolvimento do Framework.

As Funções Principais contribuem para uma compreensão de alto nível das necessidades de cibersegurança da organização:

- **Identificar (ID)** – Desenvolver o entendimento organizacional para gerenciar o risco de cibersegurança em sistemas, ativos, dados e recursos.
- **Proteger (PR)** - Desenvolver e implementar as salvaguardas apropriadas para garantir a entrega de serviços de infraestrutura crítica.
- **Detectar (DE)** - Desenvolver e implementar as atividades adequadas para identificar a ocorrência de um evento de segurança cibernética
- **Responder (RS)** - Desenvolver e implementar as atividades adequadas para tomar medidas em relação a um evento de segurança cibernética detectado.
- **Recuperar (RC)** - Desenvolver e implementar as atividades apropriadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um evento de segurança cibernética.

Em muitos aspectos, essas Funções se correlacionam com as Categorias do NICE Framework. Tabela 8 descreve as relações entre as funções do Cybersecurity Framework e as categorias do NICE Framework.

**Tabela 8 - Descrição comparativa das categorias da força de trabalho do NICE Framework correlacionadas às funções do Cybersecurity Framework**

<b>Categorias do NICE Framework</b>	<b>Descrição da Categoria</b>	<b>Funções correlacionadas ao Cybersecurity Framework</b>
Provisão de Segurança (SP)	Idealizar, criar o design e/ou construir sistemas seguros de tecnologia da informação (TI), responsáveis por aspectos de desenvolvimento do sistema e/ou da rede.	Identificar (ID), Proteger (RP)
Operar e Manter (OM)	Oferecer suporte, administração e a manutenção necessária para garantir o desempenho e a segurança eficaz e eficiente do sistema de tecnologia da informação (TI).	Proteger (PR), Detectar (DE)
Supervisionar e Governar (OV)	Proporcionar liderança, gestão, direcionamento, desenvolvimento e defesa para que a organização possa conduzir efetivamente o trabalho de segurança cibernética.	Identificar (ID), Proteger (PR), Detectar (DE), Recuperar (RC)
Proteger e Defender (PR)	Identificar, analisar e mitigar ameaças a sistemas e/ou redes internas de tecnologia da informação (TI).	Proteger (PR), Detectar (DE), Responder (RS)
Analisar (AN)	Executar análises e avaliações altamente especializadas das informações recebidas sobre cibersegurança para determinar a sua utilidade em questões de inteligência.	Identificar (ID), Detectar (DE), Responder (RS)
Coletar e Operar (CO)	Realizar operações especializadas em negação e fraude, bem como a coleta de informações de cibersegurança que podem ser usadas para desenvolver inteligência.	Detectar (DE), Proteger (PR), Responder (RS)
Investigar (IN)	Investigar eventos de cibersegurança ou crimes relacionados a sistemas de tecnologia da informação (TI), redes e evidências digitais.	Detectar (DE), Responder (RS), Recuperar (RC)

### D.1.2 Exemplo de Integração do Cybersecurity Framework com o NICE Framework

O Cybersecurity Framework e o NICE Framework foram desenvolvidos separadamente, porém, um complementa o outro ao descreverem uma abordagem hierárquica para cumprir os objetivos de segurança cibernética. Imagine o seguinte exemplo:

A função de **Resposta** do Cybersecurity Framework inclui uma categoria de **Mitigação (RS.MI)**. A categoria inclui uma subcategoria, **RS.MI-2**, apontando para o seguinte resultado: “incidentes são mitigados”. Embora o Cybersecurity Framework descreva esse resultado e forneça várias referências informativas sobre os controles de segurança para chegar a tal resultado, o Cybersecurity Framework não fornece orientação informativa sobre quem deve ser o responsável para se chegar ao resultado, ou quais são os KSAs que se aplicam a este caso.

Ao analisarmos o NICE Framework, identificamos a função de **Respondente a Incidentes de Defesa Cibernética (PR-IR-001)** na categoria **Proteger e Defender (PR)**, na área de especialidade **Resposta a Incidentes (IR)**. Podemos examinar a descrição desta função para garantir que ela se alinhe ao resultado do Cybersecurity Framework **RS.MI-2**:

Responde a interrupções dentro do domínio pertinente para mitigar ameaças imediatas e potenciais. Usa abordagens de mitigação, preparação, resposta e recuperação para maximizar a sobrevivência da vida, a preservação da propriedade e a segurança da informação. Investiga e analisa atividades de resposta relevantes e avalia a eficácia e melhorias das práticas existentes.

Investiga, analisa e responde a incidentes de segurança cibernética dentro do ambiente de rede ou enclave.

Aprendemos com o Appendix A deste documento que a pessoa cuja posição inclui esta função de trabalho pode realizar muitas tarefas aqui descritas, que se alinham com o resultado desejado do Cybersecurity Framework:

- **T0041** - Coordenar e fornecer suporte técnico especializado para técnicos de defesa cibernética em toda a empresa para resolver incidentes de defesa cibernética.
- **T0047** - Correlacionar dados de incidentes para identificar vulnerabilidades específicas e fazer recomendações que permitam a remediação rápida.
- **T0161** - Realizar análise de arquivos de log de uma variedade de fontes (ex.: registros individuais de host, registros de tráfego de rede, registros de firewall e logs do sistema de detecção de invasões [IDS]) para identificar possíveis ameaças à segurança da rede.
- **T0163** - Realizar a triagem de incidentes de defesa de segurança cibernética, para incluir a determinação de escopo, urgência e impacto potencial; identificar a vulnerabilidade específica; e fazer recomendações que possibilitem uma correção rápida.
- **T0170** - Realizar coleta inicial e pericial de imagens e inspecionar para discernir possível mitigação/remediação em sistemas corporativos.
- **T0175** - Executar tarefas de resolução de incidentes de defesa de segurança cibernética em tempo real (ex.: coletas periciais, correlação e rastreamento de invasões, análise de ameaças e remediação direta do sistema) para apoiar as equipes de resposta a incidentes implantáveis (IRTs).
- **T0214** - Receber e analisar alertas de rede de diversas fontes dentro da empresa e determinar possíveis causas desses alertas.
- **T0233** - Rastrear e documentar incidentes de defesa de segurança cibernética desde a detecção inicial até a resolução final.
- **T0246** - Escrever e publicar técnicas de defesa de segurança cibernética, orientação e relatórios sobre os resultados de incidentes para devidas partes interessadas.
- **T0262** - Empregar princípios e práticas de defesa em profundidade aprovadas (ex.: defesa em vários lugares, defesas em camadas, robustez de segurança).

- **T0278** - Coletar artefatos de invasão (ex.: código fonte, malware, Trojans) e usar os dados descobertos para permitir a mitigação de possíveis incidentes de defesa de segurança cibernética dentro da empresa.
- **T0279** - Servir como perito técnico e pessoa de contato com o pessoal da aplicação da lei para explicar detalhes do incidente conforme necessário.
- **T0312** - Coordenar medidas com os analistas de inteligência para correlacionar dados de avaliação de ameaças.
- **T0164** - Realizar análise e gerar relatórios de tendências sobre defesa de segurança cibernética.
- **T0395** - Escrever e publicar comentários pós-ação.
- **T0503** - Monitorar fontes de dados externos (ex.: sites de fornecedores de defesa de segurança cibernética, Equipes de Resposta a Emergências de Computador, Foco de Segurança) para se manter atualizado sobre a condição da ameaça de defesa da segurança cibernética e determinar quais são os problemas de segurança que podem impactar a empresa.
- **T0510** - Coordenar funções de resposta a incidentes.

Além disso, devido ao Appendix B, podemos estar cientes da ampla gama de KSAs que podem ser necessários para uma pessoa cujo cargo em segurança cibernética inclua essa função de trabalho.

Após obter essas informações, uma organização que busca alcançar o resultado descrito no Cybersecurity Framework

**RS.MI-2** poderá determinar se um ou mais funcionários possuem as habilidades necessárias para realizar as tarefas descritas. No caso de um ou mais KSAs estiverem faltando, o funcionário que deseja exercer essa função de trabalho saberá especificamente quais as áreas que precisam de melhorias, buscando aperfeiçoamento por meio de aulas acadêmicas ou treinamento no setor para obter os conhecimentos necessários. Caso um funcionário com tais especificações não seja identificado, o empregador terá em mãos as descrições específicas das Tarefas e os requisitos KSA que podem ser publicados em postagens de vaga de emprego, ou que podem ser usados para a contratação de funcionários temporários, assim aumentando o quadro de pessoal.

## **D.2 Engenharia de Segurança de Sistemas**

A Publicação Especial NIST (SP) 800-160, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [Engenharia de Segurança de Sistemas - Considerações para uma Abordagem Multidisciplinar na Engenharia de Sistemas Seguros e Confiáveis] [14], aborda as ações orientadas à engenharia necessárias para desenvolver sistemas mais defensáveis e permanentes — incluindo os componentes que formam esses sistemas e os serviços que dependem deles. O argumento inicial da publicação se baseia em um conjunto de normas internacionais bem estabelecidos para sistemas e engenharia de software, e infunde nesses sistemas as técnicas, métodos e práticas de engenharia de segurança de sistemas, bem como atividades de engenharia de software. O objetivo final é abordar questões de segurança, fundamentadas em uma perspectiva de necessidades de proteção e requisitos das

partes interessadas, e usar processos de engenharia estabelecidos para garantir que tais requisitos e necessidades sejam atendidos com a fidelidade e o rigor apropriados em todo o ciclo de vida do sistema. Aumentar a confiabilidade dos sistemas é um compromisso significativo que requer um investimento substancial em requisitos, arquitetura, design e desenvolvimento de sistemas, componentes, aplicativos e redes — além de uma mudança cultural profunda na abordagem atual de fazer "negócios como de costume".

A introdução de um conjunto disciplinado, estruturado e com base em normas de atividades e tarefas de engenharia de segurança de sistemas oferece um importante ponto de partida, o que conduz a um processo necessário de mudança. O objetivo final é obter sistemas seguros e confiáveis, que estejam totalmente habilitados a oferecer suporte a missões críticas e operações de negócios, protegendo os ativos das partes interessadas, desempenhando tais funções com um nível segurança que seja consistente com a tolerância ao risco das partes interessadas.

Os componentes de mapeamento do NICE Framework para a disciplina de especialidade descrita no NIST SP 800-160 validarão esses componentes. Os profissionais da disciplina de especialidade referente à engenharia de segurança de sistemas provavelmente se tornarão especialistas no assunto, o que poderá justificar a inclusão de KSAs e tarefas, que poderão ser acrescentadas ao NICE Framework.

### **D.3 Códigos Federais de Cibersegurança do Escritório de Gestão de Pessoal dos EUA**

Em 4 de janeiro de 2017, o Escritório de Gestão de Pessoal dos EUA (OPM) emitiu um memorando [15] intitulado “Guidance for federal agencies assigning new cybersecurity codes to positions with information technology, cybersecurity, and cyber-related functions” [“Orientação para agências federais atribuindo novos códigos de cibersegurança para cargos em tecnologia da informação, cibersegurança e funções relacionadas à cibernética”]. O memorando observa que a Lei Federal de Avaliação da Força de Trabalho em Cibersegurança de 2015 [16] exige que o OPM estabeleça procedimentos para implementar a estrutura de codificação NICE e identificar todas os cargos civis federais que requerem o desempenho de tecnologia da informação, segurança cibernética ou outras funções relacionadas à cibersegurança. A Tabela 9 mostra o mapeamento dos IDs de Função de Trabalho do NICE Framework que representam a natureza interdisciplinar do trabalho em cibersegurança para códigos de cibersegurança do OPM compatíveis com o sistema OPM Enterprise Human Resources Integration.

**Tabela 9 – Descrição Comparativa dos Ids das Funções de Trabalho Correlacionados aos Códigos de Cibersegurança do OPM**

ID da função de trabalho	Código OPM	ID da função de trabalho	Código OPM	ID da função de trabalho	Código OPM
SP-RSK-001	611	OV-LGA-001	731	AN-TWA-001	141
SP-RSK-002	612	OV-LGA-002	732	AN-EXP-001	121
SP-DEV-001	621	OV-TEA-001	711	AN-ASA-001	111
SP-DEV-002	622	OV-TEA-002	712	AN-ASA-002	112
SP-ARC-001	651	OV-MGT-001	722	AN-TGT-001	131
SP-ARC-002	652	OV-MGT-002	723	AN-TGT-002	132
SP-TRD-001	661	OV-SPP-001	751	AN-LNG-001	151
SP-SRP-001	641	OV-SPP-002	752	CO-CLO-001	311
SP-TST-001	671	OV-EXL-001	901	CO-CLO-002	312
SP-SYS-001	631	OV-PMA-001	801	CO-OPL-001	331
SP-SYS-002	632	OV-PMA-002	802	CO-OPL-002	332
OM-DTA-001	421	OV-PMA-003	803	CO-OPL-003	333
OM-DTA-002	422	OV-PMA-004	804	CO-OPS-001	321
OM-KMG-001	431	OV-PMA-005	805	IN-INV-001	221
OM-STS-001	411	PR-CDA-001	511	IN-FOR-001	211
OM-NET-001	441	PR-INF-001	521	IN-FOR-002	212
OM-ADM-001	451	PR-CIR-001	531		
OM-ANA-001	461	PR-VAM-001	541		

## Appendix E – Siglas

As siglas e abreviações selecionadas utilizadas neste artigo são definidas abaixo:

API	Application programming interface (Interface de programação de aplicativos)
CDM	Continuous Diagnostics and Mitigation (Diagnóstico e Mitigação Contínua)
CDS	Cross-Domain Solutions (Soluções de domínio cruzado)
CIO	Chief Information Officer (Diretor de TI)
CKMS	Crypto Key Management System (Sistema de gerenciamento de chaves criptográficas)
CMMI	Capability Maturity Model Integration (Integração do modelo de maturidade de capacidade)
CMS	Content Management System (Sistema de gerenciamento de conteúdo)
CNSSI	Committee on National Security Systems Instruction (Comitê de Instrução sobre Sistemas de Segurança Nacional)
COMSEC	Communications Security (Segurança das Comunicações)
COTR	Contracting Officer's Technical Representative (Representante Técnico do Oficial Contratante)
DNS	Domain Name System (Sistema de nomes de domínio)
EISA	Enterprise Information Security Architecture (Arquitetura de Segurança da Informação Empresarial)
FISMA	Federal Information Security Modernization Act (Lei Federal de Modernização da Segurança da Informação)
FOIA	Freedom of Information Act (Lei de Liberdade de Informação)
RH	Human Resource (Recursos Humanos)
IDS	Intrusion detection system (Sistema de detecção de invasões)
IP	Internet Protocol (Protocolo da Internet)
IPS	Intrusion Prevention System (Sistema de Prevenção de invasões)
IR	Incident Response (Resposta a Incidentes)
IRT	Incident Response Teams (Equipes de) Resposta a Incidentes
ISD	Instructional System Design (Design de sistemas instrucionais)
ITL	Information Technology Laboratory (Laboratório de Tecnologia da Informação)
KSA	Knowledge, Skills, and Abilities (Conhecimentos, Habilidades e Aptidões (KSAs))
LAN	Local area network (Rede local)
NICE	National Initiative for Cybersecurity Education (Iniciativa Nacional para Educação em Segurança Cibernética)
OLA	Operating-Level Agreement (Acordo de nível operacional)
OMB	Office of Management and Budget (Escritório de Gestão e Orçamento)
OPM	Office of Personnel Management (Escritório de Gestão de Pessoal)
OS	Operating system (Sistema Operacional)
OSI	Open System Interconnection (Interconexão de sistemas abertos)
P.L.	Public Law (Direito Público)
PCI	Payment Card Industry (Indústria de cartões de pagamento)
PHI	Personal Health Information (Informações pessoais sobre saúde)
PIA	Privacy Impact Assessments (Avaliações de impacto de privacidade)
PII	Personally Identifiable Information (Informações Pessoalmente Identificáveis)

PKI	Public key infrastructure (Criptografia de chave pública)
P&D	Research and Design (Pesquisa e Design)
RFID	Radio Frequency Identification (Identificação de Radiofrequência)
RMF	Risk Management Framework (Estrutura de gestão de risco)
SA&A	Security Assessment and Authorization (Avaliação e Autorização de Segurança)
SDLC	System development life cycle (Ciclo de vida de desenvolvimento de sistemas)
SLA	Service-Level Agreements (Contratos de nível de serviço)
SOP	Standard operating procedures (Procedimentos operacionais padrão)
SQL	Structured query language (Linguagem de consulta estruturada)
TCP	Transmission Control Protocol (Protocolo de Controle de Transmissão)
TTP	Tactics, techniques, and procedures (Táticas, técnicas e procedimentos)
URL	Uniform Resource Locator (Localizador de recursos uniformes)
VPN	Virtual Private Network (Rede Privada Virtual)
WAN	Wide Area Network (Rede de área ampla)

**Appendix F – Referências**

- [1] Página da Web de Revisão do NICE Framework, Instituto Nacional de Normas e Tecnologia [Website], <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-revisions>
- [2] Iniciativa Nacional para Educação em Segurança Cibernética, *Estrutura Nacional da Força de Trabalho em Cibersegurança, ver. 1,0*, <https://www.nist.gov/file/359276>
- [3] Iniciativa Nacional para Educação em Segurança Cibernética, *Estrutura Nacional da Força de Trabalho em Cibersegurança, ver. 2,0*, <https://www.nist.gov/file/359261>
- [4] Planilha de Referência para Publicação Especial NIST 800-181 <https://www.nist.gov/file/372581>
- [5] NICE Framework, Instituto Nacional de Normas e Tecnologia [Website], <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>
- [6] Departamento de Trabalho, Emprego e Administração de Treinamento dos EUA (ETA) [Website]. <https://www.doleta.gov>
- [7] Central de Informações sobre Modelos de Competência, Modelo de Competência de Cibersegurança, <https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx>
- [8] Departamento de Segurança Interna dos EUA, Kit de ferramentas de desenvolvimento da força de trabalho em cibersegurança (CWDT), <https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit>
- [9] Programa de Excelência em Cibersegurança de Baldrige, Instituto Nacional de Normas e Tecnologia [Site], <https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative>
- [10] Departamento de Segurança Interna dos EUA, Departamento de Segurança Interna dos EUA, site da ferramenta CMSI PushButtonPD™, <https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool>
- [11] *Estrutura para Melhorar a Segurança Cibernética da Infraestrutura Crítica Versão 1.0*, Instituto Nacional de Normas e Tecnologia, 12 de fevereiro de 2014, <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- [12] Ordem Executiva nº 13636, *Melhoria da Segurança Cibernética da Infraestrutura Crítica*, DCPD-201300091, 12 de fevereiro de 2013. <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>
- [13] *NIST - Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica*, Instituto Nacional de Normas e Tecnologia, 12 de fevereiro de 2014, <https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf>

- [14] Publicação Especial do NIST (SP) 800-160, *Engenharia de Segurança de Sistemas - Considerações para uma Abordagem Multidisciplinar na Engenharia de Sistemas Seguros e Confiáveis*, Instituto Nacional de Normas e Tecnologia, novembro de 2016, <https://doi.org/10.6028/NIST.SP.800-160>
- [15] Memorando sobre orientação para atribuir novos códigos de cibersegurança a cargos em tecnologia da informação, cibersegurança e funções relacionadas à cibersegurança, janeiro de 2017, <https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity>
- [16] H.R.2029 - Lei de Apropriações Consolidadas, de 2016 que contém a Divisão N- Lei de Cibersegurança de 2015, <https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf>