Cadernos de

Prospectiva Industrial de Defesa

Segmento DEFESA CIBERNÉTICA

FIA BUSINESS SCHOOL
CNI Confederação Nacional da Indústria
ABDI Agência Brasileira de Desenvolvimento Industrial
MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS

Ficha Técnica

Presidência da Republica
LUIZ INÁCIO LULA DA SILVA - ***Presidente da República Federativa do Brasil***

Ministério de Desenvolvimento, Indústria, Comércio e Serviços (MDIC)
MÁRCIO FERNANDO ELIAS ROSA - ***Ministro do Desenvolvimento, Indústria, Comércio e Serviços***

Agência Brasileira de Desenvolvimento Industrial (ABDI):
OLAVO NOLETO ALVES - ***Presidente***
RANDAL FARAH DE OLIVEIRA LEÃO - ***Diretor***
NEIDE APARECIDA DE SOUSA FREITAS - ***Diretora***
KAREN LEAL - ***Líder do Projeto Complexo Industrial da Defesa e Segurança Pública***

Confederação Nacional da Indústria (CNI):
ANTONIO RICARDO ALVAREZ ALBAN - ***Presidente***
MÁRIO SÉRGIO CARRARO TELLES – ***Diretor de Desenvolvimento Industrial***
MÁRCIO GUERRA AMORIM – ***Superintendente de Inteligência Econômica***
RAFAEL SILVA E SOUSA – ***Gerente do Observatório Nacional***
MARCELLO JOSÉ PIO – ***Especialista em Políticas e Indústria***
JULIANO ANTÔNIO SEBBEN – ***Especialista em Políticas e Indústria***

Fundação Instituto Administração da Universidade de São Paulo (FIA/USP):
Prof. Dr. NELSON BARRIZZELLI - ***Coordenador Geral***
Prof. Dr. LINO RODRIGUES - ***Coordenador***
General Div. R1 IVAN FERREIRA NEIVA FILHO - ***Coordenador***
Profa. Dra. SHEILA SERAFIM DA SILVA - ***Consultora***
Coronel R1 ALEXANDRE MAGNO FERNANDES RIBEIRO - ***Consultor***

Especialistas colaboradores:
Conteúdo desenvolvido com a colaboração de representantes da indústria, do governo e da academia.

Revisão e editoração:
Equipe da Unidade de Comunicação e Marketing (UCM) da ABDI

Prefácio

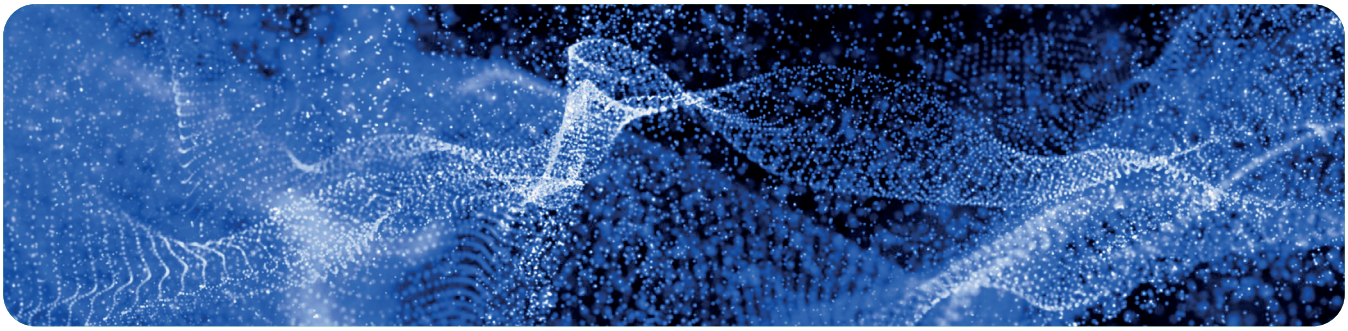
O Projeto de Avaliação e Monitoramento da Base Industrial de Defesa (BID), conduzido pela Agência Brasileira de Desenvolvimento Industrial (ABDI), constitui um esforço estruturado de produção de conhecimento estratégico sobre a capacidade produtiva, tecnológica e organizacional da indústria de defesa brasileira. Seu objetivo é ampliar a compreensão sobre os segmentos que compõem a BID, suas interdependências, desafios e potencialidades, contribuindo para a formulação de políticas públicas e estratégias de fortalecimento da soberania nacional.

A Base Industrial de Defesa brasileira caracteriza-se por sua diversidade e complexidade produtiva, reunindo desde segmentos tradicionais, como têxteis técnicos, até setores de alta intensidade tecnológica, como sistemas aeroespaciais, cibernéticos, mísseis, plataformas terrestres, navais e aéreas, sensores, comunicações e sistemas autônomos. Essa heterogeneidade exige análises segmentadas, capazes de preservar as especificidades de cada área sem perder de vista sua integração sistêmica.

É nesse contexto que se insere esta coleção de cadernos de prospectiva industrial, resultado de uma iniciativa da ABDI em parceria com o Observatório Nacional da Indústria da Confederação Nacional da Indústria (CNI) e a Fundação Instituto de Administração (FIA/USP), com base em metodologia estruturada de análise prospectiva desenvolvida pelo Serviço Nacional de Aprendizagem Industrial (SENAI). Aplicado a oito segmentos estratégicos da BID, o trabalho identifica tecnologias emergentes, eventos futuros de impacto e transformações nos perfis ocupacionais e competências requeridas, permitindo antecipar tendências e apoiar decisões estratégicas de longo prazo.

Mais do que uma análise setorial, esta iniciativa busca fortalecer capacidades nacionais em setores críticos, reduzir vulnerabilidades externas e ampliar a competitividade da indústria nacional. Em um cenário internacional marcado por aceleração tecnológica, reconfiguração das cadeias globais de suprimento e tensões geopolíticas crescentes, a capacidade de antecipação torna-se elemento central para a resiliência industrial e a autonomia estratégica do país.

Os cadernos destinam-se a formuladores de políticas públicas, gestores industriais, instituições de ensino e pesquisa e demais atores comprometidos com o fortalecimento da Base Industrial de Defesa, servindo como instrumento de apoio à tomada de decisão e à construção de estratégias de desenvolvimento produtivo, inovação e soberania tecnológica.



1. Introdução

O segmento de Defesa e Proteção Cibernética ocupa, atualmente, uma posição estratégica central na Base Industrial de Defesa (BID) brasileira, ao sustentar a segurança, a resiliência e a soberania dos sistemas digitais que apoiam as capacidades militares, governamentais e de comando e controle do Estado. Diferentemente de outros segmentos tradicionais da defesa, a ciberdefesa caracteriza-se pela elevada velocidade de transformação tecnológica, forte dependência de ativos intangíveis, alta densidade cognitiva da força de trabalho e por operar em um ambiente marcado por assimetrias geopolíticas, disputas por soberania digital e crescente judicialização e regulação internacional.

A intensificação das rivalidades geopolíticas, o endurecimento de regimes de controle de exportação, a fragmentação das cadeias globais de tecnologia, a ampliação das ameaças híbridas e o aumento da frequência e sofisticação de ataques cibernéticos têm elevado a ciberdefesa ao *status* de capacidade crítica e permanente. Nesse contexto, tecnologias como plataformas de defesa cibernética baseadas em inteligência artificial, arquiteturas Zero Trust, criptografia pós-quântica, sistemas de resposta automatizada, gêmeos digitais e inteligência para identificação de ameaças cognitivas passam a redefinir não apenas os sistemas e produtos desenvolvidos pelas empresas do segmento, mas também a organização do trabalho, os processos decisórios e os perfis profissionais demandados.

Essas transformações ocorrem em um ambiente de mercado tipicamente monopsônico ou oligopolizado, fortemente institucionalizado, no qual o Estado atua simultaneamente como regulador, indutor tecnológico e principal cliente. Tal característica impõe ciclos longos de desenvolvimento, elevados requisitos de conformidade, certificação e rastreabilidade, além de baixa elasticidade entre crescimento produtivo e emprego total. Em contrapartida, observa-se um aumento contínuo da densidade técnica, regulatória e cognitiva da força de trabalho, com maior valorização de perfis híbridos que combinam competências técnicas avançadas, capacidades cognitivas críticas e compreensão institucional e normativa.

Diante desse cenário, os desafios relacionados à formação, atualização e retenção da mão de obra tornam-se um dos principais fatores críticos de sucesso do segmento de Defesa Cibernética. A escassez estrutural de talentos, a competição global por profissionais qualificados, a rapidez da evolução tecnológica e a crescente exigência por conformidade regulatória e governança ampliam o risco de gargalos de competências que podem comprometer tanto a competitividade das empresas quanto a autonomia estratégica nacional.

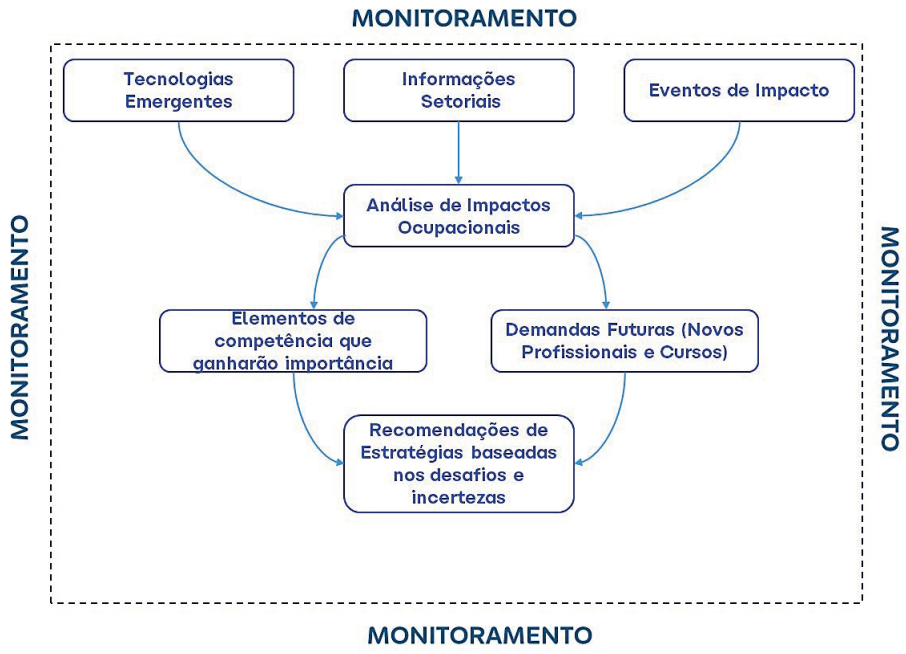
É nesse contexto que os estudos prospectivos sobre o futuro da mão de obra no segmento de Defesa e Proteção Cibernética assumem papel fundamental. Ao antecipar tecnologias emergentes, eventos não tecnológicos de alto impacto, transformações organizacionais e novas demandas de competências, os estudos de prospectiva permitem orientar decisões estratégicas de médio e longo prazo, apoiar o planejamento empresarial e estatal, reduzir assimetrias formativas e alinhar a oferta educacional às

necessidades futuras do setor.

Mais do que um exercício analítico, os estudos prospectivos aplicados à força de trabalho constituem um instrumento estruturante para a formulação e o aprimoramento de políticas públicas de formação profissional voltadas à Base Industrial de Defesa. Ao articular empresas, governo, instituições de formação profissional e institutos de ciência e tecnologia, tais estudos contribuem para a construção de capacidades nacionais sustentáveis, para o fortalecimento da soberania digital e para a consolidação de uma trajetória de desenvolvimento industrial alinhada aos desafios tecnológicos, geopolíticos e institucionais do século XXI.

Este estudo é fruto da aplicação do Modelo de Prospectiva Industrial, desenvolvido e aplicado pelo Observatório Nacional da Indústria da CNI e está baseado em pesquisas teóricas em fontes secundárias e consulta a especialistas. O estudo objetiva discutir, sugerir e priorizar ações **estratégicas, cursos e oferta de novos profissionais**, visando contribuir para o aumento da competitividade dos segmentos por meio da melhoria da oferta de mão de obra especializada. Para tal, foram consideradas as dimensões: *tecnológica, eventos futuros de impacto, evolução dos perfis profissionais, incertezas críticas (que afetam diretamente a formação de mão de obra) e desafios e incertezas*. De forma esquemática (figura 1), a aplicação do Modelo de Prospectiva seguiu o seguinte raciocínio de análise.

Figura 1 - Esquema Geral do Modelo de Prospectiva Industrial utilizado para este estudo



Fonte: Observatório Nacional da Indústria (2025)

2. Contextos Futuros

2.1) Possível impacto das tecnologias emergentes[1] no mercado de trabalho

Para fins deste estudo, considera-se como tecnologias emergentes aquelas que estão em constante evolução e que ainda não estão totalmente disseminadas (aquisição e uso) na sociedade, mas possuem o potencial de transformar profundamente diversos setores ou segmentos econômicos, incluindo o impacto na mão de obra do setor ou segmento e criação de demanda por novos profissionais. A seguir são apresentadas as tecnologias emergentes para o segmento de *defesa cibernética*, juntamente com o possível impacto[2], geral, no mercado de trabalho, utilizando a seguinte escala de impacto.

- **Impacto Alto -** Quando a tecnologia reestrutura de forma sistêmica o segmento, redefine perfis profissionais, cria ocupações e exige novas capacidades tecnológicas, organizacionais e formativas.
- **Impacto Médio–Alto –** Quando a tecnologia altera múltiplos processos, intensifica a complexidade do trabalho e promove hibridização de funções técnicas e analíticas.
- **Impacto Médio -** Quando a tecnologia provoca reconfiguração parcial de processos e demanda atualização significativa de competências existentes.
- **Impacto Baixo** - Quando a tecnologia gera apenas ajustes marginais nas tarefas e exige requalificação limitada.

Plataformas de Defesa Cibernética com IA Autônoma (*AI-driven Cyber Defense Platforms*) - Plataformas que utilizam IA avançada (ML, deep learning e modelos adaptativos) para exploração, inteligência de ameaças, detecção, correlação e resposta automática a ataques complexos em ambientes de Defesa e de infraestruturas críticas, reduzindo tempo de reação e dependência de operadores humanos.

- **Nível de impacto no segmento:** Alto
- **Principais profissionais afetados:** Engenheiros de redes, software, IA e dados; Analistas de ciberdefesa; Arquitetos de sistemas; Operadores de SOC militar, Matemáticos e Estatísticos.
- **Como o trabalho muda:** Atividades exploratórias, reativas e manuais de análise de incidentes são substituídas por supervisão de sistemas autônomos, criação e validação de modelos e ajuste de regras algorítmicas. Aumenta a complexidade cognitiva e a necessidade de competências em IA explicável e sistemas críticos.

1 Para fins deste estudo o conceito de difusão tecnológica foi redefinido, como ***o grau em que uma tecnologia se torna institucionalizada como aptidão recorrente, requisito padrão ou prática dominante em um sistema produtivo***, independentemente do número de compradores existentes. A unidade central de análise deixa de ser o ***mercado*** (com muitos fornecedores e consumidores) e passa a ser o ***sistema sociotécnico***. Com isso, as estimativas de difusão seguiram um modelo específico para mercados ***monopsônicos e oligopolizados***.

2 Os impactos das tecnologias emergentes sobre o mercado de trabalho foram estabelecidos a partir de um conjunto integrado de critérios qualitativos e estruturais. Os critérios foram os seguintes: centralidade da tecnologia no sistema produtivo do segmento, número e a natureza dos processos impactados, grau de transformação do trabalho, complexidade técnica e organizacional associada à adoção e o potencial de encadeamento produtivo e institucional.

***Cyber Ranges* Avançados com Simulação de Guerra Cibernética (*AI-enabled Cyber Ranges*) -** Ambientes de simulação hiper-realistas que reproduzem cenários de guerra cibernética, integrando redes, sistemas de armas, infraestruturas críticas e adversários simulados por IA.

- **Nível de impacto no segmento:** Médio–Alto.
- **Principais profissionais afetados:** Instrutores de defesa cibernética; Engenheiros de simulação e game; Analistas de ameaças e segurança ofensiva; Oficiais de planejamento.
- **Como o trabalho muda:** O treinamento deixa de ser baseado em cenários estáticos e passa a envolver simulações dinâmicas e adaptativas. Cresce a demanda por desenho de cenários, modelagem de ameaças e avaliação de desempenho operacional.

Sistemas de Resposta Cibernética Orquestrada e Automatizada (SOAR Militar) - Soluções que integram sensores, inteligência de ameaças e *playbooks* automatizados para resposta coordenada a incidentes cibernéticos em ambientes militares e estratégicos.

- **Nível de impacto no segmento:** Alto
- **Principais profissionais afetados:** Analistas de SOC; Engenheiros de integração, de rede e de IA; Gestores de operações cibernéticas.
- **Como o trabalho muda:** Processos manuais de resposta são substituídos por orquestração automática. O foco do trabalho migra para desenho, validação e governança de fluxos automatizados.

Tecnologias de Zero Trust para Ambientes de Defesa (*Zero Trust Defense Architectures*) - Arquiteturas de segurança que eliminam a confiança implícita em redes internas, exigindo autenticação e autorização contínuas em sistemas críticos de Defesa.

- **Nível de impacto no segmento:** Alto
- **Principais profissionais afetados:** Arquitetos de segurança; Engenheiros de redes, de dados e de IA; Gestores de identidade e acesso, Analistas de inteligência cibernética.
- **Como o trabalho muda:** A administração tradicional de redes é reconfigurada para modelos contínuos de verificação. Exige novas competências em arquitetura de confiança, políticas dinâmicas e integração com sistemas legados.

Criptografia Pós-Quântica para Sistemas de Defesa (*Post-Quantum Cryptography* – PQC) - Algoritmos criptográficos resistentes a ataques de computadores quânticos, aplicáveis a comunicações militares, comando e controle e proteção de dados sensíveis.

- **Nível de impacto no segmento:** Alto
- **Principais profissionais afetados:** Criptógrafos e criptólogos; Engenheiros de software seguro, de redes e de protocolos criptográficos; Especialistas em comunicações militares, matemáticos.
- **Como o trabalho muda:** Os protocolos criptográficos tradicionais passam a ser substituídos. Cresce a demanda por competências matemáticas avançadas, validação formal e certificação de algoritmos.

***Digital Twins* de Infraestruturas Cibernéticas Críticas de Defesa -** Gêmeos digitais que replicam, em tempo quase real, redes e sistemas cibernéticos críticos para análise de vulnerabilidades, testes de resiliência e planejamento de resposta.

- **Nível de impacto no segmento:** Médio
- **Principais profissionais afetados:** Engenheiros de produção, de automação, de sistemas e de IA; Analistas de risco; Especialistas em modelagem e simulação.
- **Como o trabalho muda:** A análise preventiva substitui abordagens reativas. O trabalho passa a envolver modelagem sistêmica, análise preditiva e simulação de falhas complexas.

Sistemas de Inteligência de Ameaças com Análise Cognitiva (*Cognitive Threat Intelligence*) - Plataformas que utilizam IA para correlacionar grandes volumes de dados, identificar padrões emergentes de ataque e antecipar comportamentos adversários no espaço cibernético.

- **Nível de impacto no segmento:** Médio-Alto.
- **Principais profissionais afetados:** Analistas de inteligência cibernética e de risco; Cientistas de dados; Oficiais de inteligência.
- **Como o trabalho muda:** A análise baseada em regras fixas é substituída por análise cognitiva e probabilística. Exige competências em interpretação de modelos e análise estratégica.

Tecnologias de Segurança para Sistemas Ciberfísicos Militares (*Cyber-Physical Security*) - Soluções específicas para proteger a integração entre sistemas digitais e físicos (armas, sensores, plataformas e logística), evitando ataques com efeitos cinéticos.

- **Nível de impacto no segmento:** Alto
- **Principais profissionais afetados:** Engenheiros de sistemas embarcados, de produção, de automação, de redes, de dados; Especialistas (técnicos) em automação; Técnicos de manutenção avançada.
- **Como o trabalho muda:** A segurança deixa de ser apenas digital e passa a integrar engenharia física e lógica. O trabalho torna-se híbrido, exigindo visão sistêmica e multidisciplinar.

Tecnologias de Engano Cibernético Militar (*Cyber Deception & Active Defense*) - Ferramentas que criam ambientes falsos (*honeypots* e *honeynets* avançados) para enganar adversários, coletar inteligência e retardar ataques.

- **Nível de impacto no segmento:** Médio
- **Principais profissionais afetados:** Analistas de defesa ativa; Engenheiros de redes; Especialistas em inteligência.
- **Como o trabalho muda:** A postura defensiva passiva é complementada por estratégias ativas. Cresce a demanda por planejamento tático e análise comportamental de atacantes.

Plataformas de Gestão de Identidades Soberanas (*Sovereign Identity Management*) - Soluções de identidade digital soberana para controle rigoroso de acessos em ambientes de Defesa, integrando identidades humanas, de máquinas e de sistemas autônomos.

- **Nível de impacto no segmento:** Médio–Alto.
- **Principais profissionais afetados:** Especialistas em IAM; Arquitetos de segurança; Gestores de compliance, criptógrafos e criptólogos.
- **Como o trabalho muda:** Processos tradicionais de controle de acesso são reconfigurados para modelos soberanos e distribuídos, exigindo novas competências em governança digital.

Ferramentas de Verificação Formal e Segurança ("safety" and "security") de Software Crítico - Tecnologias que utilizam métodos formais e automação para garantir a integridade, confiabilidade, ausência e gestão de vulnerabilidades em software crítico de Defesa.

- **Nível de impacto no segmento:** Médio
- **Principais profissionais afetados:** Engenheiros de software; Especialistas em qualidade e certificação; Testadores avançados, Matemáticos.
- **Como o trabalho muda:** Testes empíricos são complementados por verificação matemática. O trabalho ganha maior rigor técnico e exigência de formação especializada.

Plataformas Seguras de Compartilhamento de Dados Interforças (*Secure Defense Data Sharing Platforms*) - Soluções que permitem o compartilhamento seguro e controlado de dados entre Forças Armadas e órgãos estratégicos, mantendo soberania, rastreabilidade e resiliência.

- **Nível de impacto no segmento:** Médio–Alto
- **Principais profissionais afetados:** Arquitetos de dados; Especialistas em segurança da informação; Gestores de interoperabilidade, criptógrafo, criptólogos, Engenheiros de redes e de dados.
- **Como o trabalho muda:** A gestão isolada de dados dá lugar a modelos colaborativos e interoperáveis, exigindo novas competências em governança, segurança e integração.

Síntese

No conjunto, essas tecnologias reconfiguram consideravelmente as capacidades tecnológicas do segmento (automação, inteligência e resiliência), os processos críticos (detecção, resposta, treinamento, integração), e o trabalho, com aumento da complexidade cognitiva, hibridização de funções e surgimento de novos perfis profissionais especializados — exatamente como previsto no método aplicado.



2.2) Estimativa de Difusão e uso das Tecnologias Emergentes[3]

Escala de Difusão Sistêmica e Programática

- **Nível 1 – Difusão Exploratória:** pilotos, P&D, uso pontual.
- **Nível 2 – Difusão Programática Pontual:** aplicada em um programa/classe/ativo específico.
- **Nível 3 – Difusão Programática Repetida:** presente em múltiplos programas/classes, com institucionalização parcial.
- **Nível 4 – Difusão Sistêmica (Padrão):** requisito padrão, institucionalizado e recorrente.

Plataformas de Defesa Cibernética com IA Autônoma (*AI-driven Cyber Defense Platforms*)

- Estimativa de difusão em 5 anos: **Nível 1**
- Estimativa de difusão em 10 anos: **Nível 2**

Justificativa: Alta relevância para funções críticas, mas o processo de padronização/normalização e atuação de um maior número de fornecedores nacionais qualificados, afetam a difusão. Provável adoção repetida em múltiplos ambientes (SOC/CSIRT) antes de virar requisito padrão.

Cyber Ranges Avançados com Simulação de Guerra Cibernética (AI-enabled Cyber Ranges)

- Estimativa de difusão em 5 anos: **Nível 2**
- Estimativa de difusão em 10 anos: **Nível 3**

Justificativa: A incorporação programática progride por "saltos" (instalação e expansão em centros e escolas), enquanto a institucionalização organizacional cresce por de ciclos de treinamento; processos de padronização e normalização moderados e relevância para funções críticas em nível médio-alto, favorecendo a Difusão Programática Repetida.

3 A trajetória de difusão de cada tecnologia, foi estimada considerando cinco dimensões: **D1** incorporação programática (pilotos -> programa -> múltiplos programas -> requisito padrão); **D2** institucionalização organizacional (dependência de indivíduos -> processos -> integração corporativa -> governança); **D3** aptidão produtiva instalada (nº de fornecedores qualificados e continuidade); **D4** padronização/normalização (normas, requisitos, certificações e cláusulas contratuais); **D5** relevância para funções críticas (centralidade operacional e dependência sistêmica).

Convenção metodológica: como são "tecnologias emergentes específicas", o ponto de partida (2026) é **Nível 1–2**. As estimativas abaixo indicam em que nível provavelmente estarão em 5 anos e 10 anos, como proxy de institucionalização (não "market share").

A passagem para **Nível 3** exige, tipicamente, evidência de **D1** em múltiplos programas + **D2** parcial + **D3** com mais de um fornecedor; para **Nível 4**, além disso, **D4 e D5** tornam-se dominantes (requisito padrão e criticidade transversal).

Sistemas de Resposta Cibernética Orquestrada e Automatizada (SOAR Militar)

- Estimativa de difusão em 5 anos: **Nível 2**
- Estimativa de difusão em 10 anos: **Nível 3**

Justificativa: Devido a elevada relevância para funções críticas (tempo de resposta), espera-se institucionalização organizacional média , com a incorporação programática tendendo a se replicar (múltiplos SOC/órgãos). Em 10 anos, é possível tornar-se requisito relativamente disseminado para funções críticas.

Tecnologias de *Zero Trust* para Ambientes de Defesa (Zero Trust Defense Architectures)

- Estimativa de difusão em 5 anos: **Nível 3**
- Estimativa de difusão em 10 anos: **Nível 4**

Justificativa: A tecnologia Zero Trust costuma virar "arquitetura de referência", com grande impacto na governança e processos de acesso. A difusão em 5 anos ocorre em múltiplos programas e sistemas. Em 10 anos, tende a se consolidar como padrão transversal.

Criptografia Pós-Quântica para Sistemas de Defesa (Post-Quantum Cryptography – PQC)

- Estimativa de difusão em 5 anos: **Nível 2**
- Estimativa de difusão em 10 anos: **Nível 3 ou 4**

Justificativa: A rápida difusão tecnológica é justificada pela obrigatoriedade para órgãos do governo brasileiro até 2035, de acordo com a Orientação de Segurança da Informação e Cibernética (15/2024).

Digital Twins de Infraestruturas Cibernéticas Críticas de Defesa

- Estimativa de difusão em 5 anos: **Nível 2**
- Estimativa de difusão em 10 anos: **Nível 3**

Justificativa: A incorporação programática tende a começar por ambientes e ativos prioritários (pontual). A repetição (Nível 3) exige institucionalização organizacional (processos permanentes de simulação e validação) e capacidade produtiva instalada (capacidade de modelagem e atualização contínua) consolidadas em mais de um ator.

Sistemas de Inteligência de Ameaças com Análise Cognitiva (*Cognitive Threat Intelligence*)

- Estimativa de difusão em 5 anos: **Nível 2**
- Estimativa de difusão em 10 anos: **Nível 3**

Justificativa: Alta relevância para funções críticas para defesa ativa e antecipação, porém há dependência de dados, integração e governança. Em 10 anos, tende a estar presente em múltiplas

estruturas, mas nem sempre como requisito padrão único (muita heterogeneidade).

Tecnologias de Segurança para Sistemas Ciberfísicos Militares (*Cyber-Physical Security*)

- Estimativa de difusão em 5 anos: **Nível 2**
- Estimativa de difusão em 10 anos: **Nível 3**

Justificativa: Alta relevância para funções críticas (efeitos cinéticos e continuidade), mas a adoção costuma ser "por plataforma/sistema" (incorporação programática pontual), dependendo da capacidade de engenharia e integração. Em 10 anos, é plausível a repetição em múltiplos programas, com institucionalização parcial.

Tecnologias de Engano Cibernético Militar (*Cyber Deception & Active Defense*)

- Estimativa de difusão em 5 anos: **Nível 1**
- Estimativa de difusão em 10 anos: **Nível 2**

Justificativa: É altamente útil no "aprendizado" sobre o *modus operante* do inimigo, mas no segmento tende a ficar restrita a unidades e ambientes específicos e pode enfrentar limites de governança e regras de engajamento. Assim, estima-se que a difusão deverá ser mais lenta e "cirúrgica". Além disso, para seu emprego para a área de Defesa teria que ser consultado o CDCiber. No mercado civil estima-se que estas tecnologias tenham uma difusão mais rápida (5 anos = nível 3 e 10 anos = nível 4).

Plataformas de Gestão de Identidades Soberanas (Sovereign Identity Management)

- Estimativa de difusão em 5 anos: **Nível 3**
- Estimativa de difusão em 10 anos: **Nível 4**

Justificativa: Relevante para funções críticas muito alta (controle de acesso e confiança), com forte institucionalização organizacional (processo transversal) e padronização (políticas e requisitos). Em 10 anos, é justificável a possibilidade de padrão sistêmico, por ser base para a tecnologia Zero Trust e interoperabilidade segura.

Ferramentas de Verificação Formal e Segurança de *Software* Crítico

- Estimativa de difusão em 5 anos: **Nível 2**
- Estimativa de difusão em 10 anos: **Nível 3**

Justificativa: Alta relevância para funções críticas (o *software* crítico é central para Defesa). A incorporação programática tende a ocorrer inicialmente em programas sensíveis ou sistemas críticos específicos, e os métodos formais avançam por normas e exigências contratuais, mas não se tornam universais rapidamente. Contudo, a capacidade produtiva seria limitada, devido à escassez de especialistas e alto custo. Em 10 anos, é defensável a repetição em múltiplos programas críticos, sem ainda alcançar status de requisito padrão transversal. Existe a tecnologia, mas falta mão de obra

para operação.

Plataformas Seguras de Compartilhamento de Dados Interforças (*Secure Defense Data Sharing Platforms*)

- Estimativa de difusão em 5 anos: **Nível 3**
- Estimativa de difusão em 10 anos: **Nível 4**

Justificativa: Tecnologia com altíssima relevância crítica, uma vez que a interoperabilidade e coordenação interforças são funções estruturantes, além de elevada institucionalização organizacional pela necessidade de governança, processos e acordos formais. Em 10 anos, é justificável que se torne infraestrutura padrão, base para operações conjuntas e integração com outras capacidades (IAM, Zero Trust, SOAR). Está correlacionada com a evolução da criptografia pós quântica.

2.3) Outras Eventos de Impacto[4]

Escala de impacto

- **Impacto Alto** - Quando os eventos afetam o núcleo estratégico do setor ou segmento, têm ampla abrangência, reconfiguram significativamente o trabalho e geram efeitos duradouros e sistêmicos.
- **Impacto Médio-Alto** – Quando os eventos provocam mudanças relevantes em estratégias, processos e perfis profissionais, com efeitos estruturais moderados.
- **Impacto Médio**, Quando os eventos influenciam práticas e processos específicos, com efeitos limitados ao setor.
- **Impacto Baixo** – Quando os efeitos dos eventos são localizados ou temporários, sem reconfiguração estrutural.

Intensificação de rivalidades geopolíticas e "soberania digital" (fragmentação de blocos) - Aumento de tensões geopolíticas e maior ênfase dos Estados em autonomia tecnológica, estímulo ao desenvolvimento de arquiteturas tecnologias próprias (nacionais/alternativas), cadeias *friend-shoring* e restrições a fornecedores e tecnologias sensíveis.

- **Nível de impacto:** Alto
- **Principais profissionais afetados:** Relações governamentais; Comércio exterior; Jurídico; Contratos; Arquitetos de segurança; Gestores de fornecedores e risco, logística (cadeia de suprimentos).
- **Como muda o trabalho:** Cresce a demanda por gestão de risco geopolítico, *due diligence* de fornecedores, desenho de arquiteturas "soberanas" e maior complexidade contratual (cláusulas de origem, auditorias, rastreabilidade e continuidade).

4 O nível de impacto desses eventos foi definido a partir de sua centralidade estratégica, abrangência, aptidão de reconfigurar o trabalho, dependência institucional, persistência temporal e efeitos em cascata sobre o sistema produtivo. Para garantir o rigor analítico e evitar vieses, **não** foram considerados na análise: *frequência recente em notícias; avaliações subjetivas de gravidade; impactos exclusivamente tecnológicos; impactos restritos a um único projeto isolado.*

Endurecimento de controles de importação ou exportação, sanções e requisitos de compliance internacional - Ampliação de regimes e medidas nacionais e internacionais que restringem exportação, cooperação e transferência de tecnologias e serviços cibernéticos sensíveis.

- **Nível de impacto:** Alto
- **Principais profissionais afetados:** Compliance; Jurídico; Qualidade; Logística; Gestão de projetos internacionais, especialista em comércio internacional, PMO.
- **Como muda o trabalho:** O compliance deixa de ser "pós-contrato" e vira operação contínua (documentação, auditorias, rastreio de componentes/softwares, licenciamento), com aumento de especialização e padronização interna.

Crescente exigência de "ciber como requisito" em compras públicas e contratos de Defesa - Elevação de exigências de segurança (incluindo requisitos de evidência, testes, auditorias, rastreabilidade, SLAs e governança) nas aquisições e programas estratégicos.

- **Nível de impacto:** Alto
- **Principais profissionais afetados:** Gestores de proposta e licitação; Engenharia de sistemas; GRC (Governança, Risco e Compliance); Testes e validação; PMO.
- **Como muda o trabalho:** Aumenta o trabalho da engenharia de conformidade, geração de evidências, documentação técnica, gestão de requisitos e validação independente; o ciclo de vida do contrato fica mais "auditável" e intensivo em processos.

Reconfiguração do orçamento público e ciclos fiscais (pressão por eficiência e priorização) - Oscilações do espaço fiscal e disputas orçamentárias podem acelerar ou restringir programas, mudando prioridades e cronogramas.

- **Nível de impacto:** Médio–Alto
- **Principais profissionais afetados:** Planejamento e finanças; Gestores de portfólio; Vendas governamentais; Gestores de contrato e operações.
- **Como muda o trabalho:** Cresce a demanda por modelos de custo total, modularização de entregas, contratos por desempenho e capacidade de operar com incerteza (replanejamento, renegociação e gestão de escopo).

Escassez estrutural de talentos em cibersegurança e competição global por mão de obra - Déficit de profissionais e aumento da disputa por especialistas (inclusive por trabalho remoto internacional), elevando rotatividade e custos.

- **Nível de impacto:** Alto
- **Principais profissionais afetados:** Recursos Humanos; Lideranças técnicas (SOC, engenharia, criptografia); Universidades e IFPs corporativas; Segurança interna.
- **Como muda o trabalho:** Forte reconfiguração organizacional com fortalecimento de academias internas, trilhas aceleradas, políticas de retenção, times híbridos e maior padronização de processos para reduzir dependência de "especialistas raros".

Aumento do escrutínio sobre privacidade, LGPD e governança de dados em ambientes sensíveis - Pressão institucional por conformidade, transparência e governança do ciclo de vida de dados (inclusive incidentes), elevando exigências formais.

- **Nível de impacto:** Médio–Alto
- **Principais profissionais afetados:** DPO; Jurídico; GRC; Arquitetos de dados; Analistas de incidentes e auditoria.
- **Como muda o trabalho:** Expansão de funções de governança de dados, classificação, retenção, resposta a incidentes com trilhas de auditoria e integração entre segurança e jurídico/compliance.

Crescente exigência de certificações, acreditações e auditorias (produto, processo e operação) - Fortalecimento de padrões e auditorias (qualidade, segurança, continuidade, cadeia de suprimentos), com efeito sobre acesso a contratos e confiança.

- **Nível de impacto:** Alto
- **Principais profissionais afetados:** Qualidade; Segurança da informação; Auditoria interna; Engenharia de processos; Gestão de fornecedores.
- **Como muda o trabalho:** Crescimento de rotinas de evidenciação, auditorias recorrentes, automação dos processos de compliance; aumento da demanda por perfis que combinem técnica, gestão e documentação.

Maior judicialização e responsabilização por incidentes (contratual e reputacional) - Maior rigor na atribuição de responsabilidade por falhas, indisponibilidade e vazamentos, elevando risco legal e exigência de governança contratual.

- **Nível de impacto:** Médio-Alto
- **Principais profissionais afetados:** Jurídico; Gestores de contrato; Governança, Risco e Compliance (GRC); DPO, Lideranças de operações (Centrode Operações de Segurança - SOC).
- **Como muda o trabalho:** Contratos passam a exigir SLAs mais duros, planos de continuidade e relatórios de incidentes; aumenta a importância de governança, registro de decisões e rotinas de pós-incidente (lições aprendidas).

Aceleração de parcerias internacionais (ou restrições a elas) em P&D e interoperabilidade - Mudanças na política externa e em alianças podem abrir (ou fechar) acesso a projetos conjuntos, padrões e mercados.

- **Nível de impacto:** Médio–Alto.
- **Principais profissionais afetados:** P&D; Gestão de parcerias; Normalização; Programas internacionais; Segurança e compliance.
- **Como muda o trabalho:** Cresce a demanda por gestão de processos de cooperação, interoperabilidade e padronização; simultaneamente, aumenta o trabalho de compliance e proteção de conhecimento sensível (segregação de informação).

Pressões por transparência, integridade e controle anticorrupção em compras e contratos - Fortalecimento de controles, auditorias e exigências de integridade em cadeias de suprimentos e contratações públicas.

- **Nível de impacto:** Médio–Alto
- **Principais profissionais afetados:** Compliance; Auditoria; Compras; Jurídico; Relações governamentais.
- **Como muda o trabalho:** Crescimento das rotinas de integridade corporativa, *due diligence* de terceiros, rastreabilidade e documentação; redução de informalidade e aumento de especialização em conformidade operacional.

Mudanças no cenário de ameaças e percepção pública (incidentes de alto impacto) - Incidentes relevantes podem redefinir prioridades políticas e acelerar exigências de resiliência, continuidade e coordenação interinstitucional.

- **Nível de impacto:** Alto
- **Principais profissionais afetados:** Operações (SOC); Gestores de crise; Comunicação institucional; Governança; Inteligência cibernética.
- **Como muda o trabalho:** Aumenta a centralidade de gestão de crises, exercícios, prontidão 24x7, integração com stakeholders e rotinas estruturadas de resposta, com maior carga de coordenação e documentação.

Reconfiguração da cadeia de suprimentos (dependência externa, chips, hardware, serviços críticos) - Choques logísticos, barreiras comerciais ou dependências críticas podem afetar entregas e manutenção de soluções, com efeitos sistêmicos.

- **Nível de impacto:** Alto
- **Principais profissionais afetados:** Suprimentos; Engenharia; Gestão de configuração; Operações e manutenção; Planejamento.
- **Como muda o trabalho:** Cresce a demanda por gestão de continuidade de suprimentos, alternativas técnicas, qualificação de fornecedores e planejamento de ciclo de vida (peças, atualizações, substituição), com maior integração entre engenharia e compras.

3. Competências[5] que ganharão importância para o segmento

A difusão mais intensa das tecnologias emergentes e o impacto de eventos geopolíticos, econômicos, sociais e políticos possuem um considerável potencial para transformar não somente os processos

5 O conceito de competência utilizado neste estudo refere-se à **Mobilização de conhecimentos, habilidades e aptidões** necessárias ao desempenho de funções típicas do trabalho, realizada segundo padrões de **qualidade e produtividade** esperados pela natureza do trabalho incluindo a questão da empregabilidade. Os elementos que compõem uma competência podem assim ser definidos:

Habilidades (*Skills*) - O conceito de habilidade está relacionado à forma como as atividades são realizadas, à aplicação do conhecimento e à forma de agir e pensar. É desenvolvida por meio de treinamento (prática) ou experiência.

Aptidões (*abilities*) - O conceito de aptidão (*ability*) está relacionado às características das pessoas, ou seja, seu comportamento ao agir ou reagir a um produto, organização, pessoa, evento ou situação. A aptidão nem sempre é modificada ao longo do tempo. É a qualidade de ser capaz de fazer alguma coisa.

Conhecimentos - Considera-se o conhecimento como aquele explícito, que é definido por Nonaka e Takeuchi como sendo "o conhecimento transmitido por vias formais e sistemáticas, facilmente codificado por fórmulas, símbolos, normas e especificações. São facilmente difundidos pelos sistemas atuais de comunicação".

produtivos, mas também a lógica de funcionamento das empresas. Essas inovações tecnológicas podem impulsionar a implementação de novos modelos de negócio baseados em dados, hiperpersonalização, serviços integrados a produtos (servitização), produção sob demanda e cadeias digitais de valor. Em paralelo, surgem novas ferramentas gerenciais como plataformas de gestão em tempo real, sistemas baseados em inteligência artificial para apoio à decisão, metodologias ágeis aplicadas à engenharia de processos e práticas de governança baseadas em ESG e rastreabilidade digital.

Esse novo cenário impõe uma mudança substancial no perfil dos profissionais demandados pelas empresas da Base Industrial de Defesa. As tecnologias emergentes e os eventos de impacto, por si só, não transformam a indústria; eles exigem um novo conjunto de habilidades (*skills*), aptidões (*abilities*) e conhecimentos que permitam aos profissionais operarem sistemas complexos, interagirem com máquinas inteligentes, extraírem valor dos dados e colaborarem em ambientes híbridos e digitizados. Não se trata apenas de operar máquinas, mas de compreender os sistemas que as conectam, de analisar os dados que elas produzem e de tomar decisões baseadas em evidências. Isso exige uma formação sólida, constantemente atualizada e conectada às práticas do mundo do trabalho.

Portanto, há uma relação direta e intensa de impacto entre a difusão de novas tecnologias e novas configurações do ambiente de atuação, e a necessidade de reconfiguração das formações profissionais. À medida que as empresas do segmento se transformam, surgem novas funções, novos fluxos de trabalho e novas interações entre homem e máquina, exigindo dos profissionais um conjunto ampliado de competências que integram habilidades operacionais, aptidões cognitivas refinadas e conhecimentos técnicos atualizados.

Seguindo esta linha de raciocínio e baseado no contexto apresentado anteriormente, são apresentadas, a seguir, as principais habilidades, aptidões e conhecimentos que ganharão importância ao longo dos próximos 10 anos.

3.1) Habilidades (*Skills*)[6] que ganharão importância[7]

Análise e avaliação de informações e dados

Categoria: Habilidades Técnicas -> Análise e avaliação de informações e dados

Descrição: Examinar dados técnicos e operacionais para decisões baseadas em evidências, avaliando confiabilidade, riscos e impactos.

6 A tipologia utilizada para a identificação das habilidades foi baseada naquelas definidas e utilizadas pela ESCO (*European Skills, Competences, Qualifications and Occupations*) e pelo Sistema O*NET (USA).

7 As habilidades foram elencadas porque mudam o trabalho, são acionadas por múltiplas tecnologias e eventos, são institucionalmente mandatórias, apresentam risco de escassez e sustentam tanto a absorção (5 anos) quanto a institucionalização (10 anos) das aptidões do segmento.

.

Por que é importante: Essencial para IA defensiva, SOAR, inteligência de ameaças e auditorias; intensificada por exigências contratuais, compliance e incidentes de alto impacto.

Como capacitar: Estudos de caso operacionais, exercícios de correlação de eventos (simulações), laboratórios de análise pós-incidente e certificações internas.

Monitoramento, inspeção e testes

Categoria: Habilidades Técnicas -> Monitoramento, inspeção e testes

Descrição: Avaliar funcionamento e conformidade de sistemas, processos e controles de segurança.

Por que é importante: Tecnologias Zero Trust, IAM, verificação formal e ciberfísico exigem V&V contínua; eventos regulatórios ampliam a realização de auditorias e identificação de evidências.

Como capacitar: Rotação SOC–engenharia, *checklists* de ensaio, campanhas de teste e qualificação em métodos de validação.

Análise de sistemas

Categoria: Habilidades Sistêmicas -> Análise de sistemas

Descrição: Compreender sistemas complexos, interdependências e efeitos de mudanças no desempenho.

Por que é importante: Tecnologias *digital twins*, interoperabilidade interforças e arquiteturas soberanas demandam visão sistêmica. A busca pela soberania digital e cadeias críticas reforçam a necessidade.

Como capacitar: Modelagem de arquiteturas, exercícios de impacto cruzado e simulações de falhas.

Resolução de problemas complexos

Categoria: Habilidades de Resolução de Problemas Complexos

Descrição: Estruturar problemas complexos e avaliar opções para soluções robustas.

Por que é importante: Incidentes, resposta orquestrada e crises geopolíticas exigem decisões sob incerteza; reconfigura responsabilidades.

Como capacitar: Tabletop exercises, *war games* cibernéticos e análises pós-ação.

Pensamento crítico

Categoria: Habilidades Básicas -> Pensamento crítico

Descrição: Avaliar alternativas, identificar vieses e validar conclusões.

Por que é importante: Tecnologias de IA explicável (XAI), inteligência cognitiva e processos de compliance requerem julgamento humano qualificado, na redução do risco operacional e legal.

Como capacitar: Revisões por pares, auditorias simuladas e debates estruturados.

Fluência digital

Categoria: Habilidades Técnicas -> Fluência digital

Descrição: Usar ferramentas digitais para operar, integrar e manter infraestruturas de TICs com ética e eficiência.

Por que é importante: Base para todas as tecnologias emergentes, sendo uma *skill* motriz que habilita outras.

Como capacitar: Trilhas modulares por função, laboratórios hands-on e certificações técnicas.

Monitoramento de informações

Categoria: Habilidades Técnicas -> Monitoramento de informações

Descrição: Acompanhar evoluções tecnológicas, regulatórias e de ameaças.

Por que é importante: Pressões regulatórias, controles de exportação e mudanças geopolíticas exigem atualização contínua.

Como capacitar: Células de *horizon scanning*, boletins internos e comunidades de prática.

Gestão da Informação

Categoria: Habilidades de Gestão -> Gestão da Informação

Descrição: Criar e gerir sistemas para organizar, proteger e distribuir informações.

Por que é importante: LGPD, auditorias, compartilhamento interforças e governança contratual ampliam a criticidade dessa skill.

Como capacitar: Políticas de dados, exercícios de classificação/retenção e automação de compliance.

Planejamento e organização

Categoria: Habilidades Técnicas -> Planejamento e organização

Descrição: Coordenar atividades, cronogramas e recursos para cumprir objetivos.

Por que é importante: Ciclos orçamentários, contratos por desempenho e institucionalização de capacidades exigem rigorosos processos de planejamento.

Como capacitar: PMO técnico, simulações de replanejamento e gestão por marcos.

Julgamento e tomada de decisões

Categoria: Habilidades Sistêmicas -> Julgamento e tomada de decisões

Descrição: Avaliar custos, benefícios e riscos para escolher ações adequadas.

Por que é importante: Aumento da pressão regulatória sobre resposta a incidentes, priorização de investimentos e governança.

Como capacitar: Cenários decisórios, análise multicritério e exercícios de crise.

Negociação e gestão de contratos e acordos

Categoria: Habilidades Sociais -> Negociação e gestão de contratos e acordos

Descrição: Negociar e gerir termos contratuais, SLAs e requisitos.

Por que é importante: O endurecimento de compliance, auditorias e judicialização elevam a complexidade da estruturação dos contratos.

Como capacitar: Clínicas de contratos, simulações de negociação e integração jurídico–técnica.

Aprendizagem autônoma

Categoria: Habilidades Básicas -> Aprendizagem autônoma

Descrição: Aprender de forma autônoma e proativa, aplicando novos conhecimentos.

Por que é importante: Escassez de talentos e rápida evolução tecnológica exigem atualização contínua.

Como capacitar: Trilhas personalizadas, *learning sprints* e mentoria técnica.

Gestão do tempo

Categoria: Habilidades Básicas -> Gestão Pessoal e Organização do Trabalho

Descrição: Capacidade de planejar, priorizar e organizar atividades e recursos ao longo do tempo, gerenciando múltiplas demandas simultâneas, respeitando prazos críticos e mantendo desempenho consistente em contextos de pressão e incerteza.

Por que é importante: No contexto da defesa e proteção cibernética, o tempo é um recurso estratégico. A capacidade de resposta a incidentes, atualização de sistemas, análise de ameaças e implementação de medidas de segurança depende diretamente da gestão eficiente do tempo.

Como capacitar: Treinamentos em métodos de priorização (ex.: matriz de criticidade, gestão por SLA e risco); Capacitação em metodologias ágeis e gestão de tarefas (Scrum, Kanban adaptado à cibersegurança); Simulações de resposta a incidentes com restrições de tempo.

Comunicação

Categoria: Habilidades Básicas -> Comunicação e Interação

Descrição: Capacidade de transmitir, interpretar e adaptar informações técnicas e estratégicas de forma clara, precisa e adequada ao público-alvo, utilizando diferentes meios (oral, escrito e digital), incluindo comunicação inter equipes, com stakeholders e em ambientes de alta criticidade operacional.

Por que é importante: Em ambientes de defesa cibernética, caracterizados por alta complexidade técnica, interdependência entre sistemas e necessidade de resposta rápida a incidentes, a comunicação eficaz é um fator crítico para a coordenação entre equipes, tomada de decisão e mitigação de riscos.

Como capacitar: Treinamentos em comunicação técnica e redação profissional (relatórios, incident reports, briefs executivos); Simulações de gestão de crises cibernéticas com foco em comunicação inter equipes.

Tabela de Priorização[8] das Habilidades Requeridas

Escala

- **9–10** -> Prioridade **Muito Alta**
- **7–8** -> Prioridade **Alta**
- **5–6** -> Prioridade **Média**

Habilidade	Score 5 anos	Prioridade 5 anos	Score 10 anos	Prioridade 10 anos
Análise e avaliação de informações e dados	10	Muito alta	10	Muito alta
Análise de sistemas	9	Muito alta	10	Muito alta
Monitoramento de informações (tecnologia/regulação/ameaças)	9	Muito Alta	10	Muito alta
Gestão do tempo	9	Muito alta	10	Muito alta
Comunicação	9	Muito alta	10	Muito alta
Monitoramento, inspeção e testes	9	Muito alta	9	Muito alta
Resolução de problemas complexos	9	Muito alta	9	Muito alta
Fluência digital	9	Muito alta	9	Muito alta
Pensamento crítico	8	Alta	9	Muito alta
Gestão da Informação	8	Alta	9	Muito alta
Planejamento e organização	8	Alta	9	Muito Alta
Julgamento e tomada de decisões	8	Alta	9	Muito alta
Negociação e gestão de contratos e acordos	7	Alta	8	Alta

3.2) Aptidões (*abilities*)[9] que ganharão importância[10]

Atenção seletiva

Categoria: Aptidão Cognitiva

Descrição: Foco sustentado em sinais críticos em ambientes complexos e ruidosos.

Por que é importante: Operações SOC, resposta a incidentes, SOAR e cyber ranges exigem distinguir sinais relevantes de ruído informacional.

8 A priorização resulta da combinação ponderada de distintos critérios. No horizonte de 5 anos, receberam prioridade muito alta as *skills* que reconfiguram diretamente o trabalho operacional, são acionadas simultaneamente por múltiplas tecnologias emergentes (IA defensiva, SOAR, Zero Trust, IAM, cyber ranges) e por eventos não tecnológicos mandatórios (compliance, auditorias, incidentes, soberania digital), além de apresentarem risco de escassez. No horizonte de 10 anos, ganham peso adicional as *skills* que sustentam a institucionalização e a padronização das aptidões, atuam como habilidades motrizes para outras (ex. fluência digital, análise de sistemas, gestão da informação) e possuem alta transferibilidade entre programas e organizações do setor de defesa. Por isso, observa-se a elevação de prioridade em 10 anos para competências sistêmicas, decisórias e de governança, essenciais à consolidação do segmento.

9 A tipologia utilizada para a identificação das habilidades foi baseada naquelas definidas e utilizadas pela ESCO (*European Skills, Competences, Qualifications and Occupations*) e pelo Sistema O*NET (USA).

10 Essas *abilities* foram selecionadas porque sustentam o desempenho humano em ambientes críticos, são acionadas simultaneamente por múltiplas tecnologias e eventos, possuem alto impacto estrutural no trabalho e baixo poder de substituição por sistemas de automação, sendo decisivas tanto para o horizonte de 5 anos (absorção e resposta) quanto para 10 anos (institucionalização e resiliência).

Como desenvolver: Simulações com sobrecarga informacional, exercícios de triagem e cenários de interrupção controlada.

Atenção aos detalhes

Categoria: Aptidão Cognitiva

Descrição: Cuidado rigoroso com detalhes ao executar e revisar tarefas.

Por que é importante: Tecnologias Zero Trust, IAM, verificação formal e compliance dependem de precisão; pequenos erros geram falhas sistêmicas e riscos legais.

Como desenvolver: Revisões cruzadas, checklists críticos, auditorias simuladas.

Percepção de problemas

Categoria: Aptidão Cognitiva

Descrição: Reconhecer rapidamente que algo está errado ou pode dar errado.

Por que é importante: Tecnologias de IA defensiva, sistemas ciberfísicos e gestão de crises dependem de detecção precoce.

Como desenvolver: Tabletop exercises, análise de incidentes reais e indicadores de anomalia.

Raciocínio abdutivo

Categoria: Aptidão Cognitiva

Descrição: Formular a melhor explicação possível diante de evidências incompletas.

Por que é importante: Inteligência de ameaças cognitivas e resposta a ataques desconhecidos exigem hipóteses rápidas sob incerteza.

Como desenvolver: Estudos de caso *zero-day*, jogos de hipóteses e revisão pós-ação.

Raciocínio analítico (pensamento analítico)

Categoria: Aptidão Cognitiva

Descrição: Avaliar criticamente evidências, fontes e alternativas.

Por que é importante: Essencial para decisões sobre IA explicável, governança, auditorias e priorização de investimentos sob restrições orçamentárias.

Como desenvolver: Debates estruturados, análises multicritério e revisões por pares.

Flexibilidade para categorização (nível estratégico)

Categoria: Aptidão Cognitiva

Descrição: Adaptar regras e classificações conforme o contexto muda.

Por que é importante: Ambientes dinâmicos (Zero Trust, interoperabilidade interforças, soberania digital) exigem reclassificar ativos, riscos e acessos continuamente.

Como desenvolver: Exercícios de reclassificação dinâmica e simulações de mudança de política.

Velocidade de organização e resposta

Categoria: Aptidão Cognitiva

Descrição: Organizar informações rapidamente e responder de forma coerente.

Por que é importante: Incidentes cibernéticos e crises contratuais exigem respostas rápidas e coordenadas. A difusão dos Sistemas de Resposta Cibernética Orquestrada e Automatizada (SOAR) e a incidência de gestões de crises amplificam a exigência.

Como desenvolver: *Drills* de resposta rápida, cenários cronometrados e *playbooks* memorizáveis.

Memorização operativa

Categoria: Aptidão Cognitiva

Descrição: Retenção de procedimentos, passos operacionais e sequências críticas.

Por que é importante: Ações de emergência, contingência e manutenção sob restrição de acesso à documentação dependem dessa capacidade.

Como desenvolver: Treinos repetitivos, simulações periódicas e exames práticos.

Tolerância ao estresse

Categoria: Aptidão Socioemocional

Descrição: Manter desempenho eficaz sob pressão elevada.

Por que é importante: Resposta a incidentes, judicialização e crises geopolíticas elevam a carga emocional; essencial para prontidão 24x7.

Como desenvolver: Exercícios de crise, técnicas de regulação emocional e turnos simulados.

Autocontrole / Controle emocional

Categoria: Aptidão Socioemocional

Descrição: Regular emoções e evitar reações impulsivas em situações críticas.

Por que é importante: Decisões erradas sob pressão podem amplificar danos técnicos e legais; liderança técnica exige estabilidade emocional.

Como desenvolver: Treinamento em tomada de decisão sob estresse e feedback estruturado.

Adaptabilidade / Flexibilidade

Categoria: Aptidão Socioemocional

Descrição: Ajustar-se rapidamente a mudanças tecnológicas, regulatórias e organizacionais.

Por que é importante: O ritmo de mudança (tecnologias emergentes + eventos não tecnológicos) é contínuo e imprevisível no setor de defesa cibernética.

Como desenvolver: Rotação de funções, projetos interdisciplinares e aprendizagem baseada em problemas.

Responsabilidade

Categoria: Aptidão Socioemocional

Descrição: Compromisso com regras, deveres e impactos das próprias ações.

Por que é importante: Os processos de compliance, a busca pela soberania digital, os contratos e a segurança nacional exigem alto senso de responsabilidade individual e coletiva.

Como desenvolver: Cultura de *accountability*, códigos de conduta aplicados a casos reais e avaliações comportamentais.

Curiosidade e Aprendizagem Contínua

Categoria: Capacidades Cognitivas -> Aprendizagem e Adaptação

Descrição: Capacidade de buscar ativamente novos conhecimentos, explorar problemas de forma investigativa, questionar premissas estabelecidas e atualizar continuamente repertórios técnicos e conceituais diante de mudanças tecnológicas, operacionais e contextuais.

Por que é importante: Profissionais com elevada curiosidade cognitiva tendem a antecipar tendências, identificar vulnerabilidades emergentes e adaptar-se rapidamente a novos cenários operacionais. Essa *ability* sustenta a atualização permanente das competências técnicas e reduz o risco de obsolescência profissional em um ambiente altamente dinâmico e imprevisível.

Como desenvolver: Estímulo a práticas de autoaprendizagem estruturada (*learning paths*, trilhas adaptativas); Rotação em projetos e exposição a diferentes problemas e contextos operacionais; Incentivo à experimentação (laboratórios, ambientes sandbox, exercícios de exploração).

Tabela de Priorização[11] das Aptidões Requeridas

Escala adotada

- **9–10** -> Prioridade **Muito alta**
- **7–8** -> Prioridade **Alta**
- **5–6** -> Prioridade **Média**
- **1–4** -> Prioridade **Baixa**

11 As aptidões com prioridade muito alta foram aquelas amplificadas pela automação e pela complexidade tecnológica, insubstituíveis por sistemas automatizados e críticas sob estresse, ambiguidade e risco sistêmico, como atenção seletiva, percepção de problemas e controle emocional. No horizonte de 5 anos, receberam maior peso as aptidões difíceis de desenvolver tardiamente e necessárias para absorver a transição tecnológica e regulatória. Em 10 anos, as prioridades se mantêm ou aumentam para abilities que sustentam sistemas cibernéticos complexos estabilizados, atuam como base humana para múltiplas *skills* técnicas e de gestão e apresentam relevância persistente. Por isso, observa-se elevação de score em 10 anos para adaptabilidade, raciocínio abdutivo e responsabilidade, essenciais à institucionalização e à resiliência do segmento.

Aptidão	Score 5 anos	Prioridade 5 anos	Score 10 anos	Prioridade 10 anos
Atenção seletiva	10	Muito alta	10	Muito alta
Percepção de problemas	10	Muito alta	10	Muito alta
Curiosidade e Aprendizagem Contínua	9	Alta	10	Muito alta
Atenção aos detalhes	9	Muito alta	9	Muito alta
Pensamento analítico	9	Muito alta	9	Muito alta
Velocidade de organização e resposta	9	Muito alta	9	Muito alta
Tolerância ao estresse	9	Muito alta	9	Muito alta
Autocontrole / controle emocional	9	Muito alta	9	Muito alta
Raciocínio abdutivo	8	Alta	9	Muito alta
Adaptabilidade / flexibilidade	8	Alta	9	Muito alta
Responsabilidade	8	Alta	9	Muito alta
Flexibilidade para categorização	7	Alta	8	Alta
Memorização operativa	7	Alta	8	Alta

3.3) Conhecimentos que ganharão importância (comuns às ocupações)[12]

Arquiteturas de Cibersegurança para Ambientes de Defesa

Descrição: Princípios, modelos e padrões de arquitetura (defesa em profundidade, Zero Trust, segregação de domínios, interoperabilidade segura) aplicados a sistemas de Defesa.

Justificativa: Tecnologias como Zero Trust, IAM soberano e interoperabilidade interforças tornam esse conhecimento central ao projeto, integração e operação, reduzindo risco sistêmico ao longo de todo o ciclo de vida.

Governança, Risco e Compliance (GRC) em Defesa Cibernética

Descrição: Estruturas, métodos e processos formais de governança, gestão de riscos e conformidade aplicáveis a ambientes sensíveis e regulados.

Justificativa: Endurecimento regulatório, auditorias, judicialização e exigências contratuais tornam o GRC um conhecimento transversal e obrigatório, ativado por múltiplos eventos não tecnológicos.

12 Os conhecimentos formais foram selecionados por sua possibilidade de codificação, transversalidade ocupacional, conexão direta com tecnologias emergentes e tendências não tecnológicas de impacto, relevância ao longo do ciclo de vida das plataformas, contribuição à redução de riscos sistêmicos e robustez frente a cenários alternativos.

Normas, Padrões e Certificações em Segurança da Informação e Defesa

Descrição: Conjunto de normas, padrões técnicos e processos de certificação aplicáveis à segurança da informação, continuidade e confiabilidade em ambientes de Defesa.

Justificativa: A institucionalização das tecnologias emergentes depende de padronização formal; esse conhecimento reduz riscos contratuais e operacionais em cenários de alta auditoria.

Engenharia de Sistemas Ciberfísicos Seguros

Descrição: Métodos formais para projeto, integração e validação de sistemas que combinam componentes digitais e físicos sob requisitos de segurança.

Justificativa: A proteção de plataformas, sensores, sistemas embarcados e logística militar exige conhecimento codificado que conecte cibersegurança, engenharia e segurança funcional.

Operações de Defesa Cibernética e Resposta a Incidentes

Descrição: Modelos operacionais, procedimentos padronizados e *frameworks* formais para detecção e resposta, contenção e recuperação de incidentes cibernéticos.

Justificativa: Tecnologias como SOAR, SOCs avançados e *cyber ranges* ampliam a necessidade de procedimentos explícitos e treináveis, críticos para reduzir impactos de incidentes.

Inteligência de Ameaças Cibernéticas

Descrição: Métodos estruturados para coleta, análise, correlação e disseminação de informações sobre ameaças cibernéticas.

Justificativa: A adoção de IA defensiva e análise cognitiva exige conhecimento formal para garantir a confiabilidade, rastreabilidade e uso institucional da inteligência produzida.

Criptografia Aplicada e Gestão de Chaves em Ambientes Sensíveis

Descrição: Fundamentos criptográficos, gestão de chaves, políticas de uso e transição para criptografia pós-quântica em sistemas críticos.

Justificativa: A proteção de comunicações e dados sensíveis, sob pressões de soberania e longo ciclo de vida, torna esse conhecimento essencial e transversal.

Verificação, Validação e Testes de Sistemas Críticos

Descrição: Métodos formais de teste, verificação, validação e certificação de software e sistemas críticos de Defesa.

Justificativa: Tecnologias como verificação formal, *digital twins* e requisitos contratuais rigorosos tornam esse conhecimento indispensável para reduzir falhas humanas e técnicas.

Gestão do Ciclo de Vida Seguro de Sistemas Digitais

Descrição: Princípios e métodos para segurança integrada ao ciclo de vida (projeto, desenvolvimento, operação, manutenção e modernização).

Justificativa: A persistência temporal das plataformas de Defesa exige segurança *by design* e *by default*, reduzindo riscos em cenários de longo prazo e restrição orçamentária.

Compartilhamento Seguro de Dados e Interoperabilidade

Descrição: Protocolos, modelos de governança e requisitos técnicos para troca segura de dados entre organizações e sistemas de Defesa.

Justificativa: A interoperabilidade interforças, com infraestruturas críticas de interesse da Defesa, depende de regras explícitas e normatizadas de compartilhamento e controle.

Compliance Legal e Controles de Exportação em Tecnologias Sensíveis

Descrição: Regras, regimes e procedimentos formais para conformidade legal, licenciamento e controle de exportações de soluções cibernéticas sensíveis.

Justificativa: Pressões geopolíticas, sanções e controles internacionais tornam esse conhecimento crítico para viabilizar contratos, parcerias e acesso a mercados.

Gestão de Continuidade, Resiliência e Recuperação de Serviços Críticos

Descrição: Métodos e normas para planejamento de continuidade, resiliência operacional e recuperação de sistemas e serviços críticos.

Justificativa: Incidentes de alto impacto e dependência crescente de sistemas digitais exigem conhecimento formal para garantir prontidão e confiabilidade institucional.

Governança de dados (ciclo de vida da informação)

Descrição: Conjunto de princípios, normas, processos e práticas para gestão do ciclo de vida da informação — desde sua criação, classificação, armazenamento, uso, compartilhamento e proteção

até seu arquivamento ou descarte — assegurando integridade, confidencialidade, disponibilidade, rastreabilidade e conformidade regulatória.

Justificativa: A crescente digitização, interoperabilidade entre sistemas e integração com parceiros nacionais e internacionais ampliam significativamente os riscos de vazamento, manipulação ou uso indevido da informação.

Tabela de Priorização[13] dos Conhecimentos Requeridos

Escala

- **9–10** -> Prioridade **Muito alta**
- **7–8** -> Prioridade **Alta**
- **5–6** -> Prioridade **Média**

Conhecimento	Score 5 anos	Prioridade 5 anos	Score 10 anos	Prioridade 10 anos
Arquiteturas de cibersegurança para ambientes de Defesa	10	Muito alta	10	Muito alta
Governança, Risco e Compliance (GRC) em Defesa Cibernética	9	Muito alta	10	Muito alta
Operações de defesa cibernética e resposta a incidentes	9	Muito alta	10	Muito alta
Inteligência de ameaças cibernéticas	9	Muito alta	10	Muito alta
Normas, padrões e certificações em segurança da informação e Defesa	9	Muito alta	9	Muito alta
Engenharia de sistemas ciberfísicos seguros	8	Alta	9	Muito alta
Criptografia aplicada e gestão de chaves (incluindo pós-quântica)	8	Alta	9	Muito alta
Verificação, validação e testes de sistemas críticos	8	Alta	9	Muito alta
Gestão do ciclo de vida seguro de sistemas digitais	8	Alta	9	Muito alta
Compartilhamento seguro de dados e interoperabilidade	8	Alta	9	Muito alta
Gestão de continuidade, resiliência e recuperação de serviços críticos	8	Alta	9	Muito alta
Governança de dados	8	Alta	9	Muito alta
Compliance legal e controles de exportação em tecnologias sensíveis	7	Alta	8	Alta

13 No horizonte de 5 anos, receberam prioridade muito alta os conhecimentos estruturantes e mandatórios para absorção tecnológica imediata e conformidade — arquiteturas de segurança, GRC, normas/certificações e operações de resposta a incidentes — cujo risco de ausência é elevado e que reconfiguram o trabalho. No horizonte de 10 anos, observa-se elevação de prioridade para conhecimentos que sustentam a institucionalização e a longevidade das aptidões, como engenharia ciberfísica segura, V&V de sistemas críticos, ciclo de vida seguro, interoperabilidade e resiliência. Conhecimentos com maior dificuldade de internalização foram priorizados mais cedo para evitar gargalos formativos.

3.4) Matriz Integrada de Orientação Formativa para o segmento

A seguir se sugere uma Matriz Integrada de Orientação Formativa para o segmento de Defesa Cibernética da Base Industrial de Defesa (BID), consolidando *Conhecimentos + Habilidades (skills) + Aptidões (abilities)* em eixos formativos estruturantes. A matriz foi construída de forma coerente com os elementos de competência priorizados no período de 5 e 10 anos, com foco direto em currículos, capacitações corporativas e políticas públicas de formação profissional.

Eixo 1 — Arquitetura, Integração e Ciclo de Vida da Defesa Cibernética

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Arquiteturas de cibersegurança para ambientes de Defesa (Zero Trust, defesa em profundidade)	Muito Alta	Muito Alta	Núcleo curricular estruturante
Conhecimento	Engenharia de sistemas ciberfísicos seguros e ciclo de vida (SE / Secure-by-Design)	Alta	Muito Alta	Núcleo curricular estruturante
Habilidade	Análise de sistemas	Muito Alta	Muito Alta	Execução técnica integrada
Habilidade	Resolução de problemas complexos	Muito Alta	Muito Alta	Tomada de decisão técnica
Aptidão	Raciocínio abdutivo	Alta	Muito Alta	Sustentação cognitiva
Aptidão	Pensamento analítico	Muito Alta	Muito Alta	Avaliação crítica de arquiteturas

Eixo 2 — Operações, Resiliência e Resposta a Incidentes Cibernéticos

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Operações de defesa cibernética e resposta a incidentes (SOC / SOAR)	Muito Alta	Muito Alta	Núcleo operacional
Conhecimento	Gestão de continuidade, resiliência e recuperação de serviços críticos	Alta	Muito Alta	Formação para prontidão
Habilidade	Monitoramento, inspeção e testes	Muito Alta	Muito Alta	Execução operacional
Habilidade	Monitoramento de informações (ameaças, vulnerabilidades, alertas)	Alta	Muito Alta	Antecipação e prevenção
Aptidão	Atenção seletiva	Muito Alta	Muito Alta	Desempenho sob pressão
Aptidão	Tolerância ao estresse	Muito Alta	Muito Alta	Estabilidade emocional operacional

Eixo 3 — Governança, Risco, Compliance e Regulação em Defesa Cibernética

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anost	Papel formativo
Conhecimento	Governança, Risco e Compliance (GRC) em Defesa Cibernética	Muito Alta	Muito Alta	Núcleo institucional

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anost	Papel formativo
Conhecimento	Compliance legal e controles de exportação em tecnologias sensíveis	Alta	Alta	Formação regulatória
Habilidade	Gestão da informação	Alta	Muito Alta	Conformidade e rastreabilidade
Habilidade	Comunicação técnica e redação formal	Alta	Alta	Interface técnico-institucional
Aptidão	Responsabilidade	Alta	Muito Alta	Confiabilidade institucional
Aptidão	Autocontrole / controle emocional	Muito Alta	Muito Alta	Ética e governança sob risco

Eixo 4 — Inteligência de Ameaças, Dados e Tecnologias Avançadas

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Inteligência de ameaças cibernéticas (CTI)	Alta	Muito Alta	Análise estratégica
Conhecimento	Criptografia aplicada e gestão de chaves (incluindo a pós-quântica)	Alta	Alta	Especialização técnica
Habilidade	Análise e avaliação de informações e dados	Muito Alta	Muito Alta	Extração de valor informacional
Habilidade	Reconhecimento de padrões	Alta	Muito Alta	Detecção avançada
Aptidão	Percepção de problemas	Muito Alta	Muito Alta	Identificação precoce de riscos
Aptidão	Flexibilidade para categorização	Alta	Alta	Adaptação a ameaças emergentes

Eixo 5 — Integração Institucional, Interoperabilidade e Cooperação

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Compartilhamento seguro de dados e interoperabilidade interinstitucional	Alta	Muito Alta	Integração sistêmica
Conhecimento	Normas, padrões e certificações em segurança da informação e Defesa	Muito Alta	Muito Alta	Padronização e escala
Habilidade	Coordenação e contato interorganizacional	Alta	Alta	Articulação institucional
Habilidade	Planejamento e organização	Alta	Alta	Execução programática
Aptidão	Adaptabilidade / flexibilidade	Alta	Muito Alta	Resposta a ambientes voláteis
Aptidão	Orientação social (trabalho em equipe)	Alta	Alta	Cooperação intersetorial

Como se pode utilizar esta matriz

Instituições de Formação Profissional

- Utilizar os eixos como organizadores curriculares (núcleo comum + trilhas de especialização).
- Priorizar Eixos 1, 2 e 3 em cursos técnicos e de graduação.
- Explorar Eixos 4 e 5 em pós-graduação, cursos avançados e formação continuada.

Para Empresas da BID

- Usar a matriz como mapa de capacitação interna e planejamento de *Workforce*.
- Direcionar treinamentos operacionais aos Eixos 2 e 4.
- Desenvolver lideranças técnicas e institucionais a partir dos Eixos 1 e 3.
- Apoiar programas de mentorias focados nas aptidões críticas.

Instituições Responsáveis por Políticas Públicas

- Empregar os eixos como base para políticas nacionais de formação estratégica em defesa cibernética.
- Priorizar investimentos formativos nos elementos de maior relevância para os próximos 5 anos (riscos imediatos).
- Usar a matriz para alinhar educação, indústria e defesa, reduzindo assimetrias de capacitação.
- Integrar a matriz a programas de soberania digital, inovação e segurança nacional.

4. Profissionais Que Ganharão Relevância

A possível difusão das novas tecnologias e os impactos dos eventos, descritos anteriormente, poderão estabelecer um contexto futuro que demandará, por parte das empresas do segmento, profissionais que visam apoiar o setor na implementação e uso das novas tecnologias e desenvolvimento de produtos. A seguir, são apresentados os novos profissionais, nos níveis técnico e superior, que poderão ser demandados *vis a vis* a evolução tecnológica e os impactos dos eventos "não tecnológicos".

Tabela 1 – Profissionais que ganharão importância

Profissional	Atuação
Técnico em Operações de Defesa Cibernética (SOC de Defesa)	Opera e monitora ambientes de defesa cibernética (SOC/CSIRT), acompanhando alertas, indicadores de compromisso, procedimentos de resposta e registros de incidentes em sistemas críticos e ambientes regulados.
Técnico em Monitoramento e Testes de Segurança Cibernética	Executa testes, verificações e inspeções periódicas de sistemas, redes e plataformas ciberfísicas, garantindo conformidade com requisitos técnicos, normativos e contratuais.
Técnico em Gestão de Identidades e Acessos (IAM)	Implementa, opera e mantém sistemas de identidade e controle de acesso (usuários, dispositivos e sistemas), apoiando arquiteturas Zero Trust e políticas de soberania digital.

Profissional	Atuação
Técnico em Continuidade e Resiliência de Sistemas Digitais	Atua na implementação de planos de continuidade, contingência e recuperação de serviços críticos, apoiando exercícios, testes e auditorias de prontidão operacional.
Técnico em Governança de Dados Sensíveis	Organiza, classifica e controla informações sensíveis, garantindo rastreabilidade, retenção, conformidade regulatória e suporte a auditorias e compartilhamento seguro.
Engenheiro(a) de Arquiteturas de Defesa Cibernética	Projeta arquiteturas seguras para ambientes de Defesa, integrando Zero Trust, interoperabilidade, ciberfísico e requisitos institucionais ao longo do ciclo de vida das plataformas.
Engenheiro(a) de Sistemas Ciberfísicos Seguros	Integra segurança cibernética ao projeto e à validação de sistemas físicos-digitalizados (sensores, plataformas, logística, C2), reduzindo riscos de efeitos cinéticos e falhas sistêmicas.
Especialista em Resposta Avançada a Incidentes e Crises Cibernéticas	Coordena respostas a incidentes de alto impacto, liderando análises técnicas, comunicação institucional, articulação jurídica e gestão de crises em ambientes de Defesa.
Analista de Inteligência de Ameaças Cibernéticas (CTI – Defesa)	Produz inteligência estratégica e operacional sobre ameaças, correlacionando dados técnicos, contexto geopolítico e tendências emergentes para apoiar decisões de Defesa.
Especialista em Governança, Risco e *Compliance* em Defesa Cibernética	Estrutura e opera modelos de GRC específicos para Defesa, integrando normas, contratos, auditorias, controles de exportação e requisitos legais em ambientes sensíveis.
Engenheiro(a) de Verificação, Validação e Certificação de Sistemas Críticos	Desenvolve e aplica métodos formais e testes avançados para certificar softwares e sistemas críticos de Defesa, garantindo confiabilidade, rastreabilidade e conformidade.
Especialista em Criptografia Aplicada e Soberania Digital	Projeta e implementa soluções criptográficas (incluindo pós-quânticas), políticas de gestão de chaves e proteção de comunicações críticas de ciclo de vida.
Gestor(a) de Interoperabilidade e Compartilhamento Seguro de Dados	Coordena arquiteturas e políticas para troca segura de dados entre as Forças, empresas e órgãos estratégicos, assegurando governança, confiança e continuidade.
Gestor(a) de Programas de Defesa Cibernética	Planeja e gerencia programas estratégicos de defesa cibernética, integrando tecnologia, orçamento, compliance, capacitação e requisitos institucionais.
Engenheiro de IA	Desenvolve prompts, projeta modelos de linguagem, projeta, desenvolve e implementa bases de conhecimento e arquiteturas para RAG.
Técnico/especialista de Prompt	Utiliza prompts previamente desenvolvidos pelo Engenheiro de IA, elabora prompts complementares e os aperfeiçoa, com base na análise das respostas recebidas.

Síntese – tendências e perfis transversais emergentes

Tendências estruturais de perfis

- **Hibridização técnica–institucional:** Demanda por profissionais que combinam domínio técnico com compreensão regulatória, contratual e estratégica.
- **Centralidade da operação contínua:** Cresce a relevância de perfis voltados à operação, monitoramento, resposta e resiliência (não apenas desenvolvimento).
- **Institucionalização da ciberdefesa:** Aumento de funções ligadas a GRC, certificação, auditoria e governança.
- **Integração ciber–físico–organizacional:** Os novos perfis conectam engenharia, operações e políticas públicas.

Perfis transversais mais valorizados

- Profissionais com *pensamento sistêmico, atenção seletiva, tolerância ao estresse e responsabilidade institucional*.

- Capacidade de atuar em *ambientes regulados, sob pressão e com informação incompleta.*
- Formação contínua e capacidade de *aprendizagem ativa* como requisito permanente.

5. Cursos que Poderão ser Demandados pelas Empresas do Segmento[14]

Arquiteturas de Defesa Cibernética e Zero Trust — Básico

- **Público:** Engenheiros de sistemas e de redes, analistas de segurança e de negócios, gestores técnicos e de sistemas de informação, técnicos de TI.
- **Conteúdo:** Princípios de defesa em profundidade; Zero Trust; segmentação lógica; identidade como perímetro; integração com requisitos institucionais e contratuais; estudos de caso do setor de defesa.
- **Objetivo:** Alinhar a base técnica e conceitual de equipes multidisciplinares para arquiteturas seguras e institucionalizáveis, sem exposição de detalhes sensíveis.

Operações de Defesa Cibernética e Resposta a Incidentes — Intermediário

- **Público:** Equipes SOC/CSIRT, Engenheiro de IA, técnicos de operação, analistas de segurança, gestores de continuidade.
- **Conteúdo:** Modelos operacionais de SOC; *playbooks* de resposta; integração homem – sistemas de automação (SOAR em nível conceitual); Técnico/especialista de prompt, de SIEM, de detecção, inteligência de ameaças, análise de riscos, gestão de incidentes, comunicação em períodos de crise; exercícios *tabletop*.
- **Objetivo:** Fortalecer a capacidade operacional contínua e a coordenação sob incidentes de alto impacto.

Governança, Risco e Compliance (GRC) em Ambientes de Defesa — Básico

- **Público:** Engenheiros, gestores de projetos, áreas jurídicas, compliance, líderes técnicos.
- **Conteúdo:** GRC aplicado à defesa cibernética; gestão de riscos técnicos e institucionais; auditorias; requisitos contratuais; responsabilidade técnica e organizacional.
- **Objetivo:** Reduzir riscos regulatórios e jurídicos e integrar engenharia, operação e governança.

Segurança ao Longo do Ciclo de Vida de Sistemas Críticos — Intermediário

- **Público:** Engenheiros, técnicos de testes, gestores de programas, desenvolvedores.
- **Conteúdo:** *Security by design;* integração da segurança ao ciclo de vida; conceitos de verificação e validação; rastreabilidade de requisitos; impactos de longo prazo.

14 Os cursos foram selecionados com base na aderência aos vetores de transformação setorial, impacto transversal sobre múltiplos perfis, alinhamento com conhecimentos, *skills* e *abilities* prioritários, foco em requalificação contínua, neutralidade tecnológica operacional, aplicabilidade prática, modularidade formativa, adequação à estrutura de mercado, robustez frente a cenários futuros e viabilidade institucional.

- **Objetivo:** Evitar falhas estruturais decorrentes de decisões de projeto e manutenção inadequadas.

Inteligência de Ameaças Cibernéticas para Defesa — Intermediário

- **Público:** Analistas de segurança, engenheiros, gestores estratégicos, PMO.
- **Conteúdo:** Fundamentos de CTI; fontes e confiabilidade; análise de contexto geopolítico; correlação estratégica; uso institucional da inteligência, conceitos de frameworks relacionados à gestão de ameaças cibernéticas.
- **Objetivo:** Apoiar decisões técnicas e estratégicas com base em informação estruturada, não apenas reativa.

Gestão de Identidades, Acessos e Confiança Digital — Básico

- **Público:** Técnicos de TI, engenheiros, profissionais de contrainteligência, gestores de sistemas e de RH, analistas de segurança.
- **Conteúdo:** Princípios de IAM; identidade de pessoas, sistemas e dispositivos; segregação de funções; impactos organizacionais e regulatórios, identidade auto soberana.
- **Objetivo:** Apoiar a transição para modelos de acesso mais seguros e auditáveis em ambientes críticos.

Continuidade, Resiliência e Recuperação de Serviços Críticos — Básico

- **Público:** Gestores operacionais, técnicos de infraestrutura, líderes de projeto.
- **Conteúdo:** Continuidade de negócios; planos de contingência; exercícios de prontidão; integração com defesa cibernética; análise de impacto.
- **Objetivo:** Aumentar a resiliência organizacional frente a incidentes cibernéticos e crises sistêmicas.

Criptografia Aplicada e Soberania Digital — Conceitual

- **Público:** Engenheiros, gestores técnicos, profissionais de segurança da informação, desenvolvimento.
- **Conteúdo:** Fundamentos de criptografia; gestão de chaves; riscos de longo prazo; transição para criptografia pós-quântica (em nível conceitual); implicações estratégicas.
- **Objetivo:** Preparar equipes para decisões informadas sobre proteção de dados e comunicações sensíveis ao longo do tempo.

Compartilhamento Seguro de Dados e Interoperabilidade Institucional — Básico

- **Público:** Gestores de sistemas, arquitetos, áreas institucionais, Engenheiros da área de TI.
- **Conteúdo:** Princípios de interoperabilidade; protocolos de comunicação, governança de dados; controle de acesso interorganizacional; confiança e acordos institucionais.
- **Objetivo:** Viabilizar a cooperação segura entre empresas, Forças e órgãos estratégicos.

Tomada de Decisão Técnica sob Estresse e Incerteza — Transversal

- **Público:** Líderes técnicos, gestores, especialistas operacionais (todos).
- **Conteúdo:** Tomada de decisão em ambientes críticos; vieses cognitivos; priorização sob pressão; coordenação de equipes; exercícios de crise, inteligência emocional.
- **Objetivo:** Desenvolver *abilities* críticas (controle emocional, percepção de problemas, raciocínio abdutivo) essenciais à defesa cibernética.

6. Desafios na formação e atualização da mão de obra

Legenda dos atores

- **Empresas -** Organizações da Base Industrial de Defesa responsáveis pela produção, integração e entrega de bens e serviços, incluindo integradoras, fabricantes e fornecedores críticos. Atuam em ambientes regulados e dependentes de contratos públicos, com papel central na absorção tecnológica e na qualificação da força de trabalho.
- **Governo -** Órgãos públicos que formulam políticas, regulam, contratam e fiscalizam o setor de defesa, atuando como cliente dominante e indutor de padrões técnicos, regulatórios e de formação de capacidades nacionais.
- **Instituições de Formação Profissional (IFPs) -** Entidades responsáveis pela formação inicial, técnica, superior e pela capacitação contínua da mão de obra, traduzindo demandas do setor de defesa em currículos, cursos e trilhas formativas.
- **Instituições de Ciência, Tecnologia e Inovação (ICTs) -** Centros e institutos que realizam P&D aplicado, ensaios e validação tecnológica, apoiando a indústria na adoção de tecnologias emergentes e na formação avançada de especialistas.

Déficit de profissionais híbridos

Desafio: Escassez de profissionais que combinem competências técnicas em cibersegurança com compreensão de governança, compliance, contratos e soberania digital.

Justificativa: A institucionalização da defesa cibernética exige profissionais que atuem simultânea em arquitetura, operação e conformidade regulatória. Contudo, tais perfis são difíceis de formar em ciclos curtos.

Ator	Papel principal
Empresas	Definir perfis híbridos prioritários; expor profissionais a projetos reais regulados; promover rotação entre áreas técnicas, operacionais e de compliance.
Governo	Induzir programas nacionais de formação híbrida; financiar reconversão profissional em ciberdefesa; alinhar requisitos de contratação pública.
IFPs	Desenvolver currículos integrados; adotar aprendizagem baseada em projetos e casos do setor de defesa, aproximar o ambiente acadêmico com as necessidades empresariais.
ICTs	Apoiar conteúdos avançados; fornecer casos reais anonimizados; operar ambientes de experimentação regulada.

Tempo de formação incompatível com a velocidade das ameaças

Desafio: Desalinhamento entre o ritmo da evolução das ameaças cibernéticas e o tempo necessário para formar profissionais qualificados.

Justificativa: Tecnologias como IA defensiva, SOAR e criptografia pós-quântica evoluem mais rápido que os currículos formais e processos de certificação.

Ator	Papel principal
Empresas	Demandar capacitações curtas e modulares; investir em *upskilling* contínuo da força instalada.
Governo	Flexibilizar marcos regulatórios educacionais; apoiar microcredenciais e certificações rápidas.
IFPs	Atualizar currículos com maior frequência; ofertar cursos "empilháveis" e formação continuada.
ICTs	Monitorar fronteira tecnológica; transferir rapidamente novos conteúdos para a formação.

Escassez estrutural de talentos e competição intersetorial

Desafio: Forte concorrência com outros setores (financeiro, *big techs*, telecom) pelos mesmos perfis críticos.

Justificativa: O setor de defesa impõe restrições adicionais (sigilo, compliance, nacionalidade), reduzindo o pool efetivo de talentos disponíveis.

Ator	Papel principal
Empresas	Desenvolver estratégias de atração e retenção de talentos; valorizar carreiras técnicas; investir em formação interna.
Governo	Criar políticas de atração e retenção de talentos estratégicos; apoiar bolsas e incentivos.
IFPs	Ampliar oferta em áreas críticas; divulgar carreiras em defesa cibernética.
ICTs	Formar especialistas de alto nível; apoiar capacitação avançada e pós-graduação aplicada.

Dificuldade de retenção de profissionais qualificados

Desafio: Manter profissionais experientes e certificados por longos períodos.

Justificativa: Mercados civis oferecem maior flexibilidade salarial e mobilidade, enquanto a BID opera com contratos longos e estruturas mais rígidas.

Ator	Papel principal
Empresas	Criar trilhas de carreira técnica; programas de mentoria; ambientes de trabalho estáveis.
Governo	Estabelecer diretrizes para retenção em áreas sensíveis; apoiar estabilidade contratual, gerar demanda de produtos a partir dos projetos/pesquisas aplicadas já realizadas.
IFPs	Ofertar capacitação avançada para profissionais em atividade; formação ao longo da vida.
ICTs	Engajar especialistas seniores em projetos de P&D e transferência de conhecimento.

Atualização contínua da força de trabalho instalada

Desafio: Requalificar técnicos e engenheiros formados em paradigmas anteriores (perímetro clássico, TI tradicional).

Justificativa: A transição para Zero Trust, sistemas ciberfísicos e interoperabilidade exige mudança cognitiva e operacional, não apenas novos conteúdos.

Ator	Papel principal
Empresas	Mapear *gaps* de competências; financiar programas de *reskilling*; liberar tempo para capacitação.
Governo	Apoiar programas de reconversão profissional; Co financiar capacitação estratégica.
IFPs	Desenvolver cursos de transição tecnológica (Zero Trust, SOC, ciberfísico).
ICTs	Traduzir novas tecnologias em conteúdos aplicáveis à indústria.

Limitações de oferta formativa especializada

Desafio: Baixa disponibilidade de cursos específicos para defesa cibernética, sobretudo em nível técnico e tecnológico.

Justificativa: Grande parte da oferta educacional é genérica em TI e cibersegurança e não cobre requisitos institucionais, regulatórios e de defesa.

Ator	Papel principal
Empresas	Sinalizar demandas específicas; codesenvolver cursos com IFPs.
Governo	Induzir oferta especializada; garantir escala mínima e sustentabilidade econômica.
IFPs	Criar cursos específicos para defesa cibernética; formar docentes especializados.
ICTs	Apoiar infraestrutura, laboratórios e atualização tecnológica contínua.

Barreiras de acesso a ambientes realistas de treino

Desafio: Dificuldade de prover ambientes de simulação, *cyber ranges* e exercícios próximos da realidade operacional.

Justificativa: Restrições de sigilo, custo e segurança limitam o uso de dados e sistemas reais para formação prática.

Ator	Papel principal
Empresas	Disponibilizar cenários simulados; participar de exercícios conjuntos.
Governo	Financiar *cyber ranges* nacionais; definir regras de uso seguro e controlado.

Ator	Papel principal
IFPs	Integrar simulações aos currículos; formar instrutores especializados.
ICTs	Operar e manter ambientes de simulação; desenvolver cenários avançados.

Fragmentação entre formação inicial e capacitação continuada

Desafio: Falta de integração entre educação formal (técnica e superior) e programas de capacitação corporativa.

Justificativa: O setor demanda aprendizagem ao longo da vida, mas os sistemas educacionais ainda operam em silos.

Ator	Papel principal
Empresas	Integrar formação formal e treinamento interno; reconhecer microcredenciais.
Governo	Promover políticas de aprendizagem ao longo da vida; integrar sistemas educacionais.
IFPs	Articular cursos iniciais e continuados; ofertar trilhas progressivas.
ICTs	Apoiar atualização permanente de conteúdos e metodologias.

Dependência de aptidões humanas insubstituíveis

Desafio: Elevada dependência de *abilities* humanas (atenção seletiva, julgamento sob estresse, percepção de problemas).

Justificativa: Mesmo com o uso de tecnologias de automação e IA, decisões críticas permanecem humanas, exigindo desenvolvimento comportamental contínuo e difícil de escalar.

Ator	Papel principal
Empresas	Incorporar desenvolvimento socioemocional; exercícios de crise e simulações.
Governo	Reconhecer essas capacidades como estratégicas; apoiar programas específicos.
IFPs	Integrar competências comportamentais aos currículos técnicos.
ICTs	Pesquisar métodos de desenvolvimento e avaliação dessas abilities.

Incerteza regulatória e geopolítica

Desafio: Ajustar currículos e capacitações a mudanças frequentes em normas, controles de exportação e requisitos de soberania.

Justificativa: Mudanças regulatórias podem tornar, rapidamente, as formações recentes em obsoletas ou exigir requalificação acelerada.

Ator	Papel principal
Empresas	Monitorar mudanças regulatórias; adaptar rapidamente capacitações internas.
Governo	Harmonizar normas; comunicar antecipadamente mudanças relevantes.
IFPs	Atualizar conteúdos legais e institucionais; formar para adaptação regulatória.
ICTs	Analisar impactos regulatórios e geopolíticos; apoiar formulação de políticas.

Baixa padronização de perfis ocupacionais

Desafio: Ausência de referenciais nacionais consolidados de ocupações e competências em defesa cibernética.

Justificativa: Dificulta o planejamento de formação, certificação, mobilidade profissional e políticas públicas coordenadas.

Ator	Papel principal
Empresas	Definir e compartilhar perfis de referência; alinhar práticas internas.
Governo	Liderar construção de referenciais nacionais; alinhar políticas de formação.
IFPs	Usar referenciais comuns para currículos e certificações (adaptar currículos).
ICTs	Apoiar tecnicamente a definição e atualização dos referenciais.

Sustentabilidade econômica da oferta formativa

Desafio: Manter cursos especializados com turmas pequenas e alta complexidade técnica.

Justificativa: O segmento é restrito e monopsônico/oligopolizado, o que limita escala e encarece a formação.

Ator	Papel principal
Empresas	Co financiar cursos estratégicos; garantir demanda mínima.
Governo	Subsidiar formações críticas; estruturar compras públicas de capacitação.
IFPs	Otimizar modelos híbridos (presencial/online); compartilhar infraestrutura.
ICTs	Operar cursos avançados e de nicho; apoiar modelos de baixo volume e alto valor.

7. Comentários Finais

O estudo prospectivo do segmento de Defesa e Proteção Cibernética evidencia que a força de trabalho constitui, simultaneamente, o principal ativo estratégico e o principal fator de vulnerabilidade para

a consolidação das capacidades nacionais de ciberdefesa no horizonte dos próximos dez anos. Diferentemente de segmentos industriais orientados à escala produtiva, a ciberdefesa opera em um contexto monopsônico/oligopolizado, altamente institucionalizado, no qual o desempenho setorial depende menos do crescimento quantitativo do emprego e mais do adensamento técnico, cognitivo, regulatório e organizacional da mão de obra.

A análise integrada das tecnologias emergentes, de suas dinâmicas de difusão programática e sistêmica, e dos eventos não tecnológicos — regulatórios, geopolíticos, institucionais e de comércio internacional — demonstra que o segmento atravessa um processo de institucionalização acelerada da ciberdefesa. Tecnologias como arquiteturas Zero Trust, inteligência artificial aplicada à defesa cibernética, automação de resposta a incidentes, criptografia de longo prazo, segurança de sistemas ciberfísicos e interoperabilidade segura não apenas transformam produtos e serviços, mas redefinem profundamente os perfis profissionais, os métodos de trabalho e os requisitos de formação.

Nesse contexto, os resultados do estudo indicam uma mudança estrutural no perfil da demanda por profissionais, marcada pela valorização de ocupações híbridas, que combinam conhecimentos formais codificados, habilidades técnicas avançadas e aptidões críticas — como julgamento sob incerteza, atenção seletiva, percepção de problemas e controle emocional. O crescimento projetado do estoque de profissionais é moderado em termos quantitativos, mas significativo em termos qualitativos, reforçando que o principal risco para o segmento não é a falta absoluta de trabalhadores, mas a escassez de profissionais com o nível de maturidade técnica e institucional exigido.

A consolidação dos resultados em eixos formativos, bem como a priorização de conhecimentos, *skills* e *abilities*, oferece uma base objetiva para orientar tanto a requalificação da força de trabalho instalada quanto a formação de novos profissionais, em níveis técnico e superior. Destaca-se que, ao longo do horizonte analisado, a demanda por capacitação contínua tende a superar a demanda por formação inicial, em razão da rápida obsolescência de competências, da evolução das ameaças e da crescente complexidade regulatória.

O estudo também evidencia desafios estruturais relevantes: a competição intersetorial por talentos, a dificuldade de retenção de profissionais experientes, as limitações de oferta formativa especializada, o acesso restrito a ambientes realistas de treinamento e a fragmentação entre educação formal e capacitação corporativa. Tais desafios não podem ser enfrentados de forma isolada, exigindo coordenação sistêmica entre empresas, governo, instituições de formação profissional e institutos de ciência e tecnologia.

Dessa forma, a principal contribuição deste estudo prospectivo reside em oferecer um quadro integrado, coerente e acionável para o planejamento da força de trabalho do segmento de Defesa e Proteção Cibernética. Ao articular tendências tecnológicas, eventos não tecnológicos, impactos ocupacionais e implicações formativas, o estudo busca subsidiar decisões estratégicas de médio e longo prazo, fortalecendo, assim, a capacidade de antecipação dos atores envolvidos.

Por fim, os resultados reforçam que a articulação entre prospectiva, política industrial e políticas de formação profissional é condição necessária para o fortalecimento da Base Industrial de Defesa e para a preservação da soberania digital do país. Investir antecipadamente na formação, atualização e retenção de profissionais de defesa cibernética não é apenas uma resposta às transformações tecnológicas em curso, mas um imperativo estratégico de Estado, com impactos diretos sobre a segurança nacional, a competitividade industrial e a autonomia tecnológica brasileira.

Cadernos de

Prospectiva Industrial de Defesa

Segmento

DEFESA CIBERNÉTICA



FIA BUSINESS SCHOOL
CNI Confederação Nacional da Indústria
ABDI Agência Brasileira de Desenvolvimento Industrial
MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS