Cadernos de

Prospectiva Industrial de Defesa

Segmento C4ISTAR

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

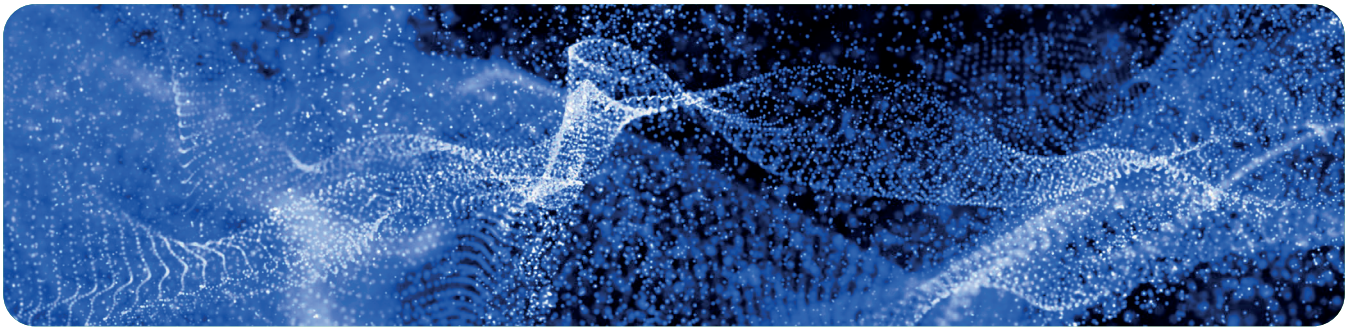
O Projeto de Avaliação e Monitoramento da Base Industrial de Defesa (BID), conduzido pela Agência Brasileira de Desenvolvimento Industrial (ABDI), constitui um esforço estruturado de produção de conhecimento estratégico sobre a capacidade produtiva, tecnológica e organizacional da indústria de defesa 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

A rápida evolução das tecnologias digitais, a intensificação das tensões geopolíticas, as transformações nos fluxos de comércio internacional e o crescente escrutínio político e institucional sobre os programas de defesa vêm alterando de forma profunda o contexto no qual os sistemas de Comando, Controle, Comunicações, Computação, Inteligência, Vigilância, Aquisição de Alvos e Reconhecimento (C4ISTAR)[1] são concebidos, desenvolvidos e operados. Esses sistemas, por sua natureza crítica e estruturante, deixaram de ser apenas conjuntos tecnológicos para se consolidarem como plataformas sociotécnicas complexas, nas quais decisões operacionais, segurança da informação, interoperabilidade interforças, soberania tecnológica e responsabilidade institucional estão intrinsecamente interligadas. Nesse cenário, as transformações não se limitam à introdução de novas soluções tecnológicas, mas se manifestam, sobretudo, na reconfiguração dos processos de trabalho, na emergência de novos perfis profissionais e na crescente exigência de competências híbridas, capazes de articular engenharia, dados, cibersegurança, operação e gestão em ambientes altamente regulados e sujeitos a riscos sistêmicos.

Diante desse contexto, os estudos prospectivos sobre o futuro da mão de obra do Sistema C4ISTAR tornam-se instrumentos estratégicos indispensáveis. Eles permitem antecipar impactos decorrentes da difusão incremental de tecnologias emergentes, da fragmentação tecnológica global, das restrições a transferências internacionais de tecnologia, da volatilidade orçamentária do Estado e do aumento do protagonismo das capacidades de Comando e Controle em missões conjuntas, interagências e de apoio ao Estado. Ao invés de responder de forma reativa às mudanças, os estudos prospectivos oferecem uma base analítica para compreender trajetórias possíveis, identificar competências críticas, reduzir riscos de descontinuidade operacional e orientar decisões mais robustas sobre formação, capacitação e gestão de pessoas em um setor caracterizado por ciclos longos, elevada dependência institucional e baixa margem para erros.

Nesse sentido, analisar o futuro da mão de obra do C4ISTAR não é apenas uma questão de dimensionamento quantitativo de profissionais, mas sobretudo de qualificação estratégica do capital humano que sustentará a Base Industrial de Defesa e as capacidades nacionais de Comando e Controle. A incorporação bem-sucedida de tecnologias como arquiteturas data-centric, inteligência artificial aplicada ao apoio à decisão, redes táticas definidas por *software*, modelos de segurança Zero Trust e automação criptográfica depende, de forma direta, da existência de profissionais capazes de integrar sistemas complexos, validar soluções críticas, operar sob pressão e tomar decisões responsáveis em ambientes de elevada incerteza técnica e institucional.

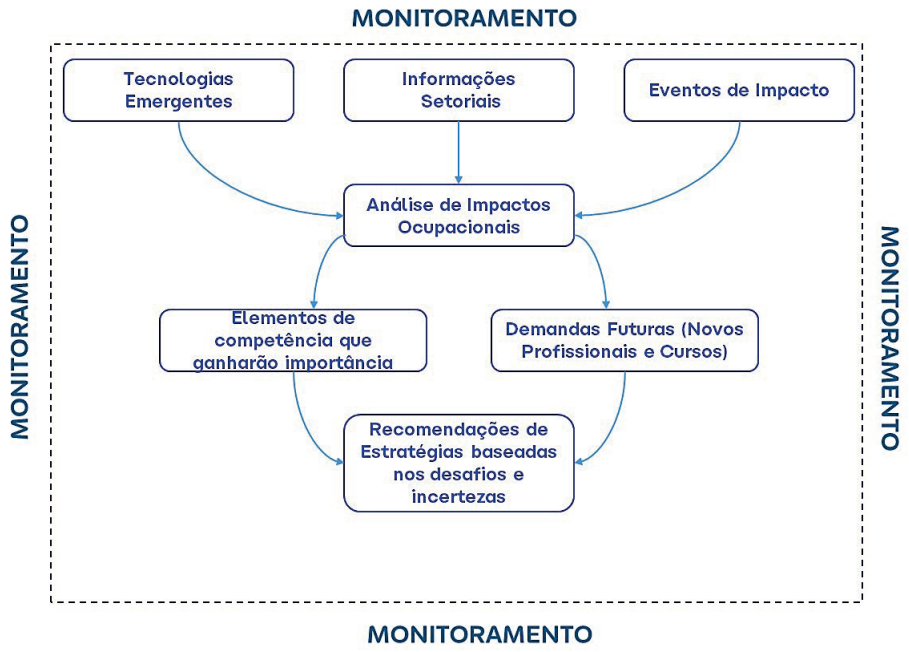
Assim, este estudo reafirma a importância de articular os resultados dos exercícios prospectivos com políticas públicas de formação profissional voltadas à Base Industrial de Defesa. Somente por meio da convergência entre governo, empresas, instituições de formação profissional e instituições de ciência, tecnologia e inovação será possível transformar sinais antecipatórios e cenários futuros em ações concretas de capacitação, atualização e retenção de talentos.

1 Para fins deste estudo optou-se por um recorte não específica para cada a força (conjunto/joint), porque obriga a tratar interoperabilidade, governança e integração interforças como "núcleo duro" do segmento. O foco sugerido está em operações no território nacional (defesa de fronteiras/infraestruturas).

A integração entre estudos prospectivos e políticas de formação constitui, portanto, um elemento central para fortalecer a autonomia tecnológica, a resiliência operacional e a sustentabilidade de longo prazo do Sistema C4ISTAR e do setor de defesa brasileiro como um todo.

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[2] 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/segmento e criação de demanda por novos profissionais.

2 Para a identificação e escolha das tecnologias emergentes foram estabelecidas camadas para a identificação das tecnologias emergentes.

A seguir são apresentadas as tecnologias emergentes sugeridas para o sistema C4ISTAR, juntamente com o possível impacto[3], 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 competências 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.



Camada A[4] — Sensoriamento e Coleta

Sensoriamento Multiestático Distribuído com Fusão Colaborativa - arquiteturas de sensores geograficamente distribuídos (radares, EO/IR, RF passivo) que operam de forma cooperativa, compartilhando medições para detecção, rastreio e classificação conjunta, inclusive com sensores de baixa assinatura, sensoriamento digital e simulação.

- **Nível de impacto no segmento:** alto.
- **Principais profissionais afetados:** engenheiros de sistemas e sensores; engenheiros de integração; analistas ISR; operadores de centros de vigilância; engenheiro eletricista; engenheiro mecatrônico; engenheiro de telecomunicação/radiofrequência.
- **Como o trabalho muda:** a operação isolada de sensores dá lugar à gestão de redes sensoriais cooperativas, exigindo competências em correlação de dados, geometria multiestática e validação de rastreios distribuídos.

3 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.

4 Camada A — Sensoriamento e coleta (multi-domínio) - radares/EO-IR, SIGINT/ELINT (quando aplicável), AIS/ADS-B, sensores de fronteira, sensores embarcados, fontes abertas estruturadas etc.

Sensores Cognitivos com Ajuste Dinâmico por IA - Sensores capazes de ajustar automaticamente parâmetros de operação (frequência, ganho, modos) com base no ambiente e na missão, utilizando aprendizado de máquina embarcado.

- **Nível de impacto no segmento:** médio–alto.
- **Principais profissionais afetados:** engenheiros eletrônicos e de software; especialistas em IA embarcada; técnicos de manutenção avançada; engenheiro de dados; profissionais de *deep learning machine.*
- **Como o trabalho muda:** redução de ajustes manuais e aumento do foco em supervisão algorítmica, validação de comportamento adaptativo e manutenção baseada em desempenho cognitivo, treinamento e validação da base de dados *(big data)* e desenvolvimento de modelos otimizados.



Camada B[5] — Comunicações e Transporte

Redes Táticas Definidas por Software (SDR/SDN Militar Integrado) - infraestruturas de comunicação tática baseadas em rádios definidos por software e redes definidas por software, permitindo reconfiguração dinâmica de topologia, largura de banda e priorização de tráfego de Comando e Controle (C2).

- **Nível de impacto no segmento:** alto.
- **Principais profissionais afetados:** engenheiros de telecomunicações; arquitetos de rede; operadores de comunicações; gestores de infraestrutura C4I[6]; analista de segurança e criptografia; engenheiro de software; engenheiro de sistemas.
- **Como o trabalho muda:** a gestão física de enlaces é substituída por orquestração lógica e remota, exigindo competências em redes IP militares, virtualização e políticas de tráfego.

5 Camada B — Transporte e comunicações (backbone + tático) - SATCOM, rádios táticos, redes IP militares, redes móveis dedicadas, enlaces de dados, gateways.

6 Comando, Controle, Comunicações, Computadores e Inteligência

Comunicações Satelitais Híbridas (GovSat + Satcom Comercial Integrado) - Integração controlada de satélites militares dedicados com constelações comerciais resilientes, sob políticas rígidas de segurança e priorização de missão.

- **Nível de impacto no segmento:** médio.
- **Principais profissionais afetados:** engenheiros de sistemas espaciais; operadores SATCOM; especialistas em segurança da informação; engenheiros de telecomunicação; profissional de cibersegurança.
- **Como o trabalho muda:** o operador passa a gerenciar múltiplas camadas orbitais e contratos técnicos, com foco em continuidade, *fallback* operacional e segurança cibernética.

Camada C[7] — Integração e Interoperabilidade

***Middleware* Militar de Integração Orientado a Dados (*Data-Centric* C4ISR *Middleware*) -** Plataformas intermediárias que desacoplam sensores, sistemas de Comando e Controle e aplicações, permitindo interoperabilidade baseada em dados e não em sistemas proprietários.

- **Nível de impacto no segmento:** alto.
- **Principais profissionais afetados:** engenheiros de software e integração; arquitetos de sistemas; testadores de interoperabilidade; engenheiro de sistemas; engenheiro de dados.
- **Como o trabalho muda:** a integração ponto-a-ponto é substituída por governança de dados, APIs e validação semântica, elevando a complexidade cognitiva do trabalho técnico.

Modelos de Dados Operacionais Compartilhados (*Joint Operational Data Models*) - Ontologias e modelos semânticos comuns para representação de entidades operacionais, eventos e estados, viabilizando os sistemas de controle e comando.

- **Nível de impacto no segmento:** médio–alto.
- **Principais profissionais afetados:** arquitetos de informação; analistas operacionais; engenheiros de sistemas; engenheiros de dados; profissional de cibersegurança.
- **Como o trabalho muda:** o desenho de sistemas passa a exigir competências em modelagem conceitual, semântica operacional e governança de dados.

7 Camada C — Integração e interoperabilidade - middleware, barramentos, APIs, gateways, tradução de mensagens, sincronização de trilhas (tracks), gestão de identidades.

Camada D[8] — Comando, Controle e Apoio à Decisão

Sistemas de Comando e Controle com Fusão Multisensor Assistida por IA - Plataformas de Comando e Controle que utilizam IA para correlacionar sensores, reduzir sobrecarga informacional e gerar alertas ou hipóteses operacionais.

- **Nível de impacto no segmento:** alto.
- **Principais profissionais afetados:** operadores de sistemas de Comando e Controle; analistas de inteligência; engenheiros de sistemas; engenheiros de simulação; validadores de sistemas críticos.
- **Como o trabalho muda:** a tomada de decisão passa de leitura manual de múltiplas telas para supervisão e validação de recomendações algorítmicas.

Sistemas de Apoio à Decisão Baseados em Simulação em Tempo Quase Real - Ferramentas que simulam cenários operacionais, impactos de decisões e alocação de meios em tempo próximo ao real, integradas aos sistemas de Comando e Controle.

- **Nível de impacto no segmento:** médio.
- **Principais profissionais afetados:** engenheiros militares de planejamento; analistas operacionais; engenheiros de simulação.
- **Como o trabalho muda:** o planejamento estático é complementado por exploração dinâmica de cenários, exigindo maior capacidade analítica e interação homem-máquina.



8 Camada D — C2 e apoio à decisão - COP conjunta, ferramentas de planejamento e coordenação, workflow operacional, gestão de missão.

Camada E[9] — Segurança e Ciberproteção do Sistema de Comando e Controle

Arquiteturas Zero Trust Aplicadas a C4ISTAR - Modelos de segurança que eliminam confiança implícita em redes C4ISTAR, exigindo autenticação contínua, segmentação, controle granular de acessos e gestão de identidade.

- **Nível de impacto no segmento:** alto.
- **Principais profissionais afetados:** especialistas em ciberdefesa; arquitetos de segurança; administradores de sistemas críticos.
- **Como o trabalho muda:** a segurança deixa de ser perimetral e passa a ser contínua e distribuída, elevando a necessidade de monitoramento e resposta ativa.

Monitoramento Cognitivo de Segurança (*AI-enabled Cyber Situational Awareness*) - Sistemas que utilizam IA para detectar comportamentos anômalos em redes C4ISTAR, correlacionando eventos cibernéticos com contextos operacionais.

- **Nível de impacto no segmento:** médio–alto.
- **Principais profissionais afetados:** analistas dos Centros de Operações de Segurança (SOC/NOC militar); engenheiros de telecomunicação; engenheiro de sistemas; gestores de risco cibernético.
- **Como o trabalho muda:** a análise reativa de alertas evolui para supervisão de sistemas autônomos de detecção, com foco em validação e resposta estratégica.

Gestão Criptográfica Automatizada para Ambientes de Comando e Controle - Soluções que automatizam geração, distribuição, rotação e revogação de chaves criptográficas em ambientes C4ISTAR complexos.

- **Nível de impacto no segmento:** médio.
- **Principais profissionais afetados:** especialistas em criptografia; operadores de comunicações seguras; gestores de infraestrutura crítica.
- **Como o trabalho muda:** redução de processos manuais sensíveis e aumento da dependência de sistemas confiáveis e auditáveis. Deve-se considerar que essa tecnologia poderá sofrer mudanças estruturais com o avanço da computação quântica e da criptografia pós-quântica.

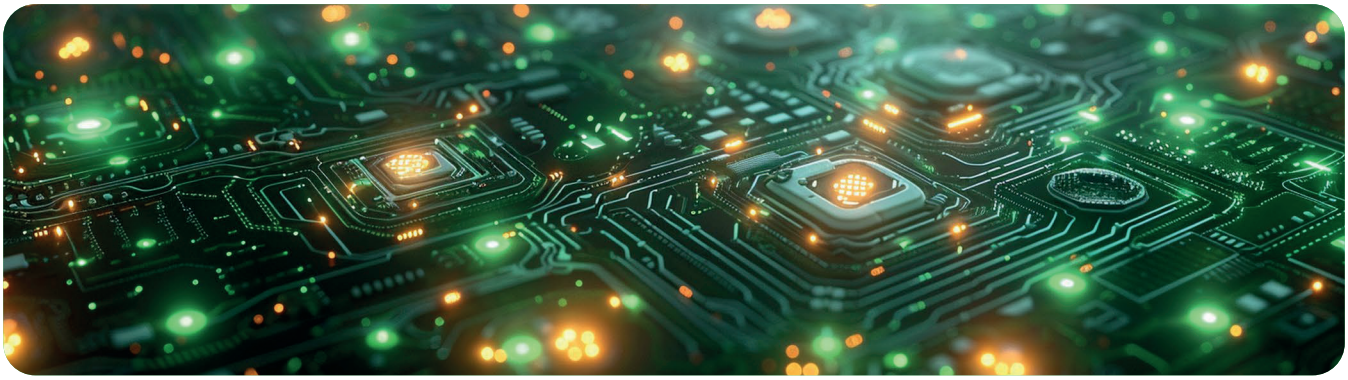
9 Camada E — Segurança e ciberproteção do C2 - criptografia, gestão de chaves, zero trust (quando adotado), SOC/monitoramento, hardening, continuidade.

Gestão quântica para Ambientes de Comando e Controle - Uso de tecnologias quânticas, como criptografia quântica e distribuição quântica de chaves, para garantir comunicações ultra seguras e maior capacidade de processamento em sistemas C4ISTAR.

- **Nível de impacto no segmento:** alto.
- **Principais profissionais afetados:** especialistas em criptografia; engenheiros de sistemas; especialistas em ciberdefesa; engenheiros de telecomunicações; cientistas de dados.
- **Como o trabalho muda:** transição para padrões de segurança resistentes à computação quântica, com aumento da complexidade na gestão de chaves e maior demanda por integração entre cibersegurança, comunicações e inteligência, exigindo novas competências técnicas e modernização de sistemas legados.

Tecnologia Transversal (A–E) - *Digital Twins* Operacionais para Arquiteturas C4ISTAR - Gêmeos digitais de redes, sensores e sistemas de Comando e Controle usados para teste, validação, treinamento e planejamento de evolução do sistema conjunto.

- **Nível de impacto no segmento:** médio-alto.
- **Principais profissionais afetados:** engenheiros de sistemas; especialistas em simulação; instrutores e planejadores.
- **Como o trabalho muda:** ensaios em campo são parcialmente substituídos por validação virtual, exigindo competências em modelagem sistêmica e análise de cenários.
- **Observação:** Essas tecnologias não devem ser tratadas como vetores isolados, mas como pacotes funcionais por camada, o que é fundamental para estimar as taxas incrementais de difusão, evitar a superestimação de impacto e conectar corretamente a relação entre tecnologia, capacidade e trabalho.



2.2) Estimativa de Difusão[10] das Tecnologias Emergentes

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.

Tecnologia emergente	Camada	Difusão (5 anos)	Difusão (10 anos)	Justificativa
Sensoriamento multiestático distribuído com fusão colaborativa	A	N2	N3	Alto valor operacional, mas depende de um processo de integração mais complexo, calibração entre sensores e aquisições pontuais. Tende a se difundir por repetição em áreas críticas, sem se tornar universal.
Sensores cognitivos com ajuste dinâmico por IA	A	N2	N3	Avança como funcionalidade embarcada em sensores específicos. Contudo, a necessidade de validação, certificação e limitam seu uso no horizonte analisado.
Redes táticas definidas por software (SDR/SDN militar integrado)	B	N3	N4	*Backbone* transversal do C4ISTAR. Mesmo sem grandes programas conjuntos, repete-se em múltiplos sistemas e tende a se tornar requisito padrão de arquitetura.
Comunicações satelitais híbridas (GovSat + comercial integrado)	B	N2	N3	Cresce por necessidade de resiliência e continuidade, mas restrições de soberania, segurança e governança impedem adoção plena como padrão universal.
Middleware militar data-centric de integração C4ISR	C	N3	N4	Elemento estrutural da interoperabilidade joint. Institucionaliza-se rapidamente como arquitetura de referência para novos sistemas e modernizações.

10 Para fins deste estudo o conceito de difusão tecnológica foi redefinido, como ***o grau em que uma tecnologia se torna institucionalizada como capacidade 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***.

Tecnologia emergente	Camada	Difusão (5 anos)	Difusão (10 anos)	Justificativa
Modelos de dados operacionais compartilhados (*Joint Operational Data Models*)	C	N3	N4	A governança de dados é condição para sistemas de Comando e Controle conjuntos. Cada novo sistema reforça a padronização semântica e acelera sua institucionalização.
Sistemas de Comando e Controle com fusão multisensor assistida por IA	D	N3	N4	Aumento da pressão por redução da sobrecarga cognitiva e maior velocidade decisória leva à incorporação progressiva como capacidade padrão do sistema de Comando e Controle.
Apoio à decisão por simulação em tempo quase real	D	N2	N4	Capacidade relevante para planejamento e centros especializados, mas permanece como ferramenta de nicho, não sendo essencial à operação cotidiana.
Arquiteturas Zero Trust aplicadas a C4ISTAR	E	N3	N4	Segurança do sistema de Comando e Controle é função crítica. A arquitetura Zero Trust tende a se consolidar como princípio obrigatório de arquitetura e governança.
Cyber situational awareness com IA (monitoramento cognitivo)	E	N3	N4	A escala e complexidade do C4ISTAR tornam inviável um sistema de segurança reativa, o que permite que a IA se institucionalize no monitoramento e resposta.
Gestão criptográfica automatizada para ambientes C4ISTAR	E	N3	N4	A automação reduz riscos operacionais e humanos. Além do mais, o forte alinhamento com requisitos de continuidade e conformidade impulsiona a difusão a nível de padronização.
Gestão quântica para Ambientes de Comando e Controle	E	as	as	as
Digital twin operacional para arquiteturas C4ISTAR		N2	N3	Tecnologia habilitadora de engenharia, testes e treinamento. Apesar do alto valor estratégico, não deve se converter em requisito operacional sistêmico.

2.3) Outros Eventos de Impacto[11]

Escala de impacto

- **Impacto Muito Alto -** Quando os eventos afetam fortemente o núcleo estratégico do setor ou segmento, têm ampla abrangência, reconfiguram completamente o trabalho e geram efeitos duradouros e sistêmicos.
- **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.

Consumo e geração de energia para suportar todos os sistemas de dados - Crescente demanda por infraestrutura energética robusta e resiliente para suportar o funcionamento contínuo de *data centers*, redes de comunicação e sistemas avançados de processamento de dados em ambientes C4ISTAR.

- **Nível de impacto:** alto.
- **Principais profissionais afetados:** engenheiro eletricista; físico; engenheiro de energia.
- **Como muda o trabalho:** aumento da complexidade na gestão energética, com necessidade de soluções eficientes e seguras para suprimento de energia, integração com fontes distribuídas e maior foco em eficiência energética para suportar operações intensivas em dados.

Mudança cultural do perfil profissional - transformação nas expectativas e valores das novas gerações, com menor interesse por atividades operacionais em campo e possíveis barreiras culturais em relação ao setor de defesa.

- **Nível de impacto:** médio-alto.
- **Principais profissionais afetados:** profissionais da indústria de defesa de forma geral, especialmente em funções operacionais.
- **Como muda o trabalho:** necessidade de adaptação das estratégias de atração e retenção de talentos, com maior valorização de ambientes digitais, flexibilidade e propósito, além de esforços para reposicionar a imagem do setor de defesa junto às novas gerações.

11 O nível de impacto desses eventos foi definido a partir de sua centralidade estratégica, abrangência, capacidade 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.*

Desvalorização do profissional técnico – Redução do reconhecimento e da atratividade de carreiras técnicas, apesar de sua importância crítica para a operação e manutenção de sistemas complexos de defesa.

- **Nível de impacto:** médio-alto.
- **Principais profissionais afetados:** técnicos da indústria de defesa.
- **Como muda o trabalho:** crescente necessidade de profissionais com perfil híbrido, combinando competências técnicas e digitais, além da ampliação de programas de formação e requalificação para suprir lacunas de mão de obra qualificada.

Intensificação da competição geopolítica e da fragmentação tecnológica global – Aumento de tensões geopolíticas e fragmentação de blocos tecnológicos (restrições cruzadas, alinhamentos estratégicos seletivos).

- **Nível de impacto:** muito alto.
- **Principais profissionais afetados:** gestores de projetos estratégicos; especialistas em cooperação internacional; engenheiros de integração; áreas de compras e contratos.
- **Como muda o trabalho:** maior complexidade na gestão de parcerias, necessidade de arquiteturas mais soberanas e esforço adicional de substituição e qualificação de fornecedores.

Restrições crescentes a exportações, importações e transferência de tecnologia sensível – Adoção mais rigorosa de regimes de controle (licenciamento, offset, compliance internacional e nacional).

- **Nível de impacto:** muito alto.
- **Principais profissionais afetados:** profissionais de compliance; jurídico-regulatório; logística internacional; gestores de cadeia de suprimentos.
- **Como muda o trabalho:** expansão do compliance contínuo, aumento da documentação técnica e jurídica com menor flexibilidade em cooperações tecnológicas internacionais.

Volatilidade fiscal e orçamentária do Estado brasileiro – ciclos de restrição orçamentária e contingenciamento que afetam a previsibilidade de investimentos em defesa.

- **Nível de impacto:** médio–alto.
- **Principais profissionais afetados:** gestores de programas; planejadores estratégicos; engenheiros de sistemas; áreas de P&D.
- **Como muda o trabalho:** o planejamento modular e incremental substitui projetos de grande escala. Aumento do foco em *retrofit*, sustentação e priorização de capacidades críticas.

Maior protagonismo das Forças Armadas em missões de apoio ao Estado (GLO, fronteiras, crises) – Uso mais frequente das capacidades C4ISTAR em contextos internos e interagências (como interface externa).

- **Nível de impacto:** médio–alto.
- **Principais profissionais afetados:** operadores de sistemas de Comando e Controle; analistas de inteligência; especialistas em interoperabilidade; gestores de operações conjuntas.
- **Como muda o trabalho:** ampliação do escopo operacional, necessidade de lidar com múltiplos atores institucionais e maior pressão por consciência situacional contínua.

Crescente judicialização, controle externo e escrutínio institucional sobre Defesa – Aumento do papel de órgãos de controle, tribunais, parlamento e opinião pública sobre programas estratégicos.

- **Nível de impacto:** médio.
- **Principais profissionais afetados:** gestores públicos; profissionais de governança; compliance; auditores internos; engenheiros de requisitos.
- **Como muda o trabalho:** maior formalização de processos, rastreabilidade de decisões técnicas e reforço de documentação e justificativas técnicas.

Pressão por soberania nacional e autonomia estratégica - Valorização política e institucional de capacidades nacionais em sistemas críticos de defesa e Comando e Controle.

- **Nível de impacto:** alto.
- **Principais profissionais afetados:** engenheiros de sistemas; gestores industriais; formuladores de política industrial; integradores nacionais.
- **Como muda o trabalho:** cresce a demanda por engenharia local, integração nacional e formação de competências críticas internas, com menor dependência externa.

Escassez e envelhecimento de profissionais altamente qualificados em defesa e sistemas críticos - Desafio demográfico e concorrência com outros setores (TI, energia, financeiro) por talentos especializados.

- **Nível de impacto:** alto.
- **Principais profissionais afetados:** engenheiros seniores; especialistas em Comando e Controle, segurança e integração; gestores de RH estratégico.
- **Como muda o trabalho:** intensificação de programas de retenção, transferência de conhecimento, capacitação acelerada e formação híbrida (militar–civil).

Aumento das exigências de segurança da informação e responsabilidade individual - Endurecimento de normas de sigilo, rastreabilidade e responsabilização pessoal em sistemas críticos.

- **Nível de impacto:** médio–alto.
- **Principais profissionais afetados:** operadores de sistemas; administradores de redes; especialistas em segurança; gestores de acesso e identidade.
- **Como muda o trabalho:** rotinas mais rígidas, maior segregação de funções e ampliação de auditorias técnicas e comportamentais.

Pressão por interoperabilidade interforças sem integração total de sistemas - Necessidade política e operacional de cooperação, sem unificação plena de plataformas e sistemas.

- **Nível de impacto:** médio.
- **Principais profissionais afetados:** arquitetos de sistemas; engenheiros de integração; gestores de interoperabilidade.
- **Como muda o trabalho:** ênfase em interfaces, governança de dados e soluções "ponte", em vez de substituição completa de sistemas legados.

Reconfiguração do papel das empresas estatais e estratégicas (Telebras, integradoras nacionais) - Mudanças institucionais no papel de empresas públicas/estratégicas no suporte ao C4ISTAR.

- **Nível de impacto:** médio.
- **Principais profissionais afetados:** gestores de contratos; engenheiros de telecom e SATCOM; formuladores de política pública.
- **Como muda o trabalho:** ajustes na governança de projetos, redefinição de responsabilidades técnicas e maior coordenação Estado–empresa.

Aumento da cooperação regional sul-americana em segurança e defesa (limitada) - Iniciativas pontuais de cooperação regional em monitoramento, fronteiras e informações.

- **Nível de impacto:** baixo–médio.
- **Principais profissionais afetados:** analistas estratégicos; oficiais de ligação; especialistas em interoperabilidade limitada.
- **Como muda o trabalho:** trabalho adicional de coordenação e padronização mínima, sem impacto estrutural profundo no C4ISTAR nacional.

Mudança no perfil de risco percebido pela sociedade (ciber, fronteiras, infraestruturas críticas) – Maior sensibilidade social e política a riscos não convencionais e sistêmicos.

- **Nível de impacto:** médio.
- **Principais profissionais afetados:** planejadores estratégicos; analistas de risco; gestores de sistemas de Comando e Controle.
- **Como muda o trabalho:** ampliação do foco em prevenção, monitoramento contínuo e comunicação institucional sobre capacidades de defesa.

3. Competências[12] 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 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*)[13], aptidões (*abilities*)[14] e conhecimentos[15] 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.

12 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:

13 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.

14 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.

15 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".

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*)[16] que ganharão importância[17]

Análise de sistemas

Categoria: Habilidades Sistêmicas -> Análise de sistemas.

Descrição: analisar como sistemas complexos (sensores–redes–C2–ciber) funcionam e como mudanças em ambientes operacionais afetam o desempenho.

Por que é importante: as tecnologias *middleware* data-centric, modelos de dados conjuntos, sistemas de Comando e Controle com IA, Zero Trust, gestão criptográfica automatizada e SDR/SDN exigem uma visão de sistema e entendimento de interdependências. Além disso, as restrições de fornecedores, soberania e volatilidade fiscal "empurram" o foco para soluções incrementais, exigindo *trade-offs* sistêmicos (e não "trocas completas"). O profissional precisa desenvolver a habilidade de enxergar correlações sistêmicas.

Como capacitar: não somente com leitura e construção de arquiteturas, mas com todos os processos e sistemáticas de análise de sistemas, exercícios de "degradação" e continuidade, análise de falhas sistêmicas;

16 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).

17 As habilidades foram selecionadas por sua transversalidade, conexão direta com impactos tecnológicos e não tecnológicos, natureza comportamental-operacional, possibilidade de desenvolvimento por prática e relevância ao longo do ciclo de vida.

Resolução de problemas complexos

Categoria: Habilidades de Resolução de Problemas Complexos -> Resolução de problemas complexos.

Descrição: estruturar problemas multicausais, avaliar opções e implementar soluções em contexto de restrições.

Por que é importante: a integração multicamada e IA no sistema de Comando e Controle aumentam a complexidade. Além do mais, a judicialização e controle externo, bem como a instabilidade orçamentaria exigem soluções tecnicamente robustas e institucionalmente defensáveis.

Como capacitar: estudos de caso, uso da ferramenta *After Action Review* (AAR), exercícios de decisão sob restrições reais.

Pensamento crítico

Categoria: Habilidades Básicas -> Pensamento Crítico.

Descrição: avaliar evidências, validar informações e identificar pontos fortes e fracos de alternativas.

Por que é importante: os sistemas de fusão com IA e *cyber situational awareness* produzem alertas/recomendações; o humano precisa validar, calibrar confiança e reduzir vieses. O movimento de escrutínio institucional e responsabilidade individual aumentam exigência de justificativas.

Como capacitar: práticas de validação cruzada, *red team*, auditoria de decisões, exercícios simulados, estudos de caso.

Análise e avaliação de informações e dados

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

Descrição: examinar dados, avaliar confiabilidade e credibilidade, além de formular recomendações com base em evidências.

Por que é importante: os modelos de dados conjuntos, juntamente com os sistemas de Comando e Controle com IA e sensoriamento cooperativo elevam volume e heterogeneidade de dados. Soma-se a isso, que a fragmentação tecnológica e restrições de importação exigem avaliar qualidade e limites das fontes e dos sistemas.

Como capacitar: exercícios com dados reais ou com metamodelos, simulações; padrões de qualidade de dados; análise de incerteza.

Gestão da Informação

Categoria: Habilidades de Gestão -> Gestão da Informação.

Descrição: organizar, recuperar, distribuir e proteger informação (incluindo sensível), com rastreabilidade.

Por que é importante: as tendências Zero Trust, automação criptográfica e interoperabilidade dependem de governança informacional (acessos, classificação, auditoria). O aumento de controles, compliance e controle externo tornam a governança "não opcional".

Como capacitar: rotinas de classificação, trilhas de auditoria, governança de acesso e registros.

Fluência digital

Categoria: Habilidades Técnicas -> Fluência digital.

Descrição: usar ferramentas digitais para instalar, manter, integrar sistemas TIC e lidar com dados de forma eficiente e ética.

Por que é importante: as tecnologias emergentes de maior impacto são *digital-intensive* (IA, integração, redes, segurança, *digital twin*), e diante da escassez de talentos aumenta necessidade de profissionais *T-shaped* capazes de transitar entre ferramentas.

Como capacitar: laboratórios *hands-on*, rotação em funções (operação–integração–segurança).

Monitoramento, Inspeção e Testes

Categoria: Habilidades Técnicas -> Monitoramento, Inspeção e Testes.

Descrição: examinar sistemas para avaliar funcionamento e conformidade com normas e requisitos.

Por que é importante: A integração *data-centric*, redes SDR/SDN, IA no sistema C2 e gestão criptográfica exigem V&V contínuos (sistemas críticos). Adicionalmente, verifica-se que as tendências de judicialização e auditorias aumentam a necessidade de evidências de conformidade e rastreabilidade.

Como capacitar: campanhas de teste, *checklists* de integração, ensaios em ambiente degradado; simulação; estudos de caso.

Monitoramento de informações

Categoria: Habilidades Técnicas -> Monitoramento de informações.

Descrição: acompanhar mudanças relevantes (pesquisa, regulações, políticas, ameaças, práticas).

Por que é importante: o ritmo de evolução da IA e cibersegurança obriga atualização contínua, e a geopolítica, controles de exportação e mudanças institucionais impactam requisitos, fornecedores e políticas de uso.

Como capacitar: leitura especializada em metodologias de monitoramento tecnológico e regulatório, *briefings*, comunidades técnicas.

Operação e controle

Categoria: Habilidades Técnicas -> Operação e controle.

Descrição: controlar operação de equipamentos e sistemas conforme normas e especificações.

Por que é importante: Sistemas de Comando e Controle com IA, redes definidas por software e cybersegurança mudam o trabalho do operador para configuração, supervisão e resposta, com maior protagonismo em missões internas e crises amplia demanda por operação 24/7.

Como capacitar: treino em consoles e cenários, SOPs (simulações operacionais), exercícios de contingência.

Planejamento e organização

Categoria: Habilidades Técnicas -> Planejamento e organização

Descrição: estabelecer cronogramas, coordenar tarefas e priorizar objetivos dentro do orçamento do projeto.

Por que é importante: a difusão incremental por camadas exige planejamento de releases, migrações e integração. Além do mais, a volatilidade orçamentária reforça modularidade, priorização e *roadmap* adaptativo.

Como capacitar: participação em gestão de projetos, planejamento por capacidades e lições aprendidas; participação em equipes de finanças.

Julgamento e tomada de decisões

Categoria: Habilidades Sistêmicas -> Julgamento e tomada de decisões.

Descrição: considerar custos/benefícios/riscos para escolher a ação mais apropriada.

Por que é importante: tecnologias de IA no sistema de Comando e Controle e cybersegurança aumentam opções e velocidade. Com isso, o decisor precisa calibrar confiança, risco e consequências. Há também a possibilidade do escrutínio institucional e soberania ampliarem o peso do risco reputacional, jurídico e estratégico.

Como capacitar: jogos de decisão, jogos de guerra, exercícios com dilemas e *trade-offs*, teoria dos jogos.

Comunicação

Categoria: Habilidades Básicas -> Comunicação.

Descrição: transmitir e receber informações com eficácia em ambientes técnicos e operacionais.

Por que é importante: a integração dos sistemas de Comando e Controle dependem de comunicação precisa (erros de coordenação geram falhas operacionais). Além disso, a cooperação interforças, controle externo e coordenação com interfaces externas exigem comunicação clara e documentável.

Como capacitar: relatórios operacionais, comunicação técnica para públicos não técnicos, estudo do público-alvo, leitura de contexto.

Tabela de Priorização[18] das Habilidades Requeridas

Skill	Categoria	Prioridade (5 anos)	Prioridade (10 anos)
Análise de sistemas	Sistêmicas	Muito Alta	Muito Alta
Resolução de problemas complexos	Complexos	Muito Alta	Muito Alta
Pensamento crítico	Básicas	Muito Alta	Muito Alta
Análise e avaliação de informações e dados	Técnicas	Muito Alta	Muito Alta
Gestão da informação	Gestão	Muito Alta	Muito Alta
Fluência digital	Técnicas	Alta	Alta
Monitoramento, inspeção e testes	Técnicas	Alta	Muito Alta

18 Para a priorização das *skills* foi dado maior peso na intensidade de reconfiguração do trabalho, número de tecnologias emergentes e eventos não tecnológicos que acionam simultaneamente a *skill* e dependência institucional e regulatória.

Tabela de Priorização[18] das Habilidades Requeridas			
Skill	**Categoria**	**Prioridade (5 anos)**	**Prioridade (10 anos)**
Monitoramento de informações	Técnicas	Alta	Alta
Operação e controle	Técnicas	Alta	Alta
Planejamento e organização	Técnicas	Alta	Alta
Julgamento e tomada de decisões	Sistêmicas	Alta	Muito Alta
Comunicação	Básicas	Alta	Alta

3.2) Aptidões (*abilities*)[19] que ganharão importância[20]

Atenção seletiva

Categoria: Capacidade Cognitiva.

Descrição: capacidade de manter foco em informações críticas por períodos prolongados, ignorando distrações em ambientes complexos e ruidosos.

Por que é importante: Sistemas de Comando e Controle com fusão multisensor e cybersegurança situational *awareness* ampliam o volume de alertas e telas, e a automação amplifica a exigência de foco. Além do mais, as operações 24/7, a pressão institucional e os riscos sistêmicos elevam o custo de lapsos de atenção.

Como desenvolver: seleção baseada em testes de atenção, simulações prolongadas, turnos controlados e treino em ambientes de sobrecarga informacional, redução do tempo de telas (celular etc.)

Percepção de problemas

Categoria: Capacidade Cognitiva.

Descrição: Capacidade de reconhecer rapidamente que algo está errado ou pode dar errado, mesmo sem diagnóstico completo.

Por que é importante: O uso de sistemas de IA e de automação desloca a atuação de determinados profissionais para processos de detecção de anomalias e *"outliers"*, uma vez que os riscos cibernéticos,

19 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).

20 As *abilities* foram selecionadas por sua natureza comportamental estável, transversalidade ocupacional, ativação recorrente por tecnologias e tendências não tecnológicas, contribuição à segurança e confiabilidade e robustez frente a cenários.

a judicialização e a defesa da soberania aumentam o impacto de falhas não detectadas.

Como desenvolver: exercícios de detecção precoce, análise de incidentes reais, treino com sinais fracos.

Raciocínio abdutivo

Categoria: Capacidade Cognitiva.

Descrição: capacidade de formular a melhor explicação possível a partir de informações incompletas ou ambíguas.

Por que é importante: a fusão de dados e IA produzem hipóteses, não certezas, e determinados profissionais precisam inferir cenários plausíveis, principalmente quanto nos deparamos com ambientes geopolíticos incertos e fragmentados exigem decisões sem evidência plena.

Como desenvolver: análise de casos ambíguos, jogos de hipóteses, exercícios de inferência sob incerteza.

Raciocínio indutivo

Categoria: Capacidade Cognitiva.

Descrição: capacidade de identificar padrões gerais a partir de múltiplos eventos ou dados aparentemente desconexos.

Por que é importante: tecnologias de sensoriamento cooperativo, cybersegurança e análise de logs exigem generalização de padrões, enquanto ataques e falhas sistêmicas evoluem por variações incrementais.

Como desenvolver: análise de séries temporais, estudos de padrões históricos, exercícios de correlação.

Velocidade de organização e resposta

Categoria: Capacidade Cognitiva.

Descrição: capacidade de rapidamente estruturar informações dispersas e responder de forma coerente.

Por que é importante: os sistemas automatizados aceleram o ciclo OODA[21], exigindo respostas humanas mais rápidas e estruturadas. Além do mais, as crises cibernéticas e operacionais estabelecem janelas curtas de decisão.

Como desenvolver: simulações com tempo restrito, exercícios de priorização rápida.

Multitarefa

Categoria: Capacidade Cognitiva.

Descrição: capacidade de alternar e gerenciar atenção entre múltiplas fontes de informação e atividades simultâneas.

Por que é importante: consoles C4ISTAR concentram dados, alertas, comunicações e decisões, e a escassez de talentos aumenta carga individual.

Como desenvolver: treino progressivo em ambientes *multi-console*, gestão cognitiva de tarefas.

Tolerância ao estresse

Categoria: Capacidade Socioemocional.

Descrição: capacidade de manter desempenho e clareza cognitiva sob pressão, risco e cobrança institucional.

Por que é importante: os sistemas críticos ampliam consequências de erro humano, além do maior protagonismo em crises, escrutínio externo e responsabilidade individual.

Como desenvolver: simulações de crise, apoio psicossocial, treino em ambientes simulados.

Autocontrole emocional

Categoria: Capacidade Socioemocional.

Descrição: capacidade de regular emoções e evitar reações impulsivas em situações críticas.

Por que é importante: as decisões assistidas por IA exigem calma para validação e não reação automática. Em ambientes altamente hierarquizados e auditáveis, as decisões emocionais são penalizadas.

Como desenvolver: treino comportamental, feedback estruturado, apoio psicossocial.

21 Ciclo OODA é um modelo de tomada de decisão que consiste em quatro etapas: Observar, Orientar, Decidir e Agir.

Adaptabilidade / Flexibilidade

Categoria: Capacidade Socioemocional.

Descrição: capacidade de ajustar rapidamente o modelo mental diante de mudanças técnicas, operacionais ou institucionais.

Por que é importante: a difusão incremental das tecnologias emergentes e as atualizações constantes exigem adaptação contínua.

Como desenvolver: rotação de funções, exposição a cenários variados, aprendizagem experiencial.

Responsabilidade

Categoria: Capacidade Socioemocional.

Descrição: tendência a cumprir deveres, regras e compromissos mesmo sob pressão.

Por que é importante: a gestão criptográfica, arquitetura zero trust e sistema de Comando e Controle exigem disciplina estrita, e a judicialização, auditorias e risco reputacional ampliam o peso do erro humano.

Como desenvolver: percepção de uma cultura organizacional forte, liderança exemplar e existência de sistemas de *accountability*.

Curiosidade e aprendizagem contínua

Categoria: Capacidade Socioemocional.

Descrição: disposição persistente para aprender, explorar e atualizar-se.

Por que é importante: a rápida evolução de IA, ciber e integração torna obsolescência constante, e a fragmentação tecnológica e soberania exigem reaprendizado frequente.

Como desenvolver: estímulo à aprendizagem, acesso a comunidades técnicas, tempo institucional para estudo.

Orientação social (trabalho em equipe)

Categoria: Capacidade Socioemocional.

Descrição: capacidade de atuar cooperativamente, respeitando papéis e competências dos outros.

Por que é importante: o C4ISTAR é um *sistema de sistemas* e as falhas surgem na interface humana. As operações conjuntas e coordenação interforças ampliam interdependência humana.

Como desenvolver: exercícios em equipes mistas, metas coletivas, avaliações por desempenho grupal.

Tabela de Priorização[22] das Aptidões Requeridas

Aptidão	Prioridade 5 anos	Prioridade 10 anos
Atenção seletiva	Muito Alta	Muito Alta
Percepção de problemas	Muito Alta	Muito Alta
Raciocínio abdutivo	Muito Alta	Muito Alta
Raciocínio indutivo	Muito Alta	Muito Alta
Velocidade de organização e resposta	Muito Alta	Muito Alta
Tolerância ao estresse	Muito Alta	Muito Alta
Responsabilidade	Muito Alta	Muito Alta
Autocontrole emocional	Muito Alta	Muito Alta
Adaptabilidade / Flexibilidade	Alta	Muito Alta
Curiosidade e aprendizagem contínua	Alta	Muito Alta
Orientação social (trabalho em equipe)	Alta	Alta
Multitarefa	Alta	Alta

3.3) Conhecimentos que ganharão importância (comuns às ocupações)[23]

Arquiteturas de Sistemas C4ISTAR e Comando e Controle

Descrição: princípios, modelos e padrões de arquitetura de sistemas de Comando e Controle conjunto, incluindo *system-of-systems*, modularidade, escalabilidade e interoperabilidade interforças.

Justificativa: é um conhecimento central e estruturante, acionado por praticamente todas as tecnologias emergentes (integração *data-centric*, C2 com IA, redes definidas por *software*). Eventos como restrições orçamentárias, soberania tecnológica e legado heterogêneo tornam o domínio das arquiteturas condição para evolução incremental e sustentável do sistema.

22 A priorização das *abilities* considerou principalmente: a intensidade da exigência cognitiva e emocional em ambientes de pressão contínua; a amplificação dessas exigências pela automação, IA e integração sistêmica; a dependência humana residual, uma vez que tais capacidades não são automatizáveis; e o risco sistêmico associado à falha humana em sistemas críticos de comando, controle e ciberdefesa.

23 Os conhecimentos formais identificados constituem a base cognitiva codificada que sustenta o funcionamento, a integração e a governança do sistema C4ISTAR e da proteção cibernética associada. Em um contexto de rápida difusão tecnológica, forte pressão geopolítica e crescente escrutínio institucional, esses conhecimentos deixam de ser especializados e passam a ser transversais, compartilhados por engenheiros, operadores, gestores e analistas. Seu domínio busca reduzir riscos sistêmicos, garantir interoperabilidade, assegurar conformidade regulatória e preservar a soberania tecnológica, podendo ser utilizado na construção de desenhos curriculares de cursos técnicos, superiores e de pós-graduação, bem como para capacitações corporativas contínuas na Base Industrial de Defesa.

Doutrina e Conceitos Operacionais de Emprego Conjunto/Combinado

Descrição: doutrina militar, conceitos de operações conjuntas e combinadas, cadeia de comando, ciclos decisórios e emprego do C4ISTAR em diferentes cenários operacionais.

Justificativa: mesmo altamente tecnológico, o C4ISTAR é orientado por conceitos doutrinários e operacionais. Mudanças no papel das Forças Armadas e maior protagonismo em missões diversas elevam a importância desse conhecimento para alinhar tecnologia, organização e decisão.

Integração de Sistemas e Interoperabilidade Interforças

Descrição: métodos, padrões e ferramentas de integração de sistemas heterogêneos (APIs, *middleware*, barramentos, *gateways*) e interoperabilidade entre forças e domínios.

Justificativa: o C4ISTAR joint evolui por integração, não por substituição. Esse conhecimento é ativado por múltiplas tecnologias (sensores distribuídos, modelos de dados conjuntos, redes táticas) e por tendências não tecnológicas como restrições fiscais e herança de sistemas legados.

Redes de Comunicações Seguras, Táticas e Estratégicas

Descrição: protocolos, topologias e tecnologias de comunicações militares: redes IP seguras, SDR/SDN, SATCOM, enlaces resilientes e operação degradada.

Justificativa: as redes são o *backbone* funcional do C4ISTAR. A fragmentação geopolítica, a busca por resiliência e a integração de comunicações híbridas (governamentais e comerciais) tornam esse conhecimento crítico e permanentemente atualizável.

Gestão e Governança de Dados Operacionais

Descrição: modelos de dados conjuntos, qualidade de dados, metadados, governança, classificação da informação e compartilhamento seguro.

Justificativa: a centralidade do C2 *data-centric* e da IA torna a governança de dados um conhecimento *não opcional*. Além disso, normas de sigilo, auditorias e controle externo reforçam sua dependência institucional.

Fundamentos de Cibersegurança aplicados ao C4ISTAR

Descrição: princípios de segurança da informação para sistemas críticos: confidencialidade, integridade, disponibilidade, resiliência, Zero Trust e defesa em profundidade, gestão de identidade.

Justificativa: a cibersegurança deixou de ser uma função especializada e passou a ser transversal ao

C4ISTAR. O aumento de ameaças cibernéticas e o alto risco sistêmico associado a falhas justificam prioridade elevada.

Criptografia aplicada e Gestão de Chaves em Ambientes Operacionais

Descrição: fundamentos criptográficos, PKI, políticas de chaves, rotação, revogação, certificação e automação criptográfica.

Justificativa: a difusão da gestão criptográfica automatizada no C4ISTAR torna indispensável o domínio formal desse conhecimento. Erros conceituais têm impacto direto na continuidade e na legitimidade do sistema de Comando e Controle.

Computação quântica

Descrição: uso de princípios da mecânica quântica para realizar processamento computacional avançado, com potencial para resolver problemas complexos de forma exponencialmente mais eficiente que os sistemas clássicos, incluindo aplicações em criptografia, otimização e simulação em ambientes C4ISTAR

Justificativa: a computação quântica tem potencial disruptivo sobre os sistemas de defesa, especialmente ao comprometer métodos criptográficos atuais e habilitar novas capacidades em análise de dados, simulação de cenários e inteligência.

Fundamentos de Inteligência Artificial e Apoio à Decisão

Descrição: princípios de IA e ML, limitações, vieses, validação de modelos e uso responsável de IA em apoio à decisão operacional.

Justificativa: com a incorporação dos Sistemas de Comando e Controle assistido por IA, os profissionais precisam compreender formalmente o funcionamento e os limites dessas tecnologias, sobretudo diante de judicialização e responsabilização humana.

Engenharia de Sistemas

Descrição: métodos formais de elicitação de requisitos, rastreabilidade, testes, certificação e aceitação de sistemas críticos. Requisitos, Verificação e Validação (V&V) de Sistemas Críticos

Justificativa: integração complexa, automação e segurança elevam a importância de V&V. Esse conhecimento reduz riscos operacionais, atrasos de programa e questionamentos institucionais.

Gestão de Riscos, Continuidade e Resiliência Operacional

Descrição: métodos de análise de risco, planejamento de contingência, redundância, continuidade

de operações e recuperação.

Justificativa: eventos geopolíticos, ciberataques e dependências críticas tornam a resiliência um requisito estratégico. O conhecimento formal sustenta decisões de projeto, operação e investimento.

Normas, Regulamentações e Compliance em Defesa

Descrição: marcos regulatórios nacionais e internacionais, controles de exportação, requisitos contratuais, auditorias e responsabilidades legais.

Justificativa: o aumento do escrutínio institucional e regulatório transforma compliance em conhecimento operacional cotidiano, não apenas jurídico.

Gestão de Programas e Projetos em Sistemas Complexos de Defesa

Descrição: métodos formais de planejamento, cronograma, custos, riscos e governança de programas complexos e de longo prazo.

Justificativa: a ausência de grandes programas únicos e a difusão incremental do C4ISTAR exigem domínio de gestão adaptativa, alinhada a restrições fiscais e institucionais.

Criação de modelos e simulações para alimentar os modelos de IA

Descrição: desenvolvimento de modelos computacionais e ambientes de simulação que geram dados sintéticos e cenários controlados para treinar, validar e testar sistemas de inteligência artificial aplicados a contextos complexos, como operações C4ISTAR.

Justificativa: a soberania em IA pede pela criação e desenvolvimento e simulações próprias para embasar a tomada de decisão. Qualquer projeto feito com IA precisa ter um treinamento adequado.



Tabela de Priorização[24] dos Conhecimentos Requeridos		
Conhecimento formal	**Prioridade 5 anos**	**Prioridade 10 anos**
Arquiteturas de Sistemas C4ISTAR e C2 Conjunto	Muito Alta	Muito Alta
Fundamentos de Cibersegurança aplicados ao C4ISTAR	Muito Alta	Muito Alta
Doutrina e Conceitos Operacionais de Emprego Conjunto	Alta	Muito Alta
Integração de Sistemas e Interoperabilidade Interforças	Muito Alta	Muito Alta
Redes de Comunicações Seguras, Táticas e Estratégicas	Muito Alta	Muito Alta
Gestão e Governança de Dados Operacionais	Muito Alta	Muito Alta
Criptografia aplicada e Gestão de Chaves	Muito Alta	Muito Alta
Fundamentos de Inteligência Artificial e Apoio à Decisão	Alta	Muito Alta
Engenharia de Requisitos e Verificação & Validação (V&V)	Alta	Muito Alta
Gestão de Riscos, Continuidade e Resiliência Operacional	Alta	Muito Alta
Normas, Regulamentações e Compliance em Defesa	Alta	Muito Alta
Gestão de Programas e Projetos em Sistemas Complexos de Defesa	Alta	Alta

3.4) Matriz Integrada de Orientação Formativa para o segmento

A seguir sugere-se uma Matriz Integrada de Orientação Formativa para o Sistema C4ISTAR, 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 do C4ISTAR

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Arquiteturas de Sistemas C4ISTAR e Comando e Controle Conjunto	Muito Alta	Muito Alta	Núcleo curricular estruturante

24 A priorização considerou principalmente o impacto direto do conhecimento na segurança, continuidade e legitimidade institucional do C4ISTAR; a transversalidade do conhecimento entre engenharia, operação e gestão; a dependência regulatória e o risco sistêmico associado a falhas conceituais; e a trajetória temporal das tecnologias e dos eventos não tecnológicos.

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Integração de sistemas e interoperabilidade interforças	Muito Alta	Muito Alta	Núcleo curricular estruturante
Conhecimento	Engenharia de requisitos e V&V de sistemas críticos	Alta	Muito Alta	Garantia de qualidade e certificação
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 da integração
Aptidão	Percepção de problemas	Muito Alta	Muito Alta	Detecção precoce de falhas sistêmicas

Eixo 2 — Comando, Controle e Apoio à Decisão (*C2 Data-Centric*)

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Doutrina e conceitos operacionais de emprego conjunto	Alta	Muito Alta	Alinhamento técnico-operacional
Conhecimento	Fundamentos de IA e apoio à decisão	Alta	Alta	Uso responsável da automação
Conhecimento	Gestão e governança de dados operacionais	Muito Alta	Muito Alta	Base de Comando e Controle orientado por dados
Habilidade	Análise e avaliação de informações e dados	Muito Alta	Muito Alta	Decisão baseada em evidências
Habilidade	Julgamento e tomada de decisões	Alta	Muito Alta	Decisão sob risco e responsabilidade
Aptidão	Atenção seletiva	Muito Alta	Muito Alta	Sustentação do desempenho cognitivo
Aptidão	Velocidade de organização e resposta	Alta	Alta	Agilidade decisória operacional

Eixo 3 — Comunicações, Redes e Infraestrutura Digital

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Redes de comunicações seguras, táticas e estratégicas	Muito Alta	Muito Alta	*Backbone* tecnológico do C4ISTAR
Conhecimento	Gestão de continuidade e resiliência de redes	Alta	Alta	Robustez operacional
Habilidade	Fluência digital	Alta	Alta	Habilitador transversal
Habilidade	Operação e controle de sistemas	Alta	Alta	Execução segura e disciplinada

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Aptidão	Multitarefa	Alta	Alta	Gestão de múltiplos fluxos informacionais
Aptidão	Velocidade de organização e resposta	Alta	Alta	Resposta a incidentes

Eixo 4 — Segurança, Ciberdefesa e Proteção da Informação

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Fundamentos de cibersegurança aplicados ao C4ISTAR	Muito Alta	Muito Alta	Condição de operação segura
Conhecimento	Criptografia aplicada e gestão de chaves	Muito Alta	Muito Alta	Garantia de confidencialidade e integridade
Conhecimento	Normas, regulamentações e compliance em Defesa	Alta	Alta	Conformidade institucional
Habilidade	Gestão da informação	Alta	Muito Alta	Governança e rastreabilidade
Habilidade	Monitoramento, inspeção e testes	Alta	Muito Alta	Verificação e validação contínua
Aptidão	Responsabilidade	Muito Alta	Muito Alta	Sustentação ética e institucional
Aptidão	Autocontrole emocional	Alta	Alta	Decisão segura sob pressão

Eixo 5 — Resiliência Operacional, Gestão e Sustentação Institucional

Dimensão	Elemento	Prioridade 5 anos	Prioridade 10 anos	Papel formativo
Conhecimento	Gestão de riscos, continuidade e resiliência operacional	Alta	Muito Alta	Sustentação sistêmica
Conhecimento	Gestão de programas e projetos em sistemas complexos	Alta	Alta	Governança de longo prazo
Habilidade	Planejamento e organização	Alta	Alta	Execução estruturada
Habilidade	Comunicação	Alta	Alta	Coordenação interforças
Aptidão	Tolerância ao estresse	Muito Alta	Muito Alta	Desempenho sob crise
Aptidão	Adaptabilidade e flexibilidade	Alta	Alta	Ajuste a mudanças tecnológicas e institucionais
Aptidão	Orientação social (trabalho em equipe)	Alta	Alta	Integração humana do sistema

Como se pode utilizar esta matriz

Instituições de Formação Profissional (IFPs)

- Transformar cada Eixo (1 a 5) em módulos curriculares ou núcleos formativos.
- Priorizar elementos com prioridade Muito Alta como conteúdos obrigatórios.
- **Para cursos de nível técnico:** foco em conhecimentos operacionais, habilidades de execução e desenvolvimento inicial de capacidades (atenção, responsabilidade).
- **Para cursos de tecnólogo/graduação:** aprofundamento em arquitetura, integração, dados e ciber, com exercícios sistêmicos.
- **Para cursos de pós-graduação:** ênfase em decisão, governança, resiliência e V&V, com estudos de caso reais.

Empresas da Base Industrial de Defesa (BID)

- **Diagnóstico interno de competências**: mapear funções e equipes contra os eixos e elementos da matriz; identificar lacunas críticas em habilidades e capacidades, não apenas em conhecimento técnico.
- **Desenho de planos de capacitação corporativa**: priorizar capacitações alinhadas aos elementos de prioridade Muito Alta e Alta; integrar treinamento técnico com desenvolvimento cognitivo e socioemocional.
- **Apoio à gestão de projetos e riscos**: usar a matriz para formar equipes balanceadas (engenharia, operação, segurança, gestão); Reduzir riscos de integração, falhas humanas e não conformidades regulatórias.

Instituições responsáveis por políticas públicas de formação profissional

- **Definição de prioridades nacionais de formação**: identificar eixos e elementos de prioridade *Muito Alta* como áreas estratégicas para investimento público; alinhar programas de capacitação às demandas reais do C4ISTAR.
- **Articulação entre oferta e demanda**: usar a matriz como linguagem comum entre governo, IFPs e empresas; Evitar sobreoferta de formações pouco aderentes às necessidades do sistema.
- **Avaliação e monitoramento de políticas**: avaliar cursos e programas financiados à luz da cobertura dos eixos formativos; atualizar periodicamente a matriz conforme evolução tecnológica e geopolítica.

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".

Profissionais de nível técnico / tecnólogo (operação, integração, V&V)

Técnico em Integração de Sistemas C4ISTAR - Atua na configuração, integração e testes de interfaces entre sensores, redes, Comando e Controle e sistemas de segurança, apoiando V&V e operação incremental em ambientes heterogêneos.

Técnico em Operação de Redes Táticas e SDN/SDR - Opera e mantém redes táticas definidas por software, SATCOM híbrido e enlaces resilientes, com foco em continuidade, degradação controlada e resposta a incidentes.

Técnico em Monitoramento Cibernético Operacional (SOC e CSOC[25] C4ISTAR) - Monitora eventos de segurança, anomalias e alertas em ambientes C4ISTAR, realizando triagem, correlação básica e acionamento de resposta conforme procedimentos operacionais padrão.

Técnico em Gestão Criptográfica Operacional - Executa procedimentos de provisão, rotação e revogação de chaves, gestão de certificados e apoio à automação criptográfica, garantindo conformidade e rastreabilidade.

Técnico em Testes, Verificação e Validação (V&V) de Sistemas Críticos - Planeja e executa testes funcionais, de integração e de segurança, documentando evidências para aceitação, auditorias e certificações.

Técnico em Governança e Qualidade de Dados Operacionais - Assegura a qualidade, classificação, metadados e conformidade de dados operacionais compartilhados, apoiando o sistema C2 data-centric e interoperabilidade.

Profissionais de formação superior (engenharia, análise, gestão)

Engenheiro(a) de Arquitetura C4ISTAR (System-of-Systems) - Projeta e governa arquiteturas modulares e interoperáveis, definindo padrões, *roadmaps* e *trade-offs* para evolução incremental com soberania e resiliência.

Engenheiro(a) de Integração e Interoperabilidade Joint - Especialista em integração de sistemas legados e novos (APIs, *middleware*, modelos de dados), lidera iniciativas interforças e reduz riscos de acoplamento.

Especialista em C2 Assistido por IA e Apoio à Decisão - Desenvolve, valida e opera soluções de IA para fusão de dados e apoio à decisão, com foco em limites, vieses, explicabilidade e responsabilização humana.

25 Centro de Operações de Segurança Cibernética

Arquiteto(a) de Segurança Cibernética para Sistemas Críticos - Define e implementa arquiteturas Zero Trust, defesa em profundidade e resiliência cibernética específicas para o C4ISTAR, integrando requisitos regulatórios.

Especialista em Governança de Dados e Informação Sensível - Estabelece políticas, modelos e controles de dados (classificação, acesso, auditoria), garantindo interoperabilidade segura e conformidade institucional.

Engenheiro(a) de Redes Táticas e Resiliência de Comunicações - Projeta redes seguras e resilientes (SDN/SDR/SATCOM), planeja redundâncias e continuidade sob degradação operacional.

Especialista em Riscos, Continuidade e Resiliência Operacional - Avalia riscos sistêmicos (técnicos, cibernéticos e institucionais), planeja contingências e coordena resposta e recuperação.

Gestor(a) de Programas C4ISTAR e Integração Complexa - Gerencia programas incrementais, cronogramas, riscos e *stakeholders*, articulando engenharia, operação, compliance e orçamento.

Especialista em Compliance Tecnológico e Regulatório em Defesa - Atua na interface técnica–jurídica, assegurando aderência a normas, controles de exportação, auditorias e responsabilidades.

5. Cursos que Poderão ser Demandados pelas Empresas do Segmento[26]

Arquitetura e Integração de Sistemas Complexos e Críticos — Fundamentos

- **Público:** técnicos de integração, analistas de desenvolvimento de sistemas (banco de dados, analistas de testes), coordenadores técnicos.
- **Conteúdo:** arquitetura *system-of-systems*; interoperabilidade joint; integração incremental; gestão de legado; V&V em ambientes integrados; estudos de caso de Sistemas C4ISTAR.
- **Objetivo:** desenvolver visão arquitetural e capacidade prática de integração sem dependência de plataformas específicas.

Arquitetura e Integração de Sistemas Complexos e Críticos — Aperfeiçoamento

- **Público:** engenheiros de sistemas, cientista de computação, gestores técnicos
- **Conteúdo:** arquitetura *system-of-systems*; interoperabilidade joint; integração incremental; gestão de legado; V&V em ambientes integrados; estudos de caso de Sistemas C4ISTAR.
- **Objetivo:** desenvolver visão arquitetural e capacidade prática de integração sem dependência de plataformas específicas.

26 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.

Cibersegurança para Sistemas Críticos — Básico

Público: técnicos de operação, engenheiros, gestores de TI e OT, profissional de TI, analistas de risco.

Conteúdo: ameaças a sistemas críticos; princípios de segurança por camadas; Zero Trust (conceitual); continuidade e resposta a incidentes; requisitos regulatórios; exercícios *tabletop*, conceitos de criptografia.

Objetivo: internalizar princípios de *security by design* e reduzir riscos operacionais e institucionais.

Criptografia Aplicada e Gestão de Chaves — Visão Operacional[27]

Público: técnicos de segurança, engenheiros de redes/sistemas, gestores de segurança da informação.

Conteúdo: fundamentos criptográficos; PKI; ciclo de vida de chaves; automação criptográfica (conceitos); auditoria e rastreabilidade; compliance.

Objetivo: garantir uso correto e governado da criptografia em ambientes C4ISTAR, sem instruções sensíveis.

Governança de Dados Operacionais e Interoperabilidade

Público: analistas de dados, engenheiros, gestores de Comando e Controle, profissionais de TI.

Conteúdo: modelos de dados conjuntos; qualidade e metadados; classificação da informação; compartilhamento seguro; governança interorganizacional.

Objetivo: sustentar o C2 *data-centric* e reduzir fricções na integração de sistemas e equipes.

IA para Apoio à Decisão em Ambientes Críticos — Fundamentos

- **Público:** analistas, engenheiros, gestores operacionais e decisores técnicos.
- **Conteúdo:** princípios de IA e ML; limites e vieses; explicabilidade; validação de modelos; uso responsável; estudos de caso de C2 assistido por IA, auditoria de sistemas.
- **Objetivo:** capacitar o uso crítico e responsável da IA como apoio à decisão, preservando responsabilidade humana.

27 Pode ser uma disciplina do item acima de Cibersegurança.

Operação e Resiliência de Redes Táticas e Infraestruturas Digitais

- **Público:** técnicos de redes, operadores, engenheiros de comunicações.
- **Conteúdo:** fundamentos de redes táticas; SDR e SDN (conceitos); SATCOM híbrido; operação degradada; continuidade e redundância; exercícios práticos.
- **Objetivo:** aumentar a resiliência operacional frente a falhas técnicas, ataques e restrições geopolíticas.

Engenharia de Sistemas

- **Público:** certificação e aceitação. Requisitos e Verificação & Validação (V&V) de Sistemas Críticos.; Análise de riscos e continuidade de negócios.
- **Conteúdo:** elicitação de requisitos; rastreabilidade; planos de teste; evidências de conformidade; certificação e aceitação. Requisitos e Verificação & Validação (V&V) de Sistemas Críticos.; Análise de riscos e continuidade de negócios.
- **Objetivo:** reduzir riscos de integração, atrasos e questionamentos regulatórios em programas C4ISTAR.

Compliance Tecnológico, Regulatório e Contratual em Defesa

- **Público:** gestores, engenheiros seniores, profissionais de contratos e qualidade; advogado; auditor.
- **Conteúdo:** marcos regulatórios; controles de exportação; requisitos contratuais; auditorias técnicas; responsabilidade institucional.
- **Objetivo:** reduzir riscos legais e reputacionais e alinhar tecnologia, contratos e políticas públicas.

Gestão de Programas e Projetos Complexos em Sistemas de Defesa

- **Público:** gerentes de projeto, líderes técnicos, gestores públicos e privados.
- **Conteúdo:** gestão incremental; governança de programas; riscos e stakeholders; restrições fiscais; coordenação interorganizacional, gestão de offset, gestão de contratos.
- **Objetivo:** melhorar a entrega de valor em contextos de longo prazo, alta complexidade e orçamento variável.

Tomada de Decisão sob Pressão em Situações Críticas

- **Público:** gestores, operadores seniores, analistas e líderes de equipes.
- **Conteúdo:** julgamento humano versus automação; vieses cognitivos; decisão sob estresse; responsabilidade e ética; simulações de crise.
- **Objetivo:** desenvolver *abilities críticas* (atenção, autocontrole, responsabilidade) em contextos C4ISTAR.

Trabalho Conjunto, Coordenação Interforças e Comunicação Técnica

- **Público:** profissionais técnicos e gestores que atuam em ambientes integrados e interagências.

- **Conteúdo:** conceitos de operações conjuntas; coordenação humana; comunicação técnica; resolução de conflitos; exercícios colaborativos.
- **Objetivo:** fortalecer a integração humana e organizacional, reduzindo falhas não técnicas do sistema.

Síntese

- Não são cursos "de nicho", mas **formações transversais**, coerentes com um setor concentrado/oligopolizado, onde poucos atores precisam de alta criticidade.
- O foco está em atualização contínua da base instalada, e não apenas em formação inicial.
- Os cursos combinam conhecimentos explícitos, *skills* de execução e aptidões (*abilities*) específicas, refletindo a natureza sociotécnica do C4ISTAR.
- A maioria é modular, permitindo trilhas progressivas (básico -> avançado -> especializado).
- Permanecem relevantes sob cenários alternativos (mais ou menos orçamento, maior ou menor regulação, choques geopolíticos).

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 (engenharia–ciber–dados–operações–normas)

Desafio: Escassez de profissionais que combinem engenharia de sistemas, redes, cibersegurança, dados e compreensão operacional.

Justificativa: O C4ISTAR evolui como *system-of-systems*, exigindo integração contínua entre domínios antes separados; formações excessivamente especializadas não cobrem a complexidade real.

Ator	Papel principal
Empresas	Definir perfis híbridos-alvo; ofertar projetos reais de integração; promover rotação entre engenharia, operação e segurança.
Governo	Induzir programas nacionais de formação híbrida; financiar reconversão profissional e bolsas estratégicas.
IFPs	Desenvolver currículos integrados e modulares; adotar aprendizagem baseada em projetos sistêmicos.
ICTs	Apoiar conteúdos avançados; fornecer ambientes de experimentação e integração tecnológica.

Dificuldade de atualização da força de trabalho já instalada (*upskilling* e *reskilling*)

Desafio: requalificar técnicos e engenheiros experientes em tecnologias digitais, IA, dados e segurança cibernética, sem interromper a operação.

Justificativa: a difusão é incremental e convivente com sistemas legados, exigindo *upskilling* contínuo — o que conflita com agendas operacionais e escassez de tempo.

Ator	Papel principal
Empresas	Mapear lacunas internas; liberar tempo produtivo para capacitação; Co financiar cursos estratégicos.
Governo	Criar incentivos fiscais e programas de requalificação; apoiar capacitação em serviço.
IFPs	Ofertar cursos curtos, "empilháveis" e modulares; flexibilizar horários e formatos híbridos.
ICTs	Traduzir avanços tecnológicos em conteúdos aplicados; apoiar atualização docente.

Baixa oferta de formação específica em C4ISTAR

- **Desafio:** ausência de cursos estruturados e padronizados voltados ao contexto conjunto, interoperável e interagências.

Justificativa: a maior parte da oferta formativa é genérica (TI, redes, ciber) e não aborda arquitetura, doutrina, governança e restrições específicas de defesa.

Ator	Papel principal
Empresas	Especificar competências críticas em um contexto *joint*; validar conteúdos formativos.
Governo	Reconhecer C4ISTAR como área estratégica; financiar cursos dedicados e pilotos curriculares.
IFPs	Estruturar trilhas específicas em C4ISTAR; integrar tecnologia, doutrina e gestão.
ICTs	Apoiar com conhecimento especializado, ensaios e laboratórios temáticos.

Dificuldade de alinhar formação técnica com doutrina e operação conjunta

Desafio: integrar conteúdos técnicos com conceitos operacionais, doutrinários e institucionais.

Justificativa: profissionais tecnicamente competentes podem falhar se não compreenderem o emprego conjunto, a cadeia de comando e a lógica operacional do sistema.

Ator	Papel principal
Empresas	Expor profissionais a contextos operacionais reais; incorporar requisitos doutrinários nos projetos.
Governo	Atualizar e difundir doutrina; facilitar interação entre forças, indústria e formadores.
IFPs	Integrar conceitos operacionais aos cursos técnicos e superiores; usar estudos de caso reais.
ICTs	Apoiar simulações e exercícios aplicados ao emprego conjunto.

Formação insuficiente em integração, V&V e gestão de riscos de sistemas críticos

Desafio: escassez de capacitação prática em integração de sistemas, verificação e validação e análise de riscos sistêmicos.

Justificativa: a maioria dos incidentes críticos decorre de falhas de integração e validação, e não de erros de componentes isolados.

Ator	Papel principal
Empresas	Institucionalizar V&V; compartilhar lições aprendidas de integração.
Governo	Estabelecer requisitos mínimos de V&V em contratos; apoiar certificação nacional.
IFPs	Incluir V&V e engenharia de requisitos como núcleo curricular.
ICTs	Ofertar infraestrutura de ensaios, testes e certificação tecnológica.

Lacunas em governança de dados e responsabilidade sobre decisões assistidas por IA

Desafio: preparar profissionais para operar Sistemas de C2 *data-centric* e IA mantendo responsabilidade humana, rastreabilidade e explicabilidade.

Justificativa: a pressão por automação cresce mais rápido do que a maturidade institucional para governar dados e decisões críticas.

Ator	Papel principal
Empresas	Implementar políticas de dados e IA responsável; treinar equipes em uso crítico da automação.
Governo	Definir diretrizes de governança, ética e responsabilização; alinhar regulação.
IFPs	Ensinar fundamentos de dados, IA e responsabilidade humana; avaliação baseada em casos.
ICTs	Pesquisar e testar métodos de explicabilidade, validação e auditoria algorítmica.

Formação insuficiente em cibersegurança para sistemas críticos

Desafio: predominância de treinamentos voltados a TI corporativa, e não a sistemas críticos e operacionais.

Justificativa: o C4ISTAR possui requisitos de disponibilidade, continuidade e segurança muito distintos do ambiente corporativo tradicional.

Ator	Papel principal
Empresas	Diferenciar ciber corporativo × ciber operacional; apoiar capacitação específica.
Governo	Estabelecer padrões de segurança para sistemas críticos; financiar formação especializada.
IFPs	Criar cursos focados em ciber para sistemas críticos e OT.
ICTs	Desenvolver laboratórios de ciberdefesa aplicada e testes de resiliência.

Dificuldade de retenção de talentos estratégicos

Desafio: concorrência com setores civis (*big tech*, energia, finanças) por profissionais de alto nível.

Justificativa: restrições salariais, burocracia e ciclos longos de projeto reduzem a atratividade do setor de defesa para talentos digitais.

Ator	Papel principal
Empresas	Criar planos de carreira técnica; valorizar especialistas e perfis sistêmicos.
Governo	Ajustar políticas de atração e retenção; apoiar bolsas e carreiras estratégicas.
IFPs	Conectar formação a oportunidades reais no setor de defesa; reduzir evasão.
ICTs	Oferecer ambientes de P&D atrativos; integrar jovens talentos a projetos relevantes.

Dependência excessiva de poucos especialistas-chave

Desafio: concentração de conhecimento crítico em indivíduos específicos.

Justificativa: a falta de programas estruturados de formação e documentação aumenta o risco operacional e institucional.

Ator	Papel principal
Empresas	Documentar conhecimento crítico; promover a redundância de competências.
Governo	Exigir planos de gestão do conhecimento em contratos estratégicos.
IFPs	Formar massa crítica mínima; padronizar conhecimentos essenciais.
ICTs	Apoiar sistematização e difusão do conhecimento técnico avançado.

Limitações de infraestrutura formativa avançada

Desafio: insuficiência de laboratórios, ambientes simulados e plataformas de teste adequadas ao C4ISTAR.

Justificativa: muitas competências (integração, decisão sob pressão, resposta a incidentes) não podem ser desenvolvidas apenas em sala de aula.

Ator	Papel principal
Empresas	Compartilhar ambientes de teste e casos reais; apoiar laboratórios conjuntos.
Governo	Investir em infraestrutura nacional de simulação e treinamento avançado.
IFPs	Operar laboratórios, simuladores e ambientes híbridos de aprendizagem.
ICTs	Desenvolver plataformas de simulação, teste e experimentação tecnológica.

Fragmentação institucional entre empresas, IFPs e governo

Desafio: baixa coordenação entre políticas públicas, oferta formativa e demandas reais das empresas.

Justificativa: sem um referencial comum (como a matriz construída), há desperdício de recursos e desalinhamento estratégico.

Fragmentação institucional entre indústria, formação e políticas públicas

Ator	Papel principal
Empresas	Participar ativamente de fóruns de alinhamento; comunicar demandas futuras.
Governo	Coordenar políticas e instrumentos; usar estudos prospectivos como insumo decisório.
IFPs	Ajustar oferta formativa com base em sinais antecipatórios; evitar sobreposição de cursos.
ICTs	Produzir evidências técnicas e prospectivas para apoiar decisões.

Dificuldade de incorporar aptidões (*abilities*) socioemocionais críticas

Desafio: desenvolver capacidades como atenção seletiva, tolerância ao estresse, responsabilidade e julgamento sob pressão.

Justificativa: o desempenho humano torna-se cada vez mais crítico à medida que o sistema se automatiza.

Ator	Papel principal
Empresas	Valorizar aptidões cognitivas e socioemocionais; treinar líderes e equipes.
Governo	Reconhecer essas capacidades em políticas e referenciais de qualificação.
IFPs	Integrar desenvolvimento socioemocional às metodologias pedagógicas.
ICTs	Apoiar métodos de avaliação e desenvolvimento dessas capacidades.

Síntese

Os desafios de formação no Sistema C4ISTAR não se restringem à escassez de conhecimento técnico, mas refletem um descompasso estrutural entre a complexidade sociotécnica do sistema e os modelos tradicionais de formação profissional. Nos próximos 10 anos, o maior risco não será a ausência de tecnologias, mas a incapacidade institucional de formar, atualizar e reter profissionais capazes de integrar, governar e decidir em ambientes altamente automatizados, regulados e sujeitos a pressões geopolíticas. Superar esses desafios exige coordenação entre empresas, IFPs e formuladores de políticas, com foco em formação modular, contínua e orientada a sistemas.

7. Comentários Finais

O estudo prospectivo sobre o futuro do Sistema C4ISTAR evidencia que os principais desafios e oportunidades associados a esse sistema transcendem a dimensão estritamente tecnológica, configurando-se como um problema estrutural de *capacidades humanas, organizacionais e institucionais*. A análise integrada das tendências tecnológicas emergentes, de sua difusão temporal em um contexto de mercado fortemente concentrado, e dos vetores não tecnológicos — geopolíticos, regulatórios, econômicos e políticos — demonstra que a sustentabilidade e a efetividade do C4ISTAR dependerão, de forma decisiva, da capacidade do país de formar, atualizar e reter uma mão de obra altamente qualificada, híbrida e adaptável.

Os resultados indicam que o C4ISTAR se consolida como um *sistema sociotécnico complexo*, no qual arquiteturas modulares, integração incremental, governança de dados, cibersegurança e apoio à decisão assistido por inteligência artificial se tornam eixos estruturantes. Nesse contexto, a evolução tecnológica não elimina o papel humano, mas o redefine, deslocando-o para funções de maior responsabilidade cognitiva, sistêmica e institucional. Profissionais técnicos, engenheiros, analistas e gestores passam a atuar menos como operadores de componentes isolados e mais como integradores, validadores, decisores e garantidores da resiliência e da legitimidade operacional do sistema.

A identificação e priorização de conhecimentos formais, habilidades e aptidões comuns ao ecossistema C4ISTAR reforçam a necessidade de perfis profissionais híbridos, capazes de articular engenharia, dados, cibersegurança, operação e gestão sob forte pressão regulatória e com baixa tolerância a falhas. O estudo demonstra que as maiores lacunas futuras não estarão apenas na ausência de tecnologias, mas na dificuldade de integrar sistemas legados, validar soluções críticas, governar decisões assistidas por automação e operar de forma coordenada em ambientes conjuntos e interagências.

Nesse sentido, a matriz integrada de orientação formativa e o mapeamento de novos perfis profissionais e cursos prioritários oferecem um referencial prático para ação, permitindo alinhar currículos, programas de capacitação corporativa e políticas públicas às trajetórias prováveis de evolução do C4ISTAR. Os desafios identificados — como o déficit de profissionais híbridos, a atualização da força de trabalho

instalada, a retenção de talentos estratégicos e a fragmentação institucional entre indústria, governo e formação — evidenciam que respostas isoladas serão insuficientes. A superação desses desafios requer coordenação sistêmica e continuidade de esforços ao longo do tempo.

Dessa forma, o estudo conclui que os exercícios prospectivos aplicados ao Sistema C4ISTAR devem ser compreendidos não como instrumentos prescritivos, mas como insumos estratégicos para a tomada de decisão, capazes de reduzir incertezas, antecipar riscos e orientar investimentos mais eficientes em capacitação e desenvolvimento de competências. A articulação entre os resultados deste estudo e políticas públicas de formação profissional voltadas à Base Industrial de Defesa é condição essencial para fortalecer a soberania tecnológica, a resiliência operacional e a sustentabilidade de longo prazo do C4ISTAR. Ao alinhar antecipação, formação e política industrial, o país amplia sua capacidade de responder a um ambiente internacional cada vez mais instável e competitivo, assegurando que o capital humano acompanhe, de forma consistente, a complexidade crescente dos sistemas de defesa contemporâneos.

Cadernos de

Prospectiva Industrial de Defesa

Segmento

C4ISTAR



FIA BUSINESS SCHOOL

CNI Confederação Nacional da Indústria

ABDI Agência Brasileira de Desenvolvimento Industrial

MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS